

Level 6 - Advanced Cyber Security

by Aleksandar Kushlev

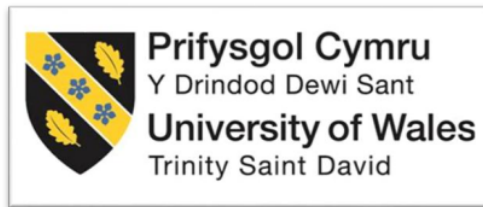
Submission date: 21-Jul-2023 09:44AM (UTC+0100)

Submission ID: 210499136

File name: 29935_Aleksandar_Kushlev_Level_6_-_Advanced_Cyber_Security_507624_904419352.docx (2.9M)

Word count: 4458

Character count: 25958



²
Advanced Cyber Security – Level 6 Assessment

Module Code: ACCB6000

Lecturer:

Olusola Adeniyi

Student Name:

Aleksandar Kushlev

Student ID:

2028393

Table of contents:

Abstract (200 words)

Task 1: Cyber Security and current technologies/mechanisms
(2000 words)

Introduction (600 words)

The CIA Triad (400 words)

Types of Attacks (600 words)

Password-based Attacks (600 words)

Task 2: Implementation and Analysis (2000 words)

Task 3: Proposal for a mitigation strategy (1000 words)

Conclusion (300 words)

Abstract

Network and cybersecurity are essential parts of an organization's security and it is becoming more important with globalization and digitalization of the world. This paper will examine potential risks, analyse threats, and propose mitigation strategy for an NGO which operates internationally and which had network and cybersecurity issues within its physical location. Firstly, the author will present the current state of cybersecurity and describe the current technologies and mechanisms. The author will then elaborate and describe different techniques/tools for network scanning enumeration, vulnerability assessment, and hacking using Kali Linux and Windows OS. As a conclusion, the author will propose a mitigation strategy to help the NGO understand their technical security weaknesses and recommend ways for the organization to strengthen their network and cybersecurity. The author concludes that the organization's first and most important step is building a comprehensive cybersecurity risk assessment to be able to identify potential vulnerabilities, hazards, and risks.

Deliverable 1: Cyber Security and current technologies/mechanisms

Introduction

Corporate cybersecurity is a top concern for organisations across industries in the connected world of today. Threats and vulnerabilities that criminal actors use to access networks, steal sensitive data, and interfere with corporate processes grow more sophisticated as technology develops. Since cyber dangers are continuously changing, organisations must remain alert and flexible to protect their digital assets and maintain client confidence.

A rise in sophisticated cyber-attacks and vulnerabilities in recent years has highlighted the necessity for strong defence mechanisms and preventative security measures. Cybercriminals use a variety of attack methods to exploit vulnerabilities in corporate networks, software, and user behaviour. The threat landscape is still varied and unpredictable, with anything from supply chain attacks that compromise trusted systems to ransomware operations that destroy vital infrastructures.

The rise of "zero-day" vulnerabilities, previously unidentified flaws in software and systems that attackers exploit before developers can release patches, has been one of the significant recent difficulties. Such flaws could have disastrous results, highlighting the importance of effective and prompt vulnerability management.

Additionally, social engineering-based assaults have increased in frequency. These attacks use trickery and manipulation to get employees to divulge confidential data or allow unauthorised access. Organisations must prioritise employee education and cybersecurity knowledge as the human element becomes a crucial target for cybercriminals in order to build a robust human firewall.

Researchers and cybersecurity experts have been working hard to create novel defence strategies and mechanisms in response to these attacks. Artificial intelligence and machine learning are used to quickly identify dangers and take action in response, giving organisations the ability to spot unusual activity and quickly eliminate potential risks.

Using Virtual Private Networks (VPNs) to safely integrate remote workforces is one of the most recent issues organisations are facing. While VPNs are crucial tools for creating secure connections, if they are not set up and maintained properly, they may unintentionally introduce additional security threats. Organisations must give priority to VPN security since cybercriminals are increasingly using old or improperly configured VPNs as access points to corporate networks.

Furthermore, it has become crucial to ensure strong cloud security as enterprises move their operations to the cloud. Although cloud services have many benefits, they also present certain hazards. Sophisticated cloud security developments are required due to issues including incorrectly configured cloud settings, data breaches, and unauthorised access to data stored in the cloud.

Adopting "defence in depth" principles, which protect the organisational infrastructure by implementing numerous levels of security controls, is another important defence tactic. A thorough security architecture, including firewalls, intrusion detection systems, strong access controls, and encryption protocols, is essential for defending against complex attacks.

Collaboration and the sharing of threat intelligence have emerged as essential elements of contemporary cybersecurity defence. Organisations can collectively improve their resistance to common dangers by combining their resources and expertise, reducing the likelihood of widespread attacks.

This study attempts to explore current risks and weaknesses that have appeared in the corporate cybersecurity landscape. It will examine major recent cyberattacks, examining their strategies, methods, and effects on businesses. The report will also look into the defence strategies and tools used by leading companies to effectively counter and minimise cyber threats.

This study aims to provide organisations and cybersecurity professionals with the knowledge required to strengthen their defence strategies, secure their data, and guarantee the continuity of business operations in an ever-evolving digital landscape by examining the most recent advancements in corporate cybersecurity.

The Cybersecurity Triad (CIA Triad)

When discussing cybersecurity and defence, it is important for the cybersecurity professional to prioritize the risks that the organization is exposed to. The three pillars of information security—*confidentiality, integrity, and availability*—are represented by the CIA triad¹:

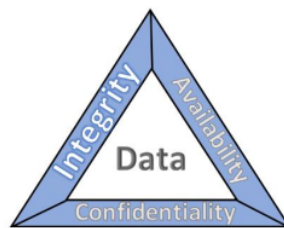


Image Source: <https://www.nist.gov>

Confidentiality is the maintenance of legally permitted constraints on the access and disclosure of information, including safeguards for protecting individual privacy and proprietary data. To be able to determine which person can access which types of data, the

¹ Cawthra. J., "Data Integrity : Detection and Responding to Ransomware and Other Destructive Events", NIST SPECIAL PUBLICATION 1800-26A, NIST.gov, December 2020 [Online] [Accessed: 15/07/2023]

appropriate controls should be in place, which means that the ³the data can be categorised as follows²:

- *Restricted*: This is the most significant information that the corporation has since it might contain trade secrets that, if revealed, might have a disastrous effect on the business.
- *Confidential*: This information must be kept private by businesses (based on a need-to-know basis). This kind of information is frequently linked to external restrictions, and if it is released, penalties and fines may be imposed.
- *Private*: This information is less sensitive. It should be kept inside the company though because it isn't meant for public consumption.
- *Public*: This data is meant for distribution to the general public and is frequently accessible and indexed online.

¹⁴**Integrity** is the prevention of erroneous information alteration or deletion as well as the assurance³ of information authenticity. This is particularly important if your business operates a transactional website (like an e-commerce website), as an attacker might attack your database and create or modify discount codes before you realise there is a problem and your products have already been sold and delivered for a significant discount.

³The fact that the attacker will apply this discount to everyone's purchases rather than just their own makes these assaults more risky. As a result, you can discover ⁶1,000 orders discounted by 99%, making it more difficult for you to figure out who launched the attack.

