5. Vulnerability Testing for TechSecure Solutions

Prepared by: Ross Moravec / A00322717

Objective

The primary goal of this vulnerability testing report is to assess the security posture of the network in the 192.168.1.0/24 subnet. The assessment aims to identify potential vulnerabilities, analyze their potential risks, and propose corrective actions to enhance the network's security. This process is critical for ensuring that systems within the network are safeguarded against potential exploitation and other malicious activities.

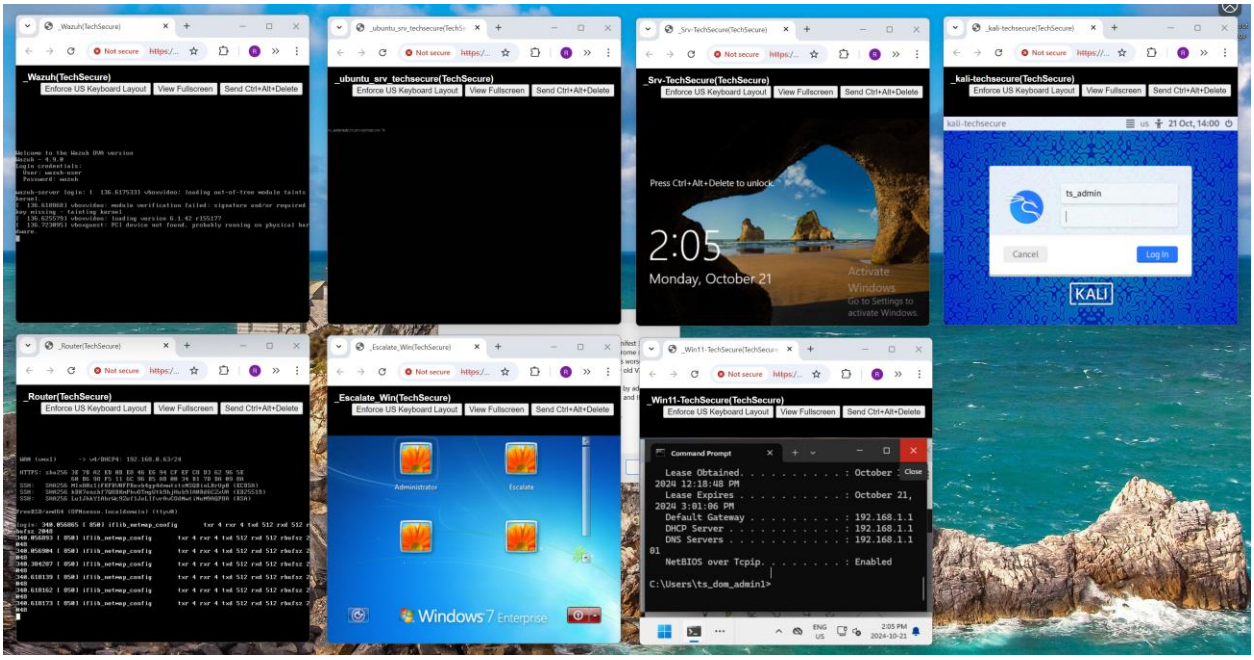
Methodology

The vulnerability assessment was conducted by scanning the network using **Nmap** and analyzing the results with a focus on identifying security weaknesses. The key tasks involved:

- **Identifying Active Devices**: Scanning the subnet to detect all live hosts and their corresponding IP addresses.
- **Port Scanning**: Detecting open ports and services running on each host to assess exposure to potential attacks.
- **Service Identification**: Analyzing the detected services, such as DNS, HTTP, SSH, and SMB, and reviewing their configuration for security risks.
- **Risk Analysis**: Identifying vulnerabilities in the detected services, including outdated software, misconfigurations, or weak security practices.
- **Corrective Actions**: Proposing specific remediation steps for each vulnerability to mitigate risks and strengthen network security.

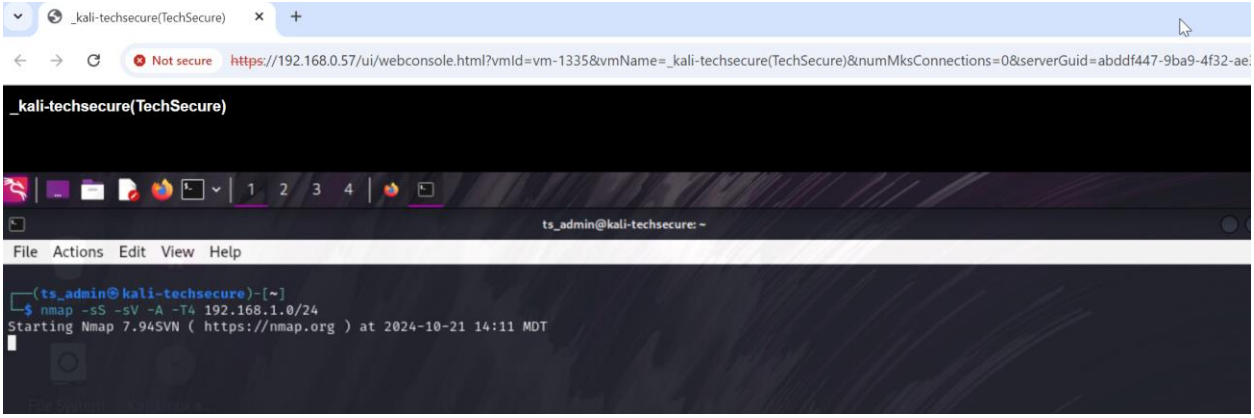
Scope of the Assessment

The network scan focused on hosts within the **192.168.1.0/24** subnet, where seven active devices were identified and examined. The report outlines findings for each host, including open ports, running services, and potential risks. Each vulnerability identified has been analyzed, and detailed recommendations have been provided to address these risks. By implementing these recommendations, the network's resilience against attacks can be significantly improved.



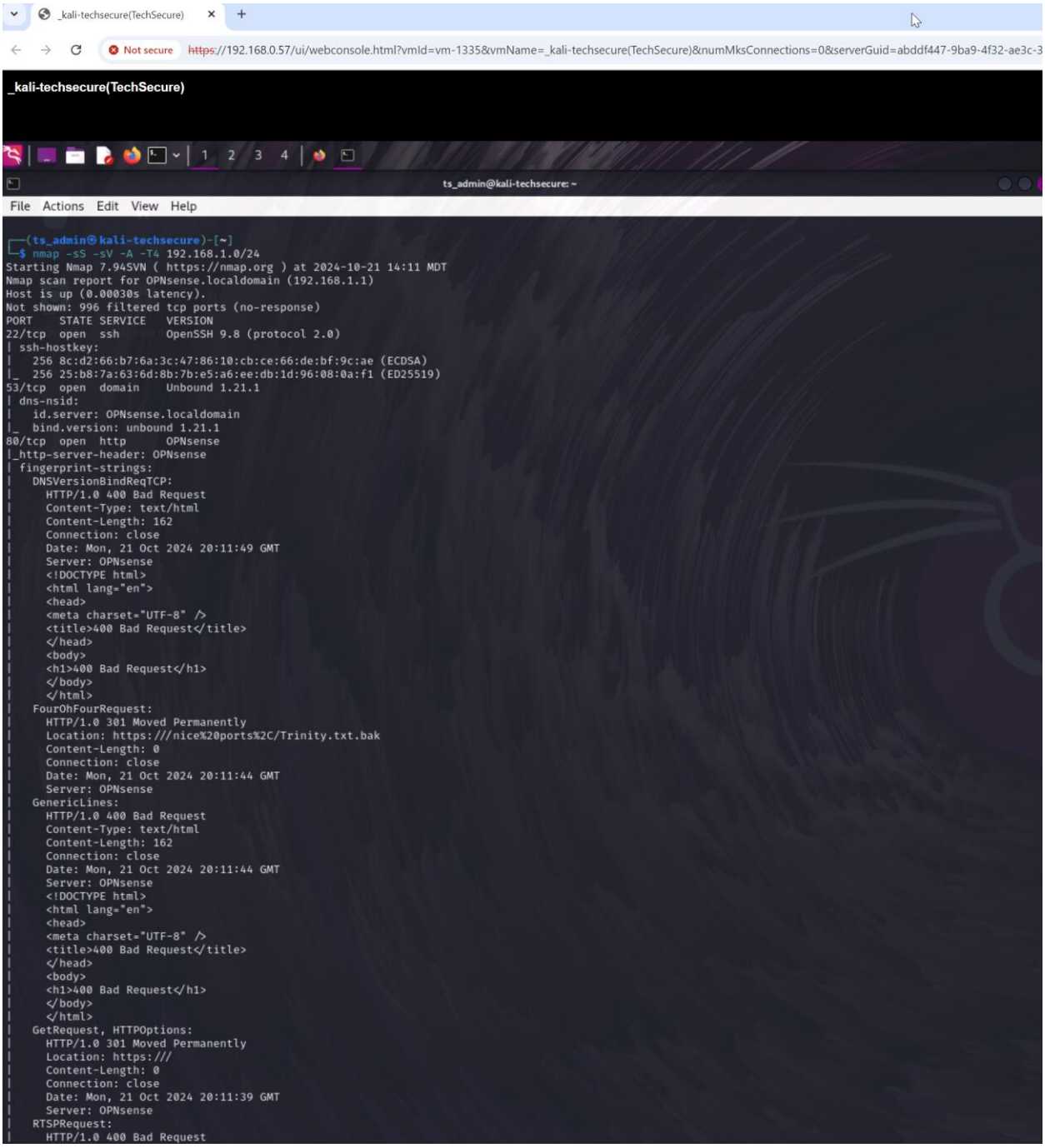
1.Screenshot of Virtual Machine Environment for Network Testing: This screenshot captures multiple virtual machines (VMs) used in a network vulnerability testing environment. The VMs are shown in a variety of states, displaying their login screens, command prompts, and desktop environments. Each VM is part of the TechSecure network, identified by their hostnames or login interfaces, and they are running different operating systems (Windows, Linux, etc.).

