

Table of Contents

CIS2710	1
Security Fundamentals.....	1
Introduction:.....	3
Activity I: Network Reconnaissance:	3
Setup and Environment:.....	3
Footprinting and Scanning:.....	3
Analysis of Findings:	6
Activity II: Network Reconnaissance Defence:.....	7
After Implementing the Firewall:	9
The Significance of Mitigating Insider Threats in a Financial Institution.....	10
Introduction.....	10
Identification of Vulnerabilities.....	10
Privileged Access Mismanagement:	10
Lack of Monitoring:.....	10
Poor Security Controls and Policy:.....	10
Inadequate Security Training:.....	10
Analysing Attack Methods.	10
Credential Misuse	10
Data Exfiltration.....	11
Bypassing Security Controls.....	11
Social Engineering	11
Defensive Measurements:	11
Technical Measures	11
Procedural Measures	12
Legal, Social, and Ethical Considerations:	12
References.....	14

Chapter 2: Network Security

Introduction:

This chapter will demonstrate the simulation of an attack and how to defend against the given attacks. This assignment aims to collect as much data as possible about the Ubuntu machine from the Kali Linux machine with minimal information, such as the IP address. Once the methods of attack have been outlined, there will be methods of defence.

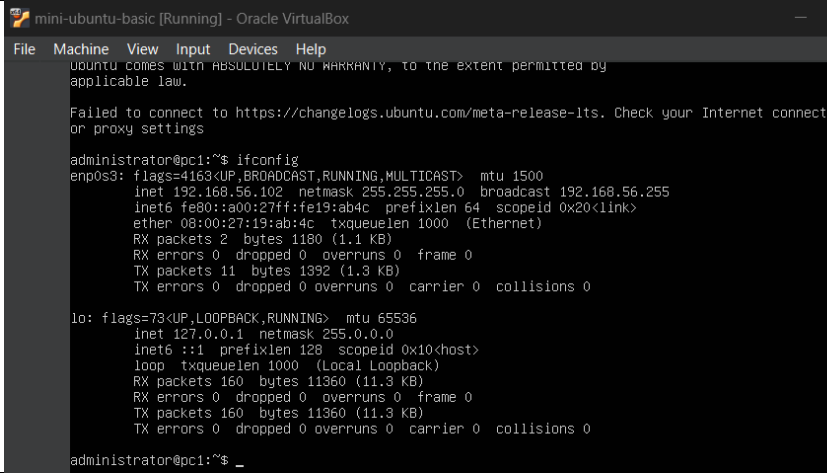
Activity I: Network Reconnaissance:

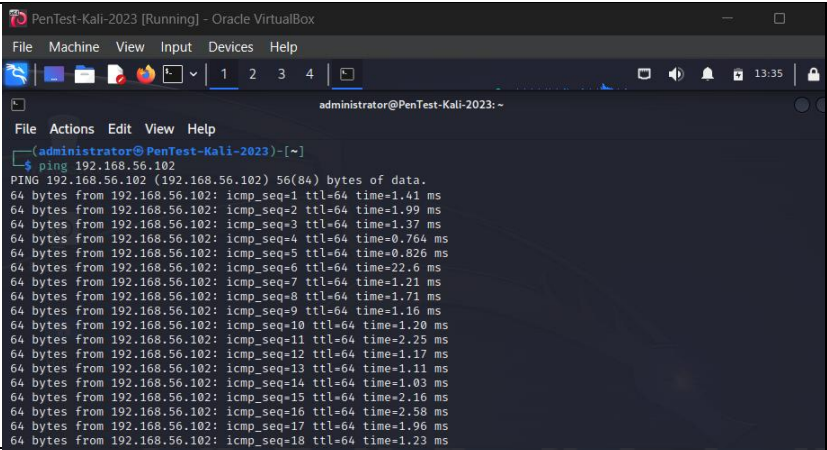
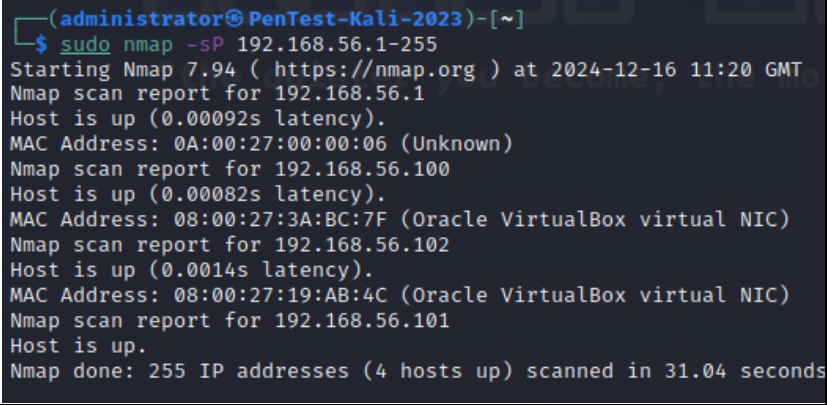
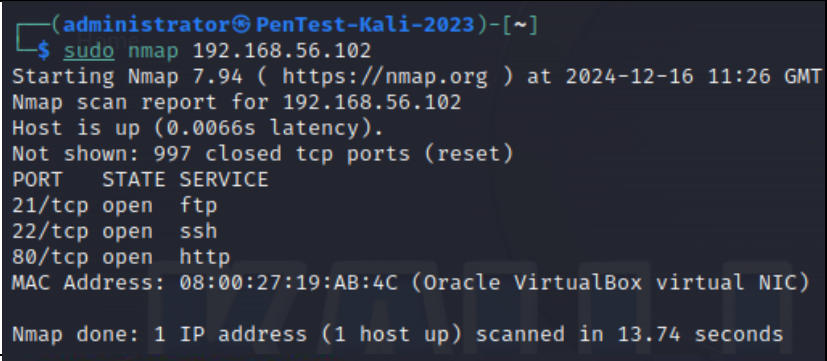
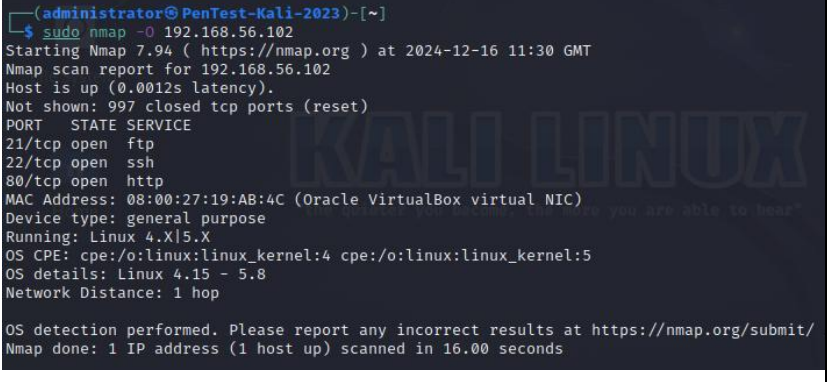
Setup and Environment:

I set both machines on Oracle VirtualBox, which is a virtualisation program which can run multiple operating systems within a host computer (GeeksforGeeks, 2024). Using a virtual machine allows a user to perform an isolated network simulation attack with both machines using a Host-only environment, which is essential as using a controlled environment like this is helpful to isolate the network to avoid potential disruptions outside of the host machine (VMware, 2019).

Footprinting and Scanning:

Footprinting is the first step in the process of gathering information to learn about all aspects of the security weaknesses to gather the potential vulnerabilities (McGreevy, 2021). Footprinting includes the process of scanning open ports, mapping network topologies and collecting information about hosts like operating systems, IP addresses and User accounts (Rathnayake, 2023).

Time of Command/Task	Tool Used	Description of Task and Tools.	Outcome of the task.
2024-12-16 11:06 GMT	N/A	‘ifconfig’ Used to identify the IP address of the target machine.	

2024-12-16 11:10 GMT	N/A	<p>‘ping 192.168.56.102’</p> <p>I pinged the target machine to verify it's reachable.</p>	 <pre> PenTest-Kali-2023 [Running] - Oracle VirtualBox File Machine View Input Devices Help administrator@PenTest-Kali-2023: ~ (administrator@PenTest-Kali-2023)-[~] \$ ping 192.168.56.102 PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data: 64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=1.41 ms 64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=1.99 ms 64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=1.37 ms 64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.764 ms 64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0.826 ms 64 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=22.6 ms 64 bytes from 192.168.56.102: icmp_seq=7 ttl=64 time=1.21 ms 64 bytes from 192.168.56.102: icmp_seq=8 ttl=64 time=1.71 ms 64 bytes from 192.168.56.102: icmp_seq=9 ttl=64 time=1.16 ms 64 bytes from 192.168.56.102: icmp_seq=10 ttl=64 time=1.20 ms 64 bytes from 192.168.56.102: icmp_seq=11 ttl=64 time=2.25 ms 64 bytes from 192.168.56.102: icmp_seq=12 ttl=64 time=1.17 ms 64 bytes from 192.168.56.102: icmp_seq=13 ttl=64 time=1.11 ms 64 bytes from 192.168.56.102: icmp_seq=14 ttl=64 time=1.03 ms 64 bytes from 192.168.56.102: icmp_seq=15 ttl=64 time=2.16 ms 64 bytes from 192.168.56.102: icmp_seq=16 ttl=64 time=2.58 ms 64 bytes from 192.168.56.102: icmp_seq=17 ttl=64 time=1.96 ms 64 bytes from 192.168.56.102: icmp_seq=18 ttl=64 time=1.23 ms </pre>
2024-12-16 11:20 GMT	Nmap	<p>‘sudo nmap -sP 192.168.56.1-255’</p> <p>Used to identify the active hosts' IP and Mac addresses in the network.</p>	 <pre> (administrator@PenTest-Kali-2023)-[~] \$ sudo nmap -sP 192.168.56.1-255 Starting Nmap 7.94 (https://nmap.org) at 2024-12-16 11:20 GMT Nmap scan report for 192.168.56.1 Host is up (0.00092s latency). MAC Address: 0A:00:27:00:00:06 (Unknown) Nmap scan report for 192.168.56.100 Host is up (0.00082s latency). MAC Address: 08:00:27:3A:BC:7F (Oracle VirtualBox virtual NIC) Nmap scan report for 192.168.56.102 Host is up (0.0014s latency). MAC Address: 08:00:27:19:AB:4C (Oracle VirtualBox virtual NIC) Nmap scan report for 192.168.56.101 Host is up. Nmap done: 255 IP addresses (4 hosts up) scanned in 31.04 seconds </pre>
2024-12-16 11:26 GMT	Nmap	<p>‘sudo nmap 192.168.56.102’</p> <p>Finds all the open ports on the target IP address machine.</p>	 <pre> (administrator@PenTest-Kali-2023)-[~] \$ sudo nmap 192.168.56.102 Starting Nmap 7.94 (https://nmap.org) at 2024-12-16 11:26 GMT Nmap scan report for 192.168.56.102 Host is up (0.0066s latency). Not shown: 997 closed tcp ports (reset) PORT STATE SERVICE 21/tcp open ftp 22/tcp open ssh 80/tcp open http MAC Address: 08:00:27:19:AB:4C (Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 13.74 seconds </pre>
2024-12-16 11:30 GMT	Nmap	<p>Sudo nmap – O 192.168.102’</p> <p>With this command, I am able to find the operating system and version, the device name, and how the target machine is on the network with the number of hops.</p>	 <pre> (administrator@PenTest-Kali-2023)-[~] \$ sudo nmap -O 192.168.56.102 Starting Nmap 7.94 (https://nmap.org) at 2024-12-16 11:30 GMT Nmap scan report for 192.168.56.102 Host is up (0.0012s latency). Not shown: 997 closed tcp ports (reset) PORT STATE SERVICE 21/tcp open ftp 22/tcp open ssh 80/tcp open http MAC Address: 08:00:27:19:AB:4C (Oracle VirtualBox virtual NIC) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.8 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 16.00 seconds </pre>

