Simulated Penetration Testing

Alexander Batker
2024

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The penetration testing findings on Upwork's network were done on April 19, 2024, and summarized in this report. Four skilled security professionals from Arizona State University conducted the tests using Kali Linux, Nmap, Enum4Linux, netcat, Nessus Vulnerability Scanning, Metasploit, and CrackMapExec. A penetration test involves simulated attacks on a network or technological systems. These tests are important to identify and help strengthen cyber security. The key findings from the three targets were open ports for Target 1, RPC and Backdoor vulnerabilities for Target 2, and remote vulnerabilities with Target 3. Some recommendations include vulnerability categorization, improved patching policy, configuration review, continuous monitoring, and further staff training.

INTRODUCTION

Project 1 involved doing OSINT collecting for Upwork to gather information about the company including, but not limited to the company profile, executive leadership, employee personas, financials, network, and social media. There was a risk assessment done solely with OSINT collection with recommendations. To continue forward, penetration testing (pen testing) was done involving three targets using a variety of tools such as Nmap/Zenmap, enum4linux, and more.

The purpose of this project report is to further our findings to evaluate Upwork's network, posturing of their system, and applications. Simulating real-world cyber-attacks helps to find and identify potential vulnerabilities that were not caught during the OSINT phase, along with other weaknesses. Goals of any security professional who partake in pen testing, assess effectiveness of current security, identify any hidden risks, and strengthen cyber defenses.

Our goal is to aid Upwork in understanding their cyber landscape, allowing for the company to make better decisions in their online presence as well as systems and networks. These reports from targets 1-3 will give insight on identified vulnerabilities, along with actionable suggestions to alleviate some of those cyber security issues which will help Upwork in their cyber resilience as they thrive and promote flexibility and working remotely.

SCOPE

There are three targets undergoing pen testing. The details of the three targets are as follows.

Target 1

Using Kali Linux, Nmap is used. First, there is a connect scan for various open ports on 192.168.122.243. Then there is a full scan. Enum4Linux is the next one used for a full analysis. Next, there's a Nessus Basic Scan run. CrackMapExec is used to find users using SMB. Continuing forward, a Metasploit SMB search is done, and therefore concludes the systems and scans used for Target 1.

Target 2

Using Kali Linux, a Nmap SYN scan is done to find open ports on 192.168.122.44. A further comprehensive scan with version detection is done using Nmap. An Enum4Linux scan is

done on the IP address for Target 2. A Nessus Basic Network Scan is done on Target 2, concluding the systems and applications used for Target 2. Metasploit is used to identify exploits of Target 2's services.

Target 3

Using Kali Linux, there's a swift Nmap sweep unveiling the active hosts on 192.168.122.8. Enum4Linux is used on Target 2 to extract system insights. A Nessus basic scan is conducted next to find critical vulnerabilities. Netcat probes the network services to see if the Target 3 system is vulnerable. Metasploit is used to exploit a vulnerability found from the Nessus scanning to conclude all that is used for the Target 3 tests.

DETAILS

4.1. Details Section One

Target 1 uses multiple methods of scanning which will be explained in the following subsection steps. The first step taken is using Kali Linux and conducting an ARP-scan to find the target host IP address which is 192.168.122.243.

