Vulnerability Assessment Report

Sam Whitehouse

Table of Contents

Executive Summary..... 3

Scan Results..... 3

Methodology..... 3

Findings.....4

- Linux Server : 172.16.14.52 4
- Windows 1 : 172.16.14.50 6
- Windows Server : 172.16.14.53 7

Risk Assessment.....8

- High Severity Vulnerabilities 9
- Medium Severity Vulnerabilities 10
- Low Severity Vulnerabilities 11

Recommendations.....12

References..... 13

Executive Summary

Vulnerability scans are a good source of information as to whether a company is resilient to a Cyber threat. One such scan was completed using Open VAS and analysed using the accompanying Greenbone interface. Vulnerabilities were identified by machine, risks to assets were identified and calculated for priority. Recommendations have been made for some minor, low complexity changes that will mitigate the risk almost completely. Some further recommendations were added to increase company Security Posture. Reference material has been provided in breadth in this report to aid in threat intelligence and incident preparation activities.

In short, default passwords must be changed immediately, Transport Layer Security should be updated as soon as possible, and, when budget allows, a firewall should be implemented to filter untrusted traffic. These remediations are relatively easy, and would cost a relatively small amount. If completed, the company would be much more resilient to bad faith internet traffic.

Scan Results

Greenbone readout is provided in **Findings** along with the breakdown of all the vulnerabilities according to corresponding Common Vulnerability Enumerations (CVEs) and mapped to related Common Weakness Enumerations (CWEs). This data can be used to isolate and remediate issues specific to network environment. The breadth of reference material provided was also intended to be used to develop internal Knowledge Base on topics covered and to aid in the Preparation stages of the Risk Management Process as well as the Incident Response Process, or to aid in Briefing executives in specifically requested elements of the data.

The **Risk Assessment** section following provides further information on each vulnerability, assessed severity levels in accordance with NIST framework, mapped to company impact and prioritized accordingly. Breadth of reference material included was also intended to develop Knowledge Base and provide resources for Executive Briefings. Mitigations are included and further explained along with the priority decisions making process in **Recommendations.**

Methodology

Scans were completed after hours on Wednesday February 7, 2024 using Greenbone application, on the “Full and Fast” setting, network discovery configured to ARP ping using a machine running Kali Linux specifically configured for the task. Vulnerabilities were enumerated, researched and analyzed for risk and impact to company assets. Wireshark was used to capture traffic from Kali machine to all targeted machines and logs were collected correlating to scan activities. All correlation data has been collected and is available for further analysis and development of Security functionality and Incident Response.

The Ubuntu server running Apache 2.4 (!72.16.14.52), the Windows server running Server 2022 (172.16.14.53) and the Windows 1 machine running Windows 10 (172.16.14.50) were selected to be scanned. Network infrastructure on Ips ranging from 172.16.14.0-3 were identified as being susceptible to impact from scan activities and were therefore removed from scan target list.

Findings

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	172.16.14.52		general/tcp	Sat, Feb 10, 2024 11:37 PM UTC
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	172.16.14.53	WIN-SERVER-2022	general/tcp	Sat, Feb 10, 2024 11:38 PM UTC
Report outdated / end-of-life Scan Engine / Environment (local)	10.0 (High)	97 %	172.16.14.50	DESKTOP-WIN10PR	general/tcp	Sat, Feb 10, 2024 11:38 PM UTC
HTTP Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	172.16.14.52		9200/tcp	Sat, Feb 10, 2024 11:54 PM UTC
Unprotected OSSEC/Wazuh ossec-authd (authd Protocol)	7.5 (High)	80 %	172.16.14.52		1515/tcp	Sat, Feb 10, 2024 11:40 PM UTC
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	5.0 (Medium)	70 %	172.16.14.52		1515/tcp	Sat, Feb 10, 2024 11:53 PM UTC
SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	5.0 (Medium)	70 %	172.16.14.52		55000/tcp	Sat, Feb 10, 2024 11:53 PM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	172.16.14.53	WIN-SERVER-2022	135/tcp	Sat, Feb 10, 2024 11:58 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	172.16.14.53	WIN-SERVER-2022	3389/tcp	Sat, Feb 10, 2024 11:54 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	98 %	172.16.14.50	DESKTOP-WIN10PR	3389/tcp	Sat, Feb 10, 2024 11:52 PM UTC