- The top row showcases terminal and login screens for systems like **Wazuh (TechSecure)**, **Ubuntu Server (TechSecure)**, **Srv-TechSecure** (Windows Server), and **Kali (TechSecure)**, used for penetration testing.
- The bottom row includes systems like **Router (TechSecure)** and a Windows machine labeled **Escalate (TechSecure)**, running **Windows 7 Enterprise**, alongside other command-line environments.



2. Kali Linux VM Running Nmap Network Scan: This screenshot shows a **Kali Linux virtual machine** named **kali-techsecure (TechSecure)** running an **Nmap network scan** command in the terminal. The user ts_admin is executing the command nmap -sS -sV -A -T4 192.168.1.0/24, which performs a stealth scan (-sS), version detection (-sV), and aggressive scan (-A) on the 192.168.1.0/24 subnet. The scan aims to identify open ports, running services, and other system information for hosts within the subnet. This scan is part of the **TechSecure network security assessment** to detect vulnerabilities.

The Nmap version running is 7.94SVN, and the scan was initiated at **14:11 MDT** on **October 21, 2024**. This is a typical use case of Kali Linux in a penetration testing and network security context.



3.Nmap Scan Results Using Kali Linux: This screenshot shows a **Kali Linux virtual machine** named **kali-techsecure (TechSecure)** displaying the output of an **Nmap scan** targeting **192.168.1.0** network. The scan was performed by the user ts_admin and executed with the command nmap -sS -sV -A -T4 192.168.1.0/24.

_kali-techsecure(TechSecure)

Not secure https://192.168.0.57/ui/webconsole.html?vmId=vm-1335&vmName=_kali-techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8

_kali-techsecure(TechSecure)

1 2 3 4

ts_admin@kali-techsecure: ~

File Actions Edit View Help

```
|   RTSPRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/html
|     Content-Length: 162
|     Connection: close
|     Date: Mon, 21 Oct 2024 20:11:39 GMT
|     Server: OPNsense
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="UTF-8" />
|     <title>400 Bad Request</title>
|     </head>
|     <body>
|     <h1>400 Bad Request</h1>
|     </body>
|_    </html>
|_http-title: Did not follow redirect to https://opnsense.localdomain/
443/tcp open  ssl/https OPNsense
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=OPNsense.localdomain/organizationName=OPNsense self-signed web certificate/stateOrProvinceName=Zuid-Holland/countryName=NL
| Subject Alternative Name: DNS:OPNsense.localdomain
| Not valid before: 2024-09-15T03:00:44
|_Not valid after:  2025-10-17T03:00:44
|_http-title: Login | OPNsense
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
|     Set-Cookie: PHPSESSID=90b8e617defd45559e1bd54628db3b5f; path=/; secure; HttpOnly; SameSite=Lax
|     Set-Cookie: PHPSESSID=90b8e617defd45559e1bd54628db3b5f; path=/; secure; HttpOnly
|     Expires: Thu, 19 Nov 1981 08:52:00 GMT
|     Cache-Control: no-store, no-cache, must-revalidate
|     Pragma: no-cache
|     Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' 'unsafe-eval';
|     X-Frame-Options: SAMEORIGIN
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Referrer-Policy: same-origin
|     Content-type: text/html; charset=UTF-8
|     Content-Length: 1603
|     Connection: close
|     Date: Mon, 21 Oct 2024 20:11:45 GMT
|     Server: OPNsense
|     <!doctype html>
|     <html lang="en-US" class="no-js">
|     <head>
|     <meta charset="UTF-8" />
|     <meta http-equiv="X-UA-Compatible" content="IE=edge">
|     <meta name="robots" content="noindex,
|   HTTPOptions:
|     HTTP/1.0 403 Forbidden
|     Set-Cookie: PHPSESSID=cd1a3d1c38b09be9ba1b4ab361363e32; path=/; secure; HttpOnly; SameSite=Lax
|     Expires: Thu, 19 Nov 1981 08:52:00 GMT
|     Cache-Control: no-store, no-cache, must-revalidate
|     Pragma: no-cache
|     Content-type: text/html; charset=UTF-8
|     Content-Length: 553
|     Connection: close
|     Date: Mon, 21 Oct 2024 20:11:50 GMT
|     Server: OPNsense
|     <html><head><title>CSRF check failed</title>
|     <script>
|     document ).ready(function() {
|     $.ajaxSetup({
|     'beforeSend': function(xhr) {
|     xhr.setRequestHeader("X-CSRFToken", "sx4GH6bqepznOTTo2oA3uQ" );
|     </script>
|     </head>
|     <body>
```

Continued Nmap Scan Results on OPNsense Firewall (192.168.1.1) - Part 2

_kali-techsecure(TechSecure)

Not secure https://192.168.0.57/ui/webconsole.html?vmId=vm-1335&vmName=_kali-techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8c

_kali-techsecure(TechSecure)

1 2 3 4

ts_admin@kali-techsecure: ~

File Actions Edit View Help

```
|     <head>
|     <meta charset="UTF-8" />
|     <title>400 Bad Request</title>
|     </head>
|     <body>
|     <h1>400 Bad Request</h1>
|     </body>
|_    </html>
|_http-title: Did not follow redirect to https://opnsense.localdomain/
443/tcp open  ssl/https OPNsense
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=OPNsense.localdomain/organizationName=OPNsense self-signed web certificate/stateOrProvinceName=Zuid-Holland/countryName=NL
| Subject Alternative Name: DNS:OPNsense.localdomain
| Not valid before: 2024-09-15T03:00:44
|_Not valid after:  2025-10-17T03:00:44
|_http-title: Login | OPNsense
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
|     Set-Cookie: PHPSESSID=90b8e617defd45559e1bd54628db3b5f; path=/; secure; HttpOnly; SameSite=Lax
|     Set-Cookie: PHPSESSID=90b8e617defd45559e1bd54628db3b5f; path=/; secure; HttpOnly
|     Expires: Thu, 19 Nov 1981 08:52:00 GMT
|     Cache-Control: no-store, no-cache, must-revalidate
|     Pragma: no-cache
|     Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline' 'unsafe-eval';
|     X-Frame-Options: SAMEORIGIN
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Referrer-Policy: same-origin
|     Content-type: text/html; charset=UTF-8
|     Content-Length: 1603
|     Connection: close
|     Date: Mon, 21 Oct 2024 20:11:45 GMT
|     Server: OPNsense
|     <!doctype html>
|     <html lang="en-US" class="no-js">
|     <head>
|     <meta charset="UTF-8" />
|     <meta http-equiv="X-UA-Compatible" content="IE=edge">
|     <meta name="robots" content="noindex,
|   HTTPOptions:
|     HTTP/1.0 403 Forbidden
|     Set-Cookie: PHPSESSID=cd1a3d1c38b09be9ba1b4ab361363e32; path=/; secure; HttpOnly; SameSite=Lax
|     Expires: Thu, 19 Nov 1981 08:52:00 GMT
|     Cache-Control: no-store, no-cache, must-revalidate
|     Pragma: no-cache
|     Content-type: text/html; charset=UTF-8
|     Content-Length: 553
|     Connection: close
|     Date: Mon, 21 Oct 2024 20:11:50 GMT
|     Server: OPNsense
|     <html><head><title>CSRF check failed</title>
|     <script>
|     document ).ready(function() {
|     $.ajaxSetup({
|     'beforeSend': function(xhr) {
|     xhr.setRequestHeader("X-CSRFToken", "sx4GH6bqepznOTTo2oA3uQ" );
|     </script>
|     </head>
|     <body>
|_    <p>CSRF check failed. Your form session may have expired, or you may not have cookies enabled.</p>
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-server-header: OPNsense
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submi
t.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.94SVN%I=7%D=10/21%Time=6716B57B%P=x86_64-pc-linux-gnu%r(
SF:GetRequest,94,"HTTP/1\.0\x20301\x20Moved\x20Permanently\r\nLocation:\x2
SF:0https:///\r\nContent-Length:\x200\r\nConnection:\x20close\r\nDate:\x20
```