2024-12-16 14:56 GMT	Nmap	<p>'Sudo nmap -p21 192.168.56.102'</p> <p>Using this command, I am able to target specific ports to check if they are open specifically.</p>	<pre>(administrator@PenTest-Kali-2023)-[~] \$ sudo nmap -p21 192.168.56.102 [sudo] password for administrator: Starting Nmap 7.94 (https://nmap.org) at 2024-12-16 14:56 GMT Nmap scan report for 192.168.56.102 Host is up (0.00076s latency). PORT STATE SERVICE 21/tcp open ftp MAC Address: 08:00:27:19:AB:4C (Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds</pre>
2024-12-16 15:03 GMT	Nmap	<p>'sudo nmap -p1-100 192.168.56.102'</p> <p>With this command, you can check for ports within a specific range. I targeted a range from 1 to 100.</p>	<pre>(administrator@PenTest-Kali-2023)-[~] \$ sudo nmap -p1-100 192.168.56.102 Starting Nmap 7.94 (https://nmap.org) at 2024-12-16 15:03 GMT Nmap scan report for 192.168.56.102 Host is up (0.00063s latency). Not shown: 97 closed tcp ports (reset) PORT STATE SERVICE 21/tcp open ftp 22/tcp open ssh 80/tcp open http MAC Address: 08:00:27:19:AB:4C (Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 13.55 seconds</pre>
2024-12-16 15:09 GMT	Nmap	<p>'sudo nmap -d --packet-trace -p21'</p> <p>This command gives step-by-step information on the scan process and a detailed log of the packets that are sent and received.</p>	<pre>(administrator@PenTest-Kali-2023)-[~] \$ sudo nmap -d --packet-trace -p21 192.168.56.102 Starting Nmap 7.94 (https://nmap.org) at 2024-12-16 15:09 GMT Timing report hostgroups: min 1, max 100000 rtt-timeouts: init 1000, min 100, max 10000 max-scan-delay: TCP 1000, UDP 1000, SCTP 1000 parallelism: min 0, max 0 max-retries: 10, host-timeout: 0 min-rate: 0, max-rate: 0 Initiating ARP Ping Scan at 15:09 Scanning 192.168.56.102 [1 port] Packet capture filter (device eth0): arp and arp[18:4] = 0x08002774 and arp[22:2] = 0x7975 SENT (0.0383s) ARP who-has 192.168.56.102 tell 192.168.56.101 RCVD (0.0389s) ARP reply 192.168.56.102 is-at 08:00:27:19:AB:4C Completed ARP Ping Scan at 15:09, 0.04s elapsed (1 total hosts) Overall sending rates: 24.30 packets / s, 1024.22 bytes / s. mass_rdns: Using DNS server 10.0.2.3 NSOCK INFO [0.1340s] nssock_ioc_new2(): nssock_ioc_new (IOD #1) NSOCK INFO [0.1340s] nssock_connect_udp(): UDP connection requested to 10.0.2.3:53 (IOD #1) EID 8 NSOCK INFO [0.1340s] nssock_trace_handler_callback(): Callback: CONNECT ERROR [Network is unreachable (101)] for I 8 [10.0.2.3:53] NSOCK INFO [0.1340s] nssock_read(): Read request from IOD #1 [10.0.2.3:53] (timeout: -1ms) EID 18 Initiating Parallel DNS resolution of 1 host. at 15:09 NSOCK INFO [0.1340s] nssock_write(): Write request for 45 bytes to IOD #1 EID 27 [10.0.2.3:53] NSOCK INFO [0.1340s] nssock_trace_handler_callback(): Callback: WRITE ERROR [Destination address required (89)] fo EID 27 [10.0.2.3:53] NSOCK INFO [4.1340s] nssock_write(): Write request for 45 bytes to IOD #1 EID 35 [10.0.2.3:53] NSOCK INFO [4.1340s] nssock_trace_handler_callback(): Callback: WRITE ERROR [Destination address required (89)] fo EID 35 [10.0.2.3:53] NSOCK INFO [8.1350s] nssock_write(): Write request for 45 bytes to IOD #1 EID 43 [10.0.2.3:53] NSOCK INFO [8.1350s] nssock_trace_handler_callback(): Callback: WRITE ERROR [Destination address required (89)] fo EID 43 [10.0.2.3:53] mass_rdns: 13.00s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 3] Completed Parallel DNS resolution of 1 host. at 15:10, 13.00s elapsed NSOCK INFO [13.1370s] nssock_ioc_delete(): nssock_ioc_delete (IOD #1) NSOCK INFO [13.1370s] nssock_delete(): nssock_delete on event #18 (type READ) DNS resolution of 1 IPs took 13.00s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0] Initiating SYN Stealth Scan at 15:10 Scanning 192.168.56.102 [1 port] Packet capture filter (device eth0): dst host 192.168.56.101 and (icmp or icmp6 or ((tcp) and (src host 192.168.5 102))) SENT (13.1572s) TCP 192.168.56.101:35696 > 192.168.56.102:21 S ttl=40 id=39687 iplen=44 seq=169960596 win=1024 < s 1460> RCVD (13.1577s) TCP 192.168.56.102:21 > 192.168.56.101:35696 SA ttl=64 id=0 iplen=44 seq=361266564 win=64240 <ms 1460> Discovered open port 21/tcp on 192.168.56.102 Completed SYN Stealth Scan at 15:10, 0.02s elapsed (1 total ports) Overall sending rates: 49.30 packets / s, 2169.20 bytes / s. Nmap scan report for 192.168.56.102</pre>
2024-12-16 15:27 GMT	Nmap	<p>'sudo nmap -sS 192.168.56.102'</p> <p>A SYN stealth scan is an efficient way of checking if ports are open without fully establishing a TCP connection.</p>	<pre>(administrator@PenTest-Kali-2023)-[~] \$ sudo nmap -sS 192.168.56.102 [sudo] password for administrator: Starting Nmap 7.94 (https://nmap.org) at 2024-12-16 15:27 GMT Nmap scan report for 192.168.56.102 Host is up (0.00033s latency). Not shown: 997 closed tcp ports (reset) PORT STATE SERVICE 21/tcp open ftp 22/tcp open ssh 80/tcp open http MAC Address: 08:00:27:19:AB:4C (Oracle VirtualBox virtual NIC) Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds</pre>