Table 1: Greenbone readout of network scan, organized by Vulnerability test

CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508	HTTP Brute Force Logins With Default Credentials Reporting	1	1	7.5 (High)
CVE-2011-1473 CVE-2011-5094	SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)	1	2	5.0 (Medium)
CVE-2011-3389 CVE-2015-0204	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	2	2	4.3 (Medium)
CVE-1999-0524	ICMP Timestamp Reply Information Disclosure	1	1	2.1 (Low)

Table 2: Greenbone readout of network scan, organized by Common Vulnerability Enumeration

Linux Server : 172.16.14.52

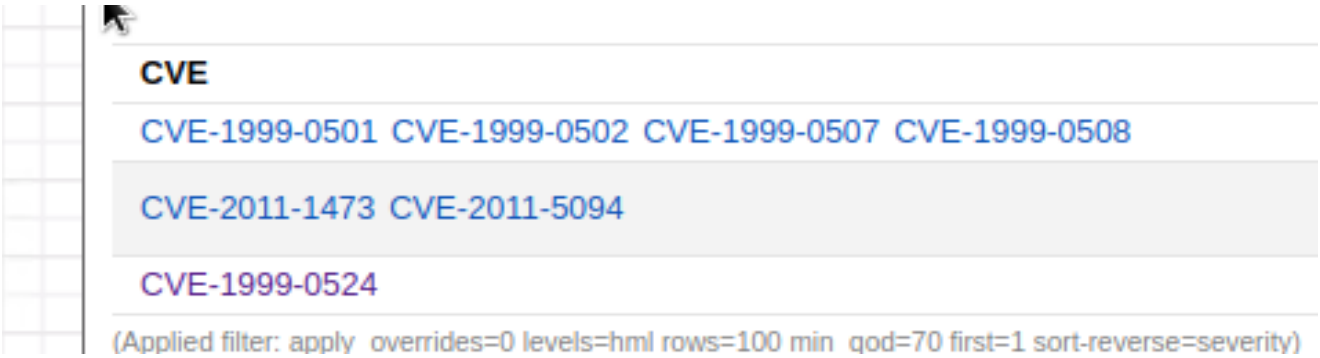

Table 3: Greenbone readout of network scan, organized by CVE for the Linux Server

1999-0501: CVE, NVD, Vendor Link (IBM), CVSS 3.0: NA, CVSS 2.0: 4.6 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

A Unix account has a guessable password.

1999-0502: CVE, NVD, Vendor (IBM), CVSS 3.0: NA, CVSS 2.0: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

A Unix account has a default, null, blank, or missing password.

1999-0507: CVE, NVD, CVSS 3.0: NA, CVSS 2.0: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

An account on a router, firewall, or other network device has a guessable password.(CVE)

1999-0508: CVE, NVD, Vendor (IBM), CVSS 3.0: NA, CVSS 2.0: 4.6 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

An account on a router, firewall, or other network device has a default, null, blank, or missing password

2011-1473: CVE, NVD, CVSS 3.0: NA, CVSS 2.0: 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

OpenSSL before 0.9.8l, and 0.9.8m through 1.x, does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection, a different vulnerability than CVE-2011-5094. NOTE: it can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment(CVE)

CWE - 264: Permissions, Privileges, and Access Controls
Weaknesses in this category are related to the management of permissions, privileges, and other security features that are used to perform access control.

2011-5094: CVE, NVD, CVSS 3.0: NA, CVSS 2.0: 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

Mozilla Network Security Services (NSS) 3.x, with certain settings of the SSL_ENABLE_RENEGOTIATION option, does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection, a different vulnerability than CVE-2011-1473. NOTE: it can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.

1999-0524: CVE, NVD, CWE CVSS 3.0: NA, CVSS2.0: 2.1 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts.