⁹Ensuring timely and dependable access to and use of information is known as **availability**. With the exception of online stores, these attacks are considered to be less hazardous; nevertheless, they are also the most prevalent form of attack. Indeed, a significant portion of the attacks executed by Hactivist collectives are primarily focused on causing disruptions to the availability of targeted systems.

Types of Attacks³

In order to effectively execute a robust defensive strategy, it is imperative to possess a comprehensive comprehension of the prevailing threat environment as well as the prevalent forms of attacks. It is essential to acknowledge that safeguarding against unforeseen threats is not feasible. Certain sources categorise attacks according to their impact area, such as network attacks and physical attacks. To be able to identify the possible dangers for the organization, it is useful to have a big-picture view of the threats such as a threat landscape:

⁷

² Bravo, C., "Mastering Defensive Security: Effective Techniques to secure your Windows, Linux, IoT, and cloud infrastructure", 1st ed., Birmingham, Packt Publishing, 2021, p.5

³ Bravo, C., "Mastering Defensive Security: Effective Techniques to secure your Windows, Linux, IoT, and cloud infrastructure", 1st ed., Birmingham, Packt Publishing, 2021, pp.6-16

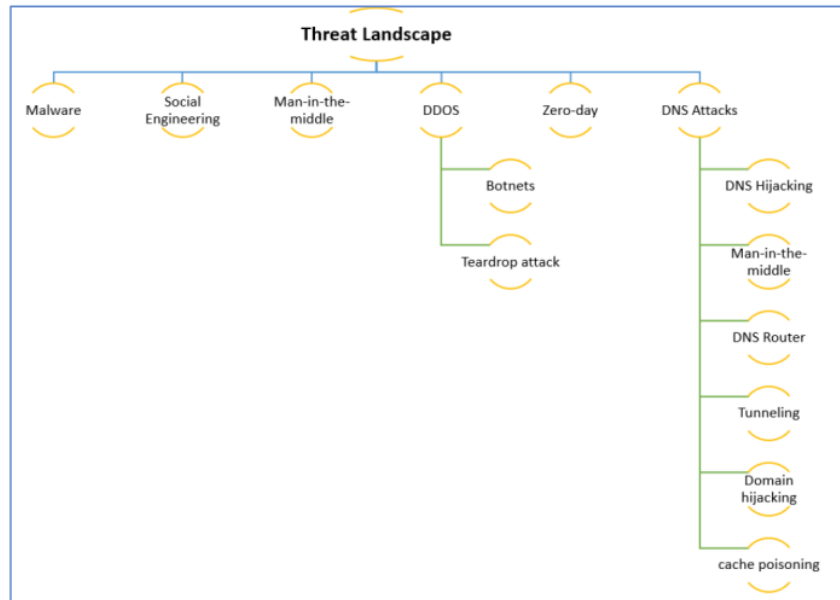


Figure 1⁴: Cybersecurity Threat Landscape

¹ (Source: Bravo, C., “Mastering Defensive Security: Effective Techniques to secure your Windows, Linux, IoT, and cloud infrastructure”, 1st ed., Birmingham, Packt Publishing, 2021, p.7)

Malware

There exist various categories of malware, encompassing Remote Access Trojans (RATs), Trojans, Worms, Ransomware, Spyware, and additional variants. Each entity possesses distinct attributes, necessitating a comprehensive comprehension of their individual traits in order to effectively counteract their potential threats.

Social Engineering

The establishment of a comprehensive cybersecurity infrastructure necessitates significant dedication of time, effort, and resources. However, the inclusion of the user, who is often the most vulnerable component, is imperative to achieve a truly robust environment.

There exist numerous instances wherein a company experiences a catastrophic attack³ not due to the compromise of their costly systems, nor as a result of being targeted by a sophisticated zero-day vulnerability, but rather because an employee unintentionally

⁴ Source: Bravo, C., “Mastering Defensive Security: Effective Techniques to secure your Windows, Linux, IoT, and cloud infrastructure”, 1st ed., Birmingham, Packt Publishing, 2021, p.7

discloses their login credentials to an attacker. The most popular form of social engineering is *phishing* where the attacker sends a fake email pretending to be a trustworthy person or business. To improve their chances of success, the attacker will first try to convince the victim that the email is real (by using company logos or pretending to be an email account or domain) and then ask the user to do something, like click on a link or open an attached PDF.

Man-in-the-middle attacks

An example of a man-in-the-middle attack could be a free wi-fi spot in the shopping centre. The free wi-fi network could be a setup by a cybercriminal and by connecting to it a user can expose their data and allow the criminal to capture it.

Regarding the employed methodology, the perpetrator may opt for a variety of techniques, including session hijacking, IP spoofing, replay attacks, or eavesdropping.

21

Denial-of-service (DOS) attack

The **Distributed Denial-of-Service (DDoS) attack**, widely regarded as the most favoured method utilised by hackers, presents a notable subject of inquiry due to its potential impact on both the attacker and the target. As previously stated, the consequences of such attacks vary depending on the specific characteristics of the targeted business. Nevertheless, it is important to note that an attacker could exploit your infrastructure to initiate a Botnet-driven assault against another organisation. This would result in significant ramifications for your company, irrespective of its industry or sector.

Teardrop attack

The teardrop attack exploits a previously identified vulnerability in which the system engages in the reassembly of fragmented packets. However, due to the presence of corruption within these packets, the system experiences a crash, resulting in the CPU being fully utilised at 100% capacity. As previously stated, this vulnerability is of antiquated nature and a system that is current and regularly updated should not be susceptible to its impact. Nevertheless, a recently discovered variant known as FragmentSmack has been found to impact contemporary operating systems, such as Windows 10 and various Linux distributions. Fortunately, there are already available solutions for both issues.

Zero-day exploits

These are exploits which are possible due to a newly-found vulnerability which has not been addressed yet by building the respective patches and updates. These particular forms of attacks pose a significant threat due to their capacity to catch us off guard. In the context of addressing such forms of attacks, prompt response is crucial. It is imperative to consistently remain vigilant for emerging vulnerabilities in order to comprehend their implications, assess their impact on your infrastructure, and devise interim measures or mitigations until an official resolution or patch becomes available.

DNS attacks

With the development of cybercrime, sophisticated DNS-related attacks have been developed:

- *DNS hijacking* - this attack typically involves the infiltration of malware onto a computer system, which subsequently alters the computer's DNS settings to direct traffic towards the attacker's DNS server rather than a reliable and trusted DNS server. Consequently, the attacker gains the ability to manipulate and redirect all network traffic at will.
- *Main-in-the-middle* - this attack employs the identical principle as the one previously referenced. The topic pertains to the act of intercepting a Domain Name System (DNS) request and subsequently responding to it by replaying with a counterfeit website. In order to accomplish this, the assailant intercepts the communication between the target and the legitimate Domain Name System (DNS) server, thereby providing the user with a deceptive response directing them to a malicious website.
- *DNS router attack* - In this scenario, the assailant exploits a vulnerability present in the router in order to execute the redirection towards the malevolent website.
- *DNS cache poisoning* - this phenomenon bears resemblance to DNS hijacking; however, in this instance, the assailant solely manipulates the DNS cache to redirect forthcoming requests towards malicious websites.

