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.

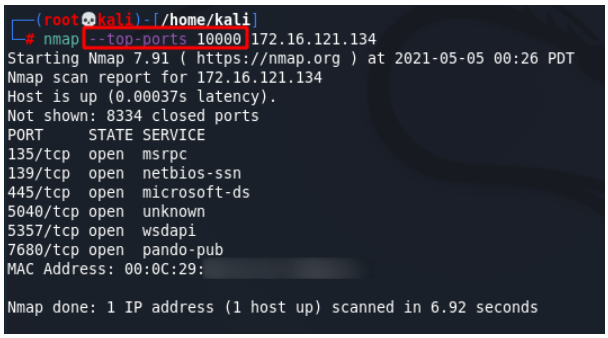
Navigating the Path of Mastery:

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.

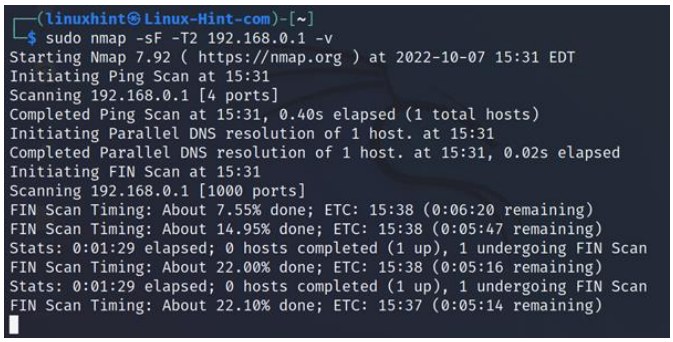
1. **UDP Scan (-sU)**

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.



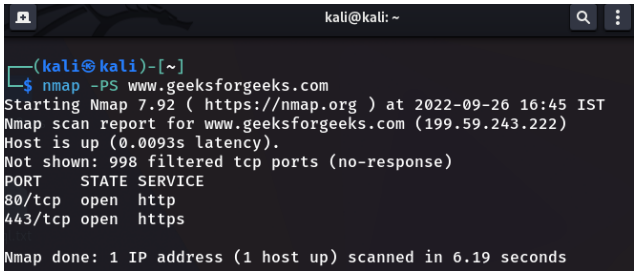
2. FIN Scan (-sF)

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 by passing the firewall. FIN packets are send to closed ports, if no response is received, it is because either the packet is dropped by firewall or the port is open.



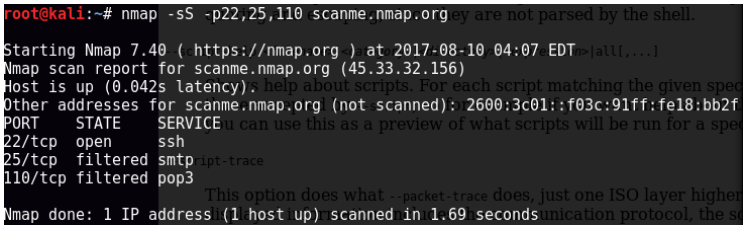
3. Ping Scan (-sP)

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 is the host is alive.



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.

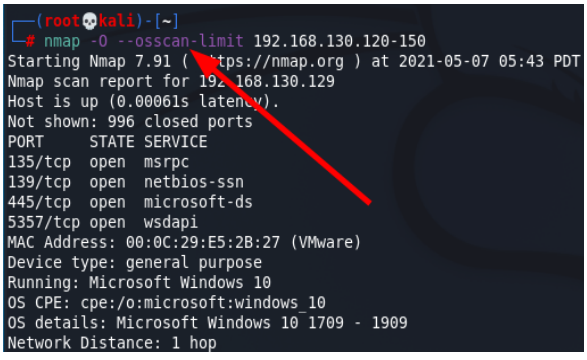


5. TCP Connect() Scan (-sT)

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.

6. Version Detection (-sV)

This technique is used to find out about specific service running on open port, it's 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.



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