jamk

Audit report

TTC6550 VLE environment audit

Kalle Jalkanen, AB8822

Learning assignment
TTC6550-3006, Joonatan Ovaska
17.12.2023
Information- and communication technology

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Contents

Tables

1 Introduction

This is auditing assignment for Auditing, Penetration Testing and Red Teaming course. Target is ethical hacking's VLE environment. The aim is to practise auditing and making report out of it.

2 Audit plan

Plan is to do auditing in four days. First day for planning, next three days for auditing and in last auditing day also analyzing and returning the document. In these days we are trying to get good picture of vulnerabilities.

Table 1 Plan Schedule

Week 50						
Mo	Tu	We	Th	Fr	Sa	Su
			Planning	Web server auditing	Workstation auditing	Firewall auditing, analyzing results
			Documentation			

2.1 Scope

In the scope of this auditing is Flare-VM, Kali, Wasdat and Pfsense. We leave Jarmo-Challenge out of scope.

2.2 Audit staff

This is one man team and that one is Kalle Jalkanen

2.3 Audit procedures

Object is to mainly use different scanners to find and identify vulnerabilities. All scans except Cis-Cat was ran on Kali Linux. List of tools and their purpose is listed in Table 4 below.

Table 2 Tools listing

Tool	Version	Purpose	Asset/Target
nmap -sV -sC <target>	7.94	Network and port scanning	Wasdat, Windows 10, Kali, PfSense (WAN), PfSense (LAN)
Cis-Cat lite	4.12	Cis-Cat benchmarks check	Windows 10
Nessus	10.6.4	Vulnerabilities scan	Wasdat, Windows 10, Kali, PfSense (WAN), PfSense (LAN)
Lynis	3.0.9	Auditing scan	Kali

3 Target environment

Target is schools ethical hacking modules environment. There are 5 machines in it, but only 4 of them are in scope.

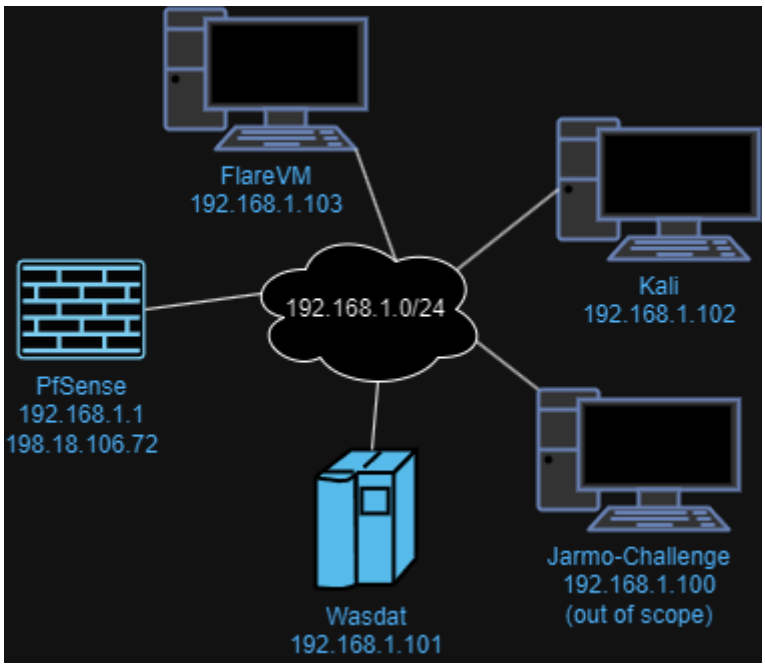
3.1 Assets

There are two workstations. One named Kali with OS Linux 6.3.0-kali1-amd64 x86_64 and Flare-VM which is Windows 10 version 21H1 (OS build 19043.1766). There is also a web server called Wasdat which is Linux 4.15.0-135-generic x86_64. All these machines are behind firewall called Pfsense with version 2.4.5.

3.2 Topology

Environment had all devices that there should be that we get in preliminary data. There was not any other devices found.

Table 3 Topology



4 Analysis and reporting

4.1 Windows Workstation (Flare VM)

Flare has open ports 135 (msrpc), 139 (netbios-ssn), 445 (Microsoft-ds), 3389 (ms-wbt-server) and 5357 (http). Cis-Cat passed only 96 of 361 checks so there are 265 security problems. Result of Cis-Cat is at end of the document in attachments. Nessus found 1 high, 5 medium vulnerabilities and 45 info.

4.1.1 Threats and vulnerabilities (Uhat ja haavoittuvuudet)

- SSL Medium Strength Cipher Suites Supported (SWEET32). High severity. The remote host supports the use of SSL ciphers that offer medium strength encryption
- SSL Certificate Cannot Be Trusted. Medium severity The server's X.509 certificate cannot be trusted
- SSL Self-Signed Certificate. Medium severity. The X.509 certificate chain for this service is not signed by a recognized certificate authority
- SMB Signing not required. Medium severity. Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server
- TLS Version 1.0 Protocol Detection. Medium severity. The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws.
- TLS Version 1.1 Protocol Deprecated. Medium severity. The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites.

4.2 Linux Workstation (Kali)

With Nessus there found 1 critical, 1 medium, 2 low vulnerabilities and 82 info. Lynis gave 2 warnings.