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 0c:5d:7b:d3:00:00, IPv4: 192.168.122.118
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.122.1   52:54:00:ff:9f:b3       (Unknown: locally administered)
192.168.122.243 0c:cb:3b:a4:00:00       (Unknown)
192.168.122.1   52:54:00:ff:9f:b3       (Unknown: locally administered) (DUP: 2)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.138 seconds (119.74 hosts/sec). 2 responded
```

Figure 1: Target 1 arp-scan to find hosts.

The next section will look at the Nmap steps taken.

4.1.1. Details Section One – Subsection One

Starting with Nmap, we initiate an ARP Ping Scan.

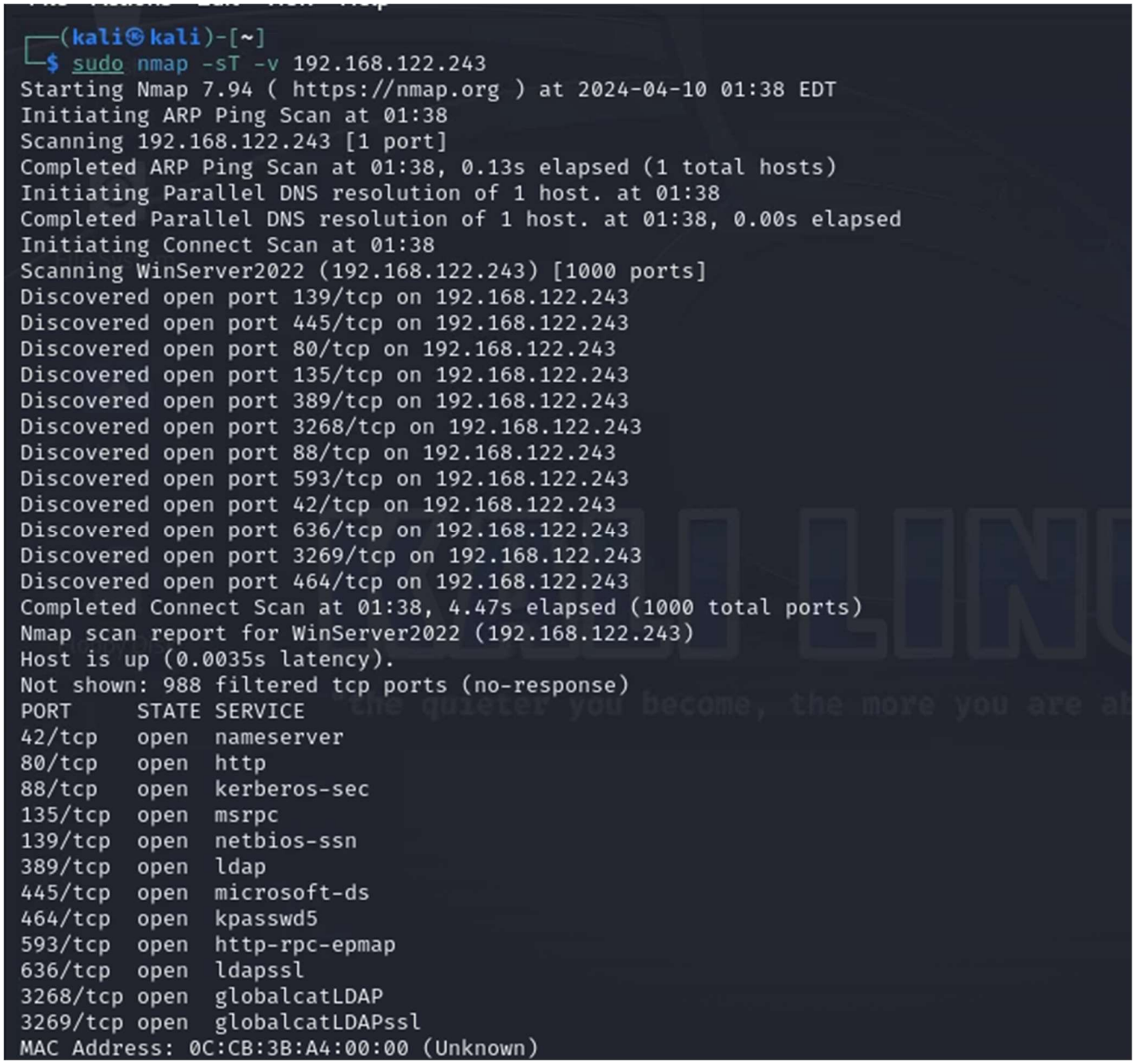

Figure 2: Target 1's Nmap connect scan, which lists various open ports and the services.

In Fig. 2, we scan for open ports, and find many open ports with the port and service name. Furthermore, we then dive deeper on the host using the Nmap command "-A" at the IP address 192.168.122.243. For Figures 3 and 4, we highlight the results discovered on the systems used on the Target 1 host.

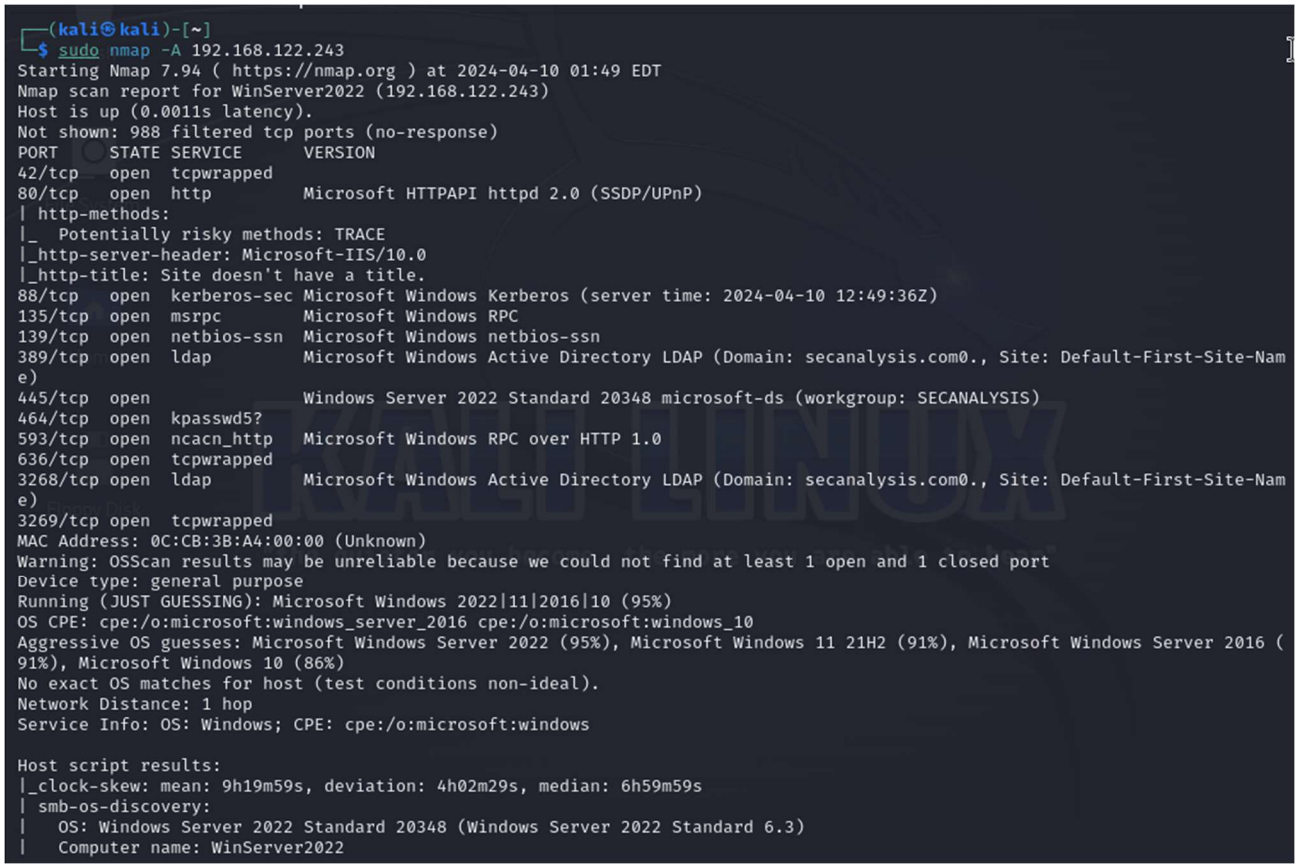

Figure 3: Target 1's -A scan results from Nmap (1/2).

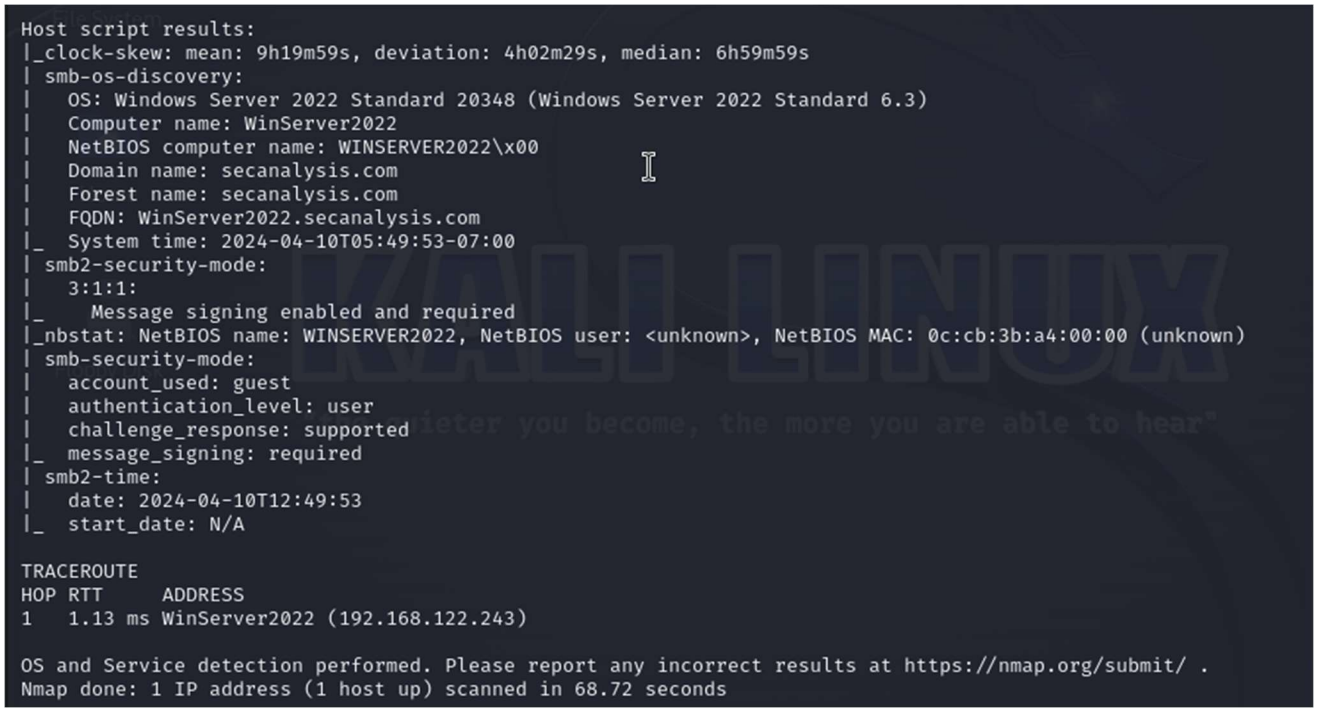

Figure 4: Target 1's -A scan results from Nmap (2/2).

Target 1 is using WinServer2022 and displays the OS, computer name, domain name, and the user level on the system being used. After this scan, we then use Enum4Linux in the next subsection.

