ESOF 422:

Advanced Software Engineering: Cyber Practices

Penetration Testing (Introduction, Reconnaissance)

Reese Pearsall

Spring 2025

Announcements

HW4 due Friday at 11:59 PM
→ Zip up your Java workspace and submit to Brightspace
→ No hardcopy needed

Fridays will be “lab days”
→ We will work through some in-class examples or
→ You will work through parts of the homework
→ Attendance is still encouraged unless I tell you otherwise

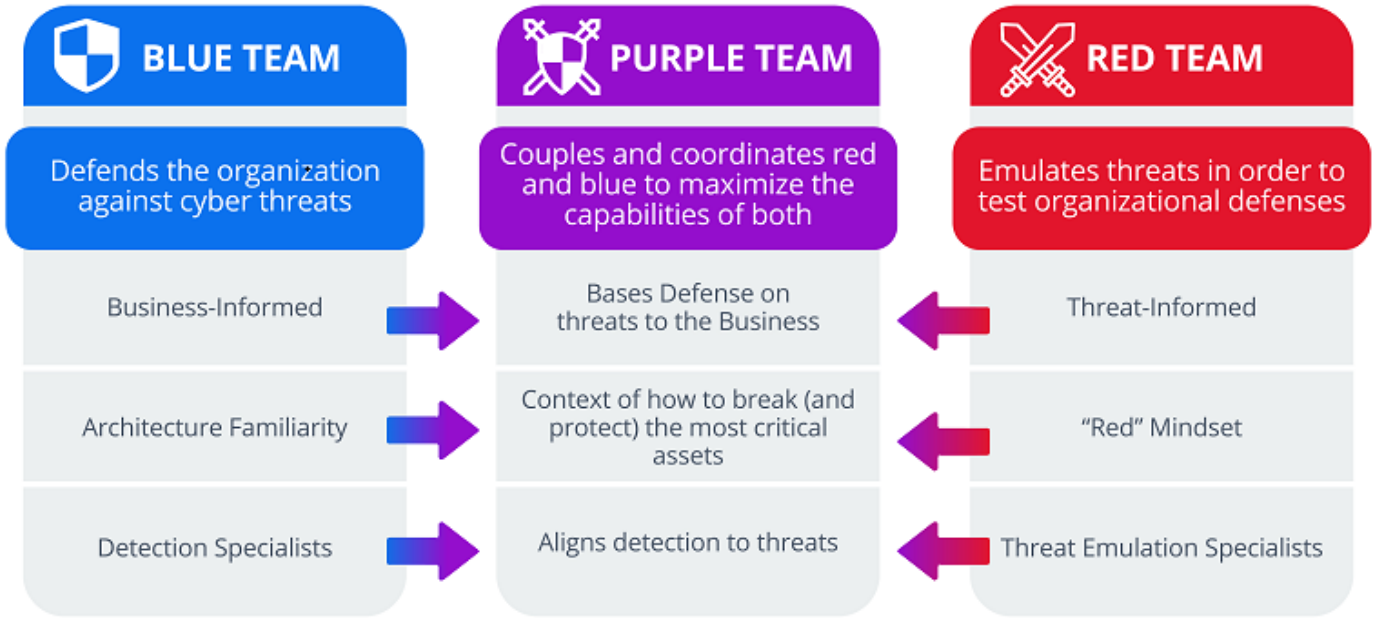
Attendance and Participation:
Class attendance and participation are highly encouraged, as they will be taken into consideration for final grades. Attendance can be worth (5% - 10%) of your grade. You are responsible for all the material covered in class. Prepare in advance for class by reading and studying the assigned text and ensuring you understand the previous lecture.

Even when vulnerabilities are fixed with a patch, those same patches can introduce new vulnerabilities ☺

Penetration Testing (pen testing) is an *authorized* simulated cyber attack launched against a system to evaluate its security

- Another instance of **ethical hacking**
- These tests are done by a security expert of a group of experts
- Helps identify vulnerabilities before attackers can exploit them
- *authorized*- an organization allows them to "hack" them (no legal consequences)
- These vulnerabilities range from simple social engineering attacks to fully-fledged RCE exploits

The process of penetration testing includes several steps, but the main parts are **finding vulnerabilities** and **exploiting** them (with permission)



"**Red Teamers**" are often the integral part of penetration tests

Types of Penetration Testing

Overt- Pen Testers work with the organization and IT team and are have full knowledge of the system and network

→ Requires less time and skill

→ Can uncover many more vulnerabilities

Covert- Pen testers have no knowledge of the system and organization's IT are not aware that they are pen testers

→ Requires more time and skill.