2024-12-16 19:55 GMT	Netcat	<p>'nc -zv 192.168.56.102 1-100'</p> <p>I scanned ports 1-100 with Netcat, which can scan across a network using the TCP or UDP protocol (Kali, 2024).</p>	<pre>(administrator@PenTest-Kali-2023)-[~] \$ nc -zv 192.168.56.102 1-100 192.168.56.102: inverse host lookup failed: Host name lookup failure (UNKNOWN) [192.168.56.102] 80 (http) open (UNKNOWN) [192.168.56.102] 22 (ssh) open (UNKNOWN) [192.168.56.102] 21 (ftp) open</pre>
2024-12-16 21:01 GMT	Masscan	<p>'Sudo masscan 192.168.56.102 -p80,22,21'</p> <p>Masscan is a TCP port scanner that transmits SYN packets. It has a similar interface to Nmap (Kali, 2024).</p>	<pre>(administrator@PenTest-Kali-2023)-[~] \$ sudo masscan 192.168.56.102 -p80,22,21 [sudo] password for administrator: Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-12-16 21:01:58 GMT Initiating SYN Stealth Scan Scanning 1 hosts [3 ports/host] Discovered open port 22/tcp on 192.168.56.102 Discovered open port 21/tcp on 192.168.56.102 Discovered open port 80/tcp on 192.168.56.102 Rate: 0.00-kpps, 100.00% done, waiting -84-secs, found=3</pre>
2024-12-17 07:18 GMT	Nmap	<p>'nmap -A'clr</p> <p>Using the command enables an aggressive scan such as OS version, script, and traceroute scanning.</p>	<pre>(administrator@PenTest-Kali-2023)-[~] \$ nmap -A 192.168.56.102 Starting Nmap 7.94 (https://nmap.org) at 2024-12-17 07:16 GMT Nmap scan report for 192.168.56.102 Host is up (0.00042s latency). Not shown: 997 closed tcp ports (conn-refused) PORT STATE SERVICE VERSION 21/tcp open ftp vsftpd 3.0.3 22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0) ssh-hostkey: _ 2048 fd:12:87:b2:a6:a1:d1:ee:29:c5:67:3c:ff:67:2d:e9 (RSA) _ 256 5f:be:58:9e:6d:b8:36:e8:8f:dc:08:ef:98:00:d3:50 (ECDSA) _ 256 95:52:5e:09:0a:05:53:5e:0b:39:c0:6c:91:6e:f7:b9 (ED25519) 80/tcp open http Apache httpd 2.4.29 ((Ubuntu)) _ http-title: The EDUVINH Company _ http-server-header: Apache/2.4.29 (Ubuntu) Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 22.39 seconds</pre>
2024-12-17 07:39 GMT	Metasploit	<p>'msfconsole'</p> <p>'show options'</p> <p>'set RHOSTS 192.168.56.102'</p> <p>'run'</p> <p>Metasploit, which is a pen-testing tool for exploiting vulnerabilities, has a built-in scanner tool that allows you to scan through a range of ports (GeeksforGeeks, 2023).</p>	<pre>msf6 > use auxiliary/scanner/portscan/tcp 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 192.168.56.102 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 192.168.56.102 RHOSTS => 192.168.56.102 msf6 auxiliary(scanner/portscan/tcp) > run [*] 192.168.56.102: - 192.168.56.102:21 - TCP OPEN [*] 192.168.56.102: - 192.168.56.102:22 - TCP OPEN [*] 192.168.56.102: - 192.168.56.102:80 - TCP OPEN [*] 192.168.56.102: - Scanned 1 of 1 hosts (100% complete) [*] Auxiliary module execution completed</pre>

Analysis of Findings:

When using Nmap compared to the other tools, they give very similar information. Overall, I have found that TCP ports 22, 21 and 80 are all open, leading to vulnerabilities towards the machine. Leaving ports open within a network is a vulnerability as it allows for a potential entry point for an attacker to bypass the firewall (Schrader, 2024).

Port 21: Uses plain text as the form of authentication, leaving usernames and passwords unencrypted, making it easy for an attacker to use sniffing tools to intercept login details.

Furthermore, if this port is not secured or disabled, an attacker can upload malware, compromising the device and potentially other devices within the network (Lee, 2024).

Port 22: While Port 22 can be used as a security alternative to port 21 for FTP, its original intended use was for system administrators who need remote access. By leaving port 22 open when the user doesn't explicitly need it, an attacker does endless damage if they can gain login access to the system. Alterability: if the user does need port 22, they could alternately use a random port, for example, between 1024 – 65535, reducing the suitability to direct port 22 attacks (Cohen, 2023)

Port 80: The vulnerabilities of leaving port 80 make it susceptible to packet sniffing, SQL injection, and packet interception. While port 80 can be secured with the alternative port 443 (HTTPS), it leaves unencrypted HTTP services not having a port; however, this isn't much of a problem in today's encryption-dominated World Wide Web. (Dirk Schrader, 2024)

Activity II: Network Reconnaissance Defence:

The firewall currently has unnecessary ports to be opened; this creates potential vulnerabilities that attackers could exploit. Attackers currently have access to a back door from ports 21 (FTP), 22(SSH) and 80(HTTP). To combat this, I will be implementing a firewall with strict port restrictions, allowing only packets which meet the correct requirements.

```
administrator@pc1:~$ sudo ufw status
[sudo] password for administrator:
Status: active

To Action From
--
21/tcp ALLOW Anywhere
22/tcp ALLOW Anywhere
80/tcp ALLOW Anywhere
21/tcp (v6) ALLOW Anywhere (v6)
22/tcp (v6) ALLOW Anywhere (v6)
80/tcp (v6) ALLOW Anywhere (v6)

administrator@pc1:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
administrator@pc1:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
administrator@pc1:~$
```

Time of Command/Task	Rules Implemented	Outcome of the task.
2024-12-17 09:09 GMT	<p>'sudo ufw deny 21/tcp'</p> <p>Because FTP transmits unencrypted data like usernames and passwords in plain text, it is very vulnerable to interception and attack. If the port is left open, it can be used for brute force attacks to gain access to the system.</p>	<pre>administrator@pc1:~\$ sudo ufw deny 21/tcp Rule updated Rule updated (v6) administrator@pc1:~\$ sudo ufw status Status: active To Action From -- 21/tcp DENY Anywhere 22/tcp ALLOW Anywhere 80/tcp ALLOW Anywhere 21/tcp (v6) DENY Anywhere (v6) 22/tcp (v6) ALLOW Anywhere (v6) 80/tcp (v6) ALLOW Anywhere (v6)</pre>