4.1.2. Details Section One – Subsection Two

Using the system Enum4Linux to do a whole Target 1 scan, we get the domain name from the results, and not much else is revealed from the Enum4Linux scan.

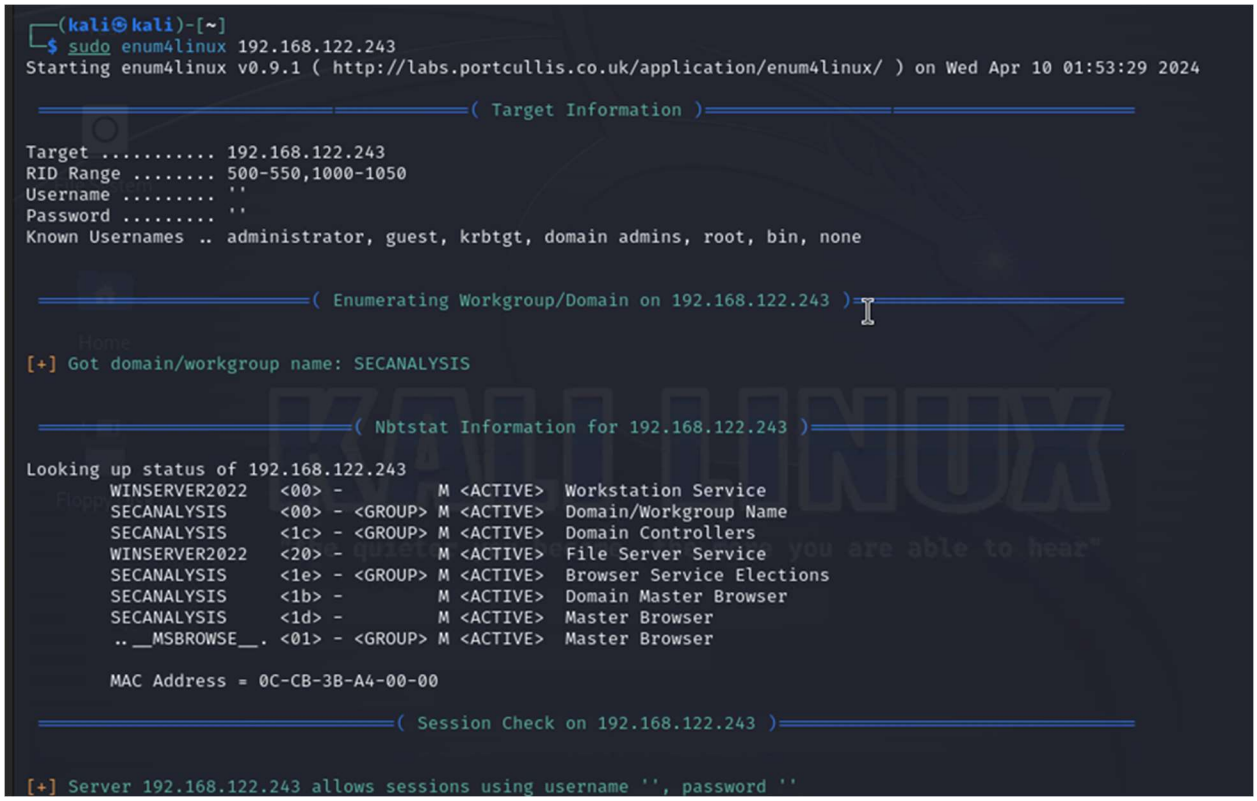

Figure 5: Target 1's Enum4Linux scan results on 192.168.122.243 (1/2).

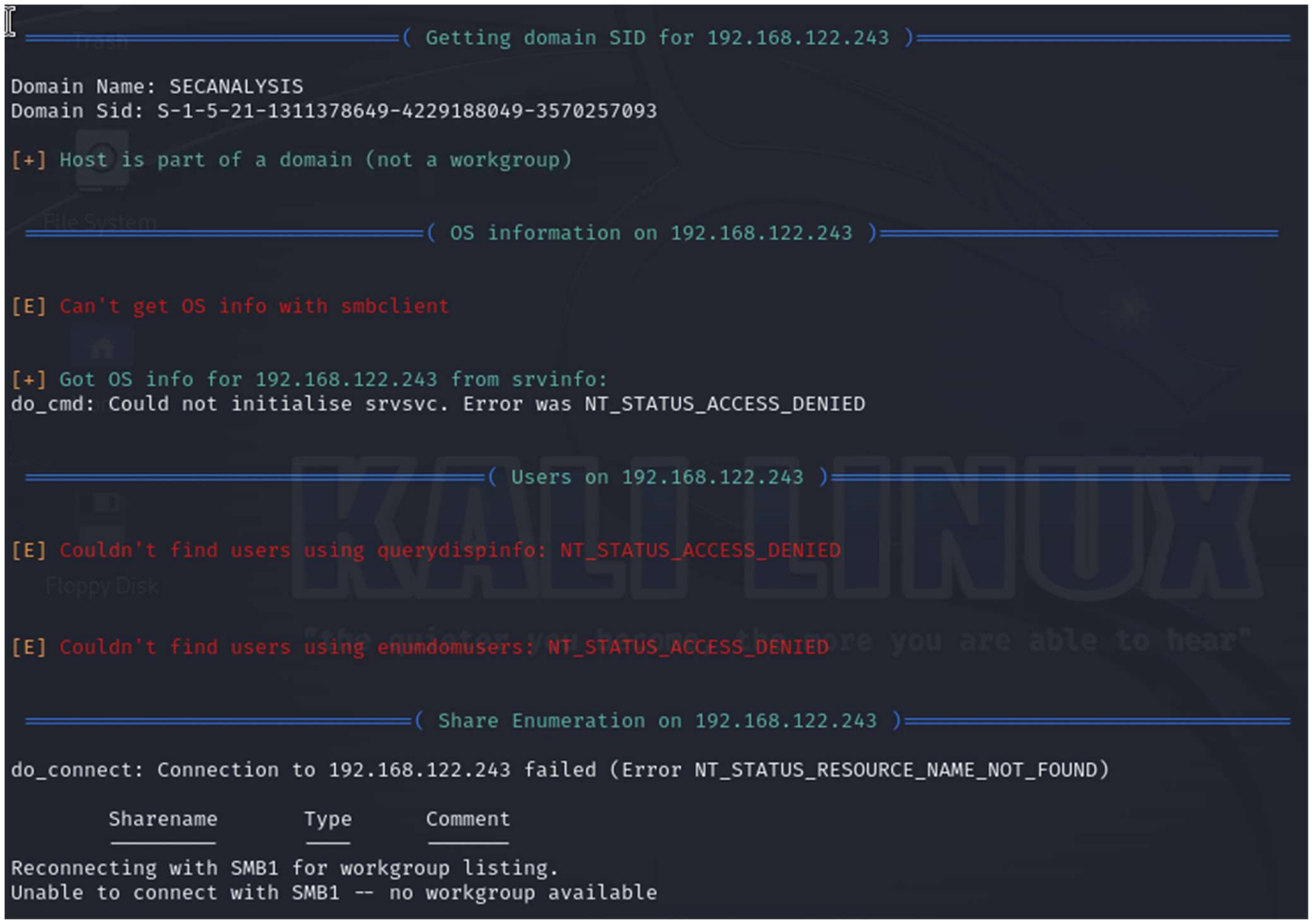

Figure 6: Target 1's Enum4Linux scan results on 192.168.122.243 (2/2).

There appears to be no users listed for Target 1 or workgroups. To further our testing, we next use Nessus to find any possible vulnerabilities that may have been missed from the first two scans on Target 1.

4.1.3. Details Section One – Subsection Three

Using Nessus, we do a basic scan for 192.168.122.243. Only informational vulnerabilities show up.

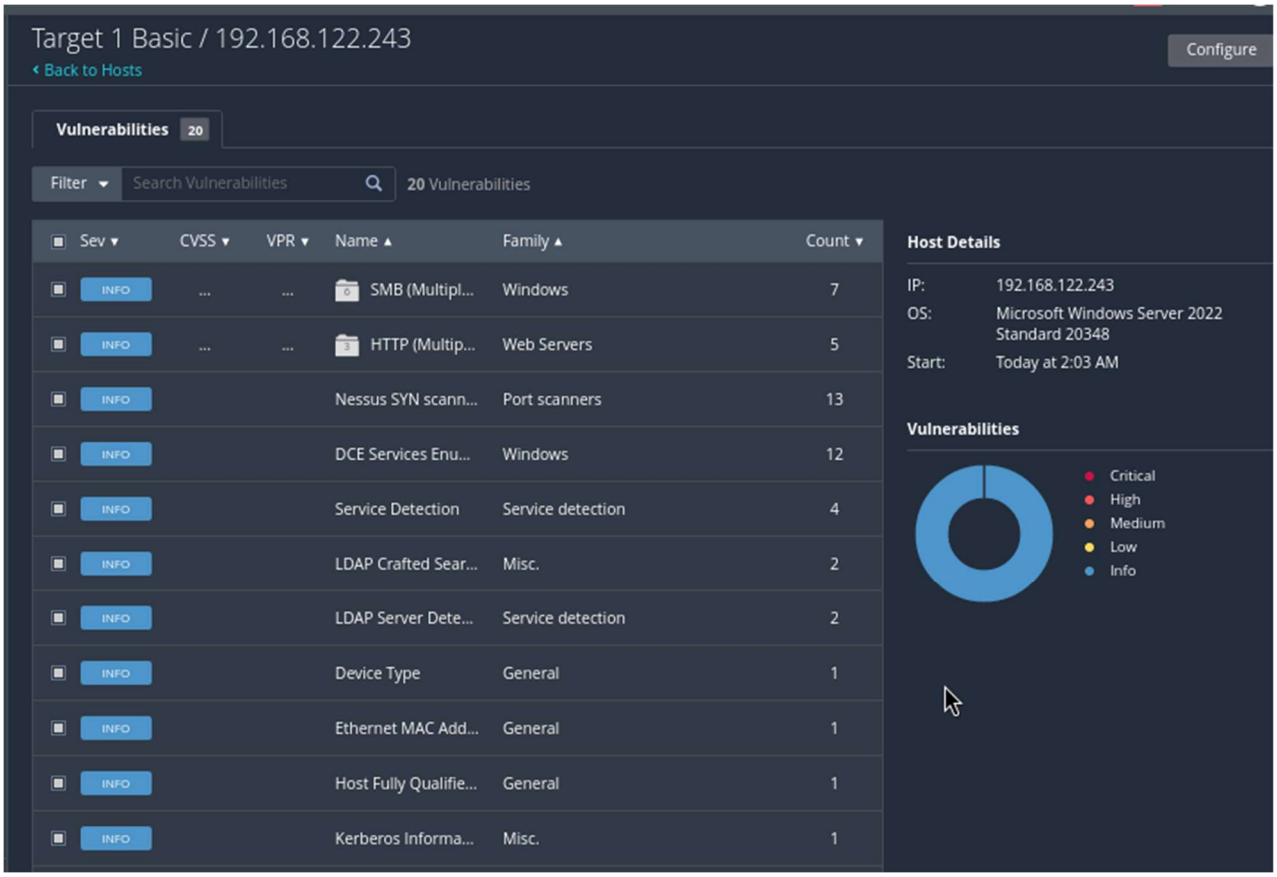

Figure 7: Target 1's Basic Network Scan on 192.168.122.243.

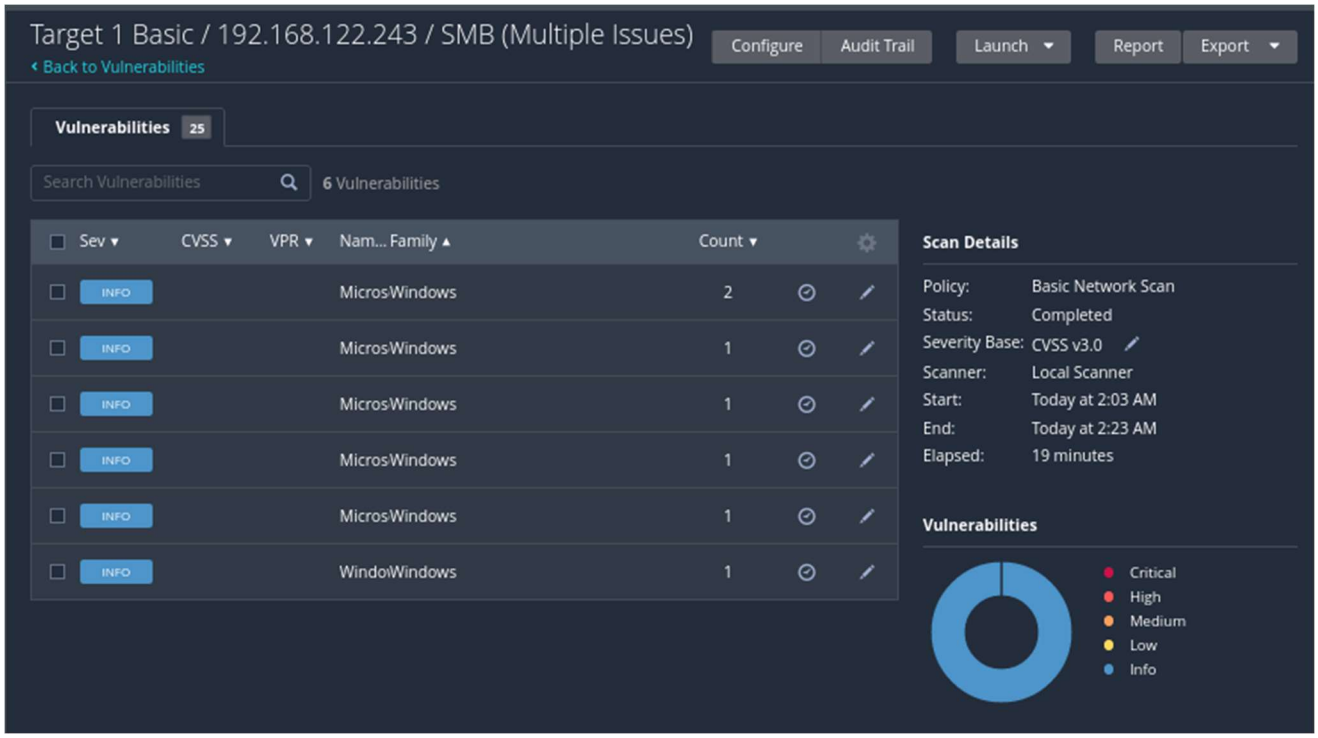

Figure 8: Target 1's Nessus Scan showcasing no critical vulnerabilities.

Due to no critical or high vulnerabilities being found, we'll take a look using two more resources: Metasploit and CrackMapExec before concluding our Target 1 testing.

4.1.4. Details Section One – Subsection Four

The next two scans of Metasploit and CrackMapExec show that not much more information is to be found with Target 1.