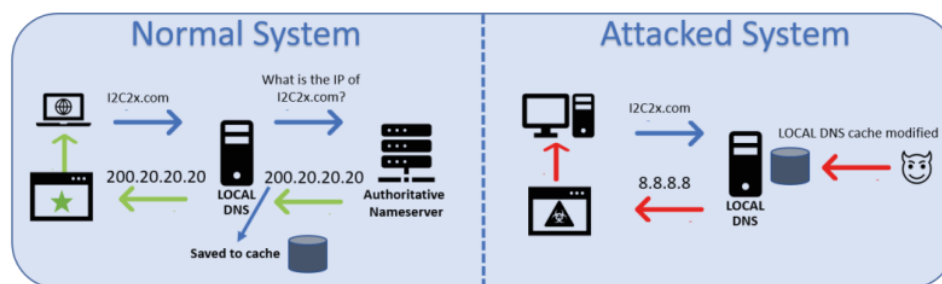


Figure 2⁵: Cache poisoning attack flow

- *DNS tunnelling* - the focus of this attack is directed towards online resources, specifically web pages and web applications. In this scenario, the perpetrator intends

⁵ Source: Bravo, C., "Mastering Defensive Security: Effective Techniques to secure your Windows, Linux, IoT, and cloud infrastructure", 1st ed., Birmingham, Packt Publishing, 2021, p.13

to manipulate the Domain Name System (DNS) settings within your domain registrar's infrastructure. This alteration would redirect all incoming traffic intended for your webpage to an alternative server. In this scenario, the perpetrators employ misspelt names or visually similar letters to deceive the user into perceiving their interaction with the authentic website.

Password-based Attacks⁶

Attacks on passwords are a popular weak point in cybersecurity. Over the past two decades, numerous experts have consistently predicted the obsolescence of passwords. However, despite the emergence of various authentication technologies, passwords have persisted and are likely to remain in use for an extended duration. Hence, it is imperative for security professionals to consistently seek innovative approaches in safeguarding against password-based attacks.

There is a variety of password attacks that a cybersecurity professional must be aware of:

- Password breaches
- Social engineering involving stolen password
- Brute-force attacks
- Dictionary attacks

To be able to address the above potential attacks, a professional should implement several rules within the organization to improve the security of passwords:

- Use of password vaults
- Password length and complexity policies
- Invest in training employees on the importance of password security

Conclusion

Since “Lending Hands” is a relatively big organization with international operations and communications, it is susceptible to a variety of risks/threats that might affect different parts of the CIA Triad and therefore a concise cybersecurity plan needs to be developed with all of the potential risks/threats addressed. For this purpose, a cybersecurity professional must always be assessing the vulnerabilities within the systems managed and this is called vulnerability assessment.

⁶ Bravo, C., “Mastering Defensive Security: Effective Techniques to secure your Windows, Linux, IoT, and cloud infrastructure”, 1st ed., Birmingham, Packt Publishing, 2021, pp. 16-24

Deliveerable 2: Implementation and Analysis

Lab Activity - Scanning and Enumeration

Part 1: Use an alternative to HPING to send ICMP/TCP/UDP Packets and analyse the target replies.

In Kali Linux we can use the “**nping**” command which is part of the Nmap suite to serve as an alternative to “**hping3**” for sending ICMP, TCP, UDP packets. For analysis of the target replies we can use “**tcpdump**”.

```
(root@kali)~/home/kali
# nping -c 4 10.0.2.4

Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2023-07-21 01:45 BST
SENT (0.0252s) ICMP [10.0.2.5 > 10.0.2.4 Echo request (type=8/code=0) id=2202
seq=1] IP [ttl=64 id=57004 iplen=28 ]
RCVD (0.0255s) ICMP [10.0.2.4 > 10.0.2.5 Echo reply (type=0/code=0) id=2202 s
eq=1] IP [ttl=128 id=4399 iplen=28 ]
SENT (1.0290s) ICMP [10.0.2.5 > 10.0.2.4 Echo request (type=8/code=0) id=2202
seq=2] IP [ttl=64 id=57004 iplen=28 ]
RCVD (1.0295s) ICMP [10.0.2.4 > 10.0.2.5 Echo reply (type=0/code=0) id=2202 s
eq=2] IP [ttl=128 id=4400 iplen=28 ]
SENT (2.0333s) ICMP [10.0.2.5 > 10.0.2.4 Echo request (type=8/code=0) id=2202
seq=3] IP [ttl=64 id=57004 iplen=28 ]
RCVD (2.0338s) ICMP [10.0.2.4 > 10.0.2.5 Echo reply (type=0/code=0) id=2202 s
eq=3] IP [ttl=128 id=4401 iplen=28 ]
SENT (3.0348s) ICMP [10.0.2.5 > 10.0.2.4 Echo request (type=8/code=0) id=2202
seq=4] IP [ttl=64 id=57004 iplen=28 ]
RCVD (3.0351s) ICMP [10.0.2.4 > 10.0.2.5 Echo reply (type=0/code=0) id=2202 s
eq=4] IP [ttl=128 id=4402 iplen=28 ]

Max rtt: 0.423ms | Min rtt: 0.299ms | Avg rtt: 0.364ms
Raw packets sent: 4 (112B) | Rcvd: 4 (184B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 3.08 seconds

(root@kali)~/home/kali
```

In the above example the local machine is sending 4 ICMP packets to the target machine with IPv4 10.0.2.4 which is a Windows 10 machine. The packets have been received successfully,

```
(root@kali)~/home/kali
# nping --tcp -p 80 10.0.2.4

Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2023-07-21 03:56 BST
SENT (0.0145s) TCP 10.0.2.5:47820 > 10.0.2.4:80 S ttl=64 id=23151 iplen=40 s
eq=6625547 win=1480
SENT (1.0378s) TCP 10.0.2.5:47820 > 10.0.2.4:80 S ttl=64 id=23151 iplen=40 s
eq=6625547 win=1480
SENT (2.0709s) TCP 10.0.2.5:47820 > 10.0.2.4:80 S ttl=64 id=23151 iplen=40 s
eq=6625547 win=1480
SENT (3.1102s) TCP 10.0.2.5:47820 > 10.0.2.4:80 S ttl=64 id=23151 iplen=40 s
eq=6625547 win=1480
SENT (4.1945s) TCP 10.0.2.5:47820 > 10.0.2.4:80 S ttl=64 id=23151 iplen=40 s
eq=6625547 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 5 (200B) | Rcvd: 0 (0B) | Lost: 5 (100.00%)
Nping done: 1 IP address pinged in 5.23 seconds

(root@kali)~/home/kali
```