2024-12-17 09:15 GMT	<p>‘sudo ufw deny 22/tcp’</p> <p>Although the system could benefit from Secure File Transfers as opposed to port 21(FTP), the user hasn’t stated the need for this utility or SSH. Therefore, closing the port altogether eliminates the risk of brute-force SSH attacks.</p>	<pre>administrator@pc1:~\$ sudo ufw deny 22/tcp Rule updated Rule updated (v6) administrator@pc1:~\$ sudo ufw status Status: active</pre> <table><thead><tr><th>To</th><th>Action</th><th>From</th></tr></thead><tbody><tr><td>--</td><td>-----</td><td>----</td></tr><tr><td>21/tcp</td><td>DENY</td><td>Anywhere</td></tr><tr><td>22/tcp</td><td>DENY</td><td>Anywhere</td></tr><tr><td>80/tcp</td><td>ALLOW</td><td>Anywhere</td></tr><tr><td>21/tcp (v6)</td><td>DENY</td><td>Anywhere (v6)</td></tr><tr><td>22/tcp (v6)</td><td>DENY</td><td>Anywhere (v6)</td></tr><tr><td>80/tcp (v6)</td><td>ALLOW</td><td>Anywhere (v6)</td></tr></tbody></table>	To	Action	From	--	-----	----	21/tcp	DENY	Anywhere	22/tcp	DENY	Anywhere	80/tcp	ALLOW	Anywhere	21/tcp (v6)	DENY	Anywhere (v6)	22/tcp (v6)	DENY	Anywhere (v6)	80/tcp (v6)	ALLOW	Anywhere (v6)																																				
To	Action	From																																																												
--	-----	----																																																												
21/tcp	DENY	Anywhere																																																												
22/tcp	DENY	Anywhere																																																												
80/tcp	ALLOW	Anywhere																																																												
21/tcp (v6)	DENY	Anywhere (v6)																																																												
22/tcp (v6)	DENY	Anywhere (v6)																																																												
80/tcp (v6)	ALLOW	Anywhere (v6)																																																												
2024-12-17 09:20 GMT	<p>“sudo ufw allow 443/tcp comment ‘accept HTTPS connections’”</p> <p>‘sudo deny 80/tcp’</p> <p>Finally, by allowing port 443(HTTPS) and closing port 80(HTTP), it enables a more secure browsing protocol preventing unencrypted HTTP traffic from passing through the firewall; therefore, even with a successful middleman attack, the data would be encrypted and need to be decrypted.</p>	<pre>administrator@pc1:~\$ sudo ufw allow 443/tcp comment 'accept HTTPS connections' Rule added Rule added (v6) administrator@pc1:~\$ sudo ufw status Status: active</pre> <table><thead><tr><th>To</th><th>Action</th><th>From</th></tr></thead><tbody><tr><td>--</td><td>-----</td><td>----</td></tr><tr><td>21/tcp</td><td>DENY</td><td>Anywhere</td></tr><tr><td>22/tcp</td><td>DENY</td><td>Anywhere</td></tr><tr><td>80/tcp</td><td>ALLOW</td><td>Anywhere</td></tr><tr><td>443/tcp</td><td>ALLOW</td><td>Anywhere</td></tr><tr><td>21/tcp (v6)</td><td>DENY</td><td>Anywhere (v6)</td></tr><tr><td>22/tcp (v6)</td><td>DENY</td><td>Anywhere (v6)</td></tr><tr><td>80/tcp (v6)</td><td>ALLOW</td><td>Anywhere (v6)</td></tr><tr><td>443/tcp (v6)</td><td>ALLOW</td><td>Anywhere (v6)</td></tr></tbody></table> <pre>administrator@pc1:~\$ sudo ufw deny 80/tcp Rule updated Rule updated (v6) administrator@pc1:~\$ sudo ufw status Status: active</pre> <table><thead><tr><th>To</th><th>Action</th><th>From</th></tr></thead><tbody><tr><td>--</td><td>-----</td><td>----</td></tr><tr><td>21/tcp</td><td>DENY</td><td>Anywhere</td></tr><tr><td>22/tcp</td><td>DENY</td><td>Anywhere</td></tr><tr><td>80/tcp</td><td>DENY</td><td>Anywhere</td></tr><tr><td>443/tcp</td><td>ALLOW</td><td>Anywhere</td></tr><tr><td>21/tcp (v6)</td><td>DENY</td><td>Anywhere (v6)</td></tr><tr><td>22/tcp (v6)</td><td>DENY</td><td>Anywhere (v6)</td></tr><tr><td>80/tcp (v6)</td><td>DENY</td><td>Anywhere (v6)</td></tr><tr><td>443/tcp (v6)</td><td>ALLOW</td><td>Anywhere (v6)</td></tr></tbody></table> <pre>administrator@pc1:~\$</pre>	To	Action	From	--	-----	----	21/tcp	DENY	Anywhere	22/tcp	DENY	Anywhere	80/tcp	ALLOW	Anywhere	443/tcp	ALLOW	Anywhere	21/tcp (v6)	DENY	Anywhere (v6)	22/tcp (v6)	DENY	Anywhere (v6)	80/tcp (v6)	ALLOW	Anywhere (v6)	443/tcp (v6)	ALLOW	Anywhere (v6)	To	Action	From	--	-----	----	21/tcp	DENY	Anywhere	22/tcp	DENY	Anywhere	80/tcp	DENY	Anywhere	443/tcp	ALLOW	Anywhere	21/tcp (v6)	DENY	Anywhere (v6)	22/tcp (v6)	DENY	Anywhere (v6)	80/tcp (v6)	DENY	Anywhere (v6)	443/tcp (v6)	ALLOW	Anywhere (v6)
To	Action	From																																																												
--	-----	----																																																												
21/tcp	DENY	Anywhere																																																												
22/tcp	DENY	Anywhere																																																												
80/tcp	ALLOW	Anywhere																																																												
443/tcp	ALLOW	Anywhere																																																												
21/tcp (v6)	DENY	Anywhere (v6)																																																												
22/tcp (v6)	DENY	Anywhere (v6)																																																												
80/tcp (v6)	ALLOW	Anywhere (v6)																																																												
443/tcp (v6)	ALLOW	Anywhere (v6)																																																												
To	Action	From																																																												
--	-----	----																																																												
21/tcp	DENY	Anywhere																																																												
22/tcp	DENY	Anywhere																																																												
80/tcp	DENY	Anywhere																																																												
443/tcp	ALLOW	Anywhere																																																												
21/tcp (v6)	DENY	Anywhere (v6)																																																												
22/tcp (v6)	DENY	Anywhere (v6)																																																												
80/tcp (v6)	DENY	Anywhere (v6)																																																												
443/tcp (v6)	ALLOW	Anywhere (v6)																																																												

After Implementing the Firewall:

Once the firewall was implemented, I proceeded to do another Nmap scan to see if the open ports had been secured.

