



Brute-Force Attacks

Cybersecurity Boot Camp
Pentesting 2 Day 1



Class Objectives

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



Perform advanced scans using Nmap.



Save and organize scan results using Metasploit workspaces and databases.



Perform a brute-force against an SSH server using Hydra.

Quick Review!

What is Scanning?

What is Enumeration?

Quick Review!

What is Scanning?

(Port) Scanning is a technique to determine which ports on a remote host are open.

What is Enumeration?

Quick Review!

What is Scanning?

(Port) Scanning is a technique to determine which ports on a remote host are open.

What is Enumeration?

Enumeration is the process of listing as much information available about a machine. This information might entail listing all of a machine's IP addresses and interfaces, installed applications, and/or registered user accounts.

Advanced Nmap and The msfconsole Database

Advanced Nmap and the msfconsole Database

We can save scan results to a built-in PostgreSQL database

- Additionally, those databases allow us to create different **workspaces** for different engagements.
- Metasploit databases can be set up in two steps:
 1. Start the pre-configured PostgreSQL service
 2. Initiate the Metasploit database.

We'll walk through these steps in the next demo.



Instructor Demonstration

Workspaces in Metasploit

Advanced Scanning

Intelligence gather is the most important phase of a penetration test because it unearths evidence of vulnerabilities that attackers may exploit. Initial intelligence gather typically consists of **host and service discovery**.

Host discovery is the process of discovering live hosts on a network.

- For example: attackers and pentesters can identify potential targets by pinging every IP address and seeing which responds.

Service discovery is the process of discovering which services are running on a reachable host.

- Typically begins with a port scan to reveal open ports on a machine.
- Then, banner grab to reveal which service is running on the port.

Scanning Technique Demo:

Next, we will walkthrough the following advanced Nmap tools and techniques:

1 OS Detection

2 UDP Scanning

3 Controlling scan speed

4 Stealth

1. Scanning Technique Demo: OS Detection

Nmap has tools that can **guess the operating system of a target machine**.

1 OS Detection

Nmap works by sending **TCP packets** to targets and listening for responses.

Let's recap TCP packets →

TCP Packets

1

OS Detection

Nmap works by sending **TCP packets** to targets and listening for responses.

| | | | | |
|---------------------|----------|-----------------|-----------------|----------------------|
| Version | IHL | Type of Service | Total Length | |
| Identification | | | Flags | Fragmentation Offset |
| Time to Live | Protocol | | Header Checksum | |
| Source Address | | | | |
| Destination Address | | | | |
| Options | | | | Padding |
| Data begins here... | | | | |

TCP responses contain a large amount of information, including:

Source and destination addresses;

TCP flags (SYN or ACK);

Protocol in use;
and more

TCP Packets

1

OS Detection

Nmap works by sending **TCP packets** to targets and listening for responses.

| | | | | |
|---------------------|----------|-----------------|-----------------|----------------------|
| Version | IHL | Type of Service | Total Length | |
| Identification | | | Flags | Fragmentation Offset |
| Time to Live | Protocol | | Header Checksum | |
| Source Address | | | | |
| Destination Address | | | | |
| Options | | | | Padding |
| Data begins here... | | | | |

Each operating system uses different software to create these TCP responses.

Windows, Mac and Linux all “speak” TCP but use different softwares.

These softwares are called an operating system’s **TCP/IP stack**.

TCP Packets

1

OS Detection

Nmap works by sending **TCP packets** to targets and listening for responses.

| | | | | |
|---------------------|----------|-----------------|-----------------|----------------------|
| Version | IHL | Type of Service | Total Length | |
| Identification | | | Flags | Fragmentation Offset |
| Time to Live | Protocol | | Header Checksum | |
| Source Address | | | | |
| Destination Address | | | | |
| Options | | | | Padding |
| Data begins here... | | | | |

Different **TCP/IP** stacks generate subtly different TCP responses.

For example, Windows generated response will contain the same raw data as a Linux generated response, but the default **Time to Live** will differ:
Windows = 128
Linux = 64

1. Scanning Technique Demo: OS Detection

Nmap has tools that can **guess the operating system of a target machine.**

1 OS Detection

Nmap sends TCP and UDP packets to target machines, and then examines its responses to determine the operating system.

Passive OS detection: process of looking for “fingerprints” in a machine’s response in order for Nmap to identify which operating system is running on a target of a port scan.

```
msf > db_nmap 192.168.1.100 -O
```

Active detection: a more complex yet more accurate process of transmitting suspiciously crafted packets onto a network and awaiting and analyzing responses.

```
msf > db_nmap 192.168.1.100 -A
```

2. Scanning Technique Demo: UDP Scanning

By default, **Nmap only scans TCP ports**.