```
msf6 > search smb

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

   #    Name                                                      Disclosure Date  Rank       Check  Description
   -    ----                                                      ---------------  ----       -----  -----------
   0    exploit/multi/http/struts_code_exec_classloader           2014-03-06       manual     No     Apache Struts
 ClassLoader Manipulation Remote Code Execution
   1    exploit/osx/browser/safari_file_policy                    2011-10-12       normal     No     Apple Safari
file:// Arbitrary Code Execution
   2    auxiliary/server/capture/smb                                               normal     No     Authenticatio
n Capture: SMB
   3    post/linux/busybox/smb_share_root                                          normal     No     BusyBox SMB S
haring
   4    exploit/linux/misc/cisco_rv340_sslvpn                     2022-02-02       good       Yes    Cisco RV340 S
SL VPN Unauthenticated Remote Code Execution
   5    auxiliary/scanner/http/citrix_dir_traversal               2019-12-17       normal     No     Citrix ADC (N
etScaler) Directory Traversal Scanner
   6    auxiliary/scanner/smb/impacket/dcomexec                   2018-03-19       normal     No     DCOM Exec
   7    auxiliary/scanner/smb/impacket/secretsdump                                 normal     No     DCOM Exec
   8    auxiliary/scanner/dcerpc/dfscoerce                                         normal     No     DFSCoerce
   9    exploit/windows/scada/ge_proficy_cimplicity_gefebt        2014-01-23       excellent  Yes    GE Proficy CI
MPLICITY gefebt.exe Remote Code Execution
   10   exploit/windows/smb/generic_smb_dll_injection             2015-03-04       manual     No     Generic DLL I
njection From Shared Resource
   11   exploit/windows/http/generic_http_dll_injection           2015-03-04       manual     No     Generic Web A
pplication DLL Injection
   12   exploit/windows/smb/group_policy_startup                  2015-01-26       manual     No     Group Policy
Script Execution From Shared Resource
   13   exploit/windows/misc/hp_dataprotector_install_service     2011-11-02       excellent  Yes    HP Data Prote
ctor 6.10/6.11/6.20 Install Service
   14   exploit/windows/misc/hp_dataprotector_cmd_exec            2014-11-02       excellent  Yes    HP Data Prote
ctor 8.10 Remote Command Execution
   15   auxiliary/server/http_ntlmrelay                                            normal     No     HTTP Client M
S Credential Relayer
   16   payload/cmd/windows/http/x64/custom/reverse_named_pipe                     normal     No     HTTP Fetch, W
indows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
   17   payload/cmd/windows/http/x64/meterpreter/reverse_named_pipe                normal     No     HTTP Fetch, W
indows x64 Reverse Named Pipe (SMB) Stager
```

Figure 9: Target 1 using Metasploit to search for SMB.

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.122.243 -u '' -p '' --users
SMB         192.168.122.243 445    WINSERVER2022    [*] Windows Server 2022 Standard 20348 x64 (name:WINSERVER2022) (domain
:secanalysis.com) (signing:True) (SMBv1:True)
SMB         192.168.122.243 445    WINSERVER2022    [+] secanalysis.com\:
SMB         192.168.122.243 445    WINSERVER2022    [-] Error enumerating domain users using dc ip 192.168.122.243: NTLM ne
eds domain\username and a password
SMB         192.168.122.243 445    WINSERVER2022    [*] Trying with SAMRPC protocol

┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.122.243 -u '' -p '' --pass-pol
SMB         192.168.122.243 445    WINSERVER2022    [*] Windows Server 2022 Standard 20348 x64 (name:WINSERVER2022) (domain
:secanalysis.com) (signing:True) (SMBv1:True)
SMB         192.168.122.243 445    WINSERVER2022    [+] secanalysis.com\:

┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.122.243 -u guest -p '' --shares
SMB         192.168.122.243 445    WINSERVER2022    [*] Windows Server 2022 Standard 20348 x64 (name:WINSERVER2022) (domain
:secanalysis.com) (signing:True) (SMBv1:True)
SMB         192.168.122.243 445    WINSERVER2022    [-] secanalysis.com\guest: STATUS_ACCOUNT_DISABLED

┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 192.168.122.243 -u admin -p '' --shares
SMB         192.168.122.243 445    WINSERVER2022    [*] Windows Server 2022 Standard 20348 x64 (name:WINSERVER2022) (domain
:secanalysis.com) (signing:True) (SMBv1:True)
SMB         192.168.122.243 445    WINSERVER2022    [-] secanalysis.com\admin: STATUS_LOGON_FAILURE
```