→ More closely simulates a real cyber attack

→ May find less vulnerabilities

Penetration Testing Phases

Preengagement Interaction- Meet with client, and discuss scope of penetration test

Penetration Testing Phases

Preengagement Interaction- Meet with client, and discuss scope of penetration test

Intelligence Gathering- Find information about client (legally)

- Who they are
- How it operates
- What mechanism are in place
- What services are open
- Openings

Penetration Testing Phases

Preengagement Interaction- Meet with client, and discuss scope of penetration test

Intelligence Gathering- Find information about client (legally)

- Who they are
- How it operates
- What mechanism are in place
- What services are open
- Openings

Threat Modeling- Identify potential vulnerabilities

Penetration Testing Phases

Preengagement Interaction- Meet with client, and discuss scope of penetration test

Intelligence Gathering- Find information about client (legally)

- Who they are
- How it operates
- What mechanism are in place
- What services are open
- Openings

Threat Modeling- Identify potential weaknesses

Vulnerability Analysis- Determine if the vulnerability exists and is viable to exploit

Penetration Testing Phases

Preengagement Interaction- Meet with client, and discuss scope of penetration test

Intelligence Gathering- Find information about client (legally)

- Who they are
- How it operates
- What mechanism are in place
- What services are open
- Openings

Threat Modeling- Identify potential weaknesses

Vulnerability Analysis- Determine if the vulnerability exists and is viable to exploit

Exploitation- Send target malicious payload to exploit vulnerability

Penetration Testing Phases

Preengagement Interaction- Meet with client, and discuss scope of penetration test

Intelligence Gathering- Find information about client (legally)

- Who they are
- How it operates
- What mechanism are in place
- What services are open
- Openings

Threat Modeling- Identify potential weaknesses

Vulnerability Analysis- Determine if the vulnerability exists and is viable to exploit

Exploitation- Send target malicious payload to exploit vulnerability

Post Exploitation- What sensitive data can be found, and how much damage can be caused.

Penetration Testing Phases

Preengagement Interaction- Meet with client, and discuss scope of penetration test

Intelligence Gathering- Find information about client (legally)

- Who they are
- How it operates
- What mechanism are in place
- What services are open
- Openings

Threat Modeling- Identify potential weaknesses

Vulnerability Analysis- Determine if the vulnerability exists and is viable to exploit

Exploitation- Send target malicious payload to exploit vulnerability

Post Exploitation- What sensitive data can be found, and how much damage can be caused.

Reporting- Provide an executive summary about weaknesses found and suggest countermeasures

Intelligence Gathering

OSINT (Open-Source Intelligence) is the process of collecting and analyzing publicly available information

