Audit report

TTKS0700-3003 VLE environment audit

Michael Herman
Toni Peltola

Project report

Instructor: Joonatan Ovaska

21.04.2023

TIC2021

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Figures

Tables

1 Introduction

Yritys Oy has commissioned an audit report to assess the current state of its network and security systems. The company's existing system is outdated and susceptible to threats. The purpose of this report is to conduct a comprehensive analysis to identify security loopholes and vulnerabilities in the network and propose strategies to bring it up to industry standards.

The report is based on the most recent ISO standards (19011-2018). These were chosen due to their widespread use in the industry. Other frameworks such as NIST and CIS are also available for consideration. The report provides an overview of the current state of Yritys Oy's network and cyber security systems. This includes an in-depth vulnerability and risk identification analysis.

The audit outlines best practices for securing the network. This includes implementing firewall rules, access controls, encryption, and regular security updates. The report notes the importance of maintaining up-to-date software and hardware. Regularly conducting regular security audits and risk assessments are also necessary to ensure ongoing protection. Adopting the recommendations outlined in the report will significantly improve the security of the company network and protect its systems against potential cyber threats.

2 Audit plan

Yritys Oy has requested an analysis of their operational environment. Within the environment there is a Linux machine, a Windows machine and an active firewall. The audit follows procedures established by ISO 19011-2018 Chapter 6.5.1 (ISO, 2018). The chapter defines the audit approach and contents herein. The auditing process has been carefully documented.

The report begins by outlining the audit timetable, purpose, scope and procedure. The target environment is then described. Nmap and Greenbone scans are performed on the target machines and ports. Specific vulnerabilities are enumerated by Metasploit. These are then discussed. Mitigation methods for possible threats are proposed. Versions are disclosed to provide a meaningful reference point for future audits. Easily reproduceable results are necessary to ensure the scientific validity of the results.

2.2 Timetable

The auditing process was divided into three weeklong segments. The planning stage established the ground-rules and laid the foundations for the process. Within this timeframe the environment was investigated on the surface level to gain an understanding of how to approach the audit and the tools necessary. This was followed by the setting up the devices needed to perform the necessary scans.

The second part of the process was to scan the system. The third and final week consisted of observing and documenting the results. Reporting to the company executives will be the final step of the process. The process was divided for the entire three-week timeframe. Full disclosure of all necessary steps was included within this document.

Table 1: Audit timetable

Audit Plan																				
Week 14							Week 15							Week 16						
Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Planning																				
		Setting up the environment																		
							vulnerability scans													
									Configuration scans											
							Other scans													
														Observations and results						
																	Project return			
Documentation																				

2.3 Purpose

Yritys Oy has provided a test environment for auditing purposes. The main objective was to perform an assessment of the environment. The assessment was based on ISO 19011-2018 Chapter 6.5.1 (2018). It was not geared towards meeting any certification requirements. The aim was instead to identify vulnerabilities and threats within the system. Fixes to potential vulnerabilities and mitigate threats were also proposed.

2.4 Scope

The auditing process focused on three instances within the environment: a Windows-based FlareVM, a Linux-based Wasdat and a pfSense firewall. The environment was assessed using system and port scans. Basic penetration testing was also performed.

2.5 Audit staff

The audit was performed by security specialists Michael Herman and Toni Peltola.

2.6 Audit procedure

Within the environment a Kali Linux instance was the main platform for vulnerability detection, port scanning and penetration testing. Penetration testing was performed in order to consider the potential risks the system might face in the future.

The tools and methods used in the auditing process were as follows:

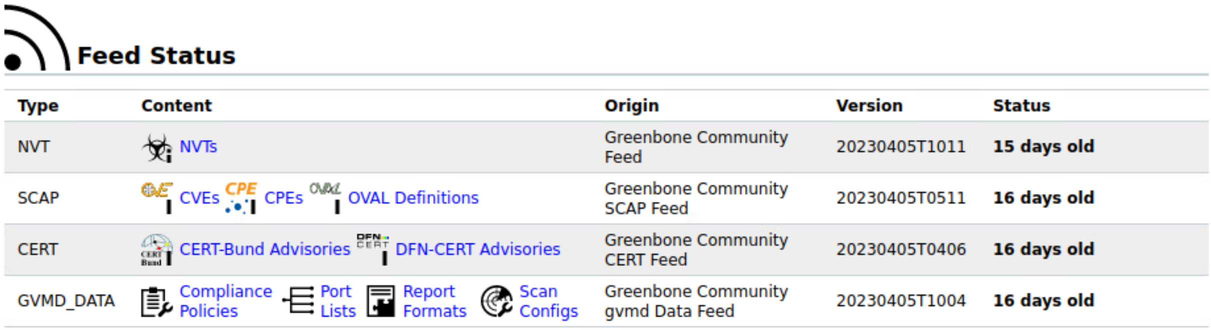
Table 2: Test framework

Tool	Version	Purpose	Asset
ISO	19011-2018 Ch 6.5.1	Check configurations against ISO audit criteria	Flare-VM, pfSense firewall, Wasdat

Table 3: Audit tools

Tool	Version	Purpose	Asset/Target
nmap -sC <target>, nmap -A <target>	7.92	Network and port scanning	Flare-VM, pfSense firewall, Wasdat
whatweb <target>	0.5.5	Network address enumeration	Flare-VM, pfSense firewall, Wasdat
Metasploit	6.1.14	Vulnerability enumeration	MSRRPC, SSH, domain, Nginx, HTTP
Greenbone	21.4.3, data feed version 20230405T1004	Vulnerability scanning	Flare-VM, pfSense firewall, Wasdat

Figure 1: Greenbone system information



Feed Status

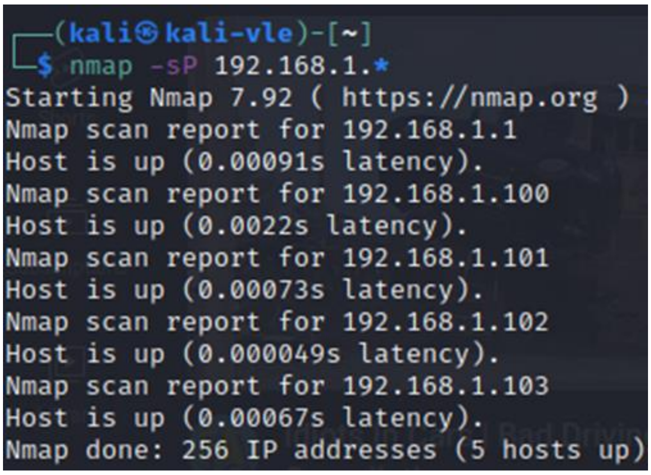
Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20230405T1011	**15 days old**
SCAP	CVEs CPEs OVAL Definitions	Greenbone Community SCAP Feed	20230405T0511	**16 days old**
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone Community CERT Feed	20230405T0406	**16 days old**
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone Community gvmd Data Feed	20230405T1004	**16 days old**

3 Target environment

3.1 Network

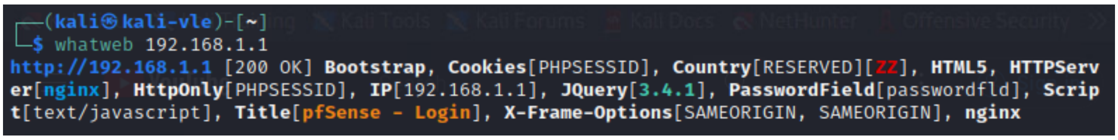
The Yritys Oy network contains three machines: Flare-VM, pfSense and Wasdat. Flare-VM is a Windows-based reverse engineering and malware analysis distribution. It has an IP address of 192.168.1.103. pfSense acts as the company firewall. It uses LAN and WAN addresses. The local address is 192.168.1.1. The Kali instance has an address of 192.168.1.102 and was used to perform the vulnerability scans.

Figure 2: Internal network addresses



```
┌──(kali㉿kali-vle)-[~]
└─$ nmap -sP 192.168.1.*
Starting Nmap 7.92 ( https://nmap.org )
Nmap scan report for 192.168.1.1
Host is up (0.00091s latency).
Nmap scan report for 192.168.1.100
Host is up (0.0022s latency).
Nmap scan report for 192.168.1.101
Host is up (0.00073s latency).
Nmap scan report for 192.168.1.102
Host is up (0.000049s latency).
Nmap scan report for 192.168.1.103
Host is up (0.00067s latency).
Nmap done: 256 IP addresses (5 hosts up)
```

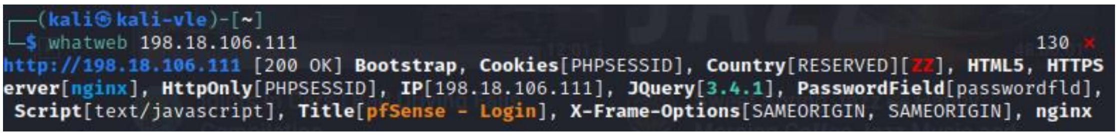
Figure 3: Internal firewall address



```
┌──(kali㉿kali-vle)-[~]
└─$ whatweb 192.168.1.1
http://192.168.1.1 [200 OK] Bootstrap, Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServ
er[nginx], HttpOnly[PHPSESSID], IP[192.168.1.1], JQuery[3.4.1], PasswordField[passwordfld], Scrip
t[text/javascript], Title[pfSense - Login], X-Frame-Options[SAMEORIGIN, SAMEORIGIN], nginx
```

The Internet-facing WAN address is 192.18.106.111.

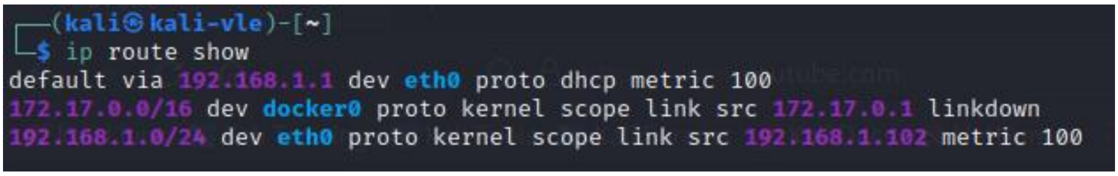
Figure 4: Internet facing firewall address



```
┌──(kali㉿kali-vle)-[~]
└─$ whatweb 198.18.106.111                                                              130 ✕
http://198.18.106.111 [200 OK] Bootstrap, Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPS
erver[nginx], HttpOnly[PHPSESSID], IP[198.18.106.111], JQuery[3.4.1], PasswordField[passwordfld],
 Script[text/javascript], Title[pfSense - Login], X-Frame-Options[SAMEORIGIN, SAMEORIGIN], nginx
```

The 192.168.1.1 LAN address is the network's default gateway.

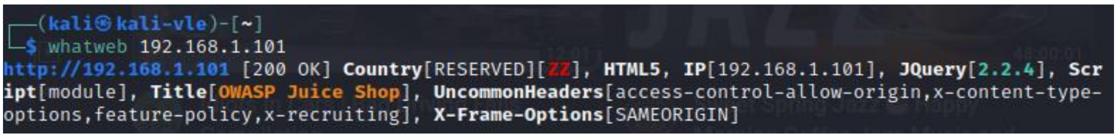
Figure 5: Default gateway



```
┌──(kali㉿kali-vle)-[~]
└─$ ip route show
default via 192.168.1.1 dev eth0 proto dhcp metric 100
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.102 metric 100
```

The Wasdat machine has an address of 192.168.101. The address contains the OWASP Juice Shop Docker container.

Figure 6: OWASP Juice Shop address



```
┌──(kali㉿kali-vle)-[~]
└─$ whatweb 192.168.1.101
http://192.168.1.101 [200 OK] Country[RESERVED][ZZ], HTML5, IP[192.168.1.101], JQuery[2.2.4], Scr
ipt[module], Title[OWASP Juice Shop], UncommonHeaders[access-control-allow-origin,x-content-type-
options,feature-policy,x-recruiting], X-Frame-Options[SAMEORIGIN]
```

3.2 Assets

3.2.1 Flare VM

Flare-VM is a virtual environment designed specifically for reverse engineering and malware analysis. The environment is virtualized because it allows for the protection and isolation of physical devices and networks from malicious activities (Mandiant, n.d.). The VM includes a wide range of tools. It contains disassemblers, debuggers, file-format parsers, decompilers, monitoring tools and utilities.

Examples of disassemblers offered in the Flare suite include Apktool and Cutter. It also includes debuggers such as IDA Free 7.0. The suit contains file-format parsers such as Hashcalc and PE-bear. There are also decompilers such as Bytecode viewer and dnSpy. Hex-editors such as HXD and the Sysinternal suite are also present. Though not explicitly linked to the Flare suite, the VM also comes with the package analysis tool Wireshark. See Appendix 1 for a more exhaustive list of available tools.

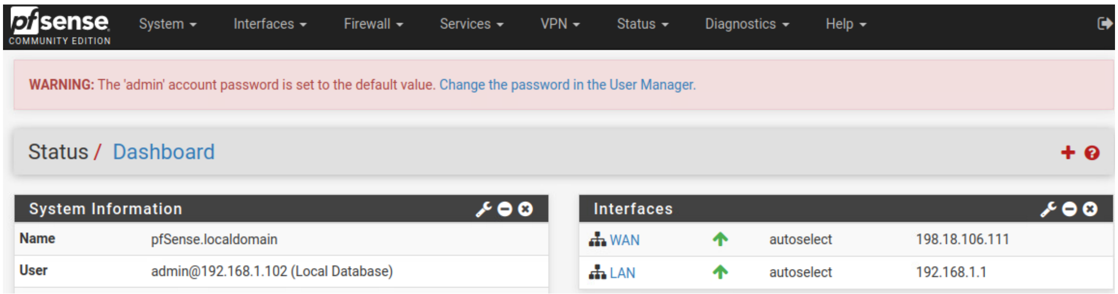
Figure 7: Flare-VM Windows environment

3.2.2 pfSense

pfSense is an open-source firewall and routing software based the FreeBSD operating system. It has a robust feature set. The firewall provides advanced features such as stateful packet inspection, virtual private network (VPN) support, network address translation (NAT), load balancing, traffic shaping, and intrusion detection and prevention system (IDPS) capabilities (pfSense, n.d.). Its flexibility makes it a popular choice for securing networks in various environments. These can range from small home networks to large enterprise networks.