Continued Nmap Scan Results on OPNsense Firewall (192.168.1.1) - Part 3

_kali-techsecure(TechSecure)

Not secure https://192.168.0.57/ui/webconsole.html?vmId=vm-1335&vmName=_kali-techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8c

_kali-techsecure(TechSecure)

1 2 3 4

ts_admin@kali-techsecure: ~

File Actions Edit View Help

```
t.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.94SVN%I=7%D=10/21%Time=6716B57B%P=x86_64-pc-linux-gnu%r(
SF:GetRequest,94,"HTTP/1\.0\x20301\x20Moved\x20Permanently\r\nLocation:\x2
SF:0https:///\r\nContent-Length:\x200\r\nConnection:\x20close\r\nDate:\x20
SF:Mon,\x2021\x20Oct\x202024\x2020:11:39\x20GMT\r\nServer:\x20OPNsense\r\n
SF:\r\n")%r(HTTPOptions,94,"HTTP/1\.0\x20301\x20Moved\x20Permanently\r\nLo
SF:cation:\x20https:///\r\nContent-Length:\x200\r\nConnection:\x20close\r\
SF:nDate:\x20Mon,\x2021\x20Oct\x202024\x2020:11:39\x20GMT\r\nServer:\x20OP
SF:Nsense\r\n\r\n")%r(RTSPRequest,136,"HTTP/1\.0\x20400\x20Bad\x20Request\
SF:r\nContent-Type:\x20text/html\r\nContent-Length:\x20162\r\nConnection:\
SF:x20close\r\nDate:\x20Mon,\x2021\x20Oct\x202024\x2020:11:39\x20GMT\r\nSe
SF:rver:\x20OPNsense\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\"en\">\n\x2
SF:0<head>\n\x20\x20<meta\x20charset=\"UTF-8\"\x20/>\n\x20\x20<title>400\x
SF:20Bad\x20Request</title>\n\x20</head>\n\x20<body>\n\x20\x20<h1>400\x20B
SF:ad\x20Request</h1>\n\x20</body>\n</html>\n")%r(FourOhFourRequest,B3,"HT
SF:TP/1\.0\x20301\x20Moved\x20Permanently\r\nLocation:\x20https:///nice%20
SF:ports%2C/Trinity\.txt\.bak\r\nContent-Length:\x200\r\nConnection:\x20cl
SF:ose\r\nDate:\x20Mon,\x2021\x20Oct\x202024\x2020:11:44\x20GMT\r\nServer:
SF:\x20OPNsense\r\n\r\n")%r(GenericLines,136,"HTTP/1\.0\x20400\x20Bad\x20R
SF:equest\r\nContent-Type:\x20text/html\r\nContent-Length:\x20162\r\nConne
SF:ction:\x20close\r\nDate:\x20Mon,\x2021\x20Oct\x202024\x2020:11:44\x20GM
SF:T\r\nServer:\x20OPNsense\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\"en\
SF:">\n\x20<head>\n\x20\x20<meta\x20charset=\"UTF-8\"\x20/>\n\x20\x20<titl
SF:e>400\x20Bad\x20Request</title>\n\x20</head>\n\x20<body>\n\x20\x20<h1>4
SF:00\x20Bad\x20Request</h1>\n\x20</body>\n</html>\n")%r(DNSVersionBindReq
SF:TCP,136,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/ht
SF:ml\r\nContent-Length:\x20162\r\nConnection:\x20close\r\nDate:\x20Mon,\x
SF:2021\x20Oct\x202024\x2020:11:49\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<!
SF:DOCTYPE\x20html>\n<html\x20lang=\"en\">\n\x20<head>\n\x20\x20<meta\x20c
SF:harset=\"UTF-8\"\x20/>\n\x20\x20<title>400\x20Bad\x20Request</title>\n\
SF:x20</head>\n\x20<body>\n\x20\x20<h1>400\x20Bad\x20Request</h1>\n\x20</b
SF:ody>\n</html>\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.94SVN%T=SSL%I=7%D=10/21%Time=6716B586%P=x86_64-pc-linux
SF:-gnu%r(GetRequest,90A,"HTTP/1\.0\x20200\x20OK\r\nSet-Cookie:\x20PHPSESS
SF:ID=90b8e617defd45559e1bd54628db3b5f;\x20path=/;\x20secure;\x20HttpOnly;
SF:\x20SameSite=Lax\r\nSet-Cookie:\x20PHPSESSID=90b8e617defd45559e1bd54628
SF:db3b5f;\x20path=/;\x20secure;\x20HttpOnly\r\nExpires:\x20Thu,\x2019\x20
SF:Nov\x201981\x2008:52:00\x20GMT\r\nCache-Control:\x20no-store,\x20no-cac
SF:he,\x20must-revalidate\r\nPragma:\x20no-cache\r\nContent-Security-Polic
SF:y:\x20default-src\x20'self';\x20script-src\x20'self'\x20'unsafe-inline'
SF:\x20'unsafe-eval';\x20style-src\x20'self'\x20'unsafe-inline'\x20'unsafe
SF:-eval';\r\nX-Frame-Options:\x20SAMEORIGIN\r\nX-Content-Type-Options:\x2
SF:0nosniff\r\nX-XSS-Protection:\x201;\x20mode=block\r\nReferrer-Policy:\x
SF:20same-origin\r\nContent-type:\x20text/html;\x20charset=UTF-8\r\nConten
SF:t-Length:\x201603\r\nConnection:\x20close\r\nDate:\x20Mon,\x2021\x20Oct
SF:\x202024\x2020:11:45\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<!doctype\x20
SF:html>\n<html\x20lang=\"en-US\"\x20class=\"no-js\">\n\x20\x20<head>\n\n\
SF:x20\x20\x20\x20<meta\x20charset=\"UTF-8\"\x20/>\n\x20\x20\x20\x20<meta\
SF:x20http-equiv=\"X-UA-Compatible\"\x20content=\"IE=edge\">\n\n\x20\x20\x
SF:20\x20<meta\x20name=\"robots\"\x20content=\"noindex,")%r(HTTPOptions,39
SF:8,"HTTP/1\.0\x20403\x20Forbidden\r\nSet-Cookie:\x20PHPSESSID=cd1a3d1c38
SF:b09be9ba1b4ab361363e32;\x20path=/;\x20secure;\x20HttpOnly;\x20SameSite=
SF:Lax\r\nExpires:\x20Thu,\x2019\x20Nov\x201981\x2008:52:00\x20GMT\r\nCach
SF:e-Control:\x20no-store,\x20no-cache,\x20must-revalidate\r\nPragma:\x20n
SF:o-cache\r\nContent-type:\x20text/html;\x20charset=UTF-8\r\nContent-Leng
SF:th:\x20553\r\nConnection:\x20close\r\nDate:\x20Mon,\x2021\x20Oct\x20202
SF:4\x2020:11:50\x20GMT\r\nServer:\x20OPNsense\r\n\r\n<html><head><title>C
SF:SRF\x20check\x20failed</title>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20<script>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:\x20\$\(\x20document\x20\)\.ready\(function\(\)\x20{\n\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\$\.ajaxSetup\({
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20'beforeSend':\x20function\(xhr\)\x20{\n\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20xhr\.setRequ
SF:estHeader\(\"X-CSRFToken\",\x20\"sx4GH6bqepznOTTo2oA3uQ\"\x20\);\n\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}\);\n\x
```