Very helpful for the penetration testing process

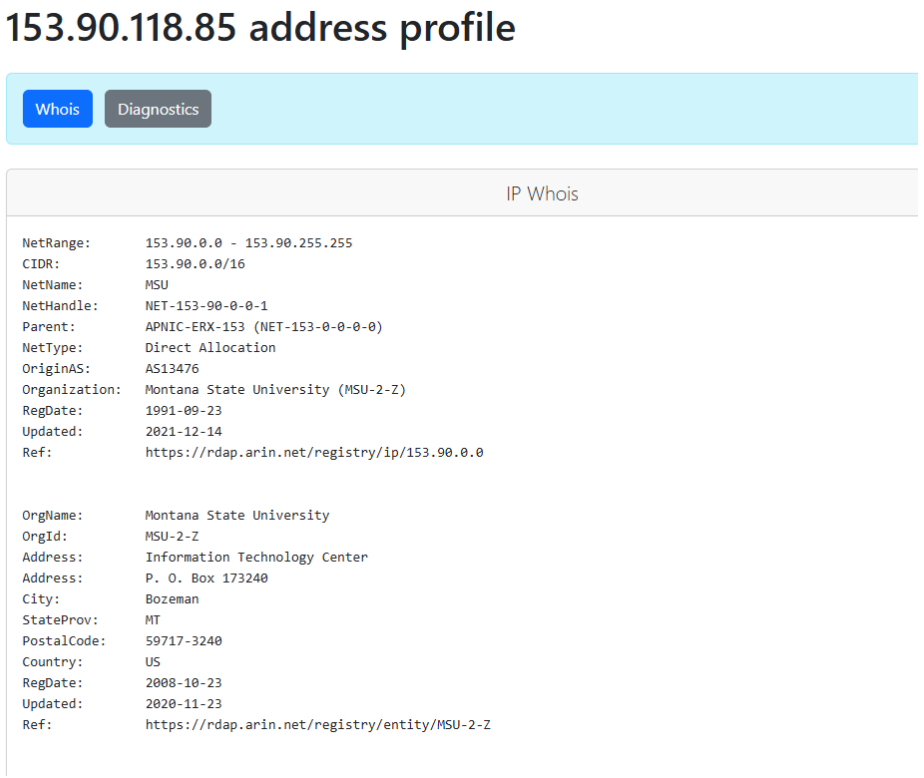
- Target Profiling
- Leaked Credentials
- Social Engineering
- Physical Access
- Identifying threat surfaces

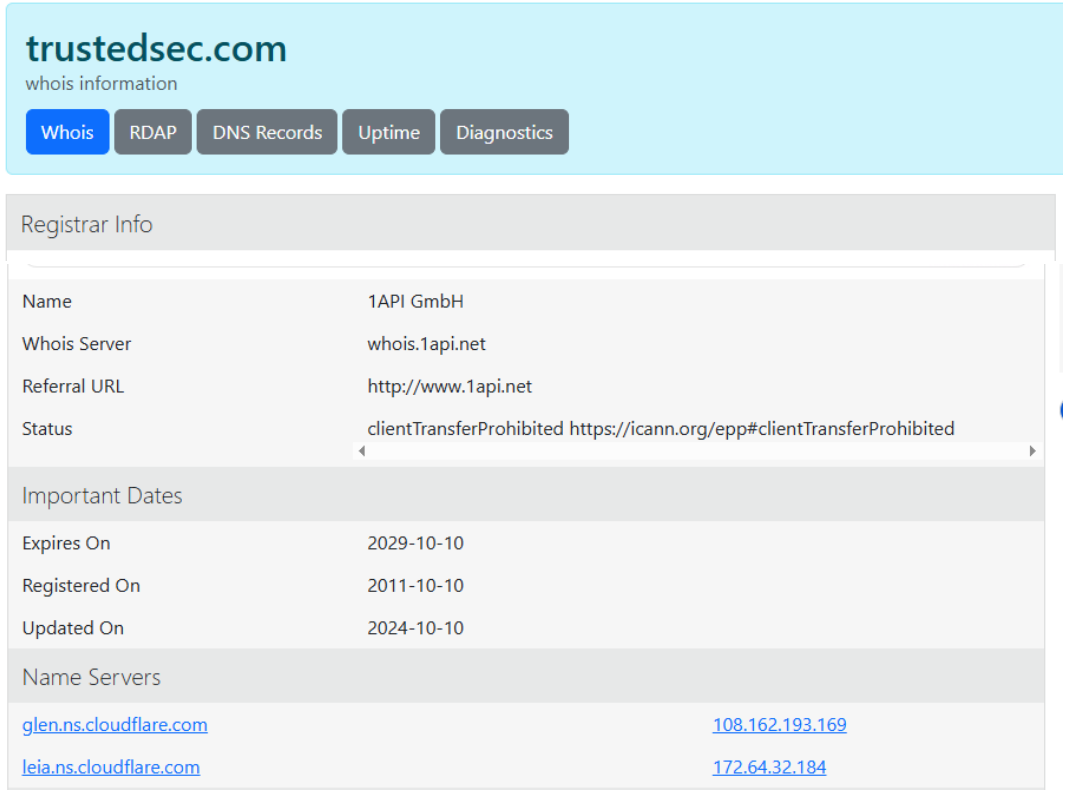
- → Newspaper and magazine articles, as well as media reports
- → Academic papers and published research
- → Books and other reference materials
- → Social media activity
- → Census data
- → Telephone directories
- → Court filings
- → Arrest records
- → Public trading data
- → Public surveys
- → Location context data
- → Breach or compromise disclosure information
- → Publicly shared cyberattack indicators like IP addresses, domain or file hashes
- → Certificate or Domain registration data
- → Application or system vulnerability data