The firewall offers a web-based graphical user interface (GUI) that makes it easy to configure and manage firewall settings. Extra functionality can be added to the firewall. There are many community-contributed packages available for download. This allows users to customize the firewall to suit their specific needs. The firewall is known for its stability, security and ease of use.

Figure 8: pfSense browser-based GUI



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / Dashboard

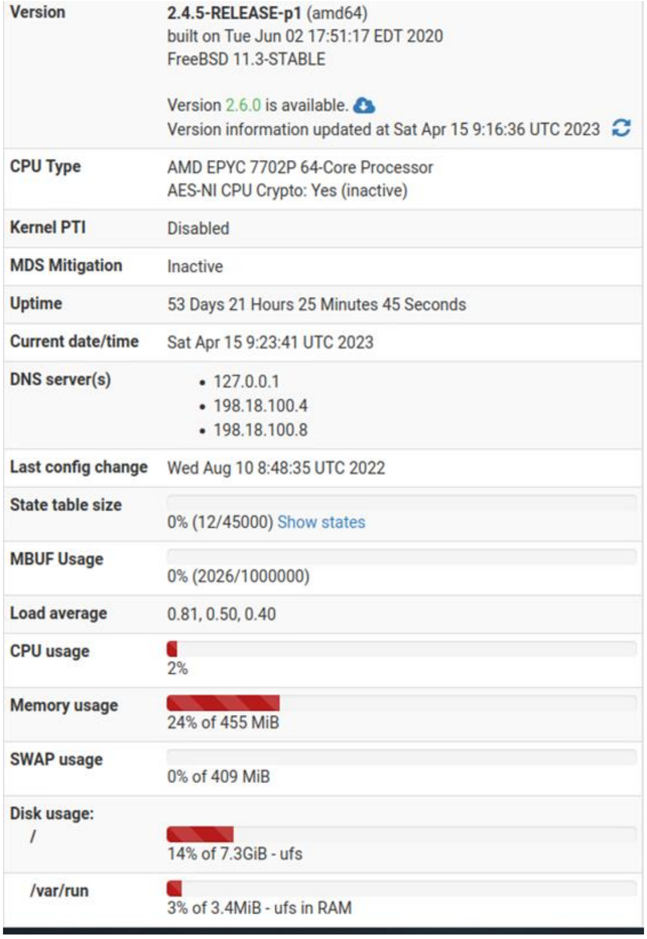
System Information

Name	pfSense.localdomain
User	admin@192.168.1.102 (Local Database)

Interfaces

WAN	↑	autoselect	198.18.106.111
LAN	↑	autoselect	192.168.1.1

Figure 9: pfSense system information

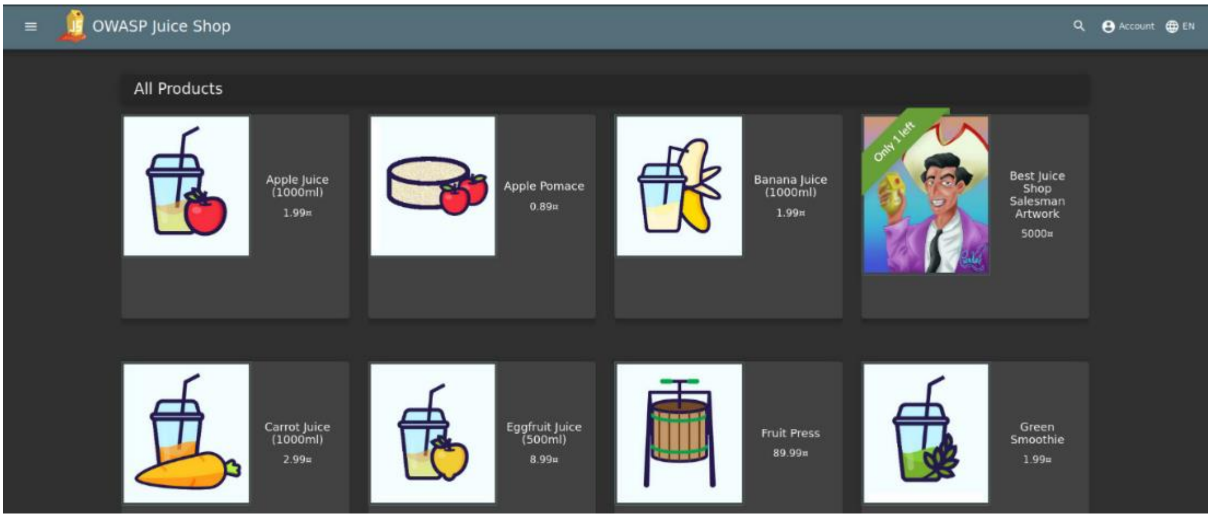


Version	**2.4.5-RELEASE-p1** (amd64) built on Tue Jun 02 17:51:17 EDT 2020 FreeBSD 11.3-STABLE Version 2.6.0 is available. Version information updated at Sat Apr 15 9:16:36 UTC 2023
CPU Type	AMD EPYC 7702P 64-Core Processor AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	53 Days 21 Hours 25 Minutes 45 Seconds
Current date/time	Sat Apr 15 9:23:41 UTC 2023
DNS server(s)	• 127.0.0.1 • 198.18.100.4 • 198.18.100.8
Last config change	Wed Aug 10 8:48:35 UTC 2022
State table size	0% (12/45000) Show states
MBUF Usage	0% (2026/1000000)
Load average	0.81, 0.50, 0.40
CPU usage	2%
Memory usage	24% of 455 MiB
SWAP usage	0% of 409 MiB
Disk usage: /	14% of 7.3GiB - ufs
/var/run	3% of 3.4MiB - ufs in RAM

3.2.3 Wasdat

The Wasdat machine contains a Docker container for the OWASP Juice Shop website.

Figure 10: OWASP Juice Shop landing page



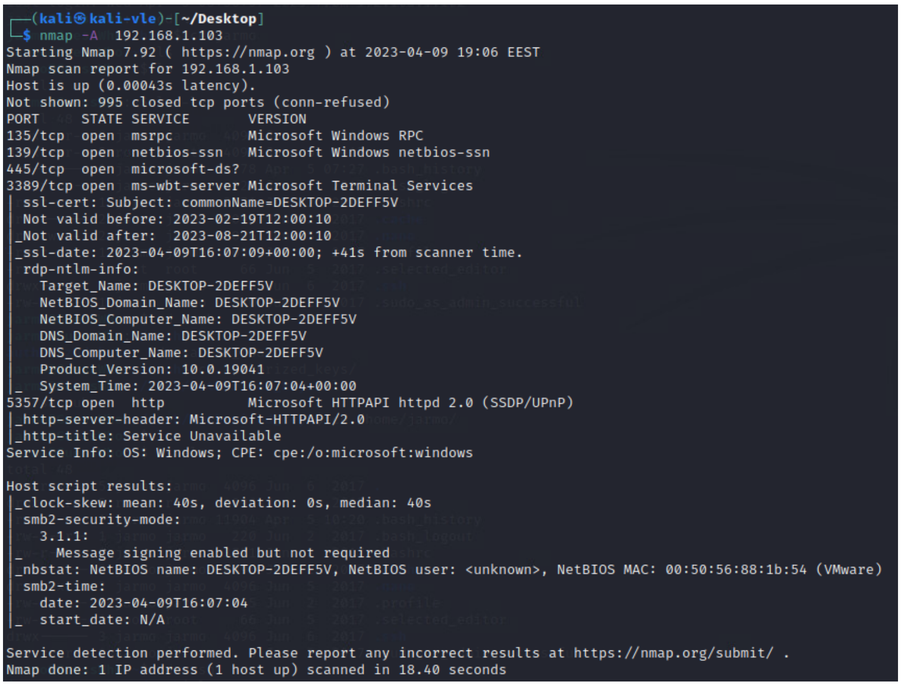
4 Port scans

Port scans were performed on all three machines in the network. The scans were performed by Nmap.

4.1 Flare-VM

An aggressive Nmap scan using the *-A* flag indicated a wide range of TCP ports were open. The services operating on these ports are vulnerable to exploitation. These included ports 135, 139, 445, 3389 and 5357.

Figure 11: Flare-VM port scan



```
┌──(kali㉿kali-vle)-[~/Desktop]
└─$ nmap -A  192.168.1.103
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-09 19:06 EEST
Nmap scan report for 192.168.1.103
Host is up (0.00043s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=DESKTOP-2DEFF5V
| Not valid before: 2023-02-19T12:00:10
|_Not valid after:  2023-08-21T12:00:10
|_ssl-date: 2023-04-09T16:07:09+00:00; +41s from scanner time.
| rdp-ntlm-info:
|   Target_Name: DESKTOP-2DEFF5V
|   NetBIOS_Domain_Name: DESKTOP-2DEFF5V
|   NetBIOS_Computer_Name: DESKTOP-2DEFF5V
|   DNS_Domain_Name: DESKTOP-2DEFF5V
|   DNS_Computer_Name: DESKTOP-2DEFF5V
|   Product_Version: 10.0.19041
|_  System_Time: 2023-04-09T16:07:04+00:00
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 40s, deviation: 0s, median: 40s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: DESKTOP-2DEFF5V, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:88:1b:54 (VMware)
| smb2-time:
|   date: 2023-04-09T16:07:04
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.40 seconds
```

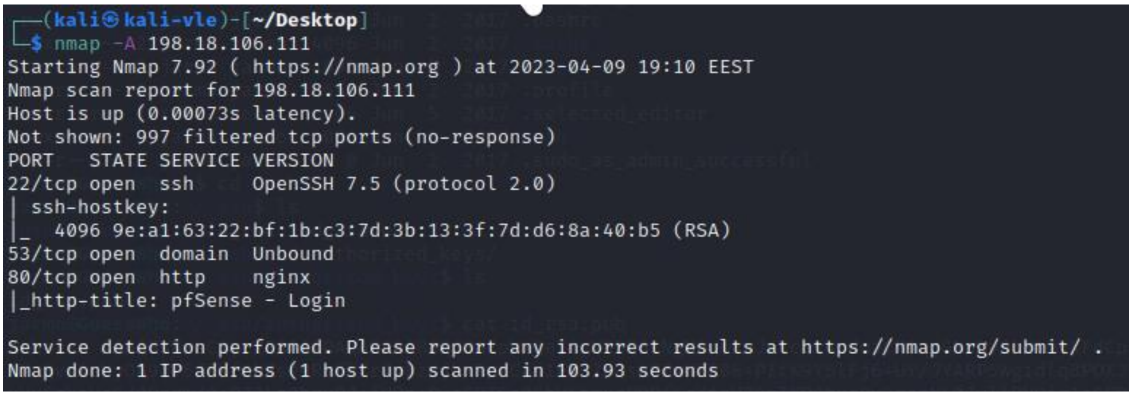
Table 4: Flare-VM vulnerable ports and services

Machine	Port	State	Service
Flare-VM	135	Open	MSRPC
	139	Open	NetBIOS-SSN
	445	Open	Microsoft-DS
	3389	Open	MS WBT Server
	5357	Open	HTTPAPI

4.2 pfSense

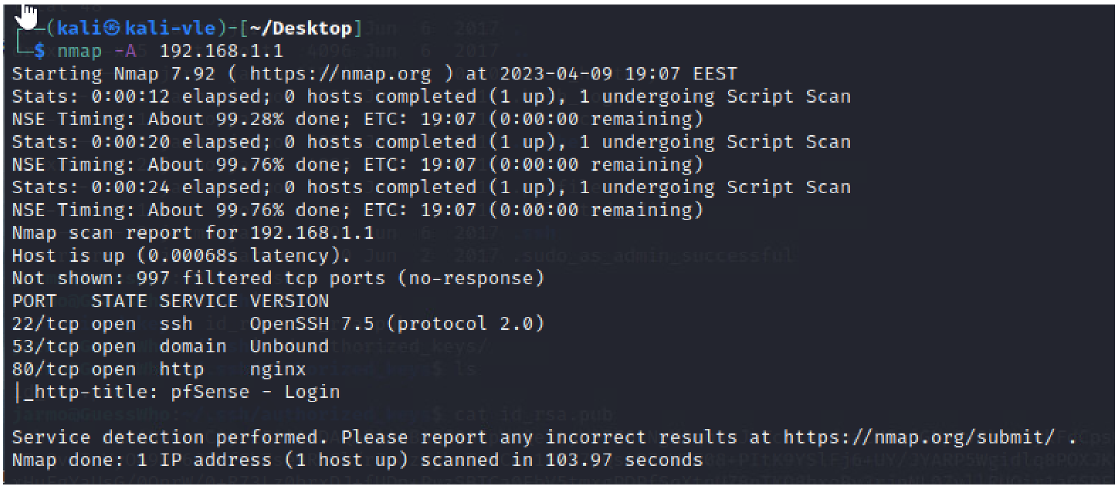
Aggressive Nmap scans were performed on both the WAN and LAN addresses of the firewall. The internet-facing address had vulnerabilities on TCP ports 22, 53 and 80. The same vulnerabilities occured in the internal address.