CWE – 200: Exposure of Sensitive Data to Unauthorized Actor

The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

Windows 1 : 172.16.14.50

CVE
CVE-2011-3389 CVE-2015-0204

Table 4: Greenbone readout of network scan, organized by CVE for Windows 1

2011-3389: CVE, NVD, CWE CVSS 3.0: NA, CVSS 2.0: 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.(CVE)

CWE: 326

The product stores or transmits sensitive data using an encryption scheme that is theoretically sound, but is not strong enough for the level of protection required.

A weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of succeeding using current attack methods and resources.(CWE)

2015-0204: CVE, NVD, CWE CVSS 3.0: NA, CVSS 2.0: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations.(CVE)

CWE: 310

Weaknesses in this category are related to the design and implementation of data confidentiality and integrity. Frequently these deal with the use of encoding techniques, encryption libraries, and hashing algorithms. The weaknesses in this category could lead to a degradation of the quality data if they are not addressed.(CWE)

Windows Server : 172.16.14.53

CVE
CVE-2011-3389 CVE-2015-0204

Table 5: Greenbone readout of network scan, organized by CVE for the Windows Server

2011-3389: CVE, NVD, CWE CVSS 3.0: NA, CVSS 2.0: 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.

CWE: 326

The product stores or transmits sensitive data using an encryption scheme that is theoretically sound, but is not strong enough for the level of protection required.

A weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of succeeding using current attack methods and resources.

2015-0204: CVE, NVD, CWE CVSS 3.0: NA, CVSS 2.0: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations.

CWE: 310

Weaknesses in this category are related to the design and implementation of data confidentiality and integrity. Frequently these deal with the use of encoding techniques, encryption libraries, and hashing algorithms. The weaknesses in this category could lead to a degradation of the quality data if they are not addressed.

Risk Assessment

Scan Results and analysis show 12 vulnerabilities total across the network. The Linux server has 2 High Severity vulnerabilities pertaining to default login credentials, 2 Medium Severity vulnerabilities pertaining to Potential Denial of Service through TLS/SSL renegotiation, and 2 Low Severity vulnerabilities pertaining to discovery of device information through ICMP enumeration. The Windows Server has 2 Medium Severity vulnerabilities, for services enumeration and a possible Man in the Middle attack over an insecure TLS version. The Windows server also has a Low Severity Vulnerability pertaining to TCP Timestamp discovery. The Windows 1 machine has a single Medium Severity vulnerability, the same Man in the Middle Attack Vector as the Windows server.

	Severity of Vulnerability		
Devices	High	Medium	Low
Linux (.52)	2	2	2
Winserver (.53)	0	2	1
Windows 1 (.50)	0	1	0

	CVE and CVSS		
Devices	High	Medium	Low
Linux (.52)	1999-0501,2,7,8 (7.5)	2011-1473(5.0) 1999-5094(4.3)	1999-0524(3.0)
Winserver (.53)		2011-3389(4.3) 2015-0204(4.3)	1999-0524(3.0)
Windows 1 (.50)		2011-3389(4.3) 2015-0204(4.3)	0

High Severity Vulnerabilities

IP	Severity	Description	Remediation
172.16.14.52 Linux	High	Unprotected OSSES/Wazuh ossec-authd (unauthorized access) on port 1515/TCP	Workaround: Enable password authentication or client certificate verification in the configuration of ossec-authd
172.16.14.52 Linux	High	HTTP Brute Force Logins with Default Credentials Reporting (unauthorized access) on port 9200/TCP	Mitigate: change the login credentials password to a strong password

CVEs 1999-0501, 02, 07 and 08 are a family of vulnerabilities related to brute force login using default credentials. There are 2 incidences of this vulnerability family found in the scan. The Linux Server currently has two ports open and unfiltered (1515, 9200), configured to accept default credentials. Accessing the web server in this manner is a low complexity exploit, deliverable over the network with a CVSS score of 7.5. The impact to Confidentiality and Integrity for any data held on this server would be high. An assailant could also impact Availability to the services this machine provides customers, employees or other stake holders. An assailant could then exploit a Trusted Relationship (T1199) by launching attacks on company clients by Impersonating (T1656) the company website to launch attacks against clients. Having access to this machine could allow for Privilege Escalation (TA0004) and Lateral Movement (TA0008) through the rest of the network, could aid in further Reconnaissance (TA0043) and Discover (TA0007) efforts. The assailant could make further Scans (T1595) from inside the network, could Create new Accounts (T1136) on this machine or other, raise the privileges of these accounts or other Account Manipulation (T1098). The access gained through these default credential could allow a threat actor to use the Linux Machine to Stage (T1074) or Exfiltrate (TA0010) data from elsewhere in the network. If any private Identity information, Payment Card data, or Health data were stolen or tampered with, the business would not be compliant with PIPEDA, PCIDSS, or GDPR.