Intelligence Gathering

Whois is a public database that stores information about registration and ownership of a particular domain and IP address

https://who.is/

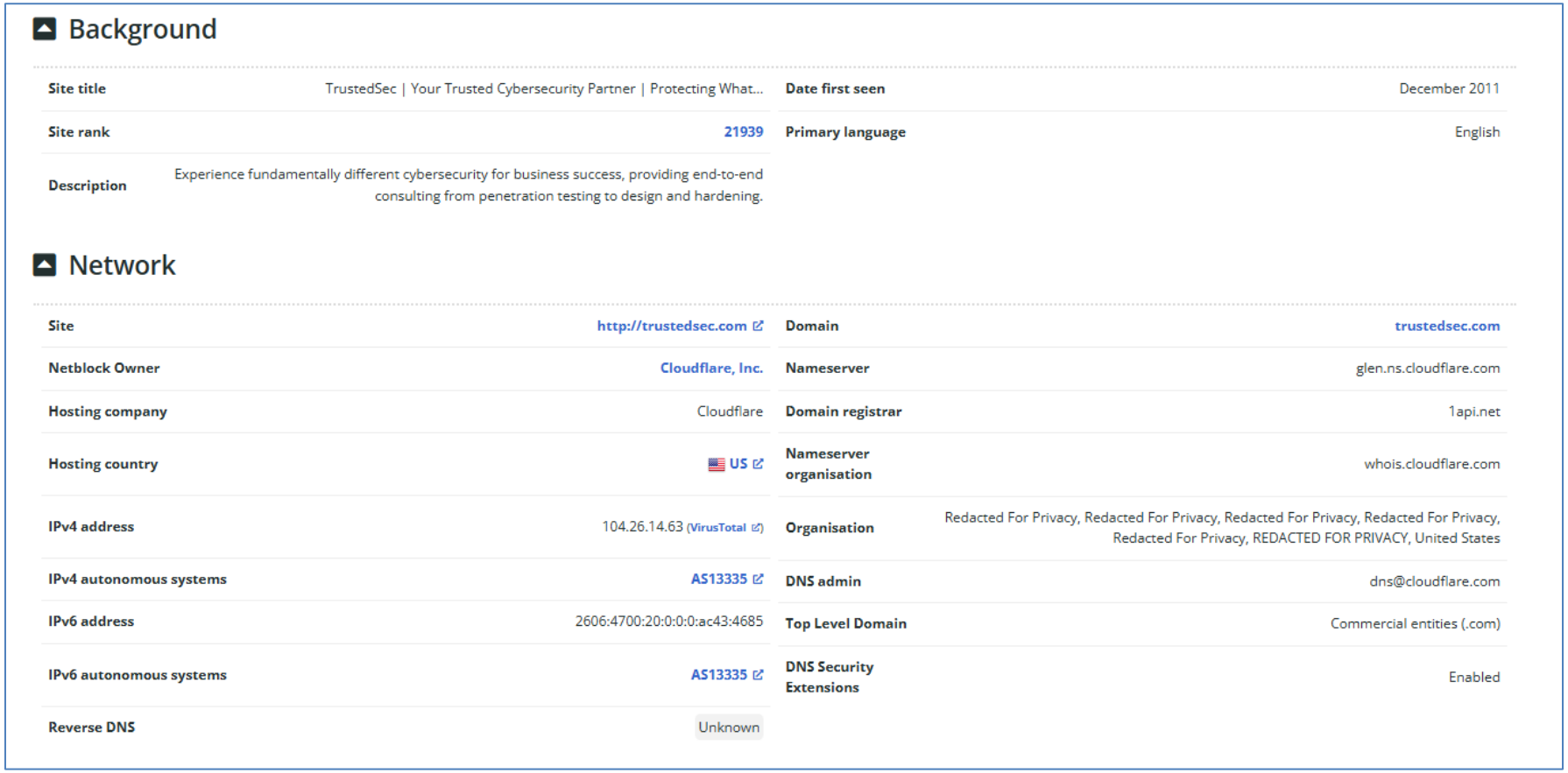




Intelligence Gathering

Netcraft is a web-based tool that can be used to find an IP address of a server hosting a particular website