By using `nping -tcp -p 80` the user is sending TCP packets to the host. All packets successfully sent.

```
(root@kali)-[/home/kali]
# nping --udp -p 80 10.0.2.4

Starting Nping 0.7.94 ( https://nmap.org/nping ) at 2023-07-21 04:00 BST
SENT (0.01925) UDP [10.0.2.5:53 > 10.0.2.4:80 ttl=64 id=60129 iplen=28
RCVD (0.01955) ICMP [10.0.2.4 > 10.0.2.5 Port unreachable (type=3/code=3) ] I
P [ttl=128 id=1 iplen=56 ]
SENT (1.02095) UDP [10.0.2.5:53 > 10.0.2.4:80 ttl=64 id=60129 iplen=28
RCVD (1.02135) ICMP [10.0.2.4 > 10.0.2.5 Port unreachable (type=3/code=3) ] I
P [ttl=128 id=2 iplen=56 ]
SENT (2.02385) UDP [10.0.2.5:53 > 10.0.2.4:80 ttl=64 id=60129 iplen=28
RCVD (2.02425) ICMP [10.0.2.4 > 10.0.2.5 Port unreachable (type=3/code=3) ] I
P [ttl=128 id=3 iplen=56 ]
SENT (3.03755) UDP [10.0.2.5:53 > 10.0.2.4:80 ttl=64 id=60129 iplen=28
RCVD (3.03795) ICMP [10.0.2.4 > 10.0.2.5 Port unreachable (type=3/code=3) ] I
P [ttl=128 id=4 iplen=56 ]
SENT (4.04015) UDP [10.0.2.5:53 > 10.0.2.4:80 ttl=64 id=60129 iplen=28
RCVD (4.04055) ICMP [10.0.2.4 > 10.0.2.5 Port unreachable (type=3/code=3) ] I
P [ttl=128 id=5 iplen=56 ]

Max rtt: 0.358ms | Min rtt: 0.288ms | Avg rtt: 0.314ms
Raw packets sent: 5 (140B) | Rcvd: 5 (280B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 4.08 seconds

(root@kali)-[/home/kali]
#
```

The user is sending UDP packets which have been sent successfully to the host by using the `hping -udp -p 80` command which means that the host is active.

[illegible]

With the `sudo tcpdump -i interface any` command we can analyse packets which have been captured over the network on any active interface. This programme lets you see what's going on in a network. `tcpdump` can look at IPv4, ICMPv4, IPv6, ICMPv6, UDP, TCP, SNMP, RIP, PIM, DVMRP, IGMP, SMB, OSPF, NFS, and a lot of other types of packets. To analyse specific packet type we can use `sudo tcpdump -i <interface> <`

² Part 2: Use an alternative to MegaPing to identify live hosts and open ports of the Target.

The Nmap tool can be used instead of ² MegaPing to identify live hosts and open ports of the target.

Identifying live hosts

```
(root@kali)-[/home/kali]
# sudo nmap -sn 10.0.2.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-21 04:40 BST
Nmap scan report for 10.0.2.1
Host is up (0.00011s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.000080s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.000074s latency).
MAC Address: 08:00:27:40:8C:A4 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00022s latency).
MAC Address: 08:00:27:63:85:42 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up (0.00017s latency).
MAC Address: 08:00:27:40:4D:0E (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.5
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.09 seconds

(root@kali)-[/home/kali]
```

Nmap is used to identify all live hosts on the network. It has scanned the whole IP range and found that there are 6 hosts which are active.

Identifying open ports

```
(root@kali)-[/home/kali]
# sudo nmap -sS -p 1-65535 10.0.2.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-21 04:44 BST
Nmap scan report for 10.0.2.1
Host is up (0.0014s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds
```

Nmap scans the target machine for open ports. The scan has been performed in the half-open mode (stealthy SYN scan) without completing the TCP 3-way handshake.

2

Part 3: Use an alternative to NetScanTools Pro to initiate various Scans

2

Nmap can be used as an alternative to NetScanTools Pro to initiate various scans.

Fingerprinting the OS and identifying services on the target machine

```
(root@kali)~[/home/kali]
# nmap -sV 10.0.2.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-21 04:56 BST
Nmap scan report for 10.0.2.4
Host is up (0.00031s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5357/tcp   open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:63:85:42 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.02 seconds
```

The above command lists the running services on the target host. As can be seen there is Windows running on the host.

```
(root@kali)~[/home/kali]
# nmap -O 10.0.2.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-21 05:00 BST
Nmap scan report for 10.0.2.4
Host is up (0.00031s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsddapi
MAC Address: 08:00:27:63:85:42 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2019 (95%), Microsoft Windows 10 1909 (94%), Microsoft Windows 11 21H2 (90%), Microsoft Windows 7 (90%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (90%), Microsoft Windows 10 1709 - 1909 (89%), Microsoft Windows Server 2008 SP1 (88%), Microsoft Windows XP SP3 (88%), Microsoft Windows XP SP2 (87%), Microsoft Windows 10 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.62 seconds
```

The above command scans for the target machine OS and makes guesses on the OS. As can be seen, the command lists the most probable OS that the machine might be using. The machine has Windows 10 on it and the results show that the probability for a Windows 10 OS is 94%.

```

root@kali:~/home/kali
# nmap -A 10.0.2.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-21 05:04 BST
Nmap scan report for 10.0.2.4
Host is up (0.00033s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5357/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 08:00:27:63:85:42 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2019 (95%), Microsoft Windows
10 1909 (94%), Microsoft Windows 11 21H2 (90%), Microsoft Windows 7 (90%), M
icrosoft Windows Server 2008 SP1 or Windows Server 2008 R2 (90%), Microsoft W
indows 10 1709 - 1909 (89%), Microsoft Windows Server 2008 SP1 (88%), Microso
ft Windows XP SP3 (88%), Microsoft Windows XP SP2 (87%), Microsoft Windows 10
(87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -32m26s
|_nbstat: NetBIOS name: DESKTOP-MFGTH6S, NetBIOS user: <unknown>, NetBIOS MAC
: 08:00:27:63:85:42 (Oracle VirtualBox virtual NIC)
|_smb2-security-mode:
|   3:1:1:
|   Message signing enabled but not required
|_smb2-time:
|   date: 2023-07-21T03:32:21
|_start_date: N/A

TRACEROUTE
HOP RTT      ADDRESS
1   0.33 ms  10.0.2.4

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.98 seconds

```

The above example ¹⁵ shows the aggressive detection mode of Nmap using -A. This mode includes four separate modes: OS detection (-O), version detection (-sV), script scanning (-sC), traceroute (--traceroute). The aggressive mode sends more probes and the probability for it to be detected is higher but it provides more detailed host information.

```

(root@kali)~/home/kali
# nmap -iR 5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-21 05:13 BST
Nmap scan report for 48.226.240.87
Host is up (0.00016s latency).
All 1000 scanned ports on 48.226.240.87 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 124.253.15.4
Host is up (0.00019s latency).
All 1000 scanned ports on 124.253.15.4 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 6.221.228.167
Host is up (0.00016s latency).
All 1000 scanned ports on 6.221.228.167 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 130.234.35.101
Host is up (0.00018s latency).
All 1000 scanned ports on 130.234.35.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 6.183.62.215
Host is up (0.00029s latency).
All 1000 scanned ports on 6.183.62.215 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 5 IP addresses (5 hosts up) scanned in 28.64 seconds

(root@kali)~/home/kali
# nmap -sn -iR 3
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-21 05:14 BST
Nmap scan report for h-158-174-11-195.priv.bahnhof.se (158.174.11.195)
Host is up (0.00087s latency).
Nmap scan report for 162-192-117-250.lightspeed.irvnca.sbcglobal.net (162.192.117.250)
Host is up (0.00087s latency).
Nmap scan report for 130.209.187.186
Host is up (0.00085s latency).
Nmap done: 3 IP addresses (3 hosts up) scanned in 0.37 seconds

```

The above example shows how to use nmap for scanning random targets on the internet.

