Cyber Security Tools and Technologies

Dr. Arshad Ali
Associate Professor
NUCES Lahore

Techniques Used by Hackers

- **Chapter 6 of the Book**

Computer Security Fundamentals

Techniques Used by Hackers

- Introduction
- Basic Terminology

Stages for an actual attack

- The Reconnaissance
  - Passive Scanning techniques
  - Active scanning techniques
    - Port scanning
    - Vulnerability Assessment
    - Enumeration
- ACTUAL ATTACKS
- Malware Creation
- Penetration Testing

Introduction

A **hacker** is a person who wants to understand a system, often by probing its weaknesses.

Penetration testing (white hat Hacking) : When hackers work for organizations, testing the organizations' system security.

Black hat hackers or crackers: people who use hacking techniques to breach systems to steal data, damage systems, or commit other cybercrimes.

Introduction

Many certifications for penetration testing

- **Offensive Security:** https://www.offensivesecurity.
- com/information-security-certifications/
- **SANS Institute:** http://pen-testing.sans.org/certification
- **EC-Council's Certified Ethical Hacker:** www.eccouncil.org.

Basic Terminology

- **White hat hacker**, which is used to describe a person who uses hacking techniques for legal/ethical purposes.
- **Black hat hacker** and cracker, which are used to describe a person who uses hacking techniques for illegal techniques.
- **A gray hat hacker** is one who was previously a black hat

hacker and turned into a white hat hacker.

- **Kiddies** people who download some tools and perform some cyber attack without really understanding it.
- **phreaking,** refers to hacking into phone
- **Red Team:** conducts penetration testing to emulate a specific adversary or type of adversary
- **Blue Team** (defensive team) attempts to stop the red team's attack.

Footprinting/ Reconnaissance

- A technique used for gathering information about computer systems and the entities they belong to
- Any intelligent/experienced hacker is going to attempt to find out information about a target before actually attempting an attack.
- A black hat hacker wants to know about your system's security.
- What may surprise you is how much information can be found easily on the Internet without even attaching to the target system.

The Reconnaissance Phase

Passive Scanning Techniques

- **Check the target organization's websites**
  - Posted information can be very useful to an attacker (like IT manager details)
  - An enterprising hacker can scan bulletin boards and discussion groups for references to IT manager and the attacker
    - might find information useful in spear phishing attacks or
    - might find information useful in social engineering.

The Reconnaissance Phase

Passive Scanning Techniques

- scan bulletin boards, chat rooms, discussion groups, and other places, looking for questions from IT staff at the target organization.
- For example, if an administrator posts in a discussion group
- asking about a particular server problem,
  - this can give the attacker valuable information about that target network.

The Reconnaissance Phase

Passive Scanning Techniques

- Through job ads
  - ASP.Net developer only
  - Network admin ad twice a year on regular basis
- specific websites that provide useful information for hackers
  - **netcraft.com** provides information about websites
    - what kind of server a site is running
    - how long it has been since the server was last rebooted.
  - **https://archive.org** archives older versions of websites
    - The frequency with which a site is archived depends on its popularity

The Reconnaissance Phase

Active Scanning Techniques

- Active scans are far more reliable but may be detected by the target system
- **Port Scanning:** process of attempting to contact each network port on the target system and see which ones are open.
  - A free tool for port scanning: Nmap (https://nmap.org)
    - Ping scan
    - Connect scan
    - STN scan (half open scan)
    - FIN Scan

The Reconnaissance Phase

Active Scanning Techniques

Vulnerability Assessment

- It involves checking a system to see if it is vulnerable to specific attacks
- Tools can be used; may be detected by an IDS

- Network administrators commonly use vulnerability assessment tools to test their own networks.

The Reconnaissance Phase

Active Scanning Techniques

Enumeration

- It is simply the process of finding out what is on the target system.
- If the target is an entire network, the attacker wants to find out what servers, computers, and printers are on that network
- If the target is a specific computer, the attacker wants to find out what users and shared folders exist on that system.