https://searchdns.netcraft.com/



Background

Site title	TrustedSec | Your Trusted Cybersecurity Partner | Protecting What...	**Date first seen**	December 2011
Site rank	21939	**Primary language**	English
Description	Experience fundamentally different cybersecurity for business success, providing end-to-end consulting from penetration testing to design and hardening.		

Network

Site	http://trustedsec.com	**Domain**	trustedsec.com
Netblock Owner	Cloudflare, Inc.	**Nameserver**	glen.ns.cloudflare.com
Hosting company	Cloudflare	**Domain registrar**	1api.net
Hosting country	US	**Nameserver organisation**	whois.cloudflare.com
IPv4 address	104.26.14.63 (VirusTotal)	**Organisation**	Redacted For Privacy, Redacted For Privacy, Redacted For Privacy, Redacted For Privacy, Redacted For Privacy, REDACTED FOR PRIVACY, United States
IPv4 autonomous systems	AS13335	**DNS admin**	dns@cloudflare.com
IPv6 address	2606:4700:20:0:0:0:ac43:4685	**Top Level Domain**	Commercial entities (.com)
IPv6 autonomous systems	AS13335	**DNS Security Extensions**	Enabled
Reverse DNS	Unknown		

Intelligence Gathering

dig or **nslookup** can be used to find domain information

mx = “mail server”

```
┌──(kali㉿kali)-[~]
└─$ sudo dig mx trustedsec.com

; <<>> DiG 9.20.4-4-Debian <<>> mx trustedsec.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43196
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 5ef63e3634af2d850100000067eae4105bbecf79d5a0c65d (good)
;; QUESTION SECTION:
;trustedsec.com.                        IN      MX

;; ANSWER SECTION:
trustedsec.com.         300     IN      MX      10 mx1-us1.ppe-hosted.com.
trustedsec.com.         300     IN      MX      20 mx2-us1.ppe-hosted.com.

;; Query time: 48 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Mon Mar 31 14:45:08 EDT 2025
;; MSG SIZE  rcvd: 133
```

