

COURSE: Top 5 Tools & Tricks for Ethical Hacking & Bug Bounties 2021

Unveiling the Ultimate Toolkit: Mastering Ethical Hacking & Bug Bounties with Top 5 Tools & Tricks 2021



Introduction:

In the dynamic landscape of cybersecurity, staying one step ahead of potential threats is paramount. Ethical hackers, penetration testers, and bug bounty hunters are the guardians of this digital realm, armed with knowledge, skills, and cutting-edge tools. Welcome to the transformative Udemy course "Top 5 Tools & Tricks for Ethical Hacking & Bug Bounties 2021." In this article, we'll provide you with a glimpse into the exciting world of this course, which unveils the quintessential tools and techniques that can empower you to become a skilled cybersecurity professional.

Navigating the Path of Mastery:

Nmap: The Network Mapper:

Begin your journey with an exploration of Nmap, the Network Mapper. Discover how this powerful tool can be used to map out networks, identify devices, and assess vulnerabilities, providing you with a comprehensive understanding of a target's infrastructure.



1. UDP Scan (-sU)

This technique is used to scan the open UDP ports of the target IP/host. Here, UDP scan sends UDP Packets to every ports of the target and waits till it get response. If, it receives error message stating that the **ICMP** is unreachable, this means that the port is closed. But, if gets any approachable response, then it means the port is open.

```
(root@kali)~# nmap --top-ports 10000 172.16.121.134
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-05 00:26 PDT
Nmap scan report for 172.16.121.134
Host is up (0.00037s latency).
Not shown: 8334 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5040/tcp  open  unknown
5357/tcp  open  wsddapi
7680/tcp  open  pando-pub
MAC Address: 00:0C:29:

Nmap done: 1 IP address (1 host up) scanned in 6.92 seconds
```

2. FIN Scan (-sF)

In Fin Scan technique, packets are sent with a Fin Flag. Sometimes, because of firewall, SYN Packets might be blocked. In such case, FIN Scan works by passing the firewall. FIN packets are sent to closed ports, if no response is received, it is because either the packet is dropped by firewall or the port is open.

```
(linuxhint@Linux-Hint-com)-[~]
└─$ sudo nmap -sF -T2 192.168.0.1 -v
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-07 15:31 EDT
Initiating Ping Scan at 15:31
Scanning 192.168.0.1 [4 ports]
Completed Ping Scan at 15:31, 0.40s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:31
Completed Parallel DNS resolution of 1 host. at 15:31, 0.02s elapsed
Initiating FIN Scan at 15:31
Scanning 192.168.0.1 [1000 ports]
FIN Scan Timing: About 7.55% done; ETC: 15:38 (0:06:20 remaining)
FIN Scan Timing: About 14.95% done; ETC: 15:38 (0:05:47 remaining)
Stats: 0:01:29 elapsed; 0 hosts completed (1 up), 1 undergoing FIN Scan
FIN Scan Timing: About 22.00% done; ETC: 15:38 (0:05:16 remaining)
Stats: 0:01:29 elapsed; 0 hosts completed (1 up), 1 undergoing FIN Scan
FIN Scan Timing: About 22.10% done; ETC: 15:37 (0:05:14 remaining)
```

3. Ping Scan (-sP)

This technique is only used to find out whether the host is available or not. Ping Scan is not used to detect open ports. It sends an ICMP echo request and in return gets ICMP echo reply if the host is alive.

```
kali@kali: ~
└─$ nmap -sP www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 16:45 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0093s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 6.19 seconds
```

4. TCP SYN Scan (-sS)

In this technique, Nmap sends SYN packets to the destination, but does not create any session. As a result, target computer won't be able to create any log of interaction as no session was initiated.

```
root@kali:~# nmap -sS -p22,25,110 scanme.nmap.org
Starting Nmap 7.40 ( https://nmap.org ) at 2017-08-10 04:07 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.042s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
110/tcp   filtered pop3
Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
```

5. TCP Connect() Scan (-sT)

UNIX socket uses a system call named **connect()** to begin TCP connection and if it succeeds, connection can be made and if it fails, connections cannot be made, basically because the port might be closed. This technique is only used to find out TCP ports and not UDP.

```
root@hacker:~# nmap -sT 192.168.56.115
Starting Nmap 6.46 ( http://nmap.org ) at 2014-06-19 07:43 IST
Nmap scan report for 192.168.56.115
Host is up (0.0069s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

6. Version Detection (-sV)

This technique is used to find out about specific service running on open port, its version and product Name. It is not used to detect open ports. However, this scan needs open ports in order to detect the version. It uses TCP SYN scan to know about the open ports.

```
(root@kali)-[~]
└─$ nmap -O --osscan-limit 192.168.130.120-150
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-07 05:43 PDT
Nmap scan report for 192.168.130.129
Host is up (0.00061s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsddapi
MAC Address: 00:0C:29:E5:2B:27 (VMware)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
```

7. Idle Scan (-sI)

Idle scan is an advance scan that does not send any packets from your IP address, instead it uses another host from the target network to send the packets.

```
root@student:~# nmap -Pn -sI 12.12.12.245 12.12.12.242
Starting Nmap 6.47 ( http://nmap.org ) at 2016-07-11 12:46 WIB
Idle scan using zombie 12.12.12.245 (12.12.12.245:80); Class: Incremental
Nmap scan report for 12.12.12.242
Host is up (0.051s latency).
Not shown: 988 closed|filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1028/tcp  open  unknown
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
MAC Address: 00:0C:29:E5:9A:E8 (VMware)
```

- You can Download Nmap for the given below link:
GitHub:- <https://github.com/nmap/nmap>