Figure 10: Target 1's results from CrackMapExec SMB.

In Details Section Two, we'll take a further look at Target 2 for possible vulnerabilities.

4.2. Details Section Two

Like Target 1, for Target 2, we'll use Kali Linux and do an ARP-scan to find addresses of active hosts which is 192.168.122.44.

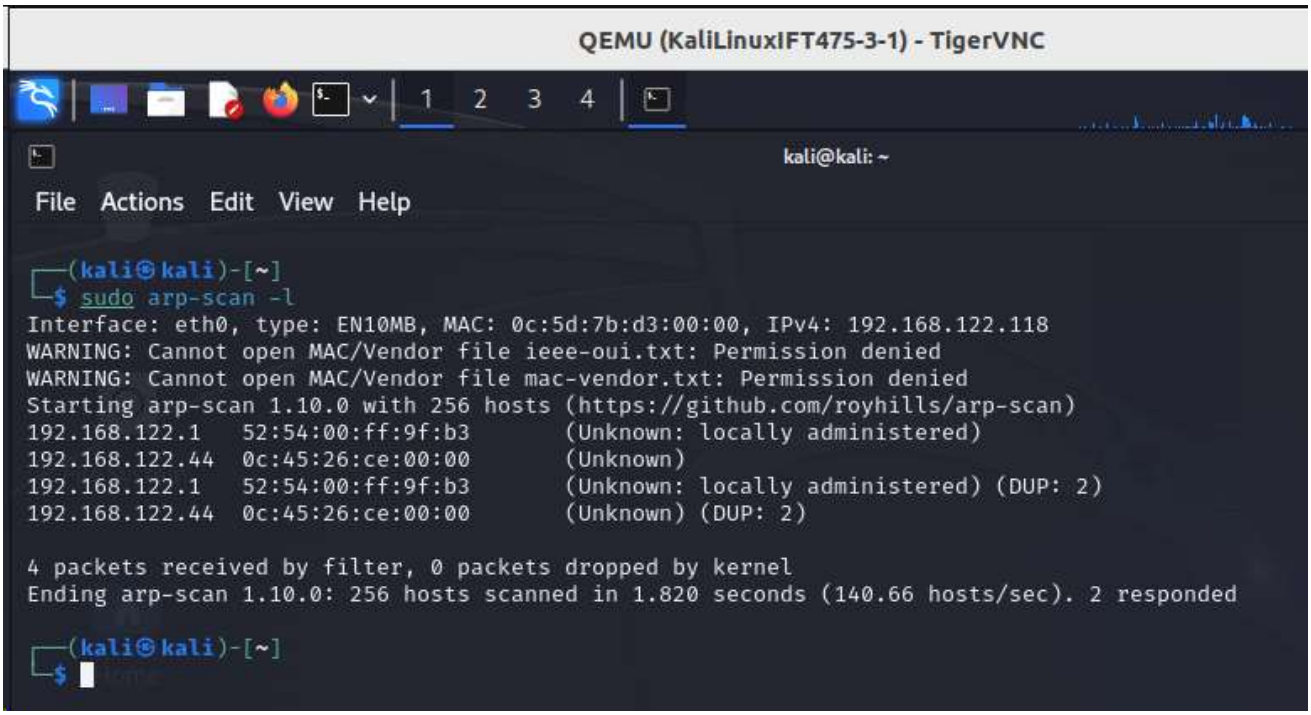

Figure 11 :Screenshot of sudo arp-scan -l to find addresses of active hosts.

In the next subsection, we'll take a look at the Nmap results of using ARP Ping Scan and then a full scan.

4.2.1. Details Section Two – Subsection One

First, we use Nmap ARP Ping Scan for 192.168.122.44 for the list of open ports.

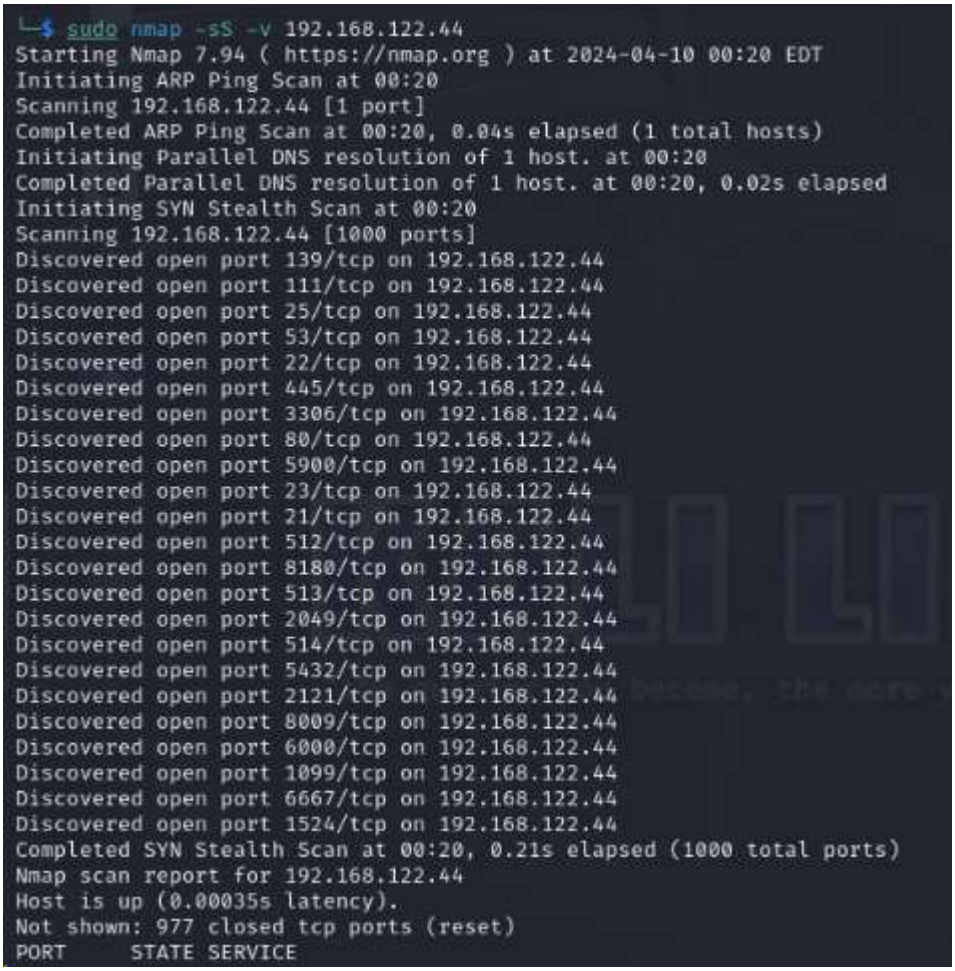

Figure 12: Screenshot of nmap -sS -v scan, a SYN scan to find open ports.