1 OS Detection

2 UDP Scanning

Sometimes, pentesters need to exploit UDP services like DNS, NetBIOS, and TFTP.

UDP scan identifies such services:

```
msf > db_nmap -sU -p 137,138,139,53,69 scanme.nmap.org
```

- Note: **-p** indicates a port scan.

3. Scanning Technique Demo: Controlling Scan Speed

Nmap has flags that **increase and decrease its scan speed**.

1 OS Detection

2 UDP Scanning

3 Controlling scan speed

Faster scans get data quicker at a higher risk of being detected by an IDS.

Slower scans wait longer for data with less of a chance of being flagged by an IDS.

```
msf > db_nmap -sU -T4
```

4. Scanning Technique Demo: Stealth

The **louder** the machine is on a network, the **more likely is it to get flagged**.

1 OS Detection

2 UDP Scanning

3 Controlling scan speed

4 Stealth

Disabling ping checks and turning off DNS lookups will help reduce the amount of traffic you put on a network.

```
msf > db_nmap -Pn -n -sU -T4
```

scanme.nmap.org



Activity: Scanning and Enumeration

In this activity, you will use Nmap to perform host and service discovery and then use Metasploit to store and explore search results.

Instructions sent via Slack

Suggested Time:
45 Minutes



Advanced Nmap Review

Remember: network interfaces are the devices that allow a computer to send and receive traffic to and from the network

- Each network interface has a different IP address, meaning that having many network interfaces allows the *same* machine to communicate on *different* subnets.
- If an attacker gains control of a machine with several network interfaces, they can use the machine to scan and exploit any of the networks it's connected to, even if they can't see them directly from their attacking machine.
- This technique is called **pivoting** and the compromised machine is called a **pivot**.

Vulnerability Assessment

After Intelligence gathering, pentesters proceed to vulnerability assessment.



So far, we've used automated vulnerability scanners such as Nessus.

While we may know how to complete an automated scan, it is important to understand the methods of manually exploiting machines.

Manually Exploiting Machines

One of the most common manual attacks is **brute-force** against a login server, such as SSH, telnet, or FTP.

- SSH and telnet allow users to interact with another system's file system. Then, attackers can upload and download files, such as backdoors or sensitive user data.
- Password-based login servers are vulnerable by design, because they are inherently susceptible to **brute-force**.
- A **brute force attack** requires the hacker to use a list of passwords in an effort to login as a given user. This list of usernames and passwords is called a **wordlist**.



Metasploit has various tools for brute-forcing login forms that can be used against a variety of protocols, including FTP, HTTP, and others.

Today, we'll use it to attack an SSH Server.

Lesson Review:

Today we covered:

Metasploit enables you to organize data in _____, which let you save scan results to a database and keep work for different engagements separated.

Lesson Review:

Today we covered:

Metasploit enables you to organize data in **workspaces**, which let you save scan results to a database and keep work for different engagements separated.

Lesson Review:

Today we covered:

In addition to host and service discovery, you can use Nmap to:

- Detect operating systems with the `-O` (passive) and `-sV` (active) flags.
- Scan UDP ports with the `-u` option.
- Perform stealthy scans with the `-sS` (“no ping”/ skip host discovery), `-sT` (no DNS name resolution), `-sX` options .
- Scan very slowly (`-T0`) or very quickly (`-T5`).

Lesson Review:

Today we covered:

In addition to host and service discovery, you can use Nmap to:

- Detect operating systems with the **-O** (passive) and **-A** (active) flags.
- Scan UDP ports with the **-sU** option.
- Perform stealthy scans with the **-Pn** (“no ping”/ skip host discovery), **-n** (no DNS name resolution), **-disable-arp-ping** options .
- Scan very slowly (**-T2**) or very quickly (**-T5**). You can use any number between 0 (one packet every five minutes) and 5 (one packet every five milliseconds)

Lesson Review




Today we Covered:

Many servers expose a password-based login service, such as SSH. These services are intrinsically vulnerable to brute-force.

Today, we used _____ to attack SSH, which can also be used against other protocols such as FTP and HTTP.

Class Objectives

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

-  Save Nmap scan results in a workspace
-  Use advanced Nmap scanning options
-  Brute-force SSH servers with Hydra



Next class we'll cover

1. Using Metasploit modules in effort to quickly exploit SSH hosts
2. Pillaging data from compromised hosts
3. Post-exploitation tactic with Meterpreter