- enumeration tools:
  - Cain and Abel
  - Sid2User
  - UserDump
  - UserInfo
  - **Netcat**

Footprinting/ Reconnaissance

- **Footprinting basics with Windows command line**
- **Ping:** The ping command sends ICMP (Internet Control Message Protocol) Used to test the reachability of a host on a IP network and measures the travel time for messages sent from the originating host to destinantion target.
- **Finding the IP address: (windows powershell)**

ping www.certifiedhacker.com

```
PS C:\Users\hp> ping www.certifiedhacker.com

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=286ms TTL=37
Reply from 162.241.216.11: bytes=32 time=288ms TTL=37
Reply from 162.241.216.11: bytes=32 time=285ms TTL=37
Reply from 162.241.216.11: bytes=32 time=286ms TTL=37

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 285ms, Maximum = 288ms, Average = 286ms
PS C:\Users\hp>
```

Footprinting/ Reconnaissance

Finding the maximum frame size on the network

Add the –f parameter to not fragment on the ping packet and -1 to set the frame size to 1500 bytes

```
PS C:\Users\hp> ping www.certifiedhacker.com -f -l 1500

Pinging certifiedhacker.com [162.241.216.11] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- This message means that the frame is too large to be on the network and needs to be fragmented
- Try different values until reach the maximum frame size
- ping www.certifiedhacker.com -f -l **1450** (it works)
- ping www.certifiedhacker.com -f -l 1475 (reach the limit)
- ping www.certifiedhacker.com -f -l 1470 (it works)
- ping www.certifiedhacker.com -f -l 1473 (reach the limit)
- ping www.certifiedhacker.com -f -l 1472 (it works)

Footprinting/ Reconnaissance

Investigate the TTL (Time to Live)

Every frame on the network has their own TTL defined. If the TTL reaches 0, the router discards the packet to prevent packet loss.

```
PS C:\Users\hp> ping www.certifiedhacker.com -i 3

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 10.101.20.1: TTL expired in transit.
Reply from 10.101.20.1: TTL expired in transit.
Reply from 10.101.20.1: TTL expired in transit.
Reply from 10.101.20.1: TTL expired in transit.
```

The –i parameter means wait time, that is the number of seconds to wait between each ping (values between 1-255

TTL expired means that the router discarded the frame, beacuse the TTL has expired (reached 0).

Footprinting/ Reconnaissance

- **tracert (windows) or traceroute (Linux):** Diagnostic tool for displaying the route and measuring transit delays of packets across an IP network**.**
- **tracert** www.certifiedhacker.com
- Trace the path to the destination and takes 23 hops for the packet to reach the specified destination.

```
PS C:\Users\hp> tracert www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

  1   <1 ms   <1 ms   <1 ms  10.104.127.1
  2   <1 ms   <1 ms   <1 ms  10.101.50.17
  3   <1 ms   <1 ms   <1 ms  10.101.20.1
  4   <1 ms   <1 ms   <1 ms  116-58-41-145.nexlinx.net.pk [116.58.41.145]
  5    1 ms   <1 ms   <1 ms  10.224.31.153
  6    1 ms    2 ms    2 ms  FE-3-0-100M-CORE.nexlinx.net.pk [202.59.80.2]
  7    1 ms    2 ms    2 ms  10.10.80.11
  8    3 ms    2 ms    4 ms  110.93.202.169
  9   27 ms   32 ms   18 ms  110.93.255.26
 10   19 ms   18 ms   18 ms  110.93.252.190
 11   19 ms   19 ms   20 ms  110.93.252.216
 12    *       *       *     Request timed out.
 13  119 ms  118 ms  118 ms  be3154.ccr32.mrs02.atlas.cogentco.com [154.54.76.217]
 14  118 ms  116 ms  117 ms  130.117.14.54
 15  141 ms  140 ms  140 ms  prs-bb1-link.ip.twelve99.net [62.115.124.54]
 16  146 ms  145 ms  145 ms  ldn-bb1-link.ip.twelve99.net [62.115.135.24]
 17  215 ms  215 ms  216 ms  nyk-bb2-link.ip.twelve99.net [62.115.113.20]
 18  284 ms  284 ms  284 ms  palo-b24-link.ip.twelve99.net [62.115.122.36]
 19  286 ms  286 ms  288 ms  salt-b2-link.ip.twelve99.net [62.115.140.53]
 20  306 ms  282 ms  283 ms  newfolddigital-ic-380138.ip.twelve99-cust.net [80.239.167.103]
 21  284 ms  284 ms  284 ms  69-195-64-103.unifiedlayer.com [69.195.64.103]
 22  288 ms  282 ms  283 ms  po97.prv-leaf1a.net.unifiedlayer.com [162.144.240.123]
 23  287 ms  286 ms  287 ms  box5331.bluehost.com [162.241.216.11]
```

Footprinting/ Reconnaissance

Checking the life span of the packet

Set the TTL (i) to 2 and count of packet (-n) to 1

ping www.certifiedhacker.com -i 2 -n 1