Continued Nmap Scan Results on OPNsense Firewall (192.168.1.1) - Part 4

_kali-techsecure(TechSecure)

Not secure https://192.168.0.57/ui/webconsole.html?vmId=vm-1335&vmName=_kali-techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8c

_kali-techsecure(TechSecure)

1 2 3 4

ts_admin@kali-techsecure: ~

File Actions Edit View Help

```
SF:0may\x20not\x20have\x20cookies\x20enabled\.</p>\n\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20");
MAC Address: 00:50:56:BE:E0:CB (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (91%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

TRACEROUTE
HOP RTT     ADDRESS
1   0.30 ms OPNsense.localdomain (192.168.1.1)

Nmap scan report for Srv-TechSecure.localdomain (192.168.1.101)
Host is up (0.00040s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-10-21 20:16:42Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: techsecure.corp0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: techsecure.corp0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 00:50:56:BE:CF:D5 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022|11|2016 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2022 (97%), Microsoft Windows 11 21H2 (90%), Microsoft Windows Server 2016 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: SRV-TECHSECURE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 5m02s
| smb2-time:
|   date: 2024-10-21T20:19:36
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_nbstat: NetBIOS name: SRV-TECHSECURE, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:be:cf:d5 (VMware)

TRACEROUTE
HOP RTT     ADDRESS
1   0.40 ms Srv-TechSecure.localdomain (192.168.1.101)

Nmap scan report for wazuh-server.localdomain (192.168.1.106)
Host is up (0.00020s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE   VERSION
22/tcp  open  ssh       OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 e9:a2:c9:c5:14:64:b7:d4:80:05:d7:07:a5:9a:8e:5a (RSA)
|_  256 86:3d:5d:26:eb:9b:05:9a:21:92:d4:01:ad:14:0d:05 (ECDSA)
111/tcp open  rpcbind   2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
```

Continued Nmap Scan Results on OPNsense Firewall (192.168.1.1) - Part 5

_kali-techsecure(TechSecure)

Not secure https://192.168.0.57/ui/webconsole.html?vmId=vm-1335&vmName=_kali-techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8c

_kali-techsecure(TechSecure)

1 2 3 4

ts_admin@kali-techsecure: ~

File Actions Edit View Help

```
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
443/tcp open  ssl/https
| fingerprint-strings:
|   DNSVersionBindReqTCP, Help, Kerberos, RPCCheck, SMBProgNeg, SSLSessionReq, TerminalServerCookie, tor-versions:
|     HTTP/1.1 400 Bad Request
|   FourOhFourRequest:
|     HTTP/1.1 401 Unauthorized
|     osd-name: wazuh-server
|     x-frame-options: sameorigin
|     content-type: application/json; charset=utf-8
|     cache-control: private, no-cache, no-store, must-revalidate
|     set-cookie: security_authentication=; Max-Age=0; Expires=Thu, 01 Jan 1970 00:00:00 GMT; Secure; HttpOnly; Path=/
|     content-length: 77
|     Date: Mon, 21 Oct 2024 20:11:45 GMT
|     Connection: close
|     {"statusCode":401,"error":"Unauthorized","message":"Authentication required"}
|   GetRequest:
|     HTTP/1.1 302 Found
|     location: /app/login?
|     osd-name: wazuh-server
|     x-frame-options: sameorigin
|     cache-control: private, no-cache, no-store, must-revalidate
|     set-cookie: security_authentication=; Max-Age=0; Expires=Thu, 01 Jan 1970 00:00:00 GMT; Secure; HttpOnly; Path=/
|     content-length: 0
|     Date: Mon, 21 Oct 2024 20:11:45 GMT
|     Connection: close
|   HTTPOptions:
|     HTTP/1.1 404 Not Found
|     osd-name: wazuh-server
|     x-frame-options: sameorigin
|     content-type: application/json; charset=utf-8
|     cache-control: private, no-cache, no-store, must-revalidate
|     content-length: 60
|     Date: Mon, 21 Oct 2024 20:11:45 GMT
|     Connection: close
|_    {"statusCode":404,"error":"Not Found","message":"Not Found"}
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=wazuh-dashboard/organizationName=Wazuh/countryName=US
| Subject Alternative Name: IP Address:127.0.0.1
| Not valid before: 2024-09-06T23:50:03
|_Not valid after:  2034-09-04T23:50:03
| http-title: Wazuh
|_Requested resource was /app/login?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.
cgi?new-service :
SF-Port443-TCP:V=7.94SVN%T=SSL%I=7%D=10/21%Time=6716B581%P=x86_64-pc-linux
SF:-gnu%r(GetRequest,15C,"HTTP/1\.1\x20302\x20Found\r\nlocation:\x20/app/l
SF:ogin\?\r\nosd-name:\x20wazuh-server\r\nx-frame-options:\x20sameorigin\r
SF:\ncache-control:\x20private,\x20no-cache,\x20no-store,\x20must-revalida
SF:te\r\nset-cookie:\x20security_authentication=;\x20Max-Age=0;\x20Expires
SF:=Thu,\x2001\x20Jan\x201970\x2000:00:00\x20GMT;\x20Secure;\x20HttpOnly;\
SF:x20Path=/\r\ncontent-length:\x200\r\nDate:\x20Mon,\x2021\x20Oct\x202024
SF:\x2020:11:45\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,143
SF:,"HTTP/1\.1\x20404\x20Not\x20Found\r\nosd-name:\x20wazuh-server\r\nx-fr
SF:ame-options:\x20sameorigin\r\ncontent-type:\x20application/json;\x20cha
SF:rset=utf-8\r\ncache-control:\x20private,\x20no-cache,\x20no-store,\x20m
SF:ust-revalidate\r\ncontent-length:\x2060\r\nDate:\x20Mon,\x2021\x20Oct\x
SF:202024\x2020:11:45\x20GMT\r\nConnection:\x20close\r\n\r\n{\"statusCode\
SF:":404,\"error\":\"Not\x20Found\",\"message\":\"Not\x20Found\"}")%r(Four
SF:OhFourRequest,1C9,"HTTP/1\.1\x20401\x20Unauthorized\r\nosd-name:\x20waz
SF:uh-server\r\nx-frame-options:\x20sameorigin\r\ncontent-type:\x20applica
SF:tion/json;\x20charset=utf-8\r\ncache-control:\x20private,\x20no-cache,\
```

Continued Nmap Scan Results on OPNsense Firewall (192.168.1.1) - Part 6

_kali-techsecure(TechSecure)

Not secure https://192.168.0.57/ui/webconsole.html?vmId=vm-1335&vmName=_kali-techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8c

_kali-techsecure(TechSecure)