Figure 13: Screenshot of nmap -sS -v scan result.

Then, we do a comprehensive scan with version detection finding further useful information on 192.168.122.44.

Figure 14: Screenshot of nmap -A scan, a comprehensive scan with version detection (1/2).

Figure 15: Screenshot of nmap -A scan (2/2).

After finishing the Nmap scans, next we'll use Enum4Linux for further information.

4.2.2. Details Section Two – Subsection Two

With the Enum4Linux scan, we find more information with Target 2 than we did with one, such as the Nbtstat Information and user information.

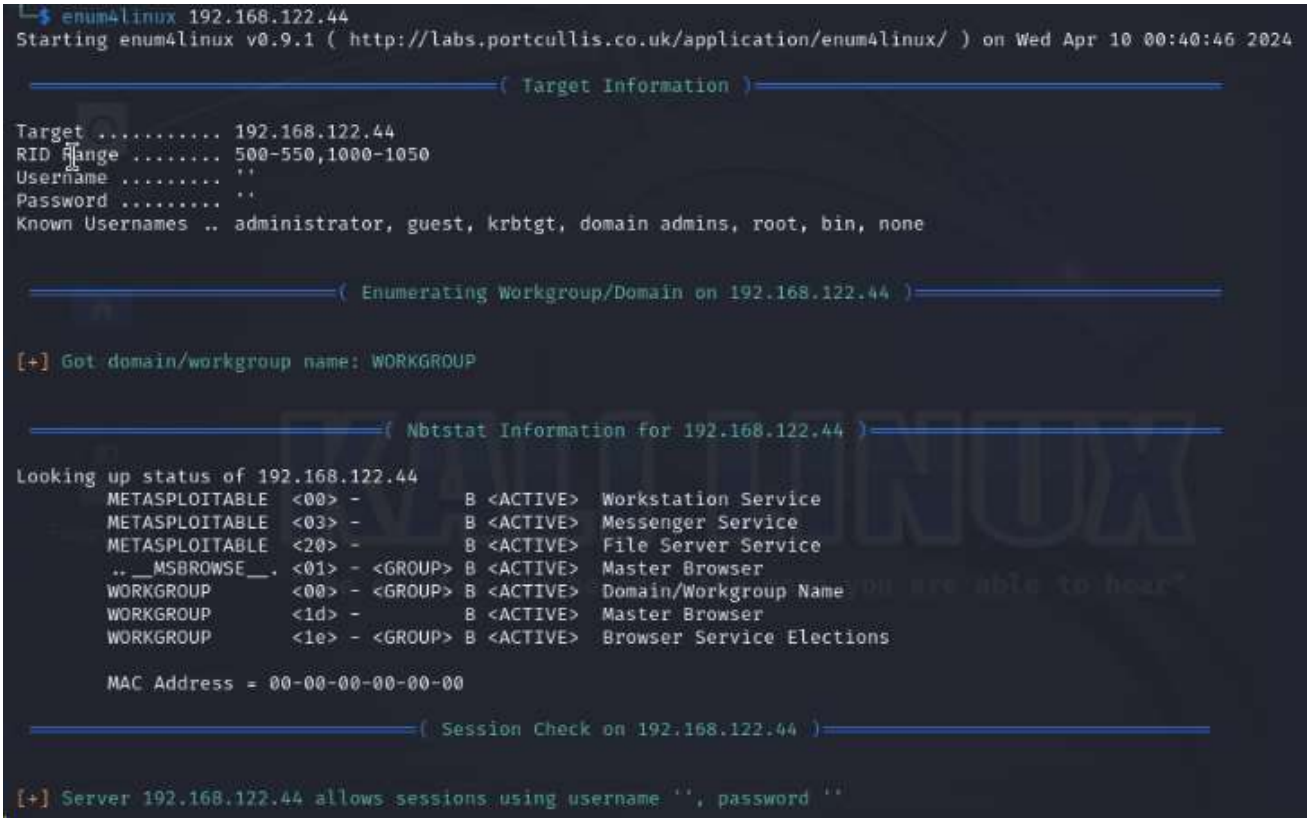

Figure 16: Screenshot of enum4linux scan results (1/2).

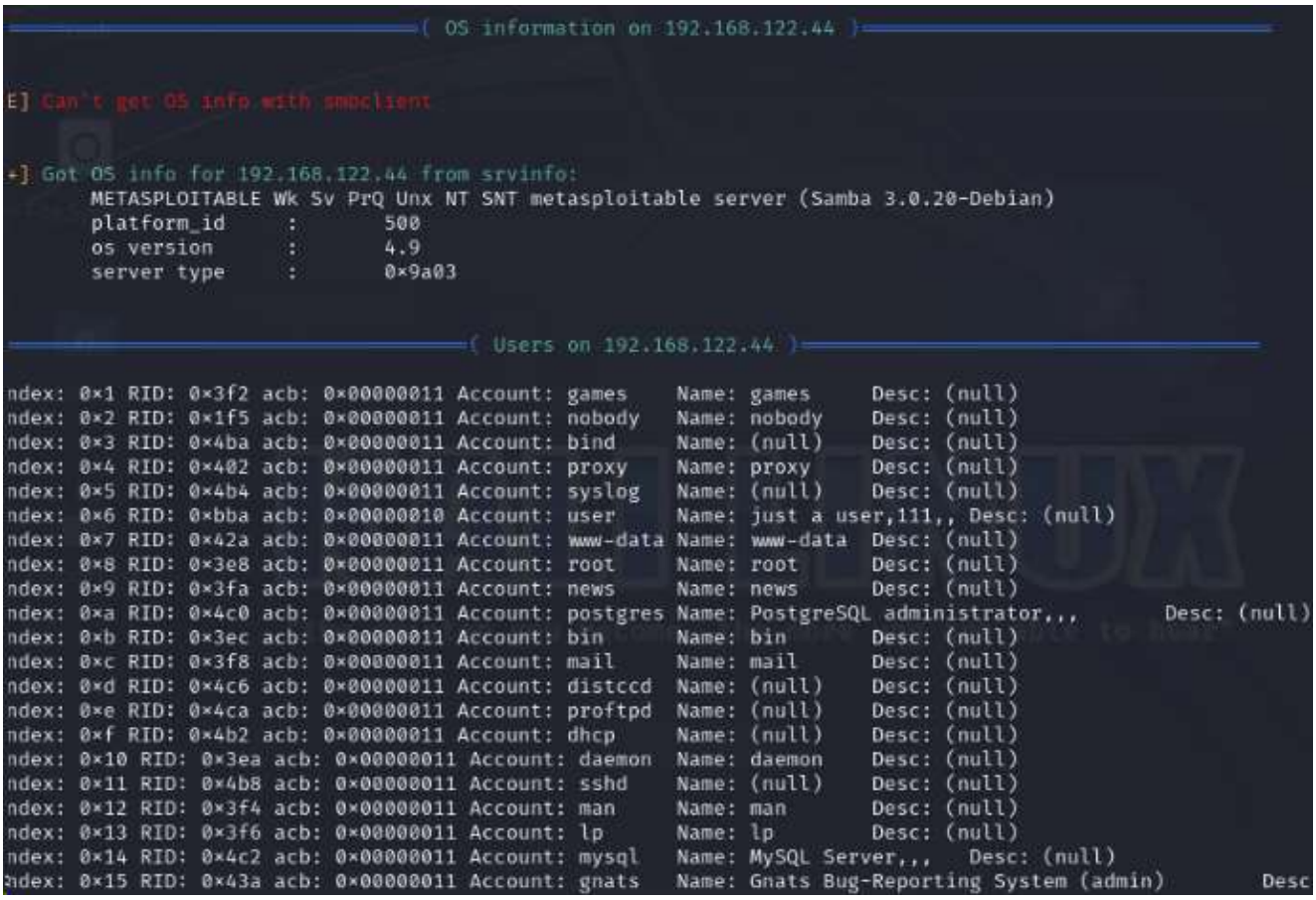

Figure 17: Screenshot of enum4linux (2/2).