Figure 12: pfSense WAN port scan



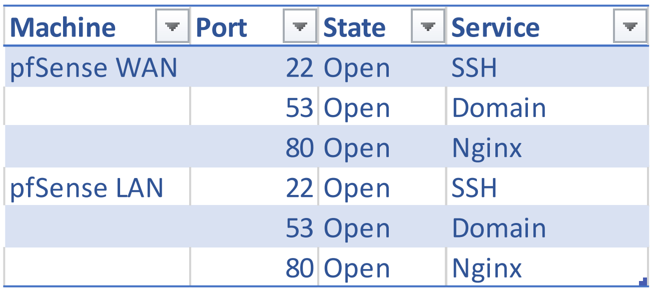
```
┌──(kali㉿kali-vle)-[~/Desktop]
└─$ nmap -A 198.18.106.111
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-09 19:10 EEST
Nmap scan report for 198.18.106.111
Host is up (0.00073s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.5 (protocol 2.0)
| ssh-hostkey:
|_  4096 9e:a1:63:22:bf:1b:c3:7d:3b:13:3f:7d:d6:8a:40:b5 (RSA)
53/tcp open  domain  Unbound
80/tcp open  http    nginx
|_http-title: pfSense - Login

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 103.93 seconds
```

Figure 13: pfSense LAN port scan



```
┌──(kali㉿kali-vle)-[~/Desktop]
└─$ nmap -A 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-09 19:07 EEST
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.28% done; ETC: 19:07 (0:00:00 remaining)
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 19:07 (0:00:00 remaining)
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.76% done; ETC: 19:07 (0:00:00 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.00068s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.5 (protocol 2.0)
53/tcp open  domain  Unbound
80/tcp open  http    nginx
|_http-title: pfSense - Login

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 103.97 seconds
```

Table 5: pfSense WAN and LAN vunerable ports and services

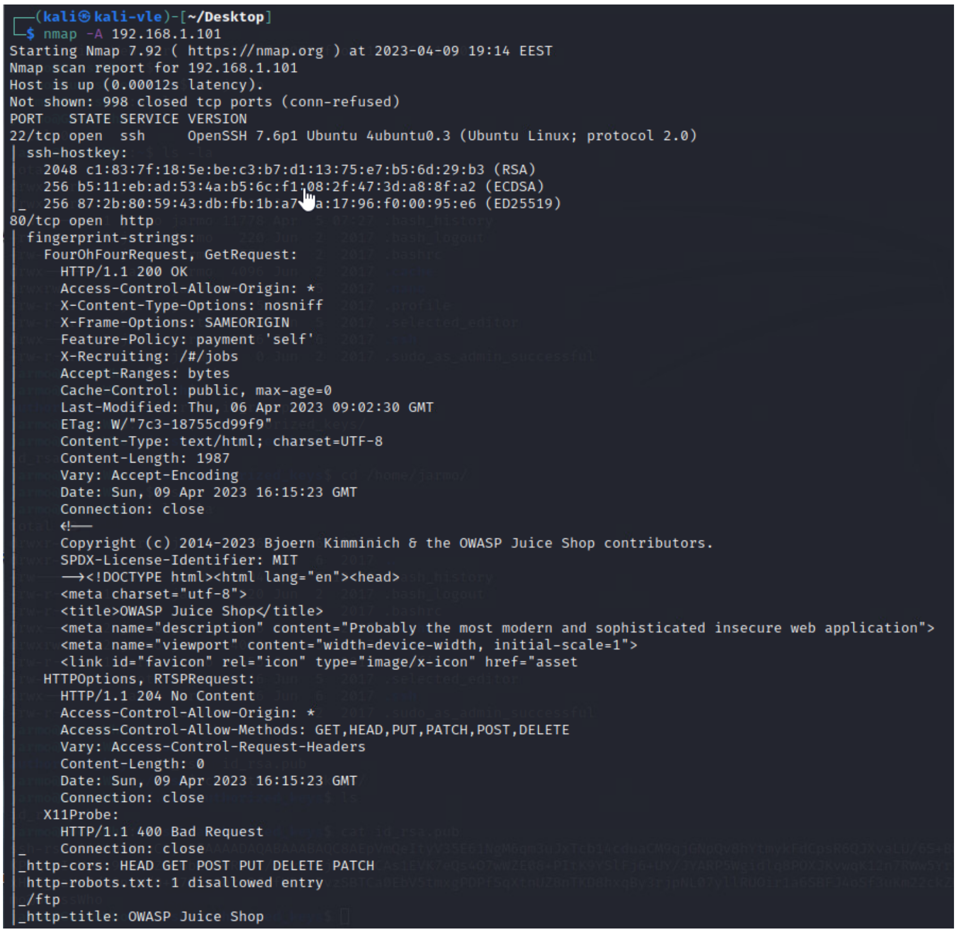


Machine	Port	State	Service
pfSense WAN	22	Open	SSH
	53	Open	Domain
	80	Open	Nginx
pfSense LAN	22	Open	SSH
	53	Open	Domain
	80	Open	Nginx

4.3 Wasdat

The Wasdat machine is highly vulnerable to exploitation. Nmap indicated a wide range of possible attack vectors associated with TCP ports 22 and 80.

Figure 14: Wasdat port scan



```
┌──(kali㉿kali-vle)-[~/Desktop]
└─$ nmap -A 192.168.1.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-09 19:14 EEST
Nmap scan report for 192.168.1.101
Host is up (0.00012s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c1:83:7f:18:5e:be:c3:b7:d1:13:75:e7:b5:6d:29:b3 (RSA)
|   256 b5:11:eb:ad:53:4a:b5:6c:f1:08:2f:47:3d:a8:8f:a2 (ECDSA)
|_  256 87:2b:80:59:43:db:fb:1b:a7[illegible]a:17:96:f0:00:95:e6 (ED25519)
80/tcp open  http
| fingerprint-strings:
|   FourOhFourRequest, GetRequest:
|     HTTP/1.1 200 OK
|     Access-Control-Allow-Origin: *
|     X-Content-Type-Options: nosniff
|     X-Frame-Options: SAMEORIGIN
|     Feature-Policy: payment 'self'
|     X-Recruiting: /#/jobs
|     Accept-Ranges: bytes
|     Cache-Control: public, max-age=0
|     Last-Modified: Thu, 06 Apr 2023 09:02:30 GMT
|     ETag: W/"7c3-18755cd99f9"
|     Content-Type: text/html; charset=UTF-8
|     Content-Length: 1987
|     Vary: Accept-Encoding
|     Date: Sun, 09 Apr 2023 16:15:23 GMT
|     Connection: close
|     <!——
|     Copyright (c) 2014-2023 Bjoern Kimminich & the OWASP Juice Shop contributors.
|     SPDX-License-Identifier: MIT
|     ——><!DOCTYPE html><html lang="en"><head>
|     <meta charset="utf-8">
|     <title>OWASP Juice Shop</title>
|     <meta name="description" content="Probably the most modern and sophisticated insecure web application">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <link id="favicon" rel="icon" type="image/x-icon" href="asset
|   HTTPOptions, RTSPRequest:
|     HTTP/1.1 204 No Content
|     Access-Control-Allow-Origin: *
|     Access-Control-Allow-Methods: GET,HEAD,PUT,PATCH,POST,DELETE
|     Vary: Access-Control-Request-Headers
|     Content-Length: 0
|     Date: Sun, 09 Apr 2023 16:15:23 GMT
|     Connection: close
|   X11Probe:
|     HTTP/1.1 400 Bad Request
|_    Connection: close
|_http-cors: HEAD GET POST PUT DELETE PATCH
| http-robots.txt: 1 disallowed entry
|_/ftp
|_http-title: OWASP Juice Shop
```

Table 6: Wasdat vulnerability and port scans

Machine	Port	State	Service
Wasdat	22	Open	SSH
	80	Open	HTTP

5 Penetration testing

Services associated with vulnerable ports were tested using Metasploit. Metasploit is an open-source framework for developing, testing and executing exploits against computer systems and networks for the purpose of identifying vulnerabilities and improving security. It provides a collection of tools and resources for penetration testing, vulnerability assessment and ethical hacking (Metasploit, n.d).

The purpose was to simulate real-world cyber-attacks in a controlled environment. This will assist Yritys Oy in identifying and fixing vulnerabilities in their systems before they can be exploited. Metasploit includes a large library of exploits, payloads, auxiliary modules, and post-exploitation modules. These can be customized and combined to create custom attacks based on specific targets and vulnerabilities.

What follows below is a summary of the exploits available for the most vulnerable services running on the company machines. Only exploits rated by Metasploit as good, excellent or great are noted.

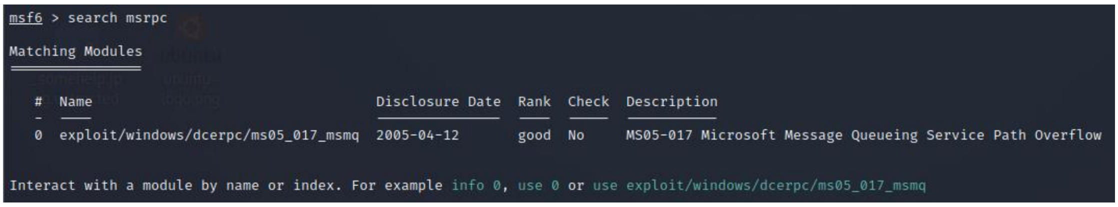
5.1 Vulnerable services

5.1.1 MSRPC

Microsoft Remote Procedure Call (MSRPC) is a protocol used for communication between networked computers in a distributed computing environment. It is commonly used in Windows operating systems. MSRPC allows programs to execute procedures on remote systems as if they were local.

The service is based on the Remote Procedure Call (RPC) model. This is a method used for inter-process communication (IPC) between processes running on different systems. MSRPC extends the standard RPC model by adding features specific to Microsoft technologies. These include support for Active Directory services, Distributed File System (DFS), and Windows Management Instrumentation (WMI). Metasploit indicates a potential vulnerability associated with the service (Barnea, 2022).

Figure 15: MSRPC exploits



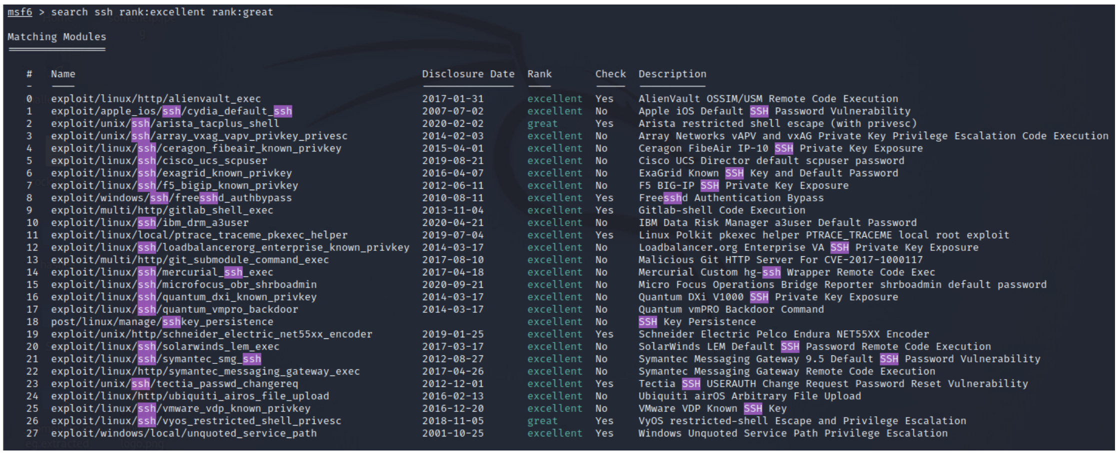
```
msf6 > search msrpc

Matching Modules
================

   #  Name                                  Disclosure Date  Rank  Check  Description
   -  ----                                  ---------------  ----  -----  -----------
   0  exploit/windows/dcerpc/ms05_017_msmq  2005-04-12       good  No     MS05-017 Microsoft Message Queueing Service Path Overflow


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/dcerpc/ms05_017_msmq
```

5.1.2 SSH

OpenSSH (Open Secure Shell) is a widely used open-source implementation of the Secure Shell (SSH) protocol. It is a cryptographic network protocol used for secure remote login, file transfer and tunneling. OpenSSH is the standard for secure remote access to Unix-based systems. It provides a secure means of accessing and managing remote servers and network devices over an unsecured network (OpenSSH, n.d).

The service provides encrypted communication between client and server. It allows users to securely authenticate themselves to a remote server using public-key cryptography or password-based authentication. It also supports secure file transfer through protocols such as SFTP (SSH File Transfer Protocol) and SCP (Secure Copy). This allows users to securely transfer files between local and remote systems. It is considered a critical tool for securing remote access to systems and managing them securely over the internet. The service is nevertheless vulnerable to exploitation. This could potentially provide attackers with privileged access to company systems.