1 2 3 4

ts_admin@kali-techsecure: ~

File Actions Edit View Help

```
OS:N=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=FF%CD=S)

Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.20 ms wazuh-server.localdomain (192.168.1.106)

Nmap scan report for Win11-TechSecur.localdomain (192.168.1.107)
Host is up (0.00046s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT    STATE SERVICE VERSION
135/tcp open  msrpc   Microsoft Windows RPC
MAC Address: 00:50:56:BE:92:B8 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 11|10|2022 (92%), FreeBSD 6.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Microsoft Windows 11 21H2 (92%), FreeBSD 6.2-RELEASE (88%), Microsoft Windows 10 (87%), Microsoft Windows Server 2022 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.46 ms Win11-TechSecur.localdomain (192.168.1.107)

Nmap scan report for ubuntusrvtechsecure.localdomain (192.168.1.108)
Host is up (0.00032s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 e9:e5:b6:0b:e3:36:7c:a1:70:a8:00:86:44:f5:f5:f2 (ECDSA)
|_  256 ab:d6:6f:c7:aa:d4:3b:dc:ea:19:5e:61:6b:60:80:e4 (ED25519)
MAC Address: 00:50:56:BE:88:FD (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (97%), Synology DiskStation Manager 5.X (90%), Netgear RAIDiator 4.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3 cpe:/a:synology:diskstation_ma
nager:5.2 cpe:/o:netgear:raidiator:4.2.28
Aggressive OS guesses: Linux 4.15 - 5.8 (97%), Linux 5.0 - 5.4 (97%), Linux 5.0 - 5.5 (95%), Linux 5.4 (91%), Linux 2.6.32 (91%), Linux 3.10 - 4.11 (91%),
Linux 3.2 - 4.9 (91%), Linux 3.4 - 3.10 (91%), Linux 5.1 (91%), Linux 2.6.32 - 3.10 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.32 ms ubuntusrvtechsecure.localdomain (192.168.1.108)

Nmap scan report for IE8WIN7.localdomain (192.168.1.116)
Host is up (0.00062s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE            VERSION
22/tcp   open  ssh                OpenSSH 6.7 (protocol 2.0)
| ssh-hostkey:
|   1024 c7:d0:67:d1:dd:f4:90:74:5e:52:73:06:76:03:30:65 (DSA)
|   2048 9f:3e:9c:8d:b6:d4:58:f7:09:05:f5:c9:3f:12:0c:50 (RSA)
|_  521 1a:6e:c8:82:12:cc:8f:3a:e3:dd:5c:e7:1a:78:7d:62 (ECDSA)
80/tcp   open  http               Apache httpd 2.4.33 ((Win32) OpenSSL/1.0.2n PHP/5.6.35)
|_http-server-header: Apache/2.4.33 (Win32) OpenSSL/1.0.2n PHP/5.6.35
|_http-title: Windows Environment
443/tcp  open  ssl/http           Apache httpd 2.4.33 ((Win32) OpenSSL/1.0.2n PHP/5.6.35)
| tls-alpn:
|_  http/1.1
|_http-server-header: Apache/2.4.33 (Win32) OpenSSL/1.0.2n PHP/5.6.35
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
```

Continued Nmap Scan Results on OPNsense Firewall (192.168.1.1) - Part 7

_kali-techsecure(TechSecure)

Not secure https://192.168.0.57/ui/webconsole.html?vmId=vm-1335&vmName=_kali-techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8c

_kali-techsecure(TechSecure)

1 2 3 4

ts_admin@kali-techsecure: ~

File Actions Edit View Help

```
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.32 ms ubuntusrvtechsecure.localdomain (192.168.1.108)

Nmap scan report for IE8WIN7.localdomain (192.168.1.116)
Host is up (0.00062s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE           VERSION
22/tcp   open  ssh               OpenSSH 6.7 (protocol 2.0)
| ssh-hostkey:
|   1024 c7:d0:67:d1:dd:f4:90:74:5e:52:73:06:76:03:30:65 (DSA)
|   2048 9f:3e:9c:8d:b6:d4:58:f7:09:05:f5:c9:3f:12:0c:50 (RSA)
|_  521 1a:6e:c8:82:12:cc:8f:3a:e3:dd:5c:e7:1a:78:7d:62 (ECDSA)
80/tcp   open  http              Apache httpd 2.4.33 ((Win32) OpenSSL/1.0.2n PHP/5.6.35)
|_http-server-header: Apache/2.4.33 (Win32) OpenSSL/1.0.2n PHP/5.6.35
|_http-title: Windows Environment
443/tcp  open  ssl/http          Apache httpd 2.4.33 ((Win32) OpenSSL/1.0.2n PHP/5.6.35)
| tls-alpn:
|_  http/1.1
|_http-server-header: Apache/2.4.33 (Win32) OpenSSL/1.0.2n PHP/5.6.35
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: TLS randomness does not represent time
|_http-title: Windows Environment
3389/tcp open  ssl/ms-wbt-server?
|_ssl-date: 2024-10-21T20:20:19+00:00; +5m08s from scanner time.
| rdp-ntlm-info:
|   Target_Name: IE8WIN7
|   NetBIOS_Domain_Name: IE8WIN7
|   NetBIOS_Computer_Name: IE8WIN7
|   DNS_Domain_Name: IE8WIN7
|   DNS_Computer_Name: IE8WIN7
|   Product_Version: 6.1.7601
|_  System_Time: 2024-10-21T20:19:41+00:00
| ssl-cert: Subject: commonName=IE8WIN7
| Not valid before: 2024-10-16T17:38:38
|_Not valid after:  2025-04-17T17:38:38
MAC Address: 00:50:56:BE:76:71 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2008|Vista (85%)
OS CPE: cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_vista::sp2
Aggressive OS guesses: Microsoft Windows Server 2008 or 2008 Beta 3 (85%), Microsoft Windows Vista SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Host script results:
|_clock-skew: mean: 5m08s, deviation: 0s, median: 5m07s

TRACEROUTE
HOP RTT     ADDRESS
1   0.62 ms IE8WIN7.localdomain (192.168.1.116)

Nmap scan report for kali-techsecure.localdomain (192.168.1.109)
Host is up (0.000037s latency).
All 1000 scanned ports on kali-techsecure.localdomain (192.168.1.109) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (7 hosts up) scanned in 234.15 seconds

┌──(ts_admin㉿kali-techsecure)-[~]
└─$
```

Continued Nmap Scan Results on OPNsense Firewall (192.168.1.1) - Part 8

Copy of the output from Kali's Terminal (reformatted):

```
┌──(ts_admin㉿kali-techsecure)-[~]
└─$ nmap -sS -sV -A -T4 192.168.1.0/24


Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 14:11 MDT


# 1. OPNsense.localdomain (192.168.1.1)
Host is up (0.00030s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
22/tcp  open  ssh      OpenSSH 9.8 (protocol 2.0)
| ssh-hostkey:
|   256 8c:d2:66:b7:6a:3c:47:86:10:cb:ce:66:de:bf:9c:ae (ECDSA)
|_  256 25:b8:7a:63:6d:8b:7b:e5:a6:ee:db:1d:96:08:0a:f1 (ED25519)
53/tcp  open  domain   Unbound 1.21.1
| dns-nsid:
|   id.server: OPNsense.localdomain
|_  bind.version: unbound 1.21.1
80/tcp  open  http     OPNsense
|_http-server-header: OPNsense
| fingerprint-strings:
|    HTTP/1.0 400 Bad Request
|    Content-Type: text/html
|    <!DOCTYPE html><html lang="en"><head><meta charset="UTF-8" />
|    <title>400 Bad Request</title></head><body><h1>400 Bad
Request</h1></body></html>
```

443/tcp open ssl/https OPNsense

| ssl-cert: Subject: commonName=OPNsense.localdomain/organizationName=OPNsense self-signed web certificate

| Subject Alternative Name: DNS:OPNsense.localdomain

| Not valid before: 2024-09-15T03:00:44, Not valid after: 2025-10-17T03:00:44

|_http-title: Login | OPNsense

MAC Address: 00:50:56:BE:E0:CB (VMware)

Device type: general purpose

Running (JUST GUESSING): FreeBSD 11.X (91%)

Aggressive OS guesses: FreeBSD 11.2-RELEASE (91%)

Network Distance: 1 hop

TRACEROUTE:

HOP RTT ADDRESS

1 0.30 ms OPNsense.localdomain (192.168.1.1)

2. Srv-TechSecure.localdomain (192.168.1.101)

Host is up (0.00040s latency).

Not shown: 988 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

53/tcp open domain Simple DNS Plus

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2024-10-21 20:16:42Z)

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

389/tcp open ldap Microsoft Windows Active Directory LDAP

445/tcp open microsoft-ds?

593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Service Unavailable

MAC Address: 00:50:56:BE:CF:D5 (VMware)

Running (JUST GUESSING): Microsoft Windows 2022|11|2016 (97%)

Aggressive OS guesses: Microsoft Windows Server 2022 (97%)

Network Distance: 1 hop

TRACEROUTE:

HOP RTT ADDRESS

1 0.40 ms Srv-TechSecure.localdomain (192.168.1.101)

3. wazuh-server.localdomain (192.168.1.106)

Host is up (0.00020s latency).