Solving this issue would implement NIST RMF controls as follows:

- Account Management (AC-2 pg. 19)
- Baseline Configuration (CM-2 pg.97)
- Identification and Authentication (IA-2 pg. 132)

The vendor Remediation for this series of vulnerabilities is to change the default login credentials, or to configure the Wazuh service to require password authentication on the ossec credentials. These mitigations are low complexity and reduce the impact to an almost zero residual risk. Services, clients and employees may currently depend on these credentials, which should be identified as soon as possible. This vulnerability must be considered very High priority and should be remediated as soon as possible to maintain even the most basic security posture.

Medium Severity Vulnerabilities

IP	Severity	Description	Remediation
172.16.14.52 Linux	Medium	SSL/TLS: Renegotiation DoS Vulnerability on ports 55000/TCP and 1515/TCP	Mitigate: Regularly update to install patch for remediation
172.16.14.53 Winserver	Medium	DCE/RPC and MSRPC Services Enumeration Reporting on port 135/TCP	Mitigate: Filter incoming traffic to port 135/TCP
172.16.14.52 Linux	Medium	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability (1024-bit) on ports 9200/TCP and 9300/TCP	Workaround: Deploy Ephemeral ECDHE or use a 2048-bit or stronger Diffie-Hellman group
172.16.14.53 Winserver	Medium	SSL/TLS: Depreciated TLSv1.0 and TLSv1.1 Protocol Detection (MITM) on port 3389/TCP	Mitigate: Disable the depreciated TLSv1.0 and/or TLSv1.1 protocols in favour of the TLSv1.2+ protocols
172.16.14.50 Windows 1	Medium	SSL/TLS: Depreciated TLSv1.0 and TLSv1.1 Protocol Detection (MITM) on port 3389/TCP	Mitigate: Disable the depreciated TLSv1.0 and/or TLSv1.1 protocols in favour of the TLSv1.2+ protocols

All machines on the network are currently vulnerable to the FREAK or BEAST Man-in-the-Middle attack procedures on open port 3389 on the Windows machines and open ports 9200 and 9300 on the Linux server. All open ports are currently unfiltered according to test. Encrypted traffic can be captured in transit over a local network, and decrypted due to the inherently insecure encryption technique that is supported across all devices scanned. The impact of these vulnerabilities would depend entirely on what data was captured but could be of great risk to Confidentiality. CVE describes the complexity as Medium, bringing the overall CVSS score to 5.0. The remediation for this vulnerability is to force the use of TLSv1.2 or later for all traffic. There are unlikely to be many dependencies that would make this fix impossible, and the remediation is of low complexity. Therefore, this fix should be completed as soon as possible. Some consideration should not, but could be made for only forcing sensitive data over TLSv1.2+.

The Linux server is currently vulnerable to a Denial of Service attack on open/ unfiltered ports 55000 and 1515 by repeatedly requesting TLS/SSL renegotiation. Limiting the amount of times that an attacker can renegotiate the TLS cipher suite would remediate this issue. Updating to TLSv1.2+ would also resolve this issue and should be done as described above. A Denial of Service attack would impact the Availability of the server to customers and staff and should be remediated as soon as possible.

The Windows server is currently configured to report the status of several services and other information over DCE/RPC and MSRPC on the open and unfiltered port 135. This Services Enumeration can aid a threat actor in Reconnaissance efforts and could lead to further incident complexity. Traffic must be filtered on port 135 at the least. Consideration should be made for closing post 135 entirely.