These figures show security risks, so we will further our research by using the Nessus Basic Network Scan in the next section.

4.2.3. Details Section Two – Subsection Three

Using the Nessus Basic Network Scan, we find several critical vulnerabilities.

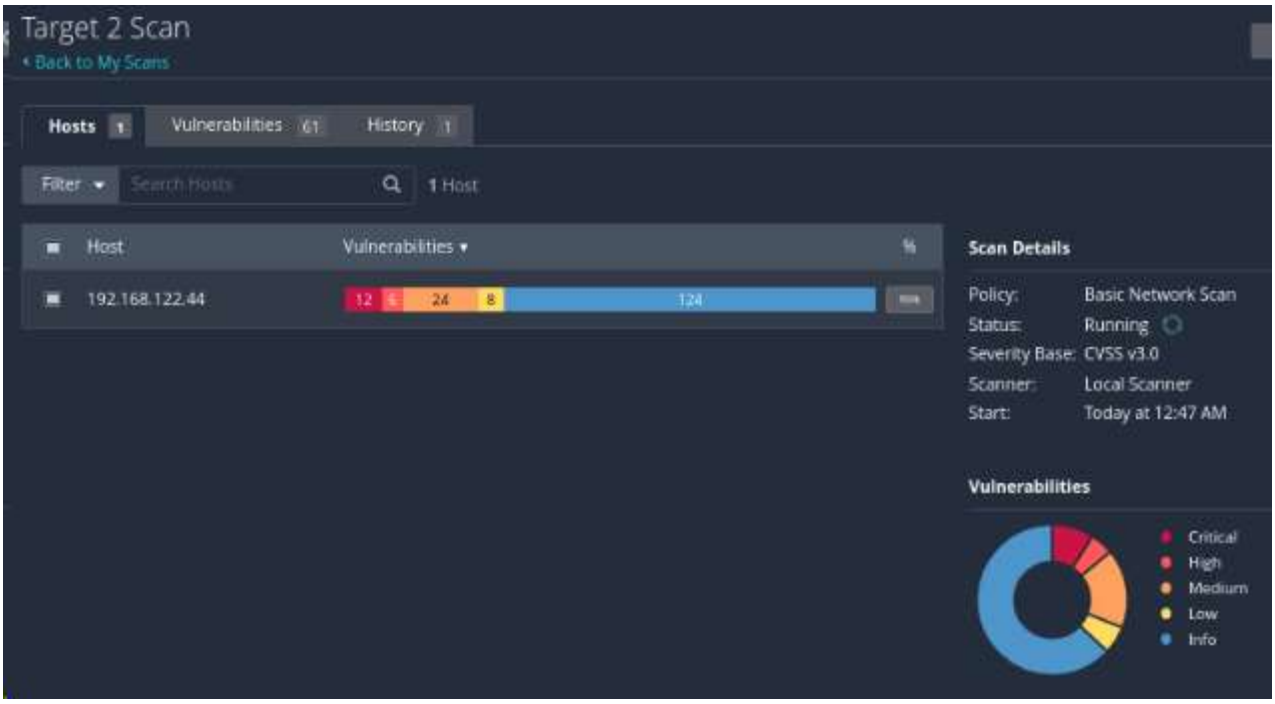

Figure 18: Screenshot of Nessus Basic Network Scan showcasing multiple critical and high vulnerabilities.

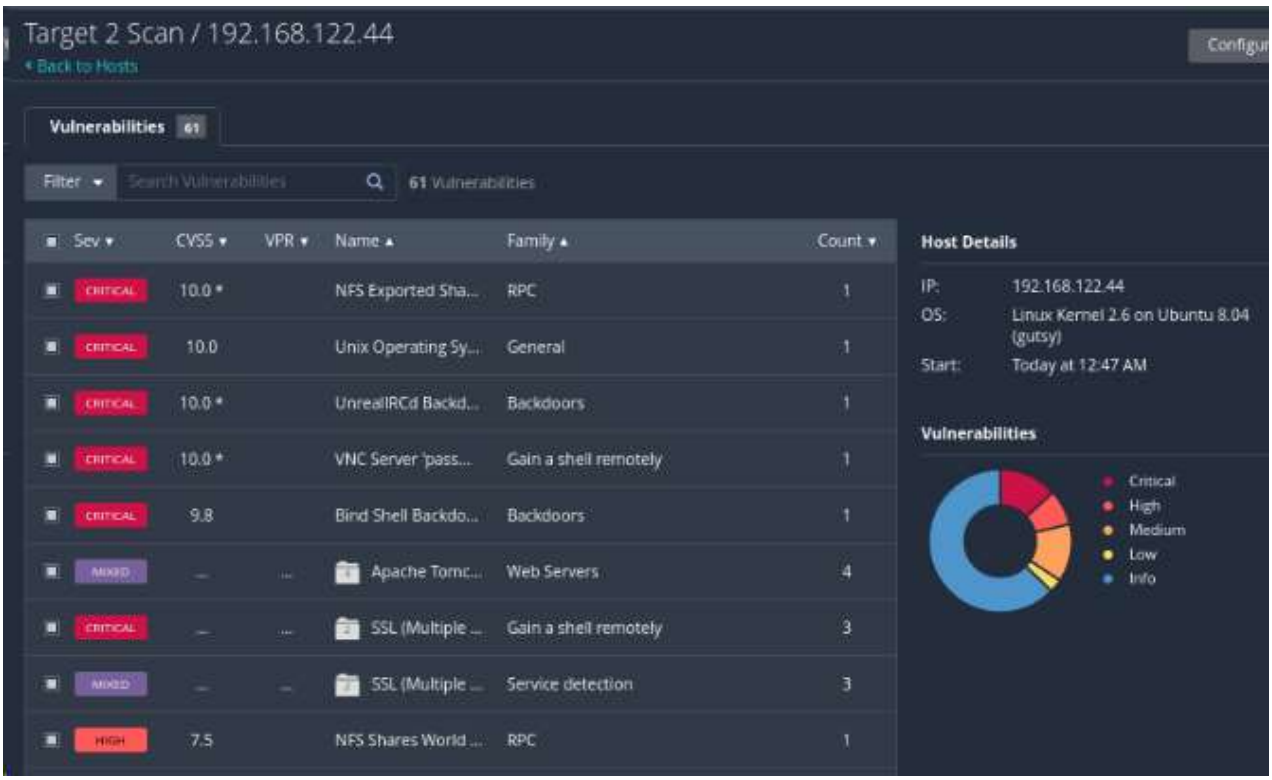

Figure 19: Screenshot of Target 2 Vulnerabilities in more details with the name and severities, along with what family or errors it belongs to.

There are several red flags that have to do RPC, Remote Shell, and Backdoors. Our final target will be in the next section.