```
PS C:\Users\hp> ping www.certifiedhacker.com -i 2 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 10.101.50.17: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

ping www.certifiedhacker.com -i 3 -n 1

```
PS C:\Users\hp> ping www.certifiedhacker.com -i 3 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 10.101.20.1: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

ping www.certifiedhacker.com -i 23 -n 1

```
PS C:\Users\hp> ping www.certifiedhacker.com -i 23 -n 1

Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=286ms TTL=37

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 286ms, Maximum = 286ms, Average = 286ms
```

Make a note of all the IP addresses from which you receive a reply.

Footprinting/ Reconnaissance

- **Nslookup:** Used for querying the DNS (Domain Name System), to obtain a domain name or IP address mapping and other specific DNS record:
- >nslookup (launch a interactive mode)
- For query IP address of a given domain, set the type to A record, then enter the target domain

```
PS C:\Users\hp> nslookup
Default Server:  NUADSVR.lhr.nu.edu.pk
Address:  172.16.99.2

> set type=A
> www.certifiedhacker.com
Server:  NUADSVR.lhr.nu.edu.pk
Address:  172.16.99.2

Non-authoritative answer:
Name:    certifiedhacker.com
Address:  162.241.216.11
Aliases:  www.certifiedhacker.com
```

Footprinting/ Reconnaissance

Nslookup:

- To obtain the Authoritative name server, set the type to CNAME record and query the target.
- lookup is done directly against the domain's authoritative name server

```
PS C:\Users\hp> nslookup
Default Server:  NUADSVR.lhr.nu.edu.pk
Address:  172.16.99.2

> set type=CANME
unknown query type: CANME
> set type=CNAME
> certifiedhacker.com
Server:  NUADSVR.lhr.nu.edu.pk
Address:  172.16.99.2