Part 4: Explore various network scanning Techniques⁷

Discover hosts with TCP SYN ping scan

```

(root@kali)~/home/kali
# nmap -sn -PS 10.0.2.1/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-21 05:21 BST
Nmap scan report for 10.0.2.1
Host is up (0.00016s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00013s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00012s latency).
MAC Address: 08:00:27:40:8C:A4 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00020s latency).
MAC Address: 08:00:27:63:85:42 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up (0.00016s latency).
MAC Address: 08:00:27:40:4D:0E (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.5
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.04 seconds

```

⁴

⁷ Calderon, P., "NMAP: network Exploration and Security Auditing Cookbook", 2nd ed., Birmingham, Packt Publishing, 2017, pp. 55-76

10

The `-sn` option instructs Nmap to bypass port scanning and conduct only host discovery. The `-PS` option instructs Nmap to conduct a TCP SYN ping scan. This variety of ping scan operates as follows:

1. Nmap transmits a TCP SYN to port 80.
2. If the port is closed, the host sends a RST transmission in response.
3. If the port is accessible, the host sends a TCP SYN/ACK transmission to indicate that a connection can be established.
4. A RST transmission is then transmitted to reset this connection.

Discover hosts with TCP SYN ping scan

```
(root@kali)-[/home/kali]
# nmap -sn -PA 10.0.2.1/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-21 05:31 BST
Nmap scan report for 10.0.2.1
Host is up (0.00013s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.000091s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.000085s latency).
MAC Address: 08:00:27:40:8C:A4 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00022s latency).
MAC Address: 08:00:27:63:85:42 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up (0.00017s latency).
MAC Address: 08:00:27:40:4D:0E (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.5
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.09 seconds
```

Similar to the TCP SYN ping scan, the TCP ACK ping scan determines whether or not a host is responding. It can be used to detect hosts that block SYN packets or ICMP echo requests, but modern firewalls that monitor connection states will likely block it because it transmits bogus TCP ACK packets associated with non-existent connections.

Discovering hosts with the IP protocol ping scan

```
(root@kali)~/home/kali
# nmap -sn -PO --packet-trace 10.0.2.1/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-21 05:37 BST
SENT (0.0176s) ARP who-has 10.0.2.1 tell 10.0.2.5
SENT (0.0178s) ARP who-has 10.0.2.2 tell 10.0.2.5
SENT (0.0179s) ARP who-has 10.0.2.3 tell 10.0.2.5
SENT (0.0180s) ARP who-has 10.0.2.4 tell 10.0.2.5
SENT (0.0180s) ARP who-has 10.0.2.6 tell 10.0.2.5
SENT (0.0182s) ARP who-has 10.0.2.7 tell 10.0.2.5
SENT (0.0182s) ARP who-has 10.0.2.8 tell 10.0.2.5
SENT (0.0183s) ARP who-has 10.0.2.9 tell 10.0.2.5
SENT (0.0184s) ARP who-has 10.0.2.10 tell 10.0.2.5
SENT (0.0184s) ARP who-has 10.0.2.11 tell 10.0.2.5
RCVD (0.0177s) ARP reply 10.0.2.1 is-at 52:54:00:12:35:00
RCVD (0.0178s) ARP reply 10.0.2.2 is-at 52:54:00:12:35:00
RCVD (0.0180s) ARP reply 10.0.2.3 is-at 08:00:27:40:8C:A4
RCVD (0.0181s) ARP reply 10.0.2.4 is-at 08:00:27:63:85:42
SENT (0.0212s) ARP who-has 10.0.2.14 tell 10.0.2.5
SENT (0.0213s) ARP who-has 10.0.2.15 tell 10.0.2.5
SENT (0.0214s) ARP who-has 10.0.2.16 tell 10.0.2.5
SENT (0.0215s) ARP who-has 10.0.2.17 tell 10.0.2.5
SENT (0.0215s) ARP who-has 10.0.2.18 tell 10.0.2.5
SENT (0.0216s) ARP who-has 10.0.2.19 tell 10.0.2.5
SENT (0.0217s) ARP who-has 10.0.2.20 tell 10.0.2.5
SENT (0.0218s) ARP who-has 10.0.2.21 tell 10.0.2.5
RCVD (0.0214s) ARP reply 10.0.2.15 is-at 08:00:27:40:4D:0E
SENT (0.0243s) ARP who-has 10.0.2.24 tell 10.0.2.5
SENT (0.0244s) ARP who-has 10.0.2.25 tell 10.0.2.5
SENT (0.1181s) ARP who-has 10.0.2.28 tell 10.0.2.5
SENT (0.1238s) ARP who-has 10.0.2.31 tell 10.0.2.5
SENT (0.1240s) ARP who-has 10.0.2.32 tell 10.0.2.5
SENT (0.1241s) ARP who-has 10.0.2.33 tell 10.0.2.5
SENT (0.1243s) ARP who-has 10.0.2.34 tell 10.0.2.5
SENT (0.1244s) ARP who-has 10.0.2.35 tell 10.0.2.5
SENT (0.1245s) ARP who-has 10.0.2.36 tell 10.0.2.5
SENT (0.1246s) ARP who-has 10.0.2.37 tell 10.0.2.5
SENT (0.1248s) ARP who-has 10.0.2.38 tell 10.0.2.5
SENT (0.1248s) ARP who-has 10.0.2.39 tell 10.0.2.5
SENT (0.1249s) ARP who-has 10.0.2.40 tell 10.0.2.5
SENT (0.1250s) ARP who-has 10.0.2.41 tell 10.0.2.5
SENT (0.1251s) ARP who-has 10.0.2.42 tell 10.0.2.5
SENT (0.1289s) ARP who-has 10.0.2.45 tell 10.0.2.5
SENT (0.1290s) ARP who-has 10.0.2.46 tell 10.0.2.5
SENT (0.1290s) ARP who-has 10.0.2.47 tell 10.0.2.5
```

By default, the above ping scan will use the protocols IGMP, IP-in-IP, and ICMP to try to determine if the host is online. Including `--packet-trace` will show more details of what happened behind the curtains:

2

Part 5: Being Anonymous on the Internet using an alternative to Proxy Switcher

```
(root@kali)-[/home/kali]
# sudo apt install tor
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  tor-geoipdb torsocks
Suggested packages:
  mixmaster torbrowser-launcher apparmor-utils nix obfs4proxy
The following NEW packages will be installed:
  tor tor-geoipdb torsocks
0 upgraded, 3 newly installed, 0 to remove and 984 not upgraded.
Need to get 3,570 kB of archives.
After this operation, 17.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://mirror.vinehost.net/kali kali-rolling/main amd64 tor amd64 0.4.7.13-1
[1,995 kB]
Get:2 http://mirror.vinehost.net/kali kali-rolling/main amd64 tor-geoipdb all 0.4.
7.13-1 [1,501 kB]
Get:3 http://mirror.vinehost.net/kali kali-rolling/main amd64 torsocks amd64 2.4.0
-1 [74.3 kB]
Fetched 3,570 kB in 1s (2,712 kB/s)
Selecting previously unselected package tor.
(Reading database ... 392998 files and directories currently installed.)
Preparing to unpack .../tor_0.4.7.13-1_amd64.deb ...
Unpacking tor (0.4.7.13-1) ...
Selecting previously unselected package tor-geoipdb.
Preparing to unpack .../tor-geoipdb_0.4.7.13-1_all.deb ...
Unpacking tor-geoipdb (0.4.7.13-1) ...
Selecting previously unselected package torsocks.
Preparing to unpack .../torsocks_2.4.0-1_amd64.deb ...
Unpacking torsocks (2.4.0-1) ...
Setting up tor (0.4.7.13-1) ...
Something or somebody made /var/lib/tor disappear.
Creating one for you again.
Something or somebody made /var/log/tor disappear.
Creating one for you again.
update-rc.d: We have no instructions for the tor init script.
update-rc.d: It looks like a network service, we disable it.
Setting up torsocks (2.4.0-1) ...
Setting up tor-geoipdb (0.4.7.13-1) ...
Processing triggers for man-db (2.11.2-1) ...
Processing triggers for kali-menu (2023.1.7) ...

(root@kali)-[/home/kali]
# sudo service tor start

(root@kali)-[/home/kali]
#
```

11

To be anonymous on the internet the user can use TOR browser. Tor is a free and open-source application that enables users to navigate the internet anonymously by routing their traffic through a network of volunteer-operated servers (nodes). The traffic is encrypted and travels through multiple relays, making it difficult to determine its origin. For better security, the user can install a VPN client and run TOR after running the VPN client making the connection more secure and anonymous.

Part 6: Identify Target Operating System with TTL

```
(root@kali)-[/home/kali]
# ping -c 1 -t 128 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=128 time=0.357 ms

— 10.0.2.4 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.357/0.357/0.357/0.000 ms

(root@kali)-[/home/kali]
#
```

Time-to-Live (TTL) is a field in the IP header of packets that specifies the maximum number of steps (routers) before a packet is discarded. Each time a router forwards a transmission, the TTL value is decreased by one. If

the TTL reaches zero, the transmission is discarded and the source may receive an ICMP Time Exceeded message.

ping -c 1 -t TTL_VALUE TARGET_IP_ADDRESS command can be used with a specific TTL value to observe responses and attempt to identify the host OS.

Part 7: Map your Network using an automatic tool

```
(root@kali)-[/home/kali]
# nmap -sn 10.0.2.1/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-21 06:08 BST
Nmap scan report for 10.0.2.1
Host is up (0.00019s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00014s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00013s latency).
MAC Address: 08:00:27:40:8C:A4 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00023s latency).
MAC Address: 08:00:27:63:85:42 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up (0.00022s latency).
MAC Address: 08:00:27:40:4D:0E (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.5
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.27 seconds
```

Scanning and mapping the active hosts on the network using `nmap -sn <target host>`

Part 8: Enumerate using NetBIOS

```
(root@kali)-[/home/kali]
# nbtscan 10.0.2.4
Doing NBT name scan for addresses from 10.0.2.4
```

IP address	NetBIOS Name	Server	User	MAC address
10.0.2.4	DESKTOP-MFGTH6S	<server>	<unknown>	08:00:27:63:85:42

```
(root@kali)-[/home/kali]
#
```

Using `nbtscan` to enumerate a Windows system by using the target IP address/range.

2

Part 9: Enumerate using Nmap and Net Use

Enumerating using Nmap

```
(root@kali)-[/home/kali]
# nmap -sU -p137 --script smb-enum-users --script-args lsaonly=true 10.0.2.4
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-21 06:19 BST
Nmap scan report for 10.0.2.4
Host is up (0.00027s latency).

PORT      STATE SERVICE
137/udp   open  netbios-ns
MAC Address: 08:00:27:63:85:42 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

2

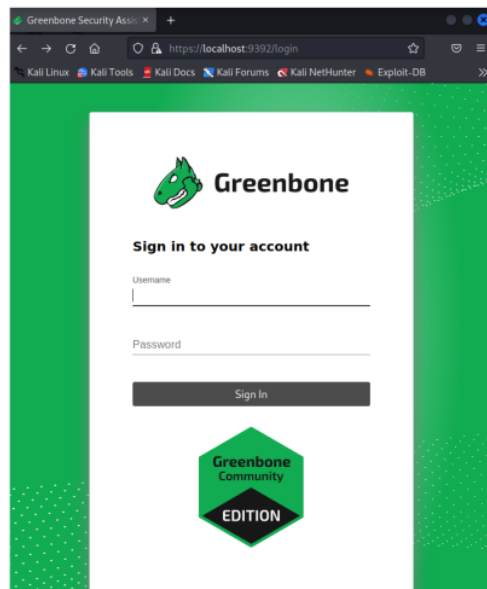
Lab Activity - Vulnerability Assessment

Task 1: Use an alternative to Nessus tool in Windows to scan for network vulnerabilities

OpenVas tool can be used as an alternative to Nessus tool in Windows.

2

Task 2: Use an alternative to Nessus tool in Kali Linux to scan for network vulnerabilities



The OpenVAS tool can be used as an alternative to Nessus

2

Task 3: Use an alternative to Nikto in Kali Linux to scan Web vulnerabilities

```
(root@kali)-[/home/kali]
# sudo apt update
Hit:1 http://mirror.vinehost.net/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
975 packages can be upgraded. Run 'apt list --upgradable' to see them.

(root@kali)-[/home/kali]
# sudo apt install wpscan
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be upgraded:
  wpscan
1 upgraded, 0 newly installed, 0 to remove and 974 not upgraded.
Need to get 58.0 kB of archives.
After this operation, 0 B of additional disk space will be used.
E: You don't have enough free space in /var/cache/apt/archives/.
```

WPscan is an alternative to Nikto for web server scanning in Kali Linux. wpscan is specifically designed to detect vulnerabilities, configuration issues, and potential security concerns on WordPress websites. It is a potent and widely-used tool for assessing WordPress security.

```
(root@kali)-[/home/kali]
# nmap --script http-open-proxy -p8080 10.0.2.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-21 08:30 BST
Nmap scan report for 10.0.2.1
Host is up (0.00010s latency).