Low Severity Vulnerabilities

IP	Severity	Description	Remediation
172.16.14.52 Linux	Low	TCP Timestamps Information Disclosure (Uptime of host may be calculated)	Mitigate: Disable TCP timestamps. Add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply settings at runtime and disable
172.16.14.53 Winserver	Low	TCP Timestamps Information Disclosure (Uptime of host may be calculated)	Mitigate: Disable TCP timestamps. Execute 'netsh int tcp set global timestamps=disabled' to disable
172.16.14.52 Linux	Low	ICMP Timestamp Reply Information Disclosure (Could be used to exploit weak time-based random number generators in other services)	Mitigate: Disable the support for ICMP timestamp on the remote host completely. Protect the remote host with a firewall and block ICMP packets travelling both directions.

The Windows and Linux server are vulnerable to a group of exploits related to ICMP and TCP timestamps all with a Severity of 3.0. Both machines can reveal how long they have been running. A threat actor can use this information to discern whether a new vulnerability has been patched. The Linux server can also reveal certain key factors about the way it may generate random numbers, which could lead to weakening of services that might rely on random number generation such as encryption. Servers should be configured to disable timestamp disclosure as outlined above.

Recommendations

Analyses of the scan findings shows that the two Highest Severity vulnerabilities, that have the highest likelihood of serious impact are also likely to be the easiest to remediate. The changing of default credentials to strong passwords in accordance with NIST controls Account Management (AC-2) and Access Enforcement (AC-3). This is the Highest Priority and should be dealt with immediately along with patching the Wazuh service to require Authentication.

Next in priority is to only allow TLSv1.2 or later for every machine on the network. Which should completed as soon as possible. This be a simple task and would go a long way to increase company security posture. Therefore this is the highest priority of the Medium Severity category. There are however some other tasks that should be considered for the Medium Priority category. A properly configured firewall could filter traffic on ports 1515, 9200, 9300 and 55000 on the Linx server, port 3389 on all Windows machines, and 135 on the Windows server. This would remediate all High and Medium threats in and of itself. When done in conjunction with mitigations provided above, the company would benefit from Security in depth. A whitelist can be made of all trusted Ips on the network, and all other traffic to these problem ports, if not all ports can be denied. A more sophisticated end point protection could use behavioral patterns of common attacks and alert the required employees.

The Low patches should be completed in due time. Machines should be patched to only reveal timestamp in trusted, necessary circumstances, if at all. The firewall provisions laid out above would also help with this vulnerability. A few more considerations could be made to further increase the depth of company Security. Vulnerabilities scans must be readministered on a regular schedule. Techniques and Tools should be continually upgraded to provided better and more up to date results. The scan parameters must be continually updated to include new vulnerabilities. It is impossible to say just how much an undetermined impact might have, but response would be slowed if too much confidence is given to the scan results alone as a source of all vulnerabilities to test for. Budget could be allocated for the paid version of Greenbone with more frequent updates. Another consideration is that the network is not currently resilient to any form of vulnerability scan such as the one completed for this report. If a threat actor were to complete such a scan, they could reveal company vulnerabilities and move to exploit them. Wireshark capture and log data should therefore be analyzed for behavioral patterns indicative of a vulnerability scan and automatic alerts and traffic filtering should be developed to reduce assailant impact.

References

NIST National Vulnerability Database for extended vulnerability explanation and CWE mapping:

https://nvd.nist.gov/

MITRE Common Vulnerability Enumeration for initial CVE entry in **Findings**, and vendor response aggregation:

https://cve.mitre.org/

MITRE Common Weakness enumeration for CWE entry in **Findings:**

https://cwe.mitre.org/

MITRE ATT&CK for Tools Techniques and Procedure mapping:

https://attack.mitre.org/

NIST Risk Management Framework SP 800-53 for mapping of Security controls:

https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Lighthouse Labs Bootcamp materials and teachers to provide context and expertise in vulnerability scans:

https://cyber.compass.lighthouselabs.ca/p/2/days/w05d1

Greenbone website for scanner troubleshooting:

https://www.greenbone.net/en/

Greenbone self guided course on Try Hack Me for scan expertise:

https://tryhackme.com/jr/greenboneappliance