Figure 16: SSH exploits

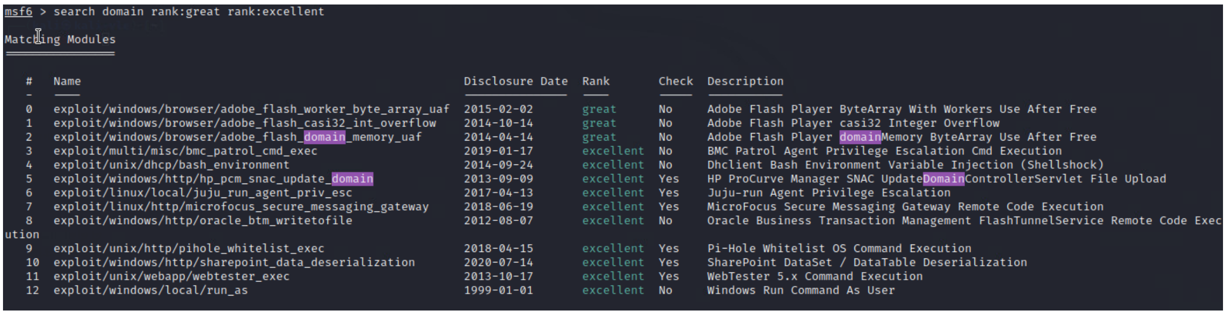


```
msf6 > search ssh rank:excellent rank:great

Matching Modules
================

   #   Name                                                       Disclosure Date  Rank       Check  Description
   -   ----                                                       ---------------  ----       -----  -----------
   0   exploit/linux/http/alienvault_exec                         2017-01-31       excellent  Yes    AlienVault OSSIM/USM Remote Code Execution
   1   exploit/apple_ios/ssh/cydia_default_ssh                    2007-07-02       excellent  No     Apple iOS Default SSH Password Vulnerability
   2   exploit/unix/ssh/arista_tacplus_shell                      2020-02-02       great      Yes    Arista restricted shell escape (with privesc)
   3   exploit/unix/ssh/array_vxag_vapv_privkey_privesc           2014-02-03       excellent  No     Array Networks vAPV and vxAG Private Key Privilege Escalation Code Execution
   4   exploit/linux/ssh/ceragon_fibeair_known_privkey            2015-04-01       excellent  No     Ceragon FibeAir IP-10 SSH Private Key Exposure
   5   exploit/linux/ssh/cisco_ucs_scpuser                        2019-08-21       excellent  No     Cisco UCS Director default scpuser password
   6   exploit/linux/ssh/exagrid_known_privkey                    2016-04-07       excellent  No     ExaGrid Known SSH Key and Default Password
   7   exploit/linux/ssh/f5_bigip_known_privkey                   2012-06-11       excellent  No     F5 BIG-IP SSH Private Key Exposure
   8   exploit/windows/ssh/freesshd_authbypass                    2010-08-11       excellent  Yes    Freesshd Authentication Bypass
   9   exploit/multi/http/gitlab_shell_exec                       2013-11-04       excellent  Yes    Gitlab-shell Code Execution
   10  exploit/linux/ssh/ibm_drm_a3user                           2020-04-21       excellent  No     IBM Data Risk Manager a3user Default Password
   11  exploit/linux/local/ptrace_traceme_pkexec_helper           2019-07-04       excellent  Yes    Linux Polkit pkexec helper PTRACE_TRACEME local root exploit
   12  exploit/linux/ssh/loadbalancerorg_enterprise_known_privkey 2014-03-17       excellent  No     Loadbalancer.org Enterprise VA SSH Private Key Exposure
   13  exploit/multi/http/git_submodule_command_exec              2017-08-10       excellent  No     Malicious Git HTTP Server For CVE-2017-1000117
   14  exploit/linux/ssh/mercurial_ssh_exec                       2017-04-18       excellent  No     Mercurial Custom hg-ssh Wrapper Remote Code Exec
   15  exploit/linux/ssh/microfocus_obr_shrboadmin                2020-09-21       excellent  No     Micro Focus Operations Bridge Reporter shrboadmin default password
   16  exploit/linux/ssh/quantum_dxi_known_privkey                2014-03-17       excellent  No     Quantum DXi V1000 SSH Private Key Exposure
   17  exploit/linux/ssh/quantum_vmpro_backdoor                   2014-03-17       excellent  No     Quantum vmPRO Backdoor Command
   18  post/linux/manage/sshkey_persistence                                        excellent  No     SSH Key Persistence
   19  exploit/unix/http/schneider_electric_net55xx_encoder       2019-01-25       excellent  Yes    Schneider Electric Pelco Endura NET55XX Encoder
   20  exploit/linux/ssh/solarwinds_lem_exec                      2017-03-17       excellent  No     SolarWinds LEM Default SSH Password Remote Code Execution
   21  exploit/linux/ssh/symantec_smg_ssh                         2012-08-27       excellent  No     Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability
   22  exploit/linux/http/symantec_messaging_gateway_exec         2017-04-26       excellent  No     Symantec Messaging Gateway Remote Code Execution
   23  exploit/unix/ssh/tectia_passwd_changereq                   2012-12-01       excellent  Yes    Tectia SSH USERAUTH Change Request Password Reset Vulnerability
   24  exploit/linux/http/ubiquiti_airos_file_upload              2016-02-13       excellent  No     Ubiquiti airOS Arbitrary File Upload
   25  exploit/linux/ssh/vmware_vdp_known_privkey                 2016-12-20       excellent  No     VMware VDP Known SSH Key
   26  exploit/linux/ssh/vyos_restricted_shell_privesc            2018-11-05       great      Yes    VyOS restricted-shell Escape and Privilege Escalation
   27  exploit/windows/local/unquoted_service_path                2001-10-25       excellent  Yes    Windows Unquoted Service Path Privilege Escalation
```

5.1.3 Domain

The domain service associated with port 53 is a distributed database system is used to translate human-friendly domain names into the IP addresses computers use to identify each other on the internet. Port 53 is used by DNS (Domain Name Service) for communication between DNS clients (such as web browsers or other applications) and DNS servers (which store and provide access to domain name information). DNS operates over both TCP and UDP. TCP port 53 is used for DNS zone transfers and other operations requiring reliable communication (Cloudflare, n.d.). There are considerable vulnerabilities associated with the domain service. It is highly vulnerable to attack.

Figure 17: Domain exploits (truncated)



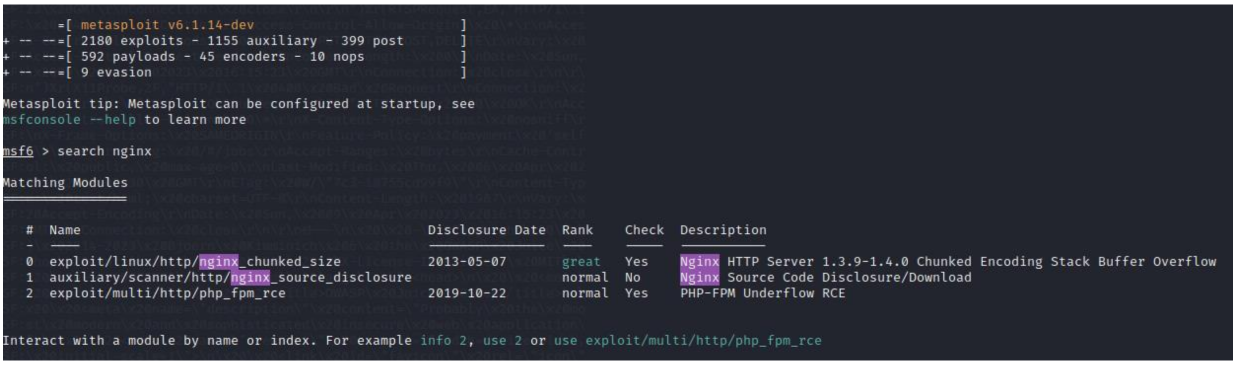
```
msf6 > search domain rank:great rank:excellent

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   exploit/windows/browser/adobe_flash_worker_byte_array_uaf  2015-02-02       great      No     Adobe Flash Player ByteArray With Workers Use After Free
   1   exploit/windows/browser/adobe_flash_casi32_int_overflow    2014-10-14       great      No     Adobe Flash Player casi32 Integer Overflow
   2   exploit/windows/browser/adobe_flash_domain_memory_uaf      2014-04-14       great      No     Adobe Flash Player domainMemory ByteArray Use After Free
   3   exploit/multi/misc/bmc_patrol_cmd_exec                     2019-01-17       excellent  No     BMC Patrol Agent Privilege Escalation Cmd Execution
   4   exploit/unix/dhcp/bash_environment                         2014-09-24       excellent  No     Dhclient Bash Environment Variable Injection (Shellshock)
   5   exploit/windows/http/hp_pcm_snac_update_domain             2013-09-09       excellent  Yes    HP ProCurve Manager SNAC UpdateDomainControllerServlet File Upload
   6   exploit/linux/local/juju_run_agent_priv_esc                2017-04-13       excellent  Yes    Juju-run Agent Privilege Escalation
   7   exploit/linux/http/microfocus_secure_messaging_gateway     2018-06-19       excellent  Yes    MicroFocus Secure Messaging Gateway Remote Code Execution
   8   exploit/windows/http/oracle_btm_writetofile                2012-08-07       excellent  No     Oracle Business Transaction Management FlashTunnelService Remote Code Exec
ution
   9   exploit/unix/http/pihole_whitelist_exec                    2018-04-15       excellent  Yes    Pi-Hole Whitelist OS Command Execution
   10  exploit/windows/http/sharepoint_data_deserialization       2020-07-14       excellent  Yes    SharePoint DataSet / DataTable Deserialization
   11  exploit/unix/webapp/webtester_exec                         2013-10-17       excellent  Yes    WebTester 5.x Command Execution
   12  exploit/windows/local/run_as                               1999-01-01       excellent  No     Windows Run Command As User
```

5.1.4 Nginx

Nginx is an open-source web server, reverse proxy server, and load balancer. It is known for its lightweight and event-driven architecture. This allows it to handle a large number of connections with low resource utilization. It uses an asynchronous, non-blocking I/O model. This making it highly suitable for serving static content, handling high levels of concurrent connections and acting as a reverse proxy for distributing incoming requests to multiple backend servers (Nginx, 2023).

It can also be used as a reverse proxy server. This allows it to distribute incoming requests to multiple backend servers, such as application servers or other web servers, to improve performance and ensure high availability. Nginx can also be used as a load balancer to evenly distribute incoming requests across multiple backend servers to optimize resource utilization. Metasploit indicates the service is highly vulnerable to exploitation.

Figure 18: Nginx exploits

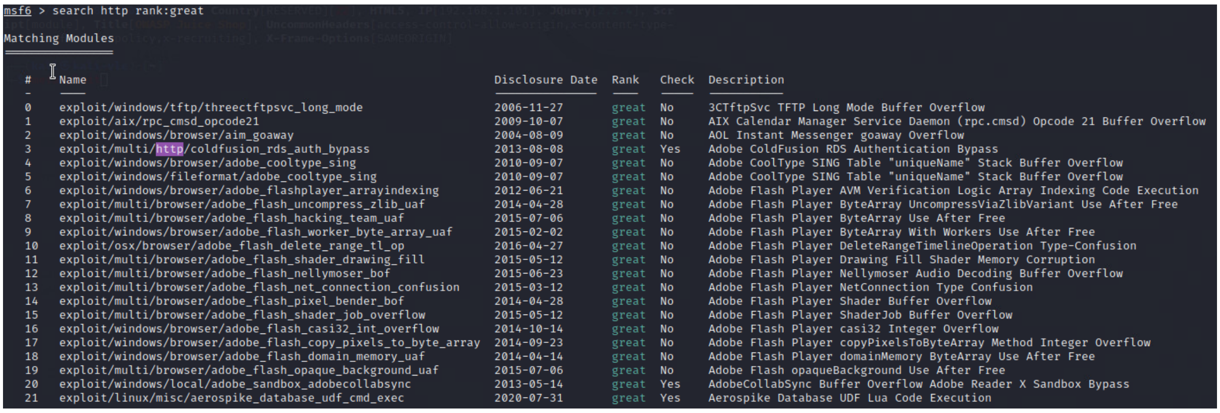


```
       =[ metasploit v6.1.14-dev                          ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more

msf6 > search nginx

Matching Modules
================

   #  Name                                         Disclosure Date  Rank    Check  Description
   -  ----                                         ---------------  ----    -----  -----------
   0  exploit/linux/http/nginx_chunked_size        2013-05-07       great   Yes    Nginx HTTP Server 1.3.9-1.4.0 Chunked Encoding Stack Buffer Overflow
   1  auxiliary/scanner/http/nginx_source_disclosure                 normal  No     Nginx Source Code Disclosure/Download
   2  exploit/multi/http/php_fpm_rce               2019-10-22       normal  Yes    PHP-FPM Underflow RCE


Interact with a module by name or index. For example info 2, use 2 or use exploit/multi/http/php_fpm_rce
```

5.1.5 HTTP

There is a universe of possibilities to exploit the HTTP service associated with port 80. Wasdat is already known to be insecure. A high level of vulnerability must therefore be assumed. The machine poses a serious security risk in its current state.

Figure 19: HTTP exploits (truncated)



```
msf6 > search http rank:great

Matching Modules
================

   #   Name                                                       Disclosure Date  Rank   Check  Description
   -   ----                                                       ---------------  ----   -----  -----------
   0   exploit/windows/tftp/threectftpsvc_long_mode               2006-11-27       great  No     3CTftpSvc TFTP Long Mode Buffer Overflow
   1   exploit/aix/rpc_cmsd_opcode21                              2009-10-07       great  No     AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
   2   exploit/windows/browser/aim_goaway                         2004-08-09       great  No     AOL Instant Messenger goaway Overflow
   3   exploit/multi/http/coldfusion_rds_auth_bypass              2013-08-08       great  Yes    Adobe ColdFusion RDS Authentication Bypass
   4   exploit/windows/browser/adobe_cooltype_sing                2010-09-07       great  No     Adobe CoolType SING Table "uniqueName" Stack Buffer Overflow
   5   exploit/windows/fileformat/adobe_cooltype_sing             2010-09-07       great  No     Adobe CoolType SING Table "uniqueName" Stack Buffer Overflow
   6   exploit/windows/browser/adobe_flashplayer_arrayindexing    2012-06-21       great  No     Adobe Flash Player AVM Verification Logic Array Indexing Code Execution
   7   exploit/multi/browser/adobe_flash_uncompress_zlib_uaf      2014-04-28       great  No     Adobe Flash Player ByteArray UncompressViaZlibVariant Use After Free
   8   exploit/multi/browser/adobe_flash_hacking_team_uaf         2015-07-06       great  No     Adobe Flash Player ByteArray Use After Free
   9   exploit/windows/browser/adobe_flash_worker_byte_array_uaf  2015-02-02       great  No     Adobe Flash Player ByteArray With Workers Use After Free
   10  exploit/osx/browser/adobe_flash_delete_range_tl_op         2016-04-27       great  No     Adobe Flash Player DeleteRangeTimelineOperation Type-Confusion
   11  exploit/multi/browser/adobe_flash_shader_drawing_fill      2015-05-12       great  No     Adobe Flash Player Drawing Fill Shader Memory Corruption
   12  exploit/multi/browser/adobe_flash_nellymoser_bof           2015-06-23       great  No     Adobe Flash Player Nellymoser Audio Decoding Buffer Overflow
   13  exploit/multi/browser/adobe_flash_net_connection_confusion 2015-03-12       great  No     Adobe Flash Player NetConnection Type Confusion
   14  exploit/multi/browser/adobe_flash_pixel_bender_bof         2014-04-28       great  No     Adobe Flash Player Shader Buffer Overflow
   15  exploit/multi/browser/adobe_flash_shader_job_overflow      2015-05-12       great  No     Adobe Flash Player ShaderJob Buffer Overflow
   16  exploit/windows/browser/adobe_flash_casi32_int_overflow    2014-10-14       great  No     Adobe Flash Player casi32 Integer Overflow
   17  exploit/windows/browser/adobe_flash_copy_pixels_to_byte_array 2014-09-23    great  No     Adobe Flash Player copyPixelsToByteArray Method Integer Overflow
   18  exploit/windows/browser/adobe_flash_domain_memory_uaf      2014-04-14       great  No     Adobe Flash Player domainMemory ByteArray Use After Free
   19  exploit/multi/browser/adobe_flash_opaque_background_uaf    2015-07-06       great  No     Adobe Flash opaqueBackground Use After Free
   20  exploit/windows/local/adobe_sandbox_adobecollabsync        2013-05-14       great  Yes    AdobeCollabSync Buffer Overflow Adobe Reader X Sandbox Bypass
   21  exploit/linux/misc/aerospike_database_udf_cmd_exec         2020-07-31       great  Yes    Aerospike Database UDF Lua Code Execution
```