PORT      STATE SERVICE
8080/tcp  closed http-proxy
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```

Checking whether a server is an open proxy.⁸

```
(root@kali)-[/home/kali]
# nmap -p80,443 --script http-methods,http-trace --script-args http-methods
.test-all=true 127.0.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-21 08:34 BST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000039s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-methods:
|_ Supported Methods: GET POST
443/tcp   closed https

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Listing supported HTTP methods⁹

4

⁸ Calderon, P., "NMAP: network Exploration and Security Auditing Cookbook", 2nd ed., Birmingham, Packt Publishing, 2017, pp. 116-120

Depending on their configuration and software, Web servers support a variety of HTTP methods, some of which may be hazardous under certain conditions. System administrators and penetration testers require a means to list available methods quickly. There are few scripts within Nmap NSE that allow us to not only enumerate these potentially dangerous methods, but also determine whether they are accessible.

2

Lab Activity – Hacking

Task 1: Use an alternative Metagoofil to extract metadata from the target

```
(root@kali)-[/home/kali]
# exiftool /home/kali/Desktop/sample.pdf
ExifTool Version Number      : 12.57
File Name                    : sample.pdf
Directory                    : /home/kali/Desktop
File Size                    : 143 kB
File Modification Date/Time   : 2023:07:21 08:45:14+01:00
File Access Date/Time        : 2023:07:21 08:47:08+01:00
File Inode Change Date/Time   : 2023:07:21 08:45:36+01:00
File Permissions              : -rw-r--r--
File Type                    : PDF
File Type Extension          : pdf
MIME Type                    : application/pdf
PDF Version                  : 1.4
Linearized                   : No
Page Count                   : 4
Language                     : en-US
Creator                      : Writer
Producer                     : LibreOffice 4.2
Create Date                   : 2017:08:16 14:44:13+02:00

(root@kali)-[/home/kali]
```

ExifTool can be used as an alternative to Metagoofil, The example above shows how the tool extracts data from a sample pdf file located on the Desktop.

4

⁹ Calderon, P., "NMAP: network Exploration and Security Auditing Cookbook", 2nd ed., Birmingham, Packt Publishing, 2017, pp. 116-120

2

Task 2: Use an alternative Responder to do LLMNR/NBT-NS Spoofing Attack