Mail servers can be found under these domains

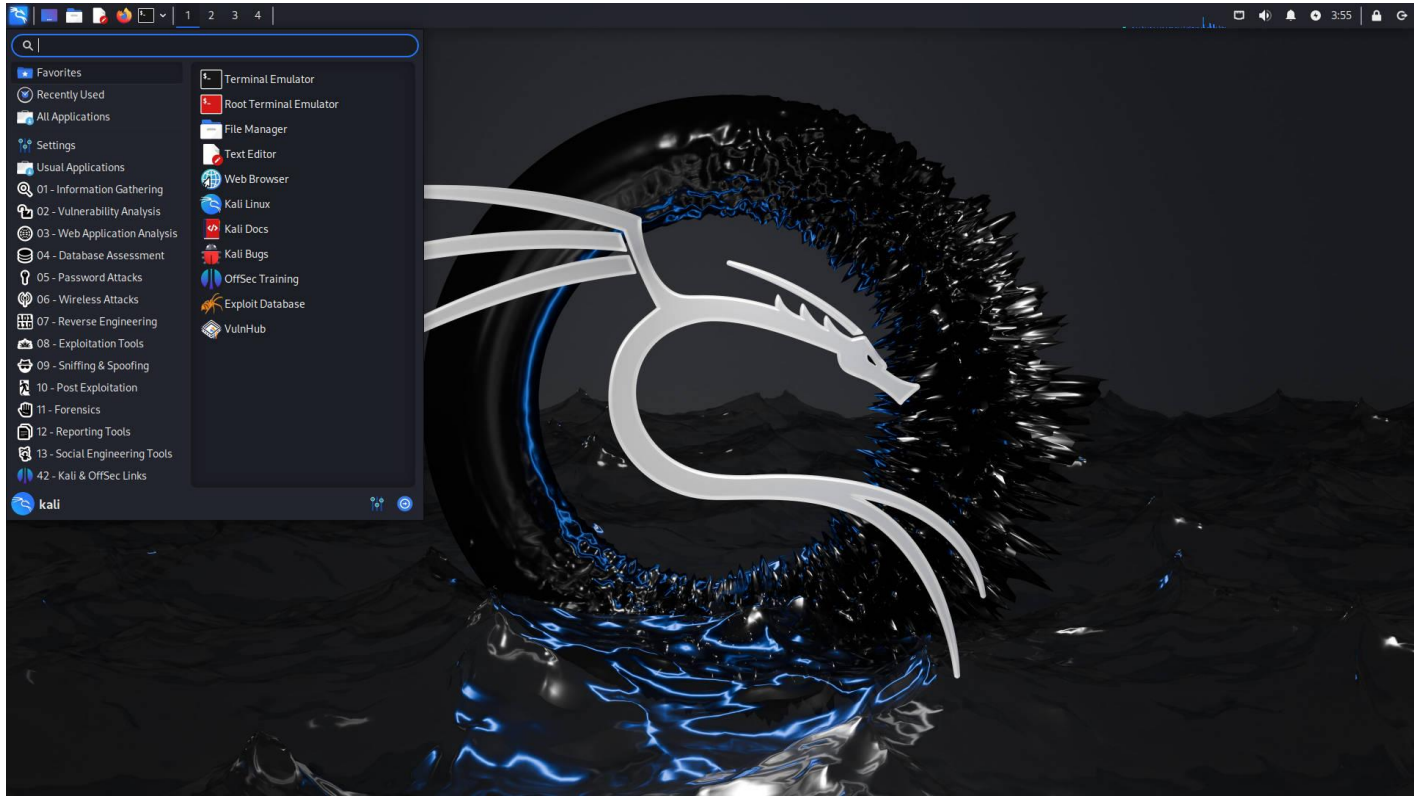
Don’t be malicious

Don’t be stupid

Your actions have consequences, and hacking can put you in prison

Kali Linux

Kali Linux is a Linux distro that comes with many offensive security tools and is designed for security testing



Commonly used for penetration testing

Metasploit

Metasploit is the go-to framework for penetration testing

- Free and open-source
- Provides endless functionality for automating routine and complex pen testing procedures

Metasploit Terminology

Exploit- how a pen tester takes advantage of a flaw

Payload- malicious code or request that we send to victim server

Shellcode- binary instructions of malicious code

Module- a built-in function that Metasploit uses for some task

Listener- a component on the pen tester's machine that waits for a connection from the victim machine

Starting Metasploit

`sudo msfconsole` will summon a Metasploit console, which understands Metasploit “commands”

Port scanning is a common first step in pen testing. **nmap** is the most popular port scanning tool

You should not nmap an address unless you have permission

```
┌──(kali㉿kali)-[~]
└─$ nmap scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 15:38 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.015s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite
```

Port scanning is a common first step in pen testing. **nmap** is the most popular port scanning tool

Metaploit has a module for nmapping a remote host!

```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) >
```

You should not nmap an address unless you have permission

We need to set the IP address of the remote host !

```
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   THREADS      1                yes       The number of concurrent threads (max one per host)
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds


View the full module info with the info, or info -d command.
```

```
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 45.33.32.156
RHOSTS ⇒ 45.33.32.156
```

Port scanning is a common first step in pen testing. **nmap** is the most popular port scanning tool

Metaploit has a module for nmapping a remote host!

```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) >
```

You should not nmap an address unless you have permission

(TCP port scanning is slightly different than nmap)

```
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 1-100
PORTS ⇒ 1-100
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 45.33.32.156
RHOSTS ⇒ 45.33.32.156
msf6 auxiliary(scanner/portscan/tcp) > run
[+] 45.33.32.156:         - 45.33.32.156:22 - TCP OPEN
[+] 45.33.32.156:         - 45.33.32.156:80 - TCP OPEN
[*] 45.33.32.156:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >
```

TCP ports 22 and 88 are open