6 Analysis and reporting

6.1 Vulnerability assessment

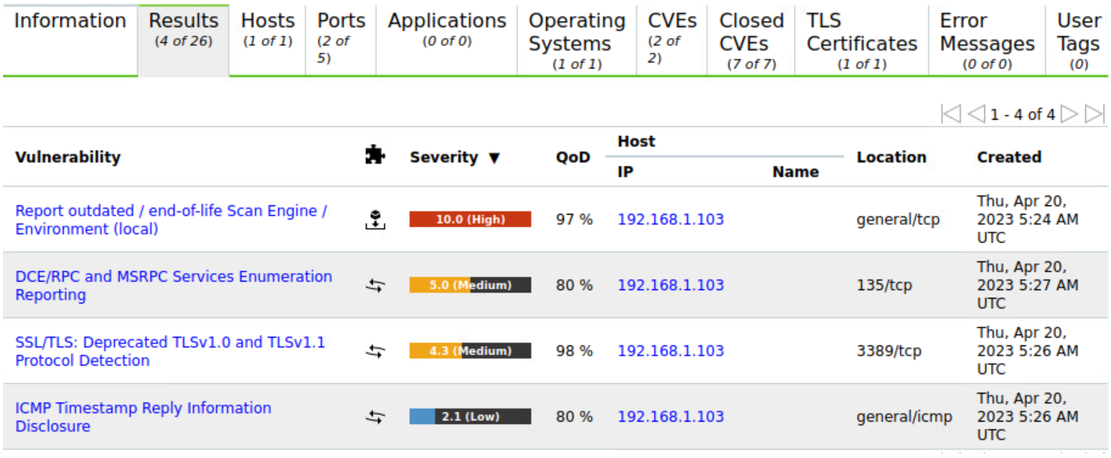
Scans were conducted using Greenbone Security Assistant. The scans were run on Greenbone version GVM-21.4.3. This was not the latest version. The data feed was fully up to date, however. The environment engine is at its end-of-life cycle. A wide array of vulnerabilities were found. These ranged from critical to insignificant. Much of the available software was severely out of date and vulnerable.

Scans uncovered multiple critical level vulnerabilities. Major improvements need to be made in order for Yritys Oy to function properly in the future. Further information concerning vulnerabilities are viewable in the images is presented in the discussion. A detailed breakdown of the scan results follows.

6.2 Flare-VM

Flare VM is in good condition according to Greenbone. The scans indicate three core vulnerabilities in the machine: two medium and one low. The machine does not require vast amounts of work to be a functional part of the business environment.

Figure 20: Flare-VM scan results



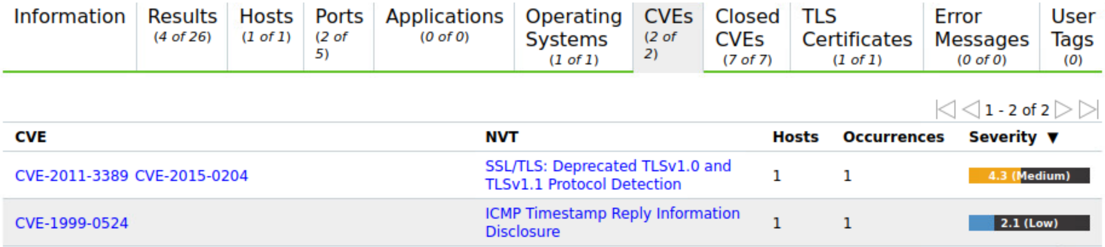
Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97 %	192.168.1.103		general/tcp	Thu, Apr 20, 2023 5:24 AM UTC
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80 %	192.168.1.103		135/tcp	Thu, Apr 20, 2023 5:27 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection		4.3 (Medium)	98 %	192.168.1.103		3389/tcp	Thu, Apr 20, 2023 5:26 AM UTC
ICMP Timestamp Reply Information Disclosure		2.1 (Low)	80 %	192.168.1.103		general/icmp	Thu, Apr 20, 2023 5:26 AM UTC

6.2.1 Threats

The main threat towards Flare-VM stems from out of date software. Much is at its end-of-life cycle. Scans did not uncover any significant software vulnerabilities but they are threats nevertheless. Potential risks in the future cannot be discounted.

There are always possibilities for zero-day vulnerabilities in outdated software. They should be also considered as threats because of the machine’s intended use. Flare-VM is above all a cyber security component. It contains a wide selection of security-related tools. If these tools are outdated they are not safe for security-related use. It is of critical importance that the available security toolset is as up to date as possible.

Figure 21: Flare-VM CVE vulnerabilities



CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-2011-3389 CVE-2015-0204	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	1	1	4.3 (Medium)
CVE-1999-0524	ICMP Timestamp Reply Information Disclosure	1	1	2.1 (Low)

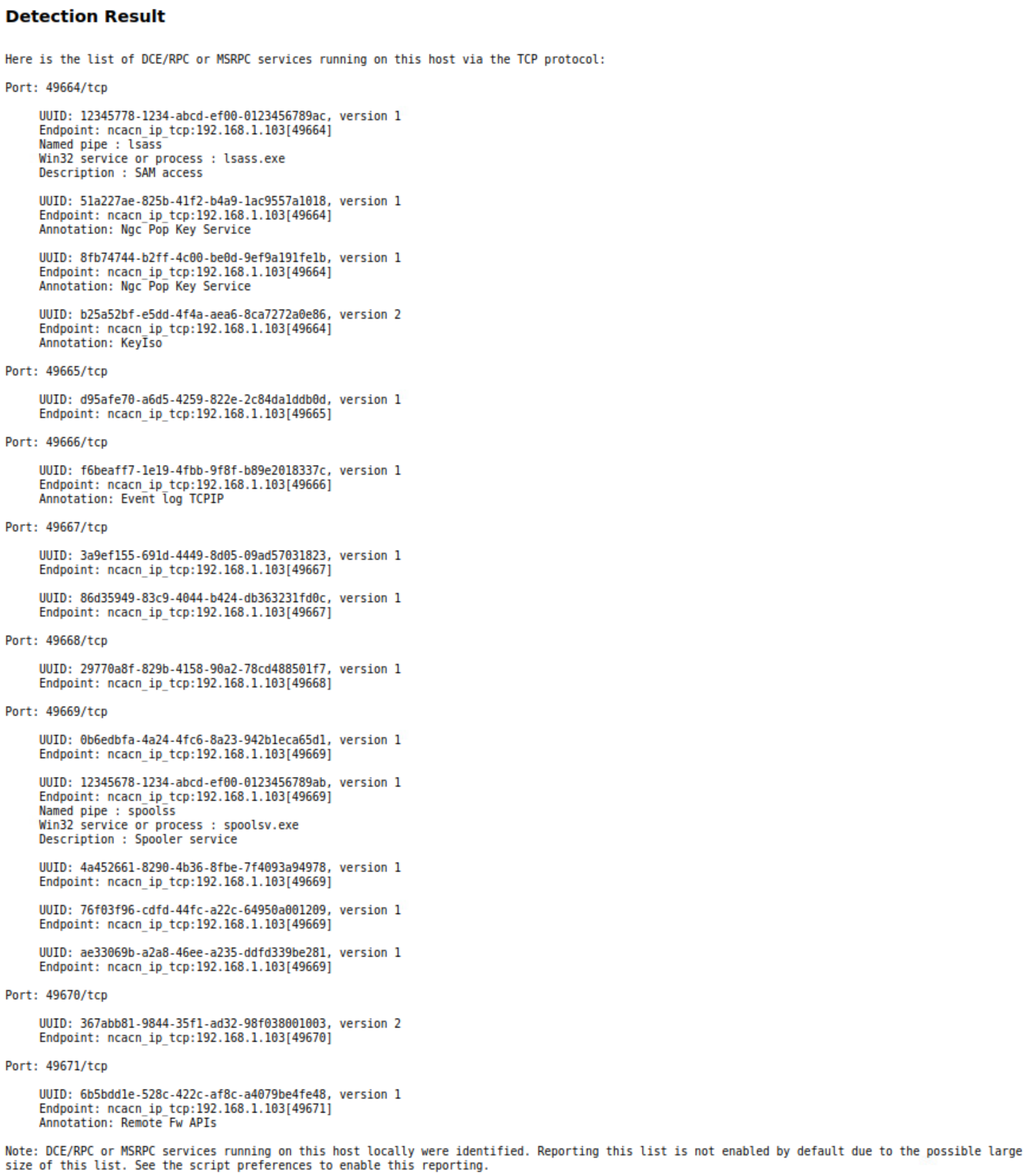
6.2.2 Vulnerabilties

There are distinct vulnerabilities on the machine. This includes a DCE/RPC and MSRPC Services Enumeration Reporting vulnerability with a 5.0 (medium) severity rating, an SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection vulnerability with a 4.3 (medium) severity rating and an ICMP Timestamp Reply Information Disclosure vulnerability with a 2.1 (low) severity.

The DCE/RPC and MSRPC Services Enumeration Reporting vulnerability affects the Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host. These can be enumerated by connecting to port 135. Malicious queries can be made using this port.

Greenbone also produces a list of potentially problematic ports in the scan report. Port scanning with Greenbone is useful because it is capable of scanning entire networks. Port scans were done with Greenbone and Nmap for a good reason. Greenbone provides a top-level view of vulnerabilities. Nmap is useful for gathering detailed information on specific IP addresses but lacks this general capability.

Figure 22: Greenbone TCP port scan results



Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: 49664/tcp

     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.103[49664]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access

     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.103[49664]
     Annotation: Ngc Pop Key Service

     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.103[49664]
     Annotation: Ngc Pop Key Service

     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.1.103[49664]
     Annotation: KeyIso

Port: 49665/tcp

     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.103[49665]

Port: 49666/tcp

     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.103[49666]
     Annotation: Event log TCPIP

Port: 49667/tcp

     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.103[49667]

     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.103[49667]

Port: 49668/tcp

     UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.103[49668]

Port: 49669/tcp

     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.103[49669]

     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.103[49669]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service

     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.103[49669]

     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.103[49669]

     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.103[49669]

Port: 49670/tcp

     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.1.103[49670]

Port: 49671/tcp

     UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.103[49671]
     Annotation: Remote Fw APIs