certifiedhacker.com
        primary name server = ns1.bluehost.com
        responsible mail addr = dnsadmin.box5331.bluehost.com
        serial  = 2024031300
        refresh = 86400 (1 day)
        retry   = 7200 (2 hours)
        expire  = 3600000 (41 days 16 hours)
        default TTL = 300 (5 mins)
>
```

- With the authoritative name server, you can determine the IP address.
- set the type to A record, then enter the primary name server

Footprinting- Tools

Maltego

- an open-source intelligence and forensics application
- gathers information about a target and represents in an easily-understandable format.
- **Your task: Explore Maltego to**
- Identify IP address
- Identify Domain and Domain Name Schema
- Identify Server Side Technology
- Identify Service Oriented Architecture (SOA) information
- Identify Name Server
- Identify Mail Exchanger
- Identify Geographical Location
- Identify Entities
- Discover Email addresses and Phone numbers

Footprinting

- **Other tools:**
- Recon-ng
- Open Source Intelligence Gathering using OSRFramework
- Information Gathering using Metasploit
- **Information Gathering using theHarvester**
- Sublist3r
- **Web Data Extractor**
- **HTTrack**
- **Tracing Emails**
- **Gathering IP and Domain Name info. using Whois Lookup**
- **Advanced Network Route Tracing using Path Analyzer Pro**
- **Automated Fingerprinting using FOCA**

Actual Attacks

SQL Script Injection

Cross Site Scripting

Cross-Site Request Forgery

Directory Traversal

Cookie Poisoning

URL Hijacking

Wireless Attacks

Cell Phone Attacks

Password Cracking

Actual Attacks

SQL Script Injection: It involves passing Structured Query Language (SQL) commands to a web application and getting the website to execute them.

SELECT * FROM tblUsers WHERE USERNAME = 'jdoe' AND PASSWORD = 'letmein’

- SQL injection works by putting some SQL into the username and password block that is always true.

An example of most basic version of SQL injection

- SELECT * FROM tblUsers WHERE USERNAME = "OR X=X’ AND PASSWORD = "OR X=X'

Actual Attacks

SQL Script Injection – Defense:

- filter all user input before processing it (input validation process)
  - prevents an attacker from entering SQL commands rather than a username and password.

❖ Unfortunately, many sites do not filter user input and are still vulnerable to SQL injection attacks

- programmer creating a website should write the code to first check for any common SQL injection symbols such as ('), (%), (=), or a (&),

❖ If those are found, stop processing and log an error.

Actual Attacks

Cross Site Scripting:

- An attacker injects client-side scripts into web pages viewed by other users and interact with code area.
- When users go to that part of the site, the attacker's script, rather than the intended website functionality, is executed.

- Such attacks can be prevented by simply filtering all user input.
- Though, all the major online shopping portals, such as Amazon.com, do filter input and are not susceptible to this attack.
  - However, many smaller sites are still susceptible to this attack.

Actual Attacks

Cross-Site Request Forgery: viewed as the other side of cross-site scripting

- **Cross-site scripting** attacks the user, based on the user's trust of a website,
- **Cross-site request forgery** attacks the website, based on the site's trust of a user.

- The trusted user, who is authenticated to the website, is tricked into sending requests to the website.
- These requests can then be used to attack the website.

Actual Attacks

Directory Traversal:

- It allows attackers to access restricted directories
  - including those containing application source code, configuration files, and critical system files, and execute commands outside the web server's root directory.
- Attackers can manipulate variables that reference files with "dot-dot-slash (../)" sequences and its variations

Examples:

- http://www.example.com/process.aspx=../../../../somedir/some file
- http://www.example.com/../../../../some dir/some file

Actual Attacks

Cookie Poisoning or Session Hijacking

- Many web applications use cookies to save information (user ID, timestamp, and so on) on client's machine.
- **Cookies are not always encrypted, they can be modified; an attack that includes this type of modification is called cookie poisoning**

- Example: Cybercriminal steals a user's cookie containing their login credentials and uses them to gain unauthorized access to the user's account

Actual Attacks

URL Hijacking

- **URL hijacking (**also called typosquatting) involves a fake URL that is very close to a real one.
- Example: original site: www.Chuckeas**tt**om.com.
- One might set up the site with only one t in the last name : www.Chuckeas**t**om.com,.

Actual Attacks

Wireless Attacks: Many wireless attacks

- **Example:** with the **evil twin attack**, a rogue wireless access point (WAP) is set up that has the same SSID as one of legitimate access points.
  - rogue WAP might be used to initiate a denial-of-service attack on legitimate access point
  - making it unable to respond to users and restricting to evil twin.
- Another wireless attack is Wi-Fi Protected Setup (WPS) attack.
- WPS requires a PIN to connect to the WAP.
- WPS attack attempts to intercept that PIN in transmission, connect to the WAP, and then steal the WPA2 password.

Actual Attacks

Cell Phone Attacks: More common attack:

Bluesnarfing: Unauthorized access of information from a Bluetooth device.

Blue jacking: The process of using another Bluetooth device that is within range and sending unsolicited messages to the target.

Bluebugging: Similar to bluesnarfing, bluebugging accesses and uses all phone features.

Pod slurping: Using a device such as an iPod to illicitly get confidential data by directly plugging it into a computer where the data are held.

Actual Attacks

Password Cracking

- Password cracking is easiest after getting a physical access to a machine.
- Many organizations (such as universities) have kiosk machines
  - where someone can use the system with minimal/guest privileges.
  - A skilled hacker can use this access to gain further access.

Malware Creation

Password Cracking

eLiTeWrap

TeraBIT Virus Maker