The Nmap scan shows that all the ports are secured and filtered. The firewall blocks the incoming traffic, which results in a filtered response from Nmap, and the firewall drops the packets. Overall, the firewall restricts network access, limiting the vulnerabilities and improving the security.

Image 1 – Showing Nmap results after firewall implementation.

```
(administrator@PenTest-Kali-2023)-[~]
$ sudo nmap 192.168.56.102
Starting Nmap 7.94 ( https://nmap.org ) at 2024-12-17 09:24 GMT
Nmap scan report for 192.168.56.102
Host is up (0.00091s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
443/tcp   closed https
MAC Address: 08:00:27:19:AB:4C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.10 seconds
```

Image 2 – Showing Nmap results after firewall implementation.

```
(administrator@PenTest-Kali-2023)-[~]
$ sudo nmap -A 192.168.56.102
[sudo] password for administrator:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-12-17 09:19 GMT
Nmap scan report for 192.168.56.102
Host is up (0.0013s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
443/tcp   closed https
MAC Address: 08:00:27:19:AB:4C (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running: Linux 2.6.X, VMware ESX Server 3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.11 cpe:/o:vmware:esx:3.0:2
OS details: Linux 2.6.11, Linux 2.6.18, Linux 2.6.18.8 (openSUSE 10.2), Linux 2.6.18.8 (openSUSE 10.2, SMP), Linux
2.6.20.6, Linux 2.6.23, Linux 2.6.39, VMware ESX Server 3.0.2
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   1.25 ms  192.168.56.102

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.49 seconds
```


Chapter 3.

The Significance of Mitigating Insider Threats in a Financial Institution

Introduction.

An insider threat is not just a cyber security risk but a potential disaster where an employee with legitimate user credentials misuses their access to an organisation's system, network or data. The traditional focus of cybersecurity on outsider threats and defensive measures leaves organisations vulnerable from within. Legitimate employees with legitimate user credentials can have authorisation to a system, network or database and unintentionally or intentionally cause catastrophic harm to the organisation. An organisation must implement adequate insider security measures and restrictions to reduce the chances of financial loss, reputation damage and legal and regulatory consequences (opentext, 2024).

This assignment is going to identify the potential vulnerabilities and the methods of insider attacks, propose robust and effective defences that are crucial for mitigating these threats, and address legal/ethical concerns.

Identification of Vulnerabilities.

Privileged Access Mismanagement: While privileged access is often granted to certain employees within a role or group of an organisation because of specific access and resource requirements, this creates a double-edged sword as they have a higher probability of being abused, misused or hijacked. Privileged users are also more vulnerable to social engineering, spear-phishing, and bribes (Noonan, 2024).

Lack of Monitoring: Without sufficient security logging and monitoring, critical security threats get missed, allowing the insiders to continue to damage the system undetected, making it challenging to identify attacks and respond promptly (Hiremath, 2024).

Poor Security Controls and Policy: An organisation that uses a weak policy, such as weak passwords and unclear security protocols, make it more susceptible to insider attacks making threats to several aspects of the organisation, for instance, the operational efficiency, the reputation, the finances and the compliance and legal issues are all vulnerable (IT, Method, 2024).

Inadequate Security Training: Employees who receive none to minimal awareness of social engineering training can become the most susceptible threat within the organisation; this is because unlike computers, which are 'black or white', 'yes or no', '0 or 1', humans are susceptible to psychological factors like fear and curiosity, which leave them in the 'grey area' in comparison (Living Security, 2024).

Analysing Attack Methods.

Table 1 – Attack Methods Linked to Vulnerabilities.

Vulnerability	Attack Method	Example
Privileged Access Mismanagement	Credential Misuse	An employee could have accessed sensitive customer data through abusing/misusing credentials, which is where they would use their own or another employee's valid credentials with higher privileges to access resources or data for malicious purposes (Kasada, 2023).

Lack of Monitoring	Data Exfiltration	An employee might have compromised sensitive customer data through data exfiltration, which is the act of copying or transferring an individual's or organisation's data without authorisation. Malicious employees who have data access and can transfer the data outside of the organisation can be challenging to detect without proper monitoring, as they often resemble ordinary network traffic (Lord, 2015), (Imperva, 2024).
Poor Security Controls and Policy	Bypassing Security Controls	A misconfigured/poorly configured system policy could allow an employee to bypass security controls with weak, leaked, and compromised passwords. Old software vulnerabilities could allow the attacker to grant access to sensitive data (Media Defense, 2022).
Inadequate Staff Security Training	Social Engineering	There are many different forms of social engineering; however, they all fall under the same aim of exploiting trust to manipulate another colleague into accessing confidential information (Carnegie Mellon University, n.d.). When it comes to an insider attack, the most probable would be a spear phishing attack, where an employee could directly manipulate another employee in an attempt to steal sensitive data (Fortinet, 2024).

Defensive Measurements:

Table 2 – Defensive Methods linked to Attack Methods.

Attack Method	Defensive Measurements
Technical Measures	
Credential Misuse	Multi-factor authentication reduces the potential for employees to misuse credentials to access confidential information, as further authentication needs to be required. MFA is a simple process of verifying the claimed identity to be legitimate by more than one form of strong authentication, for example, biometrics, RFID cards or passwords (Sanjar Ibrokhimov, 2019).
Data Exfiltration	Data loss prevention systems work by identifying sensitive information, such as 'sensitive customer data', and preventing potential data leaks through monitoring and analysing data at rest, in motion or use. DLP usually uses systems such as deep packet analysis to monitor the network traffic and detect unauthorised attempts to access, modify, or exfiltrate sensitive data (FORTINET, 2024).
Bypassing Security Controls	Identifying and addressing misconfigured default settings, such as operating systems with predefined passwords or pre-installed applications, is critical to security. Implementing software configuration management tools ensures uniformity and reliability throughout the company infrastructure (Burnham, 2021).