Note: DCE/RPC or MSRPC services running on this host locally were identified. Reporting this list is not enabled by default due to the possible large
size of this list. See the script preferences to enable this reporting.
```

The SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection vulnerability are found on a system containing known cryptographic flaws. These include CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) and CVE-2015-0204: Factoring RSA-EXPORT Keys (FREAK) attack on downgraded legacy encryption.

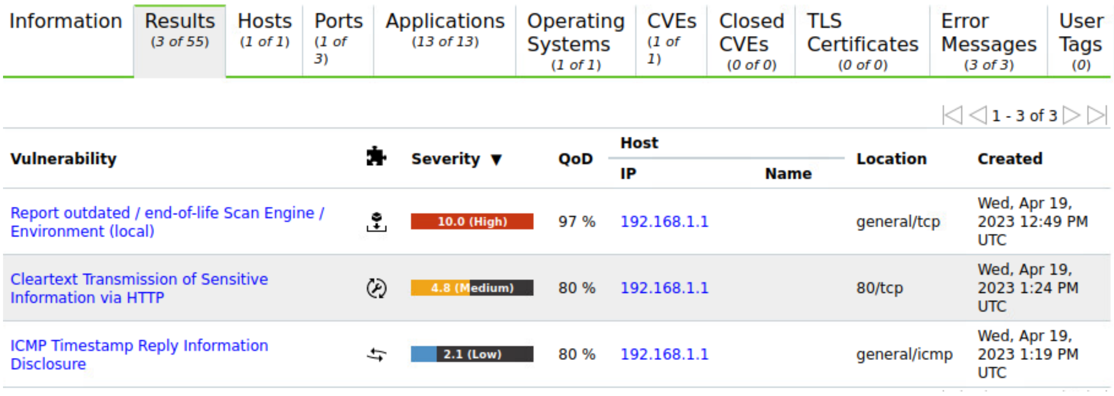
This affects all the operating systems and related software using the TLS1.0 and TLSv1.1 protocol. If the attacker is aware of these issues it is possible to eavesdrop on client connections and services. It would then be possible to gain access to sensitive data. These protocols should be updated as soon as possible.

The ICMP Timestamp Reply Information Disclosure vulnerability can be used to exploit time-based random number generators in other services. Support for the ICMP timestamp should be disabled.

6.3 pfSense

An internal scan of the PfSense firewall reveals no excessive vulnerabilities. Greenbone detected one medium level vulnerability and one low level vulnerability.

Figure 23: pfSense scan results



Information | Results (3 of 55) | Hosts (1 of 1) | Ports (1 of 3) | Applications (13 of 13) | Operating Systems (1 of 1) | CVEs (1 of 1) | Closed CVEs (0 of 0) | TLS Certificates (0 of 0) | Error Messages (3 of 3) | User Tags (0)

1 - 3 of 3

Vulnerability		Severity ▼	QoD	Host IP	Host Name	Location	Created
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97 %	192.168.1.1		general/tcp	Wed, Apr 19, 2023 12:49 PM UTC
Cleartext Transmission of Sensitive Information via HTTP		4.8 (Medium)	80 %	192.168.1.1		80/tcp	Wed, Apr 19, 2023 1:24 PM UTC
ICMP Timestamp Reply Information Disclosure		2.1 (Low)	80 %	192.168.1.1		general/icmp	Wed, Apr 19, 2023 1:19 PM UTC

6.3.1 Threats

The PfSense firewall is the first line of defense for the environment. As things stand it is working properly and does not exhibit any significant vulnerabilities. The firewall appears to be secure and running as intended. It is nevertheless prudent to consider all possible future scenarios in which the firewall could be compromised.

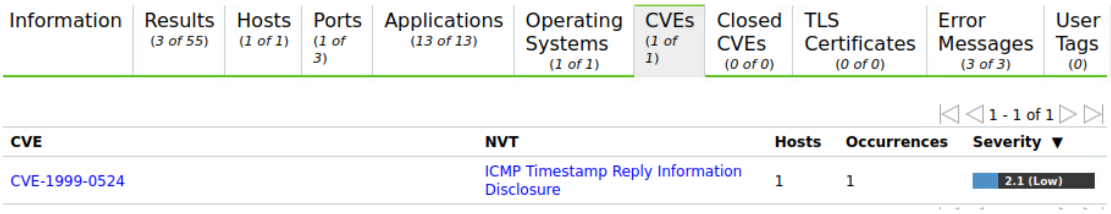
An out of date and improperly configured firewall could easily provide opportunities for potential attackers in the future. It should be noted that this particular threat assessment is based on Greenbone scan findings. It does not consider possible configuration problems.

6.3.2 Vulnerabilities

The main vulnerability on the firewall is the Cleartext Transmission of Sensitive Information via HTTP. This means there is no password encryption. Passwords are instead sent as cleartext via unencrypted HTTP. Communication between the client and the server can be compromised using a man-in-the-middle attack. Software such as Burp Suite could easily be used to intercept usernames and passwords. The ICMP

Timestamp Reply Information Disclosure vulnerability is also present in the firewall. This should be disabled as in the case of Flare VM.

Figure 24: Flare-VM CVE vulnerabilities



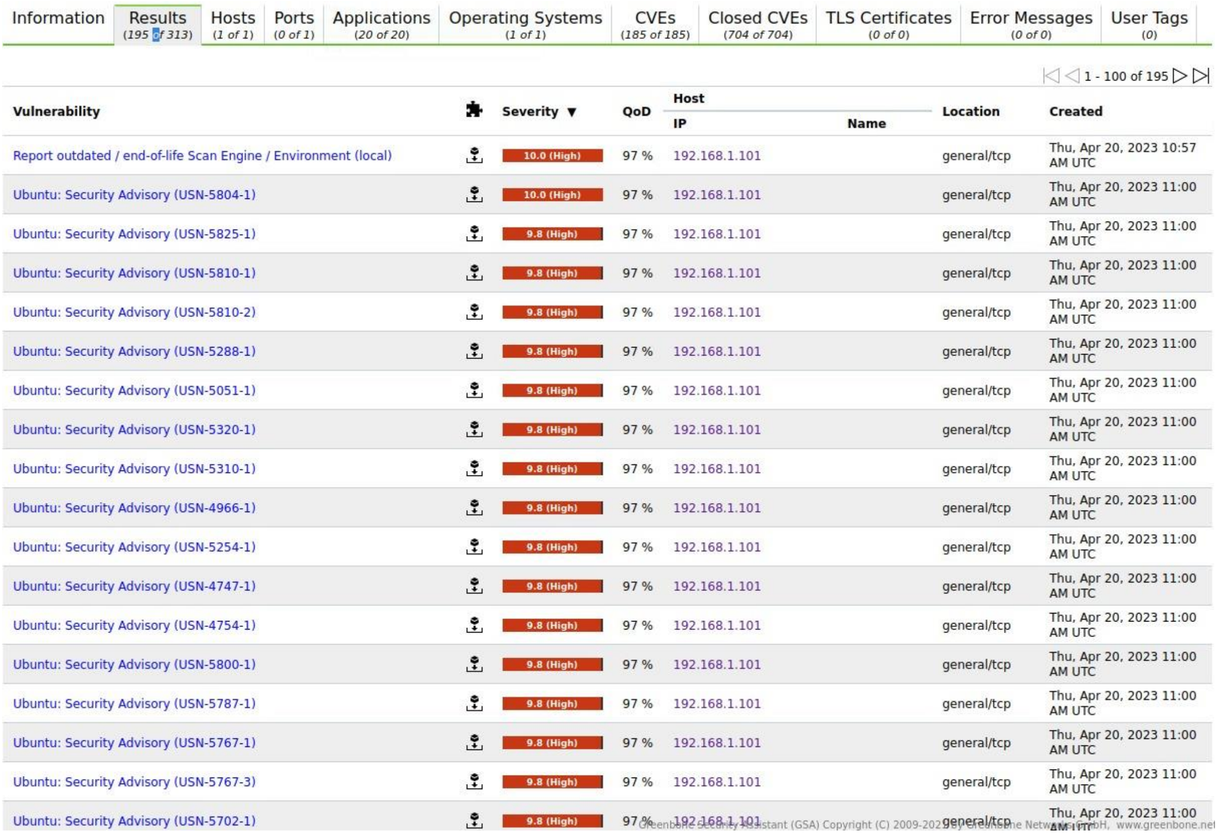
CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-1999-0524	ICMP Timestamp Reply Information Disclosure	1	1	2.1 (Low)

6.4 Wasdat

The Wasdat Linux server runs a webstore called OWASP Juice Shop. The condition of the machine can only be described as terrible. Scans reveal countless vulnerabilities. Most are on the higher end of the spectrum. A few medium and low-level vulnerabilities were also found. Given the omnipresence of high severity issues these low-level vulnerabilities are not a significant concern.

The level of threats and vulnerabilities affecting the Wasdat machine make it unsuitable for commercial and business use. The machine in its current form is frankly beyond repair. A fresh start is the most practical solution. Everything should be re-installed from the ground up.

Figure 25: Wasdat scan results (truncated)



Information | Results (195 of 313) | Hosts (1 of 1) | Ports (0 of 1) | Applications (20 of 20) | Operating Systems (1 of 1) | CVEs (185 of 185) | Closed CVEs (704 of 704) | TLS Certificates (0 of 0) | Error Messages (0 of 0) | User Tags (0)

1 - 100 of 195

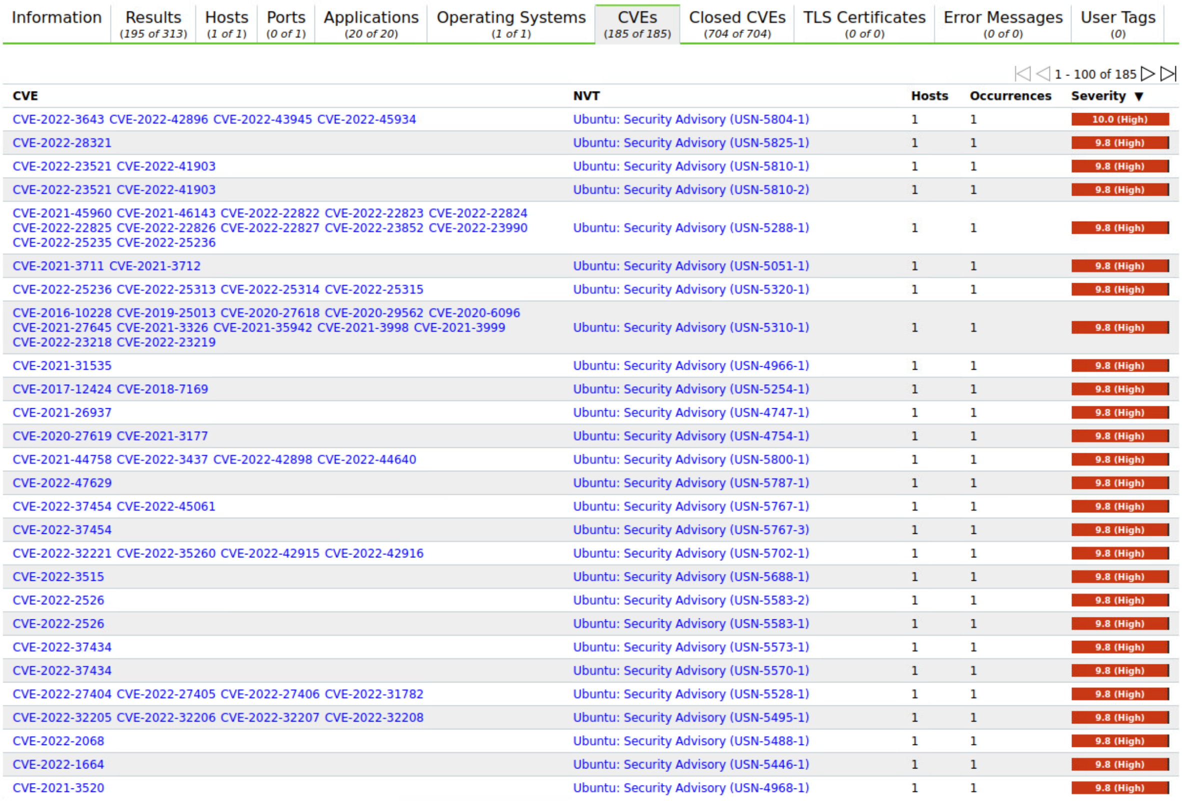
Vulnerability		Severity ▼	QoD	Host		Location	Created
				IP	Name		
Report outdated / end-of-life Scan Engine / Environment (local)		10.0 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 10:57 AM UTC
Ubuntu: Security Advisory (USN-5804-1)		10.0 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-5825-1)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-5810-1)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-5810-2)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-5288-1)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-5051-1)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-5320-1)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-5310-1)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-4966-1)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-5254-1)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-4747-1)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-4754-1)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-5800-1)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-5787-1)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-5767-1)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-5767-3)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC
Ubuntu: Security Advisory (USN-5702-1)		9.8 (High)	97 %	192.168.1.101		general/tcp	Thu, Apr 20, 2023 11:00 AM UTC

6.4.1 Threats

Greenbone scan Greenbone discovered 313 vulnerabilities on the Wasdat machine. There are 185 instances of CVE's and 704 instances of closed CVE's. The vulnerabilities are so numerous that the Wasdat machine's mere existence should be considered a threat.

Mitigating these threats individually would be a time-consuming process. The machine would be highly vulnerable to attack during any downtime. Gaining control of the machine would be easy for an experienced attacker. The instance should for this reason be isolated from the rest of the environment as soon as possible. Its presence in the network places all other machines at risk.

Figure 26: Wasdat CVE vulnerabilities (Truncated)



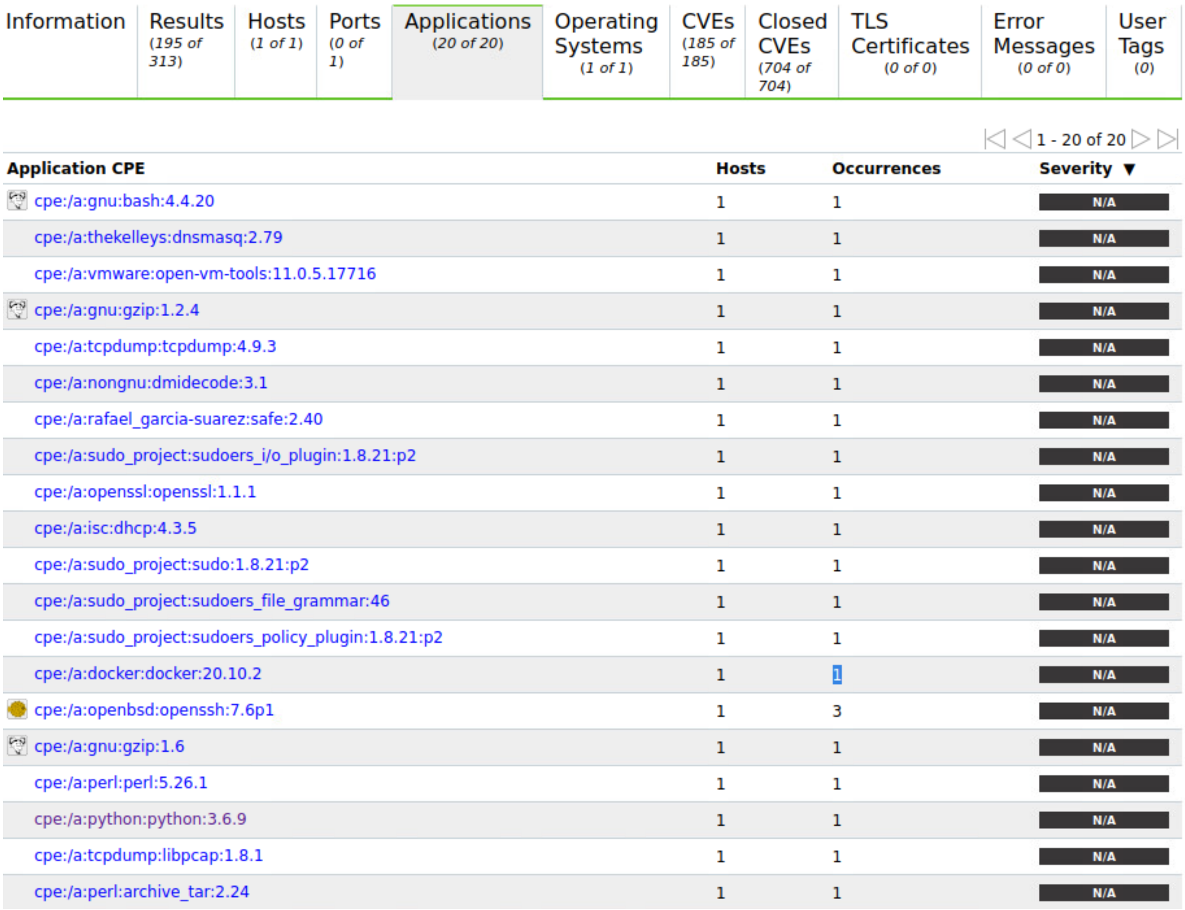
CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-2022-3643 CVE-2022-42896 CVE-2022-43945 CVE-2022-45934	Ubuntu: Security Advisory (USN-5804-1)	1	1	10.0 (High)
CVE-2022-28321	Ubuntu: Security Advisory (USN-5825-1)	1	1	9.8 (High)
CVE-2022-23521 CVE-2022-41903	Ubuntu: Security Advisory (USN-5810-1)	1	1	9.8 (High)
CVE-2022-23521 CVE-2022-41903	Ubuntu: Security Advisory (USN-5810-2)	1	1	9.8 (High)
CVE-2021-45960 CVE-2021-46143 CVE-2022-22822 CVE-2022-22823 CVE-2022-22824 CVE-2022-22825 CVE-2022-22826 CVE-2022-22827 CVE-2022-23852 CVE-2022-23990 CVE-2022-25235 CVE-2022-25236	Ubuntu: Security Advisory (USN-5288-1)	1	1	9.8 (High)
CVE-2021-3711 CVE-2021-3712	Ubuntu: Security Advisory (USN-5051-1)	1	1	9.8 (High)
CVE-2022-25236 CVE-2022-25313 CVE-2022-25314 CVE-2022-25315	Ubuntu: Security Advisory (USN-5320-1)	1	1	9.8 (High)
CVE-2016-10228 CVE-2019-25013 CVE-2020-27618 CVE-2020-29562 CVE-2020-6096 CVE-2021-27645 CVE-2021-3326 CVE-2021-35942 CVE-2021-3998 CVE-2021-3999 CVE-2022-23218 CVE-2022-23219	Ubuntu: Security Advisory (USN-5310-1)	1	1	9.8 (High)