4.2.1 Threats and vulnerabilities

Nessus:

- PHP 8.2.x < 8.2.9 Multiple Vulnerabilities. Critical severity. The version of PHP installed on the remote host is prior to 8.2.9. It is, therefore, affected by multiple vulnerabilities.
- SSL Certificate Cannot Be Trusted. Medium severity
- SSH Server CBC Mode Ciphers Enabled. Low severity. The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.
- SSH Weak MAC Algorithms Enabled. Low severity. The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Lynis:

- Found one or more vulnerable packages. [PKGS-7392]
- Redis configuration file /etc/redis/redis-openvas.conf is world readable and might leak sensitive details [DBS-1882]

4.3 Web server Linux (wasdat)

With Nessus web application test there found 2 high vulnerabilities, 4 medium and 58 info results. With nmap scan in port 80 and 8080 was nginx version 1.19.0, that version has 37 critical, 104 high, 109 medium and 133 low severity vulnerabilities. Port 22 has also old version 7.6p1 of OpenSSH and it has 12 different CVE's, 1 critical, 2 high, 8 medium and 1 low severity vulnerabilities. P

4.3.1 Threats and vulnerabilities

This instance has so many vulnerabilities, so they are limited to highest severity and couple lower severity that are good to mention.

Nessus:

- Both medium level vulnerabilities was that there is browsable web directories. Other from port 80 and other from 8080. Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.
- Web server transimts cleartext credentials at ports 80 and 8000. This was low level threath.
- Web Application Cookies Not Marked HttpOnly

nginx port 80 and 8080:

- Exposure of Resource to Wrong Sphere in curl and curl/libcurl4
- Out-of-bounds Read in db5.3/libdb5.3
- Directory Traversal in dpkg (Fixed in: 1.19.8)
- Exposure of Resource to Wrong Sphere in expat/libexpat1
- Improper Encoding or Escaping of Output in expat/libexpat1
- Multiple instances of Integer Overflow or Wraparound in expat/libexpat1
- Out-of-bounds Write in freetype/libfreetype6
- Buffer Overflow in glibc/libc-bin and glibc/libc6
- Use After Free in glibc/libc-bin and glibc/libc6
- Use After Free in gnutls28/libgnutls30
- Out-of-bounds Write in libwebp/libwebp6
- Use After Free in libwebp/libwebp6
- Use of Uninitialized Resource in libwebp/libwebp6
- Buffer Overflow in libx11/libx11-6 and libx11/libx11-data
- Out-of-bounds Write in lz4/liblz4-1
- SQL Injection in openldap/libldap-2.4-2 and openldap/libldap-common
- Buffer Overflow in openssl
- OS Command Injection in openssl
- Integer Overflow or Wraparound in zlib/zlib1g.
- Out-of-bounds Read in libbsd/libbsd0
- Off-by-one Error in libtasn1-6
- Multiple instances of Out-of-bounds Read in libwebp/libwebp6
- Integer Overflow or Wraparound in glibc/libc-bin and glibc/libc6

ssh port 22:

- The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. Critical severity.
- sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. High severity.
- scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. High severity

4.4 Firewall PfSense

From Nessus we get that inner port has 1 ciritcal, 1 medium, 1 low severity vulnerabilities and 16 infos. Outer ports has 1 critical, 2 medium severity vulnerabilities and 19 infos. Inner port has ports 22 (ssh), 53 (domain) and 80 (http) open. Outer port has port 53 (domain) open.

4.4.1 Threats and vulnerabilities

Inner port:

- Unix Operating System Unsupported Version Detection. Critical severity
- Network Time Protocol (NTP) Mode 6 Scanner. Medium severity
- DHCP Server Detection. Low severity. It is possible to get information about the network layout

Outer port:

- Unix Operating System Unsupported Version Detection. Critical severity
- Network Time Protocol (NTP) Mode 6 Scanner. Medium severity. The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.
- DNS Server Recursive Query Cache Poisoning Weakness. Medium severity. It is possible to query the remote name server for third-party names.
- SSH Server Type and Version Information. Info. It is possible to obtain information about the remote SSH server by sending an empty authentication request.

5 Risk analysis (Riskianalyysi)

Table 5 shows biggest risks, their probabilities and impact levels scale 1-5. Probability is multiplied with impact level and it gives risk level. The higher the risk level the more dangerous this scenario is.

Table 4 Risk Table

Probability					
Severity	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Certain (5)
Insignificant (1)	1	2	3	4	5
Minor (2)	2	4	6	8	10
Moderate (3)	3	6	9	12	15
Major (4)	4	8	12	16	20
Critical (5)	5	10	15	20	25

Table 5 Risk analysis

Asset	Risk	Prob-abil-ity	Im-pact	Risk level	Mitigation method
Wasdat	Attack trough open ports	3	5	15	Update all programs
Flare-VM	Man in the middle attack	1	3	3	Enforce message signing in the host's configuration.
Kali	Remote Code Execution or Denial of Ser-vice	1	2	2	Update PHP and nginx
Flare-VM	SSL/TLS At-tacks	1	2	2	Update TLS protocols
Wasdat	Web Applica-tion attacks	4	3	12	Update all used programs
Wasdat	Unauthorized SSH acces	2	3	6	Update SSH
Pfsense	Amplification Attacks via NTP leading to distributed DDoS	2	4	8	Restrict NTP mode 6 queries

6 Summary and Recommendations

The environment faces significant security risks from outdated software, unsecured protocols, and exposed services. Immediate attention is required to patch critical vulnerabilities, update insecure protocols, and enhance network security measures. Regular audits and updates are recommended to maintain security posture.

7 Conclusion/Free word

Tämä oli mielenkiintoinen tehtävä. Mielestäni tämä suoritus jäi kokonaisuutena melko suppeaksi, koska en halunnut käyttää tähän liikaa aikaa. Olen kuitenkin tyytyväinen siihen mitä sain aikaiseksi.

Liite 1. Cis-Cat result https://jamkstudent-my.sharepoint.com/:w:/g/personal/ab8822_student_jamk_fi/EUe5XMBCYGBPgpCoRwTOUKoBl9Oq4V412eu3zth82rEMTQ?e=rCSyZQ