Social Engineering	To prevent insiders from conducting social engineering attacks such as spear phishing, a phishing detection scheme and a simulated phishing attack for all employees should be implemented to strengthen further the employee's ability to detect and respond to such attacks (Gaurav Varshney, 2024).
Procedural Measures	
Credential Misuse	Conducting regular reviews of user access rights can minimise the employees' ability to misuse or abuse the corporation's resources, system management, or system service resources. Therefore, by default, user rights should be kept at a minimum, and unless user access is absolutely required to a particular system or service, access should not be granted (Beuchelt, 2013).
Data Exfiltration	Implementing a strict data handling policy will improve the integrity of the data because the organisation must follow a set of guidelines to protect, manage and responsibly use the data. Training employees regularly on handling data correctly and the consequences of data misconduct is essential for an organisation as it clearly defines what employees can access, share or export (Rawat, 2024).
Bypassing Security Controls	Following the Separation of Duties ensures that no single employee has enough control to misuse the system on their own. SOD prevents both internal and external threats, making it harder for a user to access, delete or alter data without oversight, reducing the potential for an insider attack (Rubik, 2024).
Social Engineering	People are usually the weakest link within cybersecurity; therefore, regularly educating employees with security awareness training programs on the risk of potential phishing threats limits the risk of an insider breaching confidential information (Garder, 2014).

Legal, Social, and Ethical Considerations:

Multi-factor authentication and Conducting Access Reviews:

- **Legal Implications:** MFA secures access to sensitive data, reducing the potential for unauthorised access. Regularly conducting access reviews ensures that the data is limited to only those who need it. While MFA often involves the data of biometrics or passwords, it raises privacy concerns about data protection, and the organisation must ensure the security of the data (GOV.UK, 2024).
- **Ethical Implications:** Both MFA and Access Reviews have to balance security and employee privacy. Because of the potential of MFA using personal data such as biometrics or passwords, only the required amount of data should be collected and safely stored. Similarly, Access Reviews should be fair and not intrude on the employees' privacy rights.
- **Social Implications:** MFA can be seen by employees as an inconvenience, potentially frustrating employees and impacting their productivity and user experience. Similarly, access reviews could be seen as intrusive and untrustworthy to some employees.

Data Loss Prevention and Strict Data Handling:

- **Legal Implications:** Both DLP and using a strict data handling procedure help to comply with GDPR rules as it prevents the potential for unauthorised transfer of customer-sensitive data and acts as a standard procedure for how data is stored and accessed (GOV.UK, 2024).
- **Ethical Implications:** DLP needs to monitor only the essential work-related data and avoid unnecessary personal data in order to respect the employees' privacy. Strict Data handling should be applied across all employees to prevent unfairness.
- **Social Implications:** DLP may make employees feel that they are being over-monitored and create a sense of distrust. At the same time, strict data policies can overwhelm employees having to follow strict guidelines.

Security Configuration Management and Segregations of Duties:

- **Legal Implications:** SCM is a process of ensuring the system is in line with the security needs of the business, complying with GDPR rules and regulations, and stopping fines. SoD stops the potential for an employee to access or execute critical processes without oversight, increasing the data integrity (GOV.UK, 2024).
- **Ethical Implications:** Both SCM and SoD require a balance of security measures and employee convenience as over-strict security could slow down productivity without adequate security benefits.
- **Social Implications:** SCM changes need to be clearly communicated to employees, as regularly doing so without proper communication can disrupt their work and create friction. SoD, to some employees, may be perceived as untrustworthy; therefore, adequate communication is needed to explain the security requirements.

Simulated Phishing Attack and Detection Scheme and Regular Security Awareness Training:

- **Legal Implications:** Simulated regular phishing tests and training on employees reduce the chances of human error, supporting compliance with the GDPR as employees learn and become more cautious, reducing the chance of careless behaviour. While the company could document the training and testing for GDPR compliance purposes, it should avoid collecting sensitive information beyond what is necessary, as it could violate privacy laws and employee rights.
- **Ethical Implications:** Phishing attacks must inform the employees beforehand, as performing simulations without previously informing them can be seen as intentionally trying to catch employees, causing unnecessary stress and fear. Security awareness training should be given equally, avoiding singling out individuals.
- **Social Implications:** Each employee must be tested relatively, and the tests must be seen as an educational lesson to improve security, as unfair testing can cause harm and damage workplace morals and relationships.

Overall, in this assignment, I have identified the potential insider threat vulnerabilities, explained the attack methods which the attackers could use on those vulnerabilities, how to prevent and reduce the attack methods and explained the legal, social and ethical considerations of the security measure within an organisation.

Beuchelt, G., 2013. Chapter 9 - Unix and Linux Securit. In: *Computer and Information Security Handbook (Second Edition)*. Bedford: MITRE Corporation, pp. 165-181.

Burnham, K., 2021. *What Is Security Configuration Management?*. [Online]
Available at: <https://www.tanium.com/blog/what-is-security-configuration-management/>
[Accessed 14 12 2024].

Cohen, C., 2023. *What is Port 22?*. [Online]
Available at: <https://www.cb nuggets.com/common-ports/what-is-port-22>
[Accessed 19 12 2024].

Dirk Schrader, 2024. *Identifying Common Open Port Vulnerabilities in Your Network*. [Online]
Available at: <https://blog.netwrix.com/open-ports-vulnerability-list#:~:text=Port%2080%20vulnerabilities%20include%20a,and%20cross%2Dsite%20request%20forgery.>
[Accessed 19 12 2024].

Fortinet, 2024. *Spear Phishing Definition*. [Online]
Available at: <https://www.fortinet.com/uk/resources/cyberglossary/spear-phishing>
[Accessed 27 11 2024].

FORTINET, 2024. *What Is Data Loss Prevention (DLP)?*. [Online]
Available at: <https://www.fortinet.com/uk/resources/cyberglossary/dlp>
[Accessed 14 12 2024].

Garder, B., 2014. Chapter 1 - What Is a Security Awareness Program?. In: *Building an Information Security Awareness Program*. Syngress: ISBN, pp. 1-8.

Gaurav Varshney, R. K. V. V. U. T. C. G., 2024. *Anti-phishing: A comprehensive perspective*. [Online]
Available at: <https://www.sciencedirect.com/science/article/pii/S095741742302701X>
[Accessed 14 12 2024].

GeeksforGeeks, 2023. *Using Metasploit and Nmap to Scan for Vulnerabilities in Kali Linux*. [Online]
Available at: <https://www.geeksforgeeks.org/using-metasploit-and-nmap-to-scan-for-vulnerabilities-in-kali-linux/>
[Accessed 17 12 2024].