CVE-2021-31535	Ubuntu: Security Advisory (USN-4966-1)	1	1	9.8 (High)
CVE-2017-12424 CVE-2018-7169	Ubuntu: Security Advisory (USN-5254-1)	1	1	9.8 (High)
CVE-2021-26937	Ubuntu: Security Advisory (USN-4747-1)	1	1	9.8 (High)
CVE-2020-27619 CVE-2021-3177	Ubuntu: Security Advisory (USN-4754-1)	1	1	9.8 (High)
CVE-2021-44758 CVE-2022-3437 CVE-2022-42898 CVE-2022-44640	Ubuntu: Security Advisory (USN-5800-1)	1	1	9.8 (High)
CVE-2022-47629	Ubuntu: Security Advisory (USN-5787-1)	1	1	9.8 (High)
CVE-2022-37454 CVE-2022-45061	Ubuntu: Security Advisory (USN-5767-1)	1	1	9.8 (High)
CVE-2022-37454	Ubuntu: Security Advisory (USN-5767-3)	1	1	9.8 (High)
CVE-2022-32221 CVE-2022-35260 CVE-2022-42915 CVE-2022-42916	Ubuntu: Security Advisory (USN-5702-1)	1	1	9.8 (High)
CVE-2022-3515	Ubuntu: Security Advisory (USN-5688-1)	1	1	9.8 (High)
CVE-2022-2526	Ubuntu: Security Advisory (USN-5583-2)	1	1	9.8 (High)
CVE-2022-2526	Ubuntu: Security Advisory (USN-5583-1)	1	1	9.8 (High)
CVE-2022-37434	Ubuntu: Security Advisory (USN-5573-1)	1	1	9.8 (High)
CVE-2022-37434	Ubuntu: Security Advisory (USN-5570-1)	1	1	9.8 (High)
CVE-2022-27404 CVE-2022-27405 CVE-2022-27406 CVE-2022-31782	Ubuntu: Security Advisory (USN-5528-1)	1	1	9.8 (High)
CVE-2022-32205 CVE-2022-32206 CVE-2022-32207 CVE-2022-32208	Ubuntu: Security Advisory (USN-5495-1)	1	1	9.8 (High)
CVE-2022-2068	Ubuntu: Security Advisory (USN-5488-1)	1	1	9.8 (High)
CVE-2022-1664	Ubuntu: Security Advisory (USN-5446-1)	1	1	9.8 (High)
CVE-2021-3520	Ubuntu: Security Advisory (USN-4968-1)	1	1	9.8 (High)

6.4.2 Vulnerabilities

Most of the vulnerabilities present on the Wasdat machine fall under the headline Ubuntu security advisory. Those responsible for the construction and maintenance of the website are guilty of negligence in the extreme.

Everything on the machine is outdated. Listing all application vulnerabilities would be an exercise in futility. Critical applications are all highly vulnerable. The version of Python on the machine is spectacularly out of date. The current version is 3.11.1. Wasdat is running version 3.6.9. This means attackers could easily run malicious code on the system. Much of the basic Linux software is missing. Many essential operating system updates have fallen by the wayside.

Figure 27: Outdated application versions



Application CPE	Hosts	Occurrences	Severity ▼
cpe:/a:gnu:bash:4.4.20	1	1	N/A
cpe:/a:thekelleys:dnsmasq:2.79	1	1	N/A
cpe:/a:vmware:open-vm-tools:11.0.5.17716	1	1	N/A
cpe:/a:gnu:gzip:1.2.4	1	1	N/A
cpe:/a:tcpdump:tcpdump:4.9.3	1	1	N/A
cpe:/a:nongnu:dmidecode:3.1	1	1	N/A
cpe:/a:rafael_garcia-suarez:safe:2.40	1	1	N/A
cpe:/a:sudo_project:sudoers_i/o_plugin:1.8.21:p2	1	1	N/A
cpe:/a:openssl:openssl:1.1.1	1	1	N/A
cpe:/a:isc:dhcp:4.3.5	1	1	N/A
cpe:/a:sudo_project:sudo:1.8.21:p2	1	1	N/A
cpe:/a:sudo_project:sudoers_file_grammar:46	1	1	N/A
cpe:/a:sudo_project:sudoers_policy_plugin:1.8.21:p2	1	1	N/A
cpe:/a:docker:docker:20.10.2	1	1	N/A
cpe:/a:openbsd:openssh:7.6p1	1	3	N/A
cpe:/a:gnu:gzip:1.6	1	1	N/A
cpe:/a:perl:perl:5.26.1	1	1	N/A
cpe:/a:python:python:3.6.9	1	1	N/A
cpe:/a:tcpdump:libpcap:1.8.1	1	1	N/A
cpe:/a:perl:archive_tar:2.24	1	1	N/A

7 Risk analysis

7.1 Risk matrix

Table 8 organizes the analysis above into a semi-quantitative risk matrix. The purpose of the matrix is to provide a greater understanding of the relationship between the probability and severity of potential attacks. The matrix has predefined values based on these categories. Values range from 1-25 and are color-coded.

Green risk values indicate a low probability and severity of attack. Yellow risk values indicate a medium probability and severity of attack. Red risk values indicate a high probability and severity of attack. Probability and severity values are multiplied to produce the overall risk level. Red risk values occur between the values of 15-25. Machines with risk levels in the red zone should be addressed with great urgency.

Table 7: Risk probability and severity matrix

	Severity				
Probability	1	2	3	4	5
	2	4	6	8	10
	3	6	9	12	15
	4	8	12	16	20
	5	10	15	20	25

7.2 Risk levels

The matrix was applied to the machines in the network to gain a better understanding their risk levels.

Table 8: Risk level

Asset	Risk	Probability	Impact	Risk Level
Flare-VM	Message queueing service path overflow	3	2	**6**
	DCE/RPC and MSRPC Services Enumeration Reporting vulnerability	3	1	**3**
	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol	2	4	**8**
pfSense	Cleartext Transmission of Sensitive Information via HTTP	2	5	**10**
Wasdat	Many high probability and high severity risks	5	5	**25**

Table 9 illustrates the typical risk levels confronting the company network. Risks appearing in the table are associated with specific exploitable vulnerabilities uncovered during the audit process. They are directly relevant because they correspond to a service or software in use on the company network. It is important that scan output is recontextualized to account for these details. This is an important caveat because not every vulnerability can be easily exploited.

Metasploit provides detailed lists of available exploits for a given service. But many are outdated and all are version specific. This is why most risks appear in the Goldilocks zone of risk levels. It should also be noted that the risks highlighted in the table do not reflect the totality of security challenges. They instead provide an overall picture of risk levels. But even a top-level perspective unambiguously indicates the Wasdat machine to be a serious security risk. The Flare-VM machine and pfSense firewall are in much better shape.

8 Summary and recommendations

The environment has both strengths and weaknesses. Flare-VM and the pfSense firewall are in relatively good shape. The main problem is the Wasdat machine. While not in terminal condition, both the Flare-VM and pfSense are out of date. They should not be used for commercial or business purposes in their current condition. But these systems are easily updatable and can be brought up to standard with minimal effort.

For Flare-VM the recommendation is to update all necessary software. Legacy software should be uninstalled. These are not an issue currently but might become so in the future. Regular documentation of changes within the operating system is advised. Access to the system should be tightened. Passwords should be regularly updated. The company should also familiarize itself with and implement zero-trust policies and other forms of hardening.

The same can be said of the pfSense machine. The firewall should be updated on a continuous basis. Firewall controls should also be tightened. Only minimal and as-needed access to the system should be permitted. All the port and vulnerability scans were without changing firewall settings. This is in and of itself a security risk. Only authorized personnel should have access to the firewall. Only authorized traffic should be allowed to traverse the network. This is a critical aspect of the abovementioned zero-trust policy framework.

The Wasdat machine is beyond redemption. The least-bad option is to format the hard drive and rebuild the system from scratch. The machine exhibits a smörgåsbord of vulnerabilities that endanger the entire environment. They are easily hackable and exploitable by bad actors. It might already be under a slow-burning attack given the extent of its vulnerabilities.

It is easy to overlook individual problems when they are legion. Fixing Wasdat's problems on a piecemeal basis could potentially open new backdoors and introduce additional vulnerabilities. A better solution is to build a new webstore that meets modern standards for proper business use.