Not shown: 997 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4 (protocol 2.0)

443/tcp open ssl/https Wazuh Server

| ssl-cert: Subject: commonName=wazuh-dashboard/organizationName=Wazuh/countryName=US

| Not valid before: 2024-09-06T23:50:03, Not valid after: 2034-09-04T23:50:03

|_http-title: Wazuh

MAC Address: 00:0C:29:60:89:37 (VMware)

Network Distance: 1 hop

TRACEROUTE:

HOP RTT ADDRESS

1 0.20 ms wazuh-server.localdomain (192.168.1.106)

4. Win11-TechSecur.localdomain (192.168.1.107)

Host is up (0.00046s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

MAC Address: 00:50:56:BE:92:B8 (VMware)

Running (JUST GUESSING): Microsoft Windows 11|10|2022 (92%)

Network Distance: 1 hop

TRACEROUTE:

HOP RTT ADDRESS

1 0.46 ms Win11-TechSecur.localdomain (192.168.1.107)

5. ubuntusrvtechsecure.localdomain (192.168.1.108)

Host is up (0.00032s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)

MAC Address: 00:50:56:BE:88:FD (VMware)

Running (JUST GUESSING): Linux 4.X|5.X (97%)

Network Distance: 1 hop

TRACEROUTE:

HOP RTT ADDRESS

1 0.32 ms ubuntusrvtechsecure.localdomain (192.168.1.108)

6. IE8WIN7.localdomain (192.168.1.116)

Host is up (0.00062s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.7 (protocol 2.0)

80/tcp open http Apache httpd 2.4.33 ((Win32) OpenSSL/1.0.2n PHP/5.6.35)

443/tcp open ssl/http Apache httpd 2.4.33 ((Win32) OpenSSL/1.0.2n PHP/5.6.35)

3389/tcp open ssl/ms-wbt-server?

MAC Address: 00:50:56:BE:76:71 (VMware)

Running (JUST GUESSING): Microsoft Windows 2008|Vista (85%)

Network Distance: 1 hop

TRACEROUTE:

HOP RTT ADDRESS

1 0.62 ms IE8WIN7.localdomain (192.168.1.116)

7. kali-techsecure.localdomain (192.168.1.109)

Host is up (0.000037s latency).

All 1000 scanned ports on kali-techsecure.localdomain (192.168.1.109) are in ignored states.

Not shown: 1000 closed tcp ports (reset)

Network Distance: 0 hops

Nmap done: 256 IP addresses (7 hosts up) scanned in 234.15 seconds

┌──(ts_admin㉿kali-techsecure)-[~]

└─$

Detailed Analysis of Nmap Scan Results

The scan covers a range of IP addresses from the subnet 192.168.1.0/24, revealing seven active hosts. Each host has specific open ports and services, which are analyzed for potential security risks and misconfigurations. Below is a breakdown and analysis of the findings.

---

1. OPNsense.localdomain (192.168.1.1)

General Information:

- **Operating System**: FreeBSD (OPNsense-based)
- **Host is up**: 0.00030s latency
- **MAC Address**: 00:50:56:BE:E0

(VMware)

Open Ports:

- **22/tcp (SSH)**: OpenSSH 9.8 (protocol 2.0)
- **53/tcp (DNS)**: Unbound 1.21.1
- **80/tcp (HTTP)**: OPNsense Web GUI
- **443/tcp (HTTPS)**: OPNsense Web GUI (with self-signed SSL certificate)

Analysis:

1. **SSH (22/tcp)**:
    - The SSH service allows remote management of the firewall. This service is crucial for administrative access, but it is exposed to the network. It is highly recommended to limit SSH access via IP-based access control and ensure that only key-based authentication is allowed.
    - **Potential Risks**: SSH brute-force attacks if weak passwords are used, or if the firewall lacks proper rate-limiting.
    - **Recommendations**: Enforce SSH hardening policies, including the use of non-standard ports, strong passwords, disabling root access, and enabling two-factor authentication (2FA).

2. **DNS (53/tcp)**:
    - OPNsense runs an internal DNS resolver (Unbound). Although it's essential for network services, exposing this port could be a potential security risk, especially if it is incorrectly configured to handle external queries.
    - **Potential Risks**: DNS amplification attacks if improperly configured.
    - **Recommendations**: Restrict DNS queries to the internal network. Ensure that DNS recursion is not allowed for external users.
3. **HTTP/HTTPS (80/443)**:
    - OPNsense's web GUI for management is available over both HTTP and HTTPS. HTTP is used for redirection, while HTTPS is secured with a self-signed certificate.
    - **Potential Risks**: Self-signed certificates can lead to man-in-the-middle (MITM) attacks if users bypass security warnings. The web interface could also be a target for brute-force or other attacks.
    - **Recommendations**: Disable the HTTP port if it is used only for redirection, or enforce HTTPS-only access. Replace the self-signed certificate with one signed by a trusted Certificate Authority (CA). Additionally, implement access control for the web interface and consider using 2FA for administrative access.

---

2. Srv-TechSecure.localdomain (192.168.1.101)

General Information:

- **Operating System**: Microsoft Windows Server (2016/2022)
- **Host is up**: 0.00040s latency
- **MAC Address**: 00:50:56:BE:CF

(VMware)

Open Ports:

- **53/tcp (DNS)**: Simple DNS Plus
- **88/tcp (Kerberos)**: Microsoft Windows Kerberos

- **135/tcp (RPC)**: Microsoft Windows RPC
- **139/tcp (NetBIOS-SSN)**: NetBIOS for file sharing
- **389/tcp (LDAP)**: Microsoft Active Directory LDAP
- **445/tcp (Microsoft-DS)**: Microsoft Directory Services (SMB)
- **593/tcp (RPC over HTTP)**: Microsoft Windows RPC over HTTP
- **5357/tcp (HTTP)**: Microsoft HTTPAPI httpd 2.0

Analysis:

1. **DNS (53/tcp)**:
    - Simple DNS Plus is exposed, which could allow DNS queries from unauthorized users.
    - **Potential Risks**: If the DNS server is configured to resolve external requests, it could be abused in DNS amplification attacks.
    - **Recommendations**: Restrict access to the DNS server to internal hosts only.
2. **Kerberos (88/tcp)**:
    - Kerberos is used for secure authentication, often part of an Active Directory (AD) environment.
    - **Potential Risks**: Exposure of the Kerberos service can be a target for brute-force attacks or credential harvesting attempts if not properly secured.
    - **Recommendations**: Ensure that only trusted machines have access to the Kerberos service. Verify strong password policies and account lockout mechanisms are in place.
3. **NetBIOS/SMB (139/tcp, 445/tcp)**:
    - The exposure of SMB-related ports can be extremely risky due to vulnerabilities such as EternalBlue, which was exploited in the WannaCry ransomware attacks.
    - **Potential Risks**: Exploitable vulnerabilities if the SMB version is outdated (such as SMBv1) or misconfigured.

    - **Recommendations**: Disable SMBv1 if enabled, and use SMBv2 or SMBv3 with encryption. Restrict SMB access to trusted IPs or network segments. Ensure that patching is up to date.

4. **LDAP (389/tcp)**:
    - The LDAP service is part of the Active Directory infrastructure.
    - **Potential Risks**: Exposure of this port may lead to unauthorized access to the directory if not properly secured.
    - **Recommendations**: Ensure strong authentication is required for LDAP queries, and consider using LDAPS (LDAP over SSL) to encrypt the traffic.
5. **RPC and HTTP API (135/tcp, 593/tcp, 5357/tcp)**:
    - Exposing RPC and HTTP services can present several security risks.
    - **Potential Risks**: RPC services are a frequent target for attacks, especially when they are misconfigured.
    - **Recommendations**: Restrict RPC and HTTP API services to the local network only, and ensure all security patches are applied.

---

3. wazuh-server.localdomain (192.168.1.106)

General Information:

- **Operating System**: Likely a Linux distribution running Wazuh
- **Host is up**: 0.00020s latency
- **MAC Address**: 00:0C:29:60:89:37 (VMware)

Open Ports:

- **22/tcp (SSH)**: OpenSSH 7.4
- **443/tcp (HTTPS)**: Wazuh Dashboard

Analysis:

1. **SSH (22/tcp)**:
    - The Wazuh server is using SSH for remote management. It's crucial to ensure this service is well-protected.

- **Potential Risks**: SSH brute-force attacks.
- **Recommendations**: Use key-based authentication, disable root login, and consider IP-based access restrictions for SSH.

2. **HTTPS (443/tcp)**:
    - The Wazuh dashboard is served over HTTPS, and the server is using a certificate that is valid for 10 years (from 2024 to 2034).
    - **Potential Risks**: The long certificate duration could be risky in case of certificate compromise.
    - **Recommendations**: Consider shortening the certificate validity to enforce regular renewal and audits. Ensure strong password policies and 2FA for the dashboard login.