GeeksforGeeks, 2024. *What is Virtualbox?*. [Online]
Available at: <https://www.geeksforgeeks.org/what-is-virtualbox/>
[Accessed 05 12 2024].

GOV.UK, 2024. *Data protection*. [Online]
Available at: <https://www.gov.uk/data-protection>
[Accessed 14 12 2024].

Hiremath, O., 2024. *Risk of Security and Monitoring Logging Failures*. [Online]
Available at: <https://www.softwaresecured.com/post/risk-of-security-and-monitoring-logging-failures#:~:text=Attackers%20can%20continue%20to%20damage,respond%20quickly%20to%20mitigate%20them.>
[Accessed 23 11 2024].

Imperva, 2024. *Data Exfiltration*. [Online]
Available at: <https://www.imperva.com/learn/data-security/data-exfiltration/>
[Accessed 27 11 2024].

IT, Method, 2024. *The Consequences of Weak IT Policy*. [Online]
Available at: <https://method-it.co.uk/resources/the-consequences-of-weak-it-policy#:~:text=Increased%20vulnerability%20to%20cyber%20attacks.%20Weak%20IT,act>

rs%20do%20target%20small%20businesses%20like%20yours.

[Accessed 27 11 2024].

Kali, 2024. *Masscan*. [Online]

Available at: <https://www.kali.org/tools/masscan/>

[Accessed 16 12 2024].

Kali, 2024. *Netcat*. [Online]

Available at: <https://www.kali.org/tools/netcat/>

[Accessed 16 12 2024].

Kasada, 2023. *What is Credential Abuse? And Why are Credential Stuffing Attacks So Common?*. [Online]

Available at: <https://www.kasada.io/what-is-credential-abuse/>

[Accessed 27 11 2024].

Lee, B., 2024. *Analyzing TCP port 21 FTP vulnerabilities*. [Online]

Available at: <https://specopssoft.com/blog/tcp-port-21-ftp-vulnerabilities/>

[Accessed 19 12 2024].

Living Security, 2024. *What Is Social Engineering? Examples & How To Prevent It*. [Online]

Available at: <https://www.livingsecurity.com/blog/social-engineering-guide>

[Accessed 27 11 2024].

Lord, N., 2015. *What is Data Exfiltration? (Definition & Prevention)*. [Online]

Available at: <https://www.digitalguardian.com/blog/what-data-exfiltration>

[Accessed 27 11 2024].

McGreevy, J., 2021. *Footprinting: What, s.l.:* SANS Institute.

Media Defense, 2022. *Weak Security Controls and Practices*. [Online]

Available at: [https://media.defense.gov/2022/May/17/2002998718/-1/-](https://media.defense.gov/2022/May/17/2002998718/-1/-1/0/CSA_WEAK_SECURITY_CONTROLS_PRACTICES_EXPLOITED_FOR_INITIAL_ACCESS.PDF)

[1/0/CSA_WEAK_SECURITY_CONTROLS_PRACTICES_EXPLOITED_FOR_INITIAL_ACCESS.PDF](https://media.defense.gov/2022/May/17/2002998718/-1/-1/0/CSA_WEAK_SECURITY_CONTROLS_PRACTICES_EXPLOITED_FOR_INITIAL_ACCESS.PDF)

[Accessed 27 11 2024].

Noonan, L., 2024. *Why Privileged Users Are a Major Security Risk*. [Online]

Available at: <https://www.metacompliance.com/blog/cyber-security-awareness/why-privileged-users-are-a-major-security-risk>

[Accessed 22 11 2024].

opentext, 2024. *What is an Insider Threat?*. [Online]

Available at: <https://www.opentext.com/en-gb/what-is/insider-threat>

[Accessed 23 11 2024].

Rathnayake, D., 2023. *Understanding Cybersecurity Footprinting: Techniques and Strategies*. [Online]

Available at: [https://www.tripwire.com/state-of-security/understanding-cybersecurity-footprinting-techniques-and-](https://www.tripwire.com/state-of-security/understanding-cybersecurity-footprinting-techniques-and-strategies#:~:text=Footprinting%20is%20the%20first%20step,IP%20addresses%2C%20and%20user%20accounts.)

[strategies#:~:text=Footprinting%20is%20the%20first%20step,IP%20addresses%2C%20and%20user%20accounts.](https://www.tripwire.com/state-of-security/understanding-cybersecurity-footprinting-techniques-and-strategies#:~:text=Footprinting%20is%20the%20first%20step,IP%20addresses%2C%20and%20user%20accounts.)

[Accessed 19 12 2024].

Rawat, P., 2024. *Data Handling Policy & Its Advantages*. [Online]

Available at: <https://www.infosectrain.com/blog/data-handling-policy-its-advantages/>

[Accessed 14 12 2024].

Rubik, 2024. *What Is Separation of Duties in Cybersecurity?*. [Online]

Available at: <https://www.rubrik.com/insights/what-is-separation-of-duties-in-cybersecurity>

[Accessed 14 12 2024].

Sanjar Ibrokhimov, K. L. H. A. A. A.-A. h. j. l. M. S., 2019. *Multi-Factor Authentication in Cyber Physical System: A State of Art Survey*. [Online]

Available at: <https://ieeexplore.ieee.org/document/8701960/authors#authors>

[Accessed 13 12 2024].

Schrader, D., 2024. *Identifying Common Open Port Vulnerabilities in Your Network*. [Online]

Available at: <https://blog.netwrix.com/open-ports-vulnerability-list>

[Accessed 19 12 2024].

VMware, 2019. *Configuring Host-Only Networking*. [Online]

Available at: [https://docs.vmware.com/en/VMware-Workstation-](https://docs.vmware.com/en/VMware-Workstation-Pro/17/com.vmware.ws.using.doc/GUID-93BDF7F1-D2E4-42CE-80EA-4E305337D2FC.html)

[Pro/17/com.vmware.ws.using.doc/GUID-93BDF7F1-D2E4-42CE-80EA-4E305337D2FC.html](https://docs.vmware.com/en/VMware-Workstation-Pro/17/com.vmware.ws.using.doc/GUID-93BDF7F1-D2E4-42CE-80EA-4E305337D2FC.html)

[Accessed 05 12 2024].