The company should consider customer and transaction safety, GDPR standards and other necessary security measures when building future webstores. This will secure the company's reputation as a responsible actor in the field of commerce. The company does not want to find itself in a situation where lax security causes measurable damage to the customer-base.

9 Conclusions and reflections

The task was very interesting. It presented a unique opportunity for a deep dive into the auditing process. It was completed using a learning-by-doing approach. In this way it was possible to reflect the subtle granularities of the process and results while drawing appropriate conclusions.

A key takeaway was that audits should be scientific. They should follow rules and meet appropriate standards. These include not only formal standards such as those promoted by the ISO. They should also meet standards for argumentation. The purpose of an audit is ultimately to build a case for a course of action. Audits should therefore be approached systematically and follow an internal logic.

It was important that the report also be readable and engaging. The audience of the report was management so the report was written with this in mind. The idea was that the report should be a living document. It was important that it also fulfill the basic scientific criteria of reproducibility. These were the foundational principles around which the processes and elements of the audit were organized.

Some technical challenges were encountered. These primarily related to Kali and Greenbone. The tools allocated were useful but temperamental. Fixing these resulted in a broken Kali instance. But these challenges were ultimately overcome. It was possible to salvage the necessary information without sacrificing the consistency and scope of the report.

A great deal was learned from the experience. Considerable efforts were made to ensure the final document met the task requirements. In our estimation the report clearly demonstrates the strengths and weaknesses of the environment and provides systematic solutions to the problems therein. We think the final result speaks for itself.

10 Works cited

Barnea, B. (2022, December 8). *An overview of MS-RPC and its security mechanisms*. Akamai. Retrieved April 15, 2023, from https://www.akamai.com/blog/security-research/msrpc-security-mechanisms

Features. (n.d.). OpenSSH. Retrieved April 15, 2023, from https://www.openssh.com/features.html

FLARE VM *Update*. (n.d.). Mandiant. Retrieved April 15, 2023, from https://www.mandiant.com/resources/blog/flare-vm-update

International Organization for Standardization. (2018). ISO/IEC 19011-2018:2018:fi. *In Suomen Standardisoimisliitto*. ISO/IEC 2018.

Nginx. (2023, April 11). *Advanced load balancer, web server, & reverse proxy*. NGINX. Retrieved April 15, 2023, from https://www.nginx.com/

pfSense Plus Firewall. (n.d.). pfSense. Retrieved April 15, 2023, from https://www.netgate.com/pfsense-plus-applications/firewall

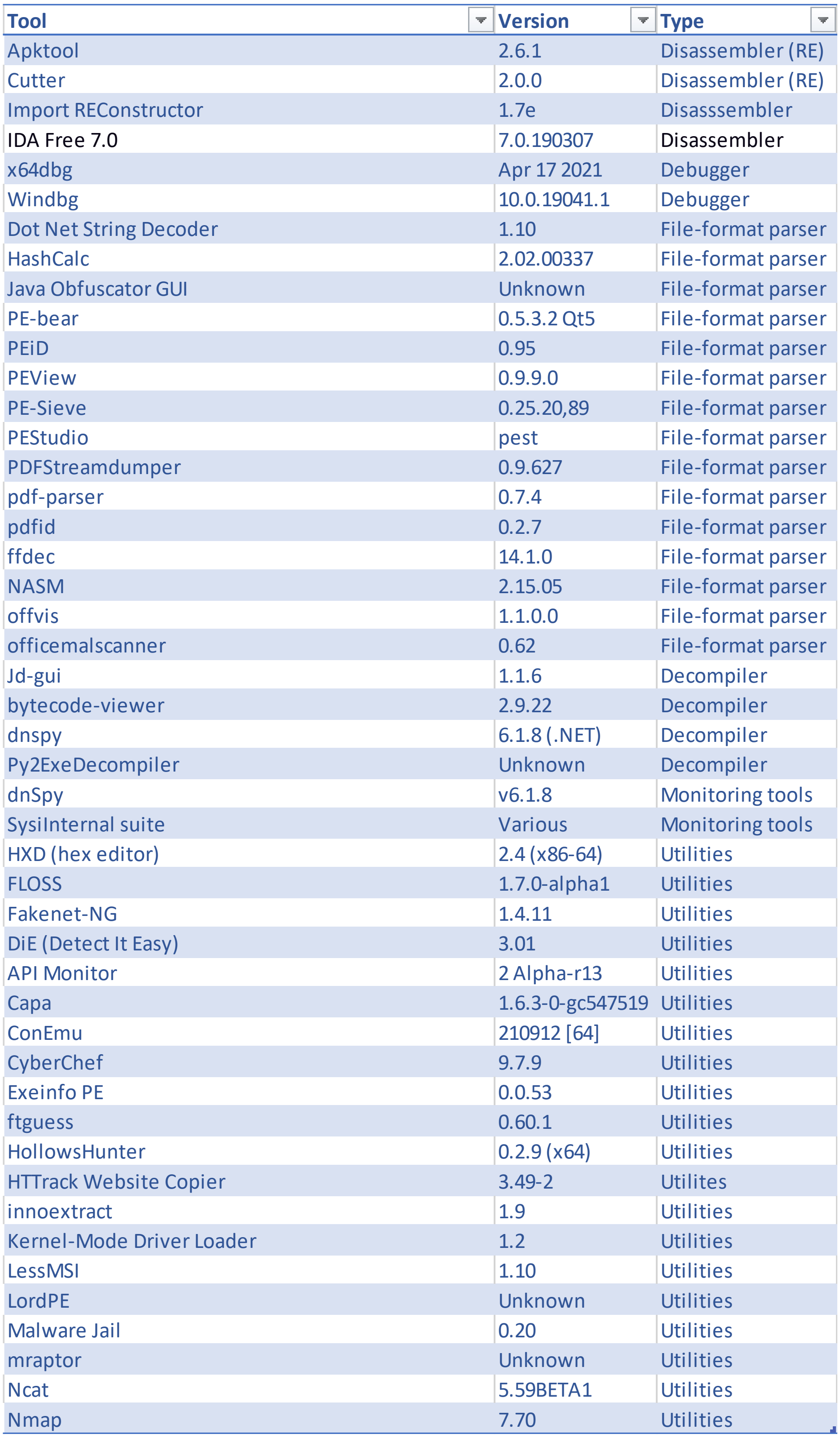
Penetration Testing Software, Pen Testing Security. (n.d.). Metasploit. Retrieved April 15, 2023, from https://www.metasploit.com/

What is DNS? | How DNS works. (n.d.) Cloudflare. Retrieved April 15, 2023, from https://www.cloudflare.com/learning/dns/what-is-dns/

11 Appendices

11.1 Appendix 1: Malware analysis tools

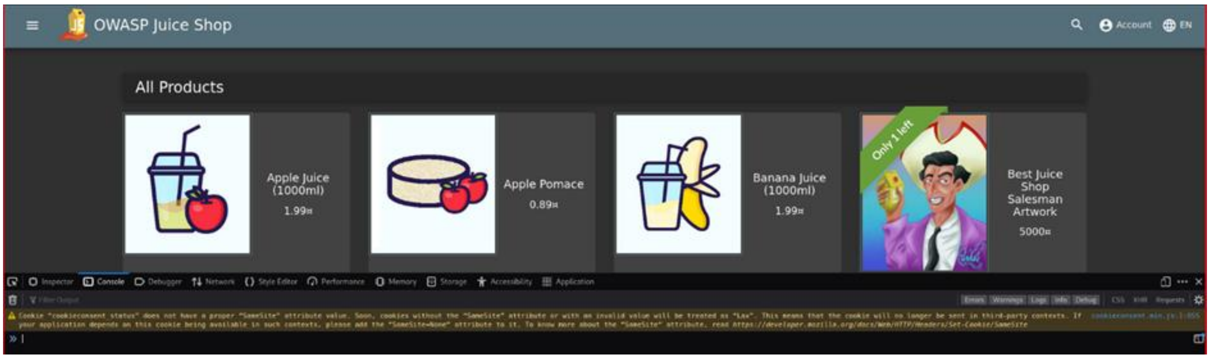
Table 9: Flare-VM tools



Tool	Version	Type
Apktool	2.6.1	Disassembler (RE)
Cutter	2.0.0	Disassembler (RE)
Import REConstructor	1.7e	Disasssembler
IDA Free 7.0	7.0.190307	Disassembler
x64dbg	Apr 17 2021	Debugger
Windbg	10.0.19041.1	Debugger
Dot Net String Decoder	1.10	File-format parser
HashCalc	2.02.00337	File-format parser
Java Obfuscator GUI	Unknown	File-format parser
PE-bear	0.5.3.2 Qt5	File-format parser
PEiD	0.95	File-format parser
PEView	0.9.9.0	File-format parser
PE-Sieve	0.25.20,89	File-format parser
PEStudio	pest	File-format parser
PDFStreamdumper	0.9.627	File-format parser
pdf-parser	0.7.4	File-format parser
pdfid	0.2.7	File-format parser
ffdec	14.1.0	File-format parser
NASM	2.15.05	File-format parser
offvis	1.1.0.0	File-format parser
officemalscanner	0.62	File-format parser
Jd-gui	1.1.6	Decompiler
bytecode-viewer	2.9.22	Decompiler
dnspy	6.1.8 (.NET)	Decompiler
Py2ExeDecompiler	Unknown	Decompiler
dnSpy	v6.1.8	Monitoring tools
SysInternal suite	Various	Monitoring tools
HXD (hex editor)	2.4 (x86-64)	Utilities
FLOSS	1.7.0-alpha1	Utilities
Fakenet-NG	1.4.11	Utilities
DiE (Detect It Easy)	3.01	Utilities
API Monitor	2 Alpha-r13	Utilities
Capa	1.6.3-0-gc547519	Utilities
ConEmu	210912 [64]	Utilities
CyberChef	9.7.9	Utilities
Exeinfo PE	0.0.53	Utilities
ftguess	0.60.1	Utilities
HollowsHunter	0.2.9 (x64)	Utilities
HTTrack Website Copier	3.49-2	Utilites
innoextract	1.9	Utilities
Kernel-Mode Driver Loader	1.2	Utilities
LessMSI	1.10	Utilities
LordPE	Unknown	Utilities
Malware Jail	0.20	Utilities
mraptor	Unknown	Utilities
Ncat	5.59BETA1	Utilities
Nmap	7.70	Utilities

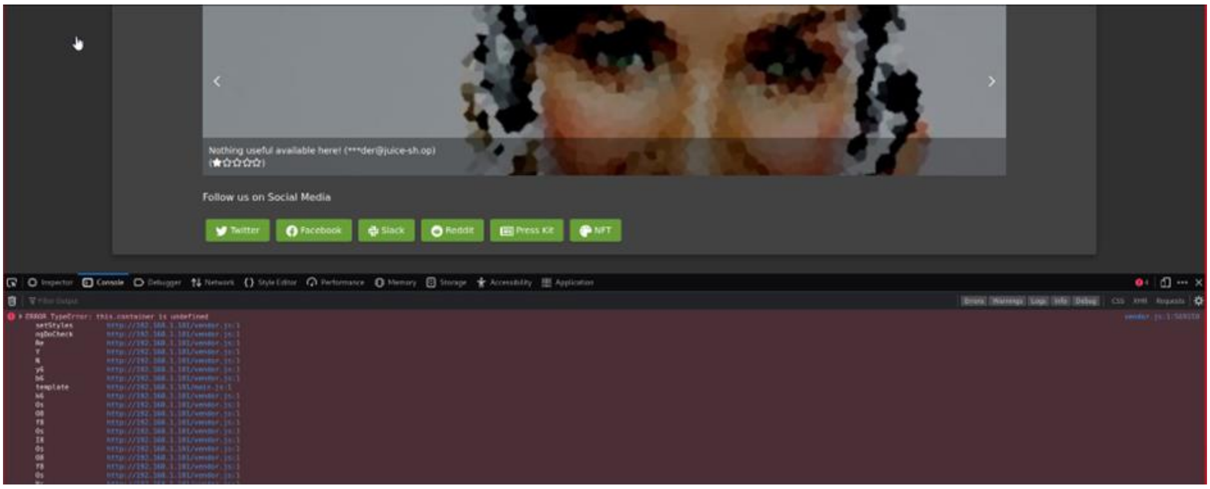
11.2 Appendix 2: Visible security vulnerabilities

Figure 28: Improper Samesite attribute



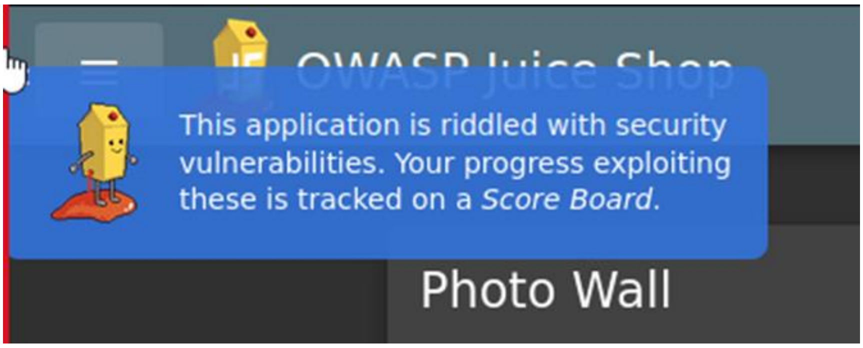
```
⚠ Cookie "cookieconsent_status" does not have a proper "SameSite" attribute value. Soon, cookies without the "SameSite" attribute or with an invalid value will be treated as "Lax". This means that the cookie will no longer be sent in third-party contexts. If     cookieconsent.min.js:1:855
  your application depends on this cookie being available in such contexts, please add the "SameSite=None" attribute to it. To know more about the "SameSite" attribute, read https://developer.mozilla.org/docs/Web/HTTP/Headers/Set-Cookie/SameSite
```

Figure 29: Undefined container



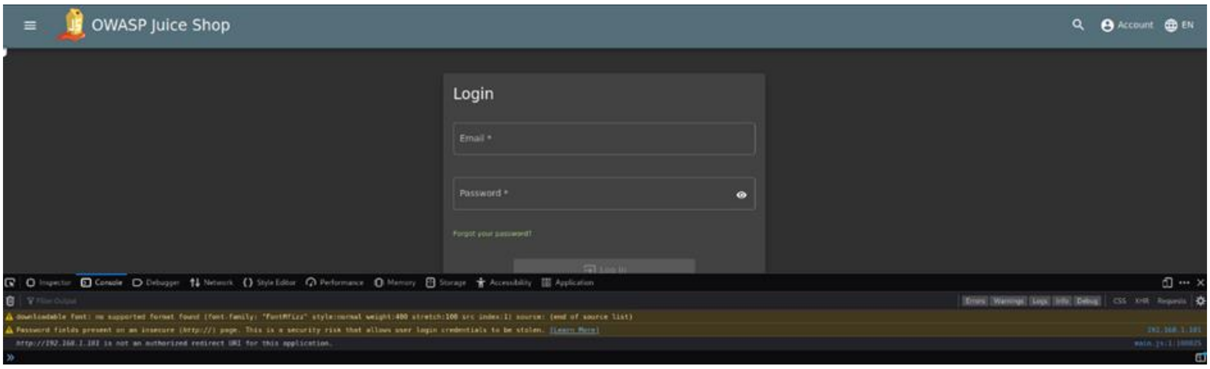
```
● ▸ ERROR TypeError: this.container is undefined                                   vendor.js:1:569318
      setStyles      http://192.168.1.101/vendor.js:1
      ngDoCheck      http://192.168.1.101/vendor.js:1
      Re             http://192.168.1.101/vendor.js:1
      Y              http://192.168.1.101/vendor.js:1
      N              http://192.168.1.101/vendor.js:1
      y6             http://192.168.1.101/vendor.js:1
      b6             http://192.168.1.101/vendor.js:1
      template       http://192.168.1.101/main.js:1
      W6             http://192.168.1.101/vendor.js:1
      Os             http://192.168.1.101/vendor.js:1
      O8             http://192.168.1.101/vendor.js:1
      F8             http://192.168.1.101/vendor.js:1
      Os             http://192.168.1.101/vendor.js:1
      I8             http://192.168.1.101/vendor.js:1
      Os             http://192.168.1.101/vendor.js:1
      O8             http://192.168.1.101/vendor.js:1
      F8             http://192.168.1.101/vendor.js:1
      Os             http://192.168.1.101/vendor.js:1
```

Figure 30: Vulnerability login popup



This application is riddled with security vulnerabilities. Your progress exploiting these is tracked on a *Score Board*.

Figure 31: Insecure password field



```
⚠ downloadable font: no supported format found (font-family: "FontMfizz" style:normal weight:400 stretch:100 src index:1) source: (end of source list)
⚠ Password fields present on an insecure (http://) page. This is a security risk that allows user login credentials to be stolen. [Learn More]    192.168.1.101
  http://192.168.1.101 is not an authorized redirect URI for this application.    main.js:1:100825
```