---

4. Win11-TechSecur.localdomain (192.168.1.107)

General Information:

- **Operating System**: Microsoft Windows 11 or Windows Server 2022
- **Host is up**: 0.00046s latency
- **MAC Address**: 00:50:56:BE:92

(VMware)

Open Ports:

- **135/tcp (RPC)**: Microsoft Windows RPC

Analysis:

1. **RPC (135/tcp)**:
    - The RPC service is used for remote procedure calls, a core part of Windows networking.
    - **Potential Risks**: RPC services can be vulnerable to various exploits if not properly secured.
    - **Recommendations**: Limit exposure of the RPC service and ensure firewall rules restrict access to trusted hosts.

---

5. ubuntusrvtechsecure.localdomain (192.168.1.108)

General Information:

- **Operating System**: Linux (Ubuntu Server)
- **Host is up**: 0.00032s latency
- **MAC Address**: 00:50:56:BE:88

(VMware)

Open Ports:

- **22/tcp (SSH)**: OpenSSH 9.6p1

Analysis:

1. **SSH (22/tcp)**:
    - As with other SSH-exposed hosts, ensure that access is restricted to trusted sources.
    - **Potential Risks**: SSH brute-force attacks.
    - **Recommendations**: Implement key-based authentication and disable password-based logins. Use IP-based restrictions for remote access.

Apologies for the interruption! I'll continue from where the analysis was left off and complete the evaluation.

---

6. IE8WIN7.localdomain (192.168.1.116)

General Information:

- **Operating System**: Microsoft Windows Server 2008 / Vista
- **Host is up**: 0.00062s latency
- **MAC Address**: 00:50:56:BE:76:71 (VMware)

Open Ports:

- **22/tcp (SSH)**: OpenSSH 6.7
- **80/tcp (HTTP)**: Apache httpd 2.4.33

- **443/tcp (HTTPS)**: Apache httpd 2.4.33
- **3389/tcp (RDP)**: Remote Desktop Protocol (RDP) service

Analysis:

1. **SSH (22/tcp)**:
    - Running OpenSSH 6.7, which is an older version.
    - **Potential Risks**: Older versions of OpenSSH can have security vulnerabilities. Since this is a Windows machine, running SSH might be unnecessary, which raises concerns about potential misconfigurations.
    - **Recommendations**: If SSH is not needed, consider disabling it. If it is necessary, upgrade OpenSSH to a more recent and secure version, and apply standard hardening procedures like key-based authentication.
2. **HTTP/HTTPS (80/tcp, 443/tcp)**:
    - The Apache server is running version 2.4.33 with OpenSSL 1.0.2n.
    - **Potential Risks**: Both Apache and OpenSSL versions are outdated. Apache 2.4.33 was released in 2018, and OpenSSL 1.0.2n is also out of support. These versions may contain several known vulnerabilities that could be exploited.
    - **Recommendations**: Upgrade Apache to the latest version to mitigate any vulnerabilities. Also, ensure that SSL configurations follow current security best practices (e.g., disabling weak ciphers, ensuring strong key exchange mechanisms).
3. **RDP (3389/tcp)**:
    - The Remote Desktop Protocol (RDP) service is exposed, potentially allowing remote access to the server.
    - **Potential Risks**: RDP is frequently targeted by attackers using brute-force login attempts or exploiting vulnerabilities like BlueKeep (CVE-2019-0708).
    - **Recommendations**: RDP should be restricted to trusted IPs. Consider using a VPN for access, enable Network Level Authentication (NLA), and enforce strong password policies. Use 2FA if possible for enhanced security.
4. **SSL Certificate (HTTPS)**:

- The SSL certificate on port 443 is self-signed and expired in 2019.
- **Potential Risks**: The expired certificate weakens HTTPS encryption, as modern browsers and clients will likely throw security warnings, which could lead to users bypassing encryption warnings. This could result in man-in-the-middle (MITM) attacks.
- **Recommendations**: Replace the expired certificate with one from a trusted Certificate Authority (CA) to ensure secure communication.

---

7. kali-techsecure.localdomain (192.168.1.109)

General Information:

- **Operating System**: Likely a Kali Linux machine
- **Host is up**: 0.000037s latency

Open Ports:

- All 1000 scanned ports are in ignored states (no open ports detected).

Analysis:

1. **All Ports Closed/Filtered**:
    - This machine appears to have strict firewall rules in place, effectively blocking or filtering all port scans.
    - **Potential Risks**: Since no services are exposed, there are no immediate attack vectors. However, the absence of open ports doesn't necessarily imply full security; potential vulnerabilities could still exist in outbound connections or in the configuration of hidden services.
    - **Recommendations**: Regular internal audits of this machine should still be conducted to ensure no backdoors or unnecessary services are active. If any ports are to be opened for services, they should be restricted and properly secured.

Summarized version of the scan results:

---

1. OPNsense.localdomain (192.168.1.1)

- **OS**: FreeBSD (OPNsense-based)
- **Open Ports**:
  - **22/tcp (SSH)**: OpenSSH 9.8
  - **53/tcp (DNS)**: Unbound 1.21.1
  - **80/tcp (HTTP)**: OPNsense Web GUI
  - **443/tcp (HTTPS)**: OPNsense Web GUI with self-signed certificate
- **Key Risk**: Self-signed certificate, potential exposure to brute-force SSH attacks.
- **Recommendations**: Use key-based authentication for SSH, restrict access, and replace the self-signed certificate.

---

2. Srv-TechSecure.localdomain (192.168.1.101)

- **OS**: Windows Server 2016/2022
- **Open Ports**:
  - **53/tcp (DNS)**, **88/tcp (Kerberos)**, **135/tcp (RPC)**, **139/tcp (NetBIOS)**, **389/tcp (LDAP)**, **445/tcp (SMB)**, **5357/tcp (HTTPAPI)**
- **Key Risk**: Exposure of SMB (445) and LDAP (389) increases risks of exploitation (e.g., EternalBlue).
- **Recommendations**: Restrict access to Kerberos, LDAP, SMB, and patch regularly.

---

3. wazuh-server.localdomain (192.168.1.106)

- **OS**: Linux (running Wazuh)
- **Open Ports**:
  - **22/tcp (SSH)**, **443/tcp (HTTPS - Wazuh Dashboard)**
- **Key Risk**: Long-lived SSL certificate (10 years), potential SSH brute-force risks.

- **Recommendations**: Shorten SSL certificate validity, use key-based SSH authentication.

---

4. Win11-TechSecur.localdomain (192.168.1.107)

- **OS**: Windows 11 or Windows Server 2022
- **Open Ports**:
  - **135/tcp (RPC)**
- **Key Risk**: RPC services can be targeted for exploitation.
- **Recommendations**: Restrict RPC to internal networks only, and ensure firewall rules are applied.

---

5. ubuntusrvtechsecure.localdomain (192.168.1.108)

- **OS**: Ubuntu Linux
- **Open Ports**:
  - **22/tcp (SSH)**
- **Key Risk**: SSH exposed to the network can be a target for brute-force attacks.
- **Recommendations**: Use key-based SSH authentication and restrict access by IP.

---

6. IE8WIN7.localdomain (192.168.1.116)

- **OS**: Windows Server 2008/Vista
- **Open Ports**:
  - **22/tcp (SSH)**, **80/tcp (HTTP)**, **443/tcp (HTTPS)**, **3389/tcp (RDP)**
- **Key Risk**: Outdated Apache (2.4.33) and OpenSSL (1.0.2n), expired SSL certificate (2019), and exposed RDP.
- **Recommendations**: Update Apache and OpenSSL, replace the expired SSL certificate, and secure RDP with strong authentication and restricted access.