```
(root@kali)-[/home/kali]
# ifconfig eth0 down

(root@kali)-[/home/kali]
# ifconfig eth0 hw ether 00:11:22:33:44:55

(root@kali)-[/home/kali]
# ifconfig eth0 up

(root@kali)-[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.7 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::211:22ff:fe33:4455 prefixlen 64 scopeid 0<link>
    ether 00:11:22:33:44:55 txqueuelen 1000 (Ethernet)
    RX packets 8941 bytes 10078204 (9.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5438 bytes 730480 (713.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1790 bytes 9095813 (8.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1790 bytes 9095813 (8.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)-[/home/kali]
```

Spoofing MAC address with ifconfig

2

Task 3: Create Rainbow Tables and Use them to crack hashes

Deliverable 3: Propose a mitigation strategy

The application of a control, system, mechanism, or strategy ¹ to reduce the probability or impact of the risk to an acceptable level constitutes mitigation. Implementation of Biometric Access Control, implementation of an Intrusion Prevention System, and security testing prior to system release are examples of mitigation.¹⁰

An ethical hacker's goal is to assist the NGO in identifying and mitigating cybersecurity threats and enhancing their overall security posture. The following comprehensive proposal addresses their technical security weaknesses and strengthens their cyberspace based on the above-mentioned scenario:

- ¹⁸ **Cybersecurity Risk Assessment:** Conduct a comprehensive cybersecurity risk assessment in order to identify potential vulnerabilities, hazards, and risks that the NGO faces. This evaluation should encompass both physical and informational assets, such as building security, laptops, access controls, fund sources, banking information, and beneficiary data.
- *Conduct mandatory and periodic security awareness training* for all employees, including the property manager and other businesses that share the building. Ensure the training addresses the most recent cybersecurity threats, best practises, and the significance of protecting sensitive data.
- *Implement robust email security measures* to defend against fraudulent attacks. Conduct simulated phishing exercises to evaluate employee reactivity to phishing emails and reinforce training.
- ²⁰ **Multi-Factor Authentication (MFA):** Implement multi-factor authentication (MFA) for accessing sensitive information and critical systems. MFA provides an additional layer of security and aids in preventing unauthorised access.
- *Ensure that laptops and other IT assets are properly configured* with the most recent security updates, upgrades, and secure settings. Implement centralised configuration management to keep the security of all devices uniform.
- *Network Segmentation:* Segment the network in order to segregate critical assets from less sensitive systems. This will restrict the assailants' lateral movement in the event of a breach.
- ¹⁹ **Conduct Periodic Vulnerability Scans and Penetration Tests:** Conduct periodic vulnerability scans and penetration tests to proactively identify and remediate vulnerabilities. This aids in identifying and addressing vulnerabilities prior to their exploitation by malicious actors.

¹ ¹⁰ Bravo, C., "Mastering Defensive Security: Effective Techniques to secure your Windows, Linux, IoT, and cloud infrastructure", 1st ed., Birmingham, Packt Publishing, 2021, p.64

- *Encryption of Data:* Implement robust data encryption for sensitive data in transit and at rest. Encryption safeguards information even when it is intercepted or taken.
- *Plan for Responding to Incidents:* Develop and routinely update a plan to guide the organization's response to a cybersecurity incident. The plan should include roles, responsibilities, and procedures for effectively containing and mitigating potential security vulnerabilities.
- *Management of Third-Party Risk:* Evaluate and monitor the security posture of third-party vendors and businesses that share the building. Ensure they adhere to cybersecurity best practises and have implemented the appropriate security controls.
- *Conduct routine security audits and assessments* to evaluate the efficacy of implemented security measures and identify areas for improvement.
- *Continuous Monitoring:* Implement continuous monitoring and recording of network activities in order to detect and respond immediately to security incidents.

Assumptions:

- The building's property manager and occupants will work together to implement and maintain cybersecurity measures.
- The non-profit organisation has dedicated IT personnel or access to external cybersecurity specialists.

By implementing these measures, the NGO will be able to substantially improve its cybersecurity position, reduce cyber threats, and protect its physical and digital assets, allowing it to continue its mission of assisting vulnerable populations worldwide with confidence and security.

Conclusion

The report has highlighted the significance of adopting a comprehensive cybersecurity strategy that includes network security, endpoint protection, user awareness training, incident response plans, and risk assessments. A comprehensive defence-in-depth strategy is essential for protecting against complex cyber threats.

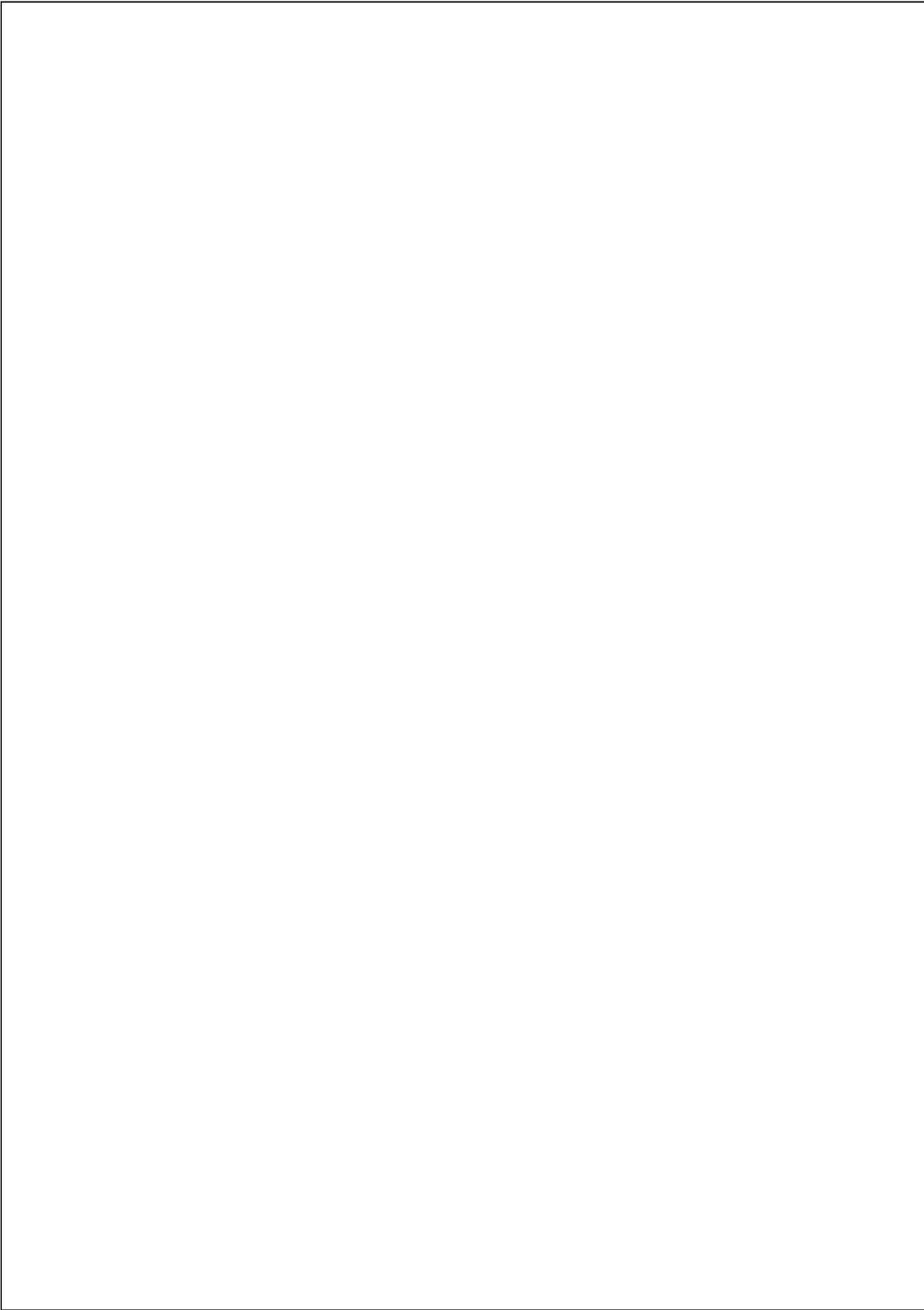
It is essential to recognise that despite the fact that VPNs are valuable instruments for securing communications, they do not exist in a vacuum. To prevent unauthorised access, organisations must carefully manage VPN access, perform regular updates, and employ strong authentication mechanisms. In addition, VPNs may introduce single points of failure, making redundancy and failover mechanisms essential for continuous operations.

In conclusion, for an organisation to effectively mitigate network and cybersecurity risks, the deployment and administration of VPNs are essential components. To establish a resilient and secure environment, a holistic approach to cybersecurity, supported by ongoing

education and awareness, proactive risk assessments, and regular audits, is essential. By incorporating VPN technology into a comprehensive cybersecurity strategy, organisations can bolster their defences, mitigate risks, and secure their most valuable assets, thereby fostering a safer and more resilient digital ecosystem.

Reference:

- [1] Cawthra. J., "Data Integrity : Detection and Responding to Ransomware and Other Destructive Events", NIST⁸ SPECIAL PUBLICATION 1800-26A, NIST.gov, December 2020 [Online] <https://www.nccoe.nist.gov/publication/1800-26/VoIA/index.html> [Accessed: 15/07/2023]
- [2] Bravo, C., "Mastering Defensive Security: Effective Techniques to secure your Windows, Linux, IoT, and cloud infrastructure", 1st ed., Birmingham, Packt Publishing, 2021, p.5
- [3] Bravo, C., "Mastering Defensive Security: Effective Techniques to secure your Windows, Linux, IoT, and cloud infrastructure", 1st ed., Birmingham, Packt Publishing, 2021, pp.6-16
- [4] Bravo, C., "Mastering Defensive Security: Effective Techniques to secure your Windows, Linux, IoT, and cloud infrastructure", 1st ed., Birmingham, Packt Publishing, 2021, p.7
- [5] Bravo, C., "Mastering Defensive Security: Effective Techniques to secure your Windows, Linux, IoT, and cloud infrastructure", 1st ed., Birmingham, Packt Publishing, 2021, p.13
- [6] Bravo, C., "Mastering Defensive Security: Effective Techniques to secure your Windows, Linux, IoT, and cloud infrastructure", 1st ed., Birmingham, Packt Publishing, 2021, pp.16-24
- [7] Calderon, P., "NMAP: network Exploration and Security Auditing Cookbook", 2nd ed., Birmingham, Packt Publishing, 2017, pp. 55-76
- [8] Calderon, P., "NMAP: network Exploration and Security Auditing Cookbook", 2nd ed., Birmingham, Packt Publishing, 2017, pp. 116-120
- [9] Calderon, P., "NMAP: network Exploration and Security Auditing Cookbook", 2nd ed., Birmingham, Packt Publishing, 2017, pp. 116-120
- [10] Bravo, C., "Mastering Defensive Security: Effective Techniques to secure your Windows, Linux, IoT, and cloud infrastructure", 1st ed., Birmingham, Packt Publishing, 2021, p.64



Level 6 - Advanced Cyber Security

ORIGINALITY REPORT

23%

SIMILARITY INDEX

15%

INTERNET SOURCES

2%

PUBLICATIONS

18%

STUDENT PAPERS

PRIMARY SOURCES

1

Submitted to Manukau Institute of Technology

Student Paper

5%

2

Submitted to University of Wales, Lampeter

Student Paper

5%

3

www.packtpub.com

Internet Source

3%

4

Submitted to Edith Cowan University

Student Paper

2%

5

ebin.pub

Internet Source

2%

6

www.safaribooksonline.com

Internet Source

1%

7

Submitted to University of Bradford

Student Paper

1%

8

Submitted to American InterContinental University

Student Paper

1%

9

Submitted to UI, Springfield

1 %

10

hub.packtpub.com

Internet Source

1 %

11

Submitted to University of New Mexico
System

Student Paper

<1 %

12

www.utupub.fi

Internet Source

<1 %

13

Submitted to American Public University
System

Student Paper

<1 %

14

Submitted to UOW Malaysia KDU University
College Sdn. Bhd

Student Paper

<1 %

15

www.oreilly.com

Internet Source

<1 %

16

Submitted to RGIT Australia

Student Paper

<1 %

17

Submitted to New Mexico State University

Student Paper

<1 %

18

Submitted to NCC Education

Student Paper

<1 %

19

Submitted to RMIT University

Student Paper

<1 %

20

www.anomali.com

Internet Source

<1 %

21

www.slideshare.net

Internet Source

<1 %

22

helion.pl

Internet Source

<1 %

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off