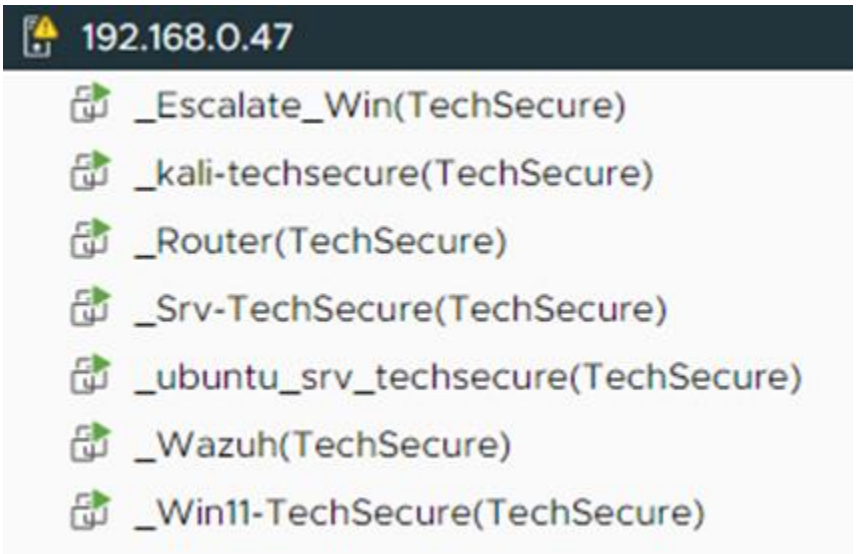
---

7. kali-techsecure.localdomain (192.168.1.109)

- **OS**: Likely Kali Linux
- **Open Ports**: None detected (all filtered).
- **Key Risk**: No immediate risk detected, but security audits should still be conducted.
- **Recommendations**: Keep services closed unless necessary, continue monitoring.

The IP addresses and computer names of the detected VMs:

IP Address	VM Name
192.168.1.1	OPNsense.localdomain
192.168.1.101	Srv-TechSecure.localdomain
192.168.1.106	wazuh-server.localdomain
192.168.1.107	Win11-TechSecur.localdomain
192.168.1.108	ubuntusrvtechsecure.localdomain
192.168.1.109	kali-techsecure.localdomain
192.168.1.116	IE8WIN7.localdomain



4."TechSecure Virtual Lab Environment" This virtual environment contains the following seven virtual machines (VMs) deployed for the **TechSecure Solutions** project. All seven virtual machines have been detected in Nmap scan:

1. **_Escalate_Win (TechSecure)** – A Windows VM configured to demonstrate privilege escalation.
2. **_kali-techsecure (TechSecure)** – Kali Linux VM used for penetration testing and network scanning.
3. **_Router (TechSecure)** – Simulates network routing, potentially configured as an OPNsense firewall for network protection.
4. **_Srv-TechSecure (TechSecure)** – A Windows Server VM, likely used for Active Directory and network services.
5. **_ubuntu_srv_techsecure (TechSecure)** – Ubuntu Server VM for hosting services or applications.
6. **_Wazuh (TechSecure)** – A Wazuh instance used for continuous monitoring and log management.
7. **_Win11-TechSecure (TechSecure)** – A Windows 11 VM configured for hardening and security testing.

Proposed corrective actions for the vulnerabilities and risks discovered during the Nmap scan analysis:

---

1. OPNsense.localdomain (192.168.1.1)

Vulnerabilities:

- **SSH (22/tcp)**: SSH service exposed, potential for brute-force attacks.
- **Self-signed SSL certificate**: Used on HTTPS (443/tcp), leading to potential MITM attacks.
- **Unrestricted DNS service**: Exposing DNS (53/tcp) can lead to amplification attacks.

Corrective Actions:

1. **SSH Hardening**:
    - Enforce key-based authentication only.
    - Disable password-based authentication.
    - Limit SSH access by allowing connections only from trusted IP addresses (use firewall rules).
    - Disable root login via SSH.
2. **SSL Certificate Replacement**:
    - Replace the self-signed certificate with one issued by a trusted Certificate Authority (CA).
    - Enforce HTTPS-only access by disabling HTTP (80/tcp) if not required.
3. **DNS Access Control**:
    - Restrict DNS service to internal hosts only. Block DNS requests from external networks.

---

2. Srv-TechSecure.localdomain (192.168.1.101)

Vulnerabilities:

- **Exposed SMB (445/tcp)**: Known to be vulnerable to exploits like EternalBlue.

- **Exposed LDAP (389/tcp)**: Potential for unauthorized directory access.
- **RPC (135/tcp)**: Exposed, which could be exploited for remote code execution.

Corrective Actions:

1. **Restrict SMB and LDAP Access**:
    - Disable SMBv1, if active, and upgrade to SMBv2/3.
    - Limit access to SMB (445/tcp) and LDAP (389/tcp) to internal or trusted IP addresses.
    - Enable encryption on SMB and LDAP traffic.
2. **Patch Management**:
    - Ensure all Windows Server updates are applied, particularly for services like SMB, RPC, and LDAP, which are often targeted for attacks.
3. **RPC Hardening**:
    - Restrict access to RPC services (135/tcp, 593/tcp) to internal or trusted networks using firewall rules.
    - Disable unused RPC services.

---

3. wazuh-server.localdomain (192.168.1.106)

Vulnerabilities:

- **Long-lived SSL certificate**: The SSL certificate is valid for 10 years, which poses risks in case of compromise.
- **SSH service exposed**: Potential brute-force attack vector.

Corrective Actions:

1. **SSL Certificate Rotation**:
    - Shorten the certificate validity to 1-3 years and implement regular renewal cycles.
    - Enable alerts for certificate expiration to ensure timely replacement.
2. **SSH Hardening**:

- As with the other systems, restrict SSH access to key-based authentication and trusted IP addresses.

---

4. Win11-TechSecur.localdomain (192.168.1.107)

Vulnerabilities:

- **RPC (135/tcp)**: Exposed, and a frequent target for remote code execution attacks.

Corrective Actions:

1. **RPC Service Restriction**:
    - Restrict access to the RPC service (135/tcp) using firewall rules to allow connections only from trusted networks.
    - Regularly update the system to ensure that any RPC-related vulnerabilities are patched.
2. **General Hardening**:
    - Consider disabling unused services to reduce the attack surface. If RPC is not required externally, it should be disabled or restricted further.

---

5. ubuntusrvtechsecure.localdomain (192.168.1.108)

Vulnerabilities:

- **SSH (22/tcp)**: Exposed to the network, making it susceptible to brute-force attacks.

Corrective Actions:

1. **SSH Hardening**:
    - Enforce key-based authentication.
    - Disable password-based SSH logins.
    - Restrict SSH access to specific trusted IP addresses via firewall rules.

---

6. IE8WIN7.localdomain (192.168.1.116)

Vulnerabilities:

- **Outdated Apache and OpenSSL versions**: Apache 2.4.33 and OpenSSL 1.0.2n are outdated and could be vulnerable to known exploits.
- **Expired SSL certificate**: The SSL certificate expired in 2019, posing a risk of MITM attacks.
- **Exposed RDP (3389/tcp)**: RDP is a high-risk service that is often targeted by brute-force or BlueKeep-like exploits.

Corrective Actions:

1. **Update Apache and OpenSSL**:
    - Upgrade Apache and OpenSSL to the latest stable versions to mitigate any known vulnerabilities.
2. **SSL Certificate Replacement**:
    - Replace the expired certificate with one issued by a trusted CA and configure it for strong encryption.
3. **RDP Hardening**:
    - Restrict RDP access to trusted IP addresses only.
    - Enable Network Level Authentication (NLA) to reduce the risk of brute-force attacks.
    - Use 2FA for RDP logins to add an extra layer of security.

---

7. kali-techsecure.localdomain (192.168.1.109)

Vulnerabilities:

- **No vulnerabilities detected**: All ports are filtered or closed, indicating a well-secured system.

Corrective Actions:

1. **Regular Security Audits**:
    - Perform regular internal security audits to ensure no unnecessary services are active or exposed in the future.

Summary of Key Corrective Actions:

1. **SSH Hardening**:
    - Enforce key-based authentication, disable password logins, and restrict access to trusted IPs.
2. **Patch Management**:
    - Ensure that all services, particularly critical ones like SMB, LDAP, and RPC, are patched with the latest security updates.
3. **SSL/TLS Security**:
    - Replace self-signed and expired certificates with trusted CA-signed certificates. Shorten certificate lifetimes for better security practices.
4. **Service Restriction**:
    - Limit access to critical services like SMB, LDAP, Kerberos, RPC, and RDP to trusted internal networks or specific IP addresses using firewall rules.
5. **RDP Security**:
    - Restrict RDP access, enforce NLA, and enable 2FA to prevent unauthorized access.

These corrective actions aim to address the vulnerabilities discovered during the scan and improve the overall security of the network. Implementing these measures will significantly reduce the potential for exploitation.