4.2.4. Details Section Two – Subsection Four

For this section we'll use Metasploit for MySQL and HTTP.

```
msf6 > search name:mysql type:exploit

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

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  exploit/linux/mysql/mysql_yassl_getname           2010-01-25       good       No     MySQL yaSSL CertDecoder::Ge
tName Buffer Overflow
   1  exploit/linux/mysql/mysql_yassl_hello             2008-01-04       good       No     MySQL yaSSL SSL Hello Messa
ge Buffer Overflow
   2  exploit/windows/mysql/mysql_yassl_hello           2008-01-04       average    No     MySQL yaSSL SSL Hello Messa
ge Buffer Overflow
   3  exploit/multi/mysql/mysql_udf_payload             2009-01-16       excellent  No     Oracle MySQL UDF Payload Ex
ecution
   4  exploit/windows/mysql/mysql_start_up              2012-12-01       excellent  Yes    Oracle MySQL for Microsoft
Windows FILE Privilege Abuse
   5  exploit/windows/mysql/mysql_mof                   2012-12-01       excellent  Yes    Oracle MySQL for Microsoft
Windows MOF Execution
   6  exploit/windows/mysql/scrutinizer_upload_exec     2012-07-27       excellent  Yes    Plixer Scrutinizer NetFlow
and sFlow Analyzer 9 Default MySQL Credential


Interact with a module by name or index. For example info 6, use 6 or use exploit/windows/mysql/scrutinizer_upload_
exec
```

Figure 20: A screenshot of using Metasploit to search for SQL exploits.

```
msf6 > search name:http type:exploit

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/windows/http/cogent_datahub_request_headers_bof  2013-07-26       normal     Yes    Cogent DataHub
HTTP Server Buffer Overflow
   1   exploit/linux/http/ddwrt_cgibin_exec                  2009-07-20       excellent  No     DD-WRT HTTP Dae
mon Arbitrary Command Execution
   2   exploit/multi/http/drupal_drupageddon                 2014-10-15       excellent  No     Drupal HTTP Par
ameter Key/Value SQL Injection
   3   exploit/windows/http/easyfilesharing_post             2017-06-12       normal     No     Easy File Shari
ng HTTP Server 7.2 POST Buffer Overflow
   4   exploit/windows/http/easyfilesharing_seh              2015-12-02       normal     No     Easy File Shari
ng HTTP Server 7.2 SEH Overflow
   5   exploit/windows/browser/getgodm_http_response_bof     2014-03-09       normal     No     GetGo Download
Manager HTTP Response Buffer Overflow
   6   exploit/windows/http/httpdx_handlepeer                2009-10-08       great      Yes    HTTPDX h_handle
peer() Function Buffer Overflow
   7   exploit/windows/ftp/httpdx_tolog_format               2009-11-17       great      Yes    HTTPDX tolog()
Function Format String Vulnerability
   8   exploit/windows/http/httpdx_tolog_format              2009-11-17       great      Yes    HTTPDX tolog()
Function Format String Vulnerability
   9   exploit/linux/misc/jenkins_ldap_deserialize           2016-11-16       excellent  Yes    Jenkins CLI HTT
P Java Deserialization Vulnerability
   10  exploit/multi/http/joomla_http_header_rce             2015-12-14       excellent  Yes    Joomla HTTP Hea
der Unauthenticated Remote Code Execution
   11  exploit/windows/http/kolibri_http                     2010-12-26       good       Yes    Kolibri HTTP Se
rver HEAD Buffer Overflow
```

Figure 21: A screenshot of using Metasploit to search for HTTP exploits.

After identifying the services used on Target 2, Metasploit was used to find relevant exploits that target those services.

4.3. Details Section Three

In our concluding section, we use Kali Linux once more to find the IP Address which is 192.168.122.8. Then, we'll use the following scans to find vulnerabilities on Target 3 using Nmap, Enum4Linux, Nessus, netcat, and Metasploit. We use ifconfig to find the IP address first, before diving into Nmap scans.

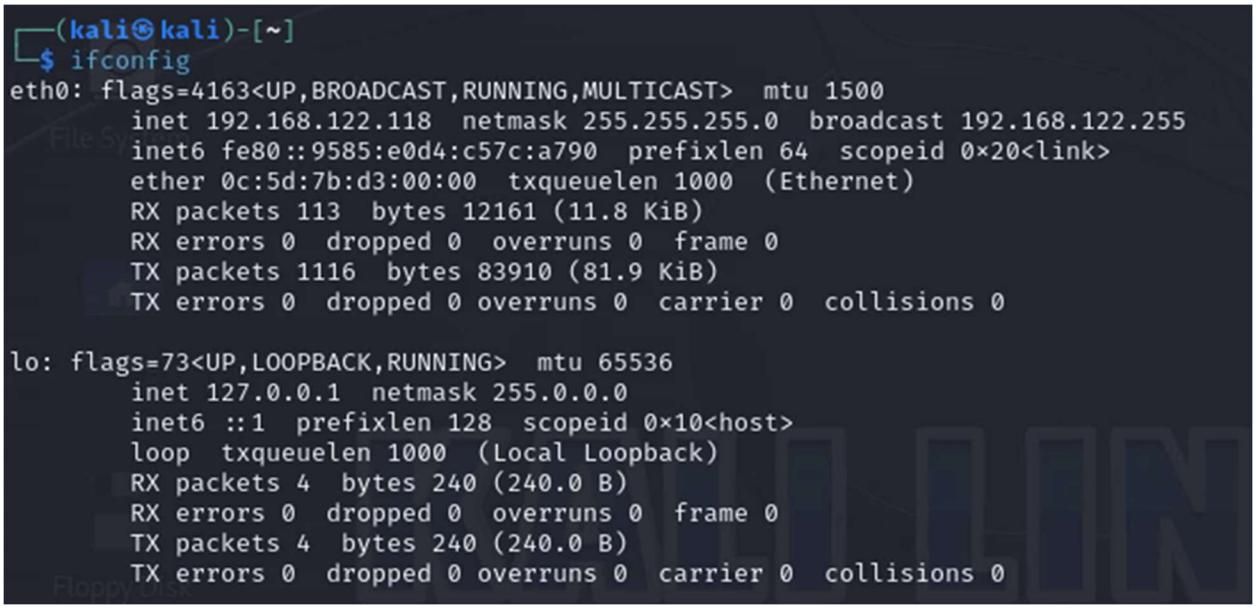

Figure 22: Peering into the Matrix: Network Interface Configuration.

4.3.1. Details Section Three – Subsection One

The first scan on Target 3 is to find active hosts.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.122.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-08 01:42 EDT
Nmap scan report for msnc-as9-app000.apporto.com (192.168.122.1)
Host is up (0.00091s latency).
Nmap scan report for vagrant-2008R2 (192.168.122.8)
Host is up (0.0019s latency).
Nmap scan report for kali (192.168.122.118)
Host is up (0.0021s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.93 seconds

┌──(kali㉿kali)-[~]
└─$
```

Figure 23: A swift Nmap sweep unveils active hosts.

Next, we find what services are being used on 192.168.122.8.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.122.8
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-08 01:47 EDT
Nmap scan report for vagrant-2008R2 (192.168.122.8)
Host is up (0.0022s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE SERVICE             VERSION
21/tcp    open  ftp                 Microsoft ftpd
22/tcp    open  ssh                 OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http                Microsoft IIS httpd 7.5
135/tcp   open  msrpc               Microsoft Windows RPC
139/tcp   open  netbios-ssn         Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds        Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3306/tcp  open  mysql               MySQL 5.5.20-log
3389/tcp  open  ssl/ms-wbt-server?
4848/tcp  open  ssl/http            Oracle Glassfish Application Server
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13               Apache Jserv (Protocol v1.3)
8080/tcp  open  http                Sun GlassFish Open Source Edition  4.0
8181/tcp  open  ssl/intermapper?
8383/tcp  open  http                Apache httpd
9200/tcp  open  wap-wsp?
49152/tcp open  msrpc               Microsoft Windows RPC
49153/tcp open  msrpc               Microsoft Windows RPC
49154/tcp open  msrpc               Microsoft Windows RPC
49155/tcp open  msrpc               Microsoft Windows RPC
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at
 https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8181-TCP:V=7.94%T=SSL%I=7%D=4/8%Time=66138502%P=x86_64-pc-linux-gnu
SF:%r(GetRequest,128C,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Mon,\x2008\x20Ap
SF:r\x202024\x2005:47:47\x20GMT\r\nContent-Type:\x20text/html\r\nConnectio
SF:n:\x20close\r\nContent-Length:\x204626\r\n\r\n<!DOCTYPE\x20HTML\x20PUBL
SF:IC\x20\"-//W3C//DTD\x20HTML\x204\.01\x20Transitional//EN\">\n<html\x20l
SF:ang=\"en\">\n<!--\nDO\x20NOT\x20ALTER\x20OR\x20REMOVE\x20COPYRIGHT\x20N
SF:OTICES\x20OR\x20THIS\x20HEADER\.\n\nCopyright\x20\(c\)\x202010,\x202013
SF:\x20Oracle\x20and/or\x20its\x20affiliates\.\x20All\x20rights\x20reserve
SF:d\.\n\nUse\x20is\x20subject\x20to\x20License\x20Terms\n-->\n<head>\n<st
```

Figure 24: Digital Reconnaissance: uncovering services with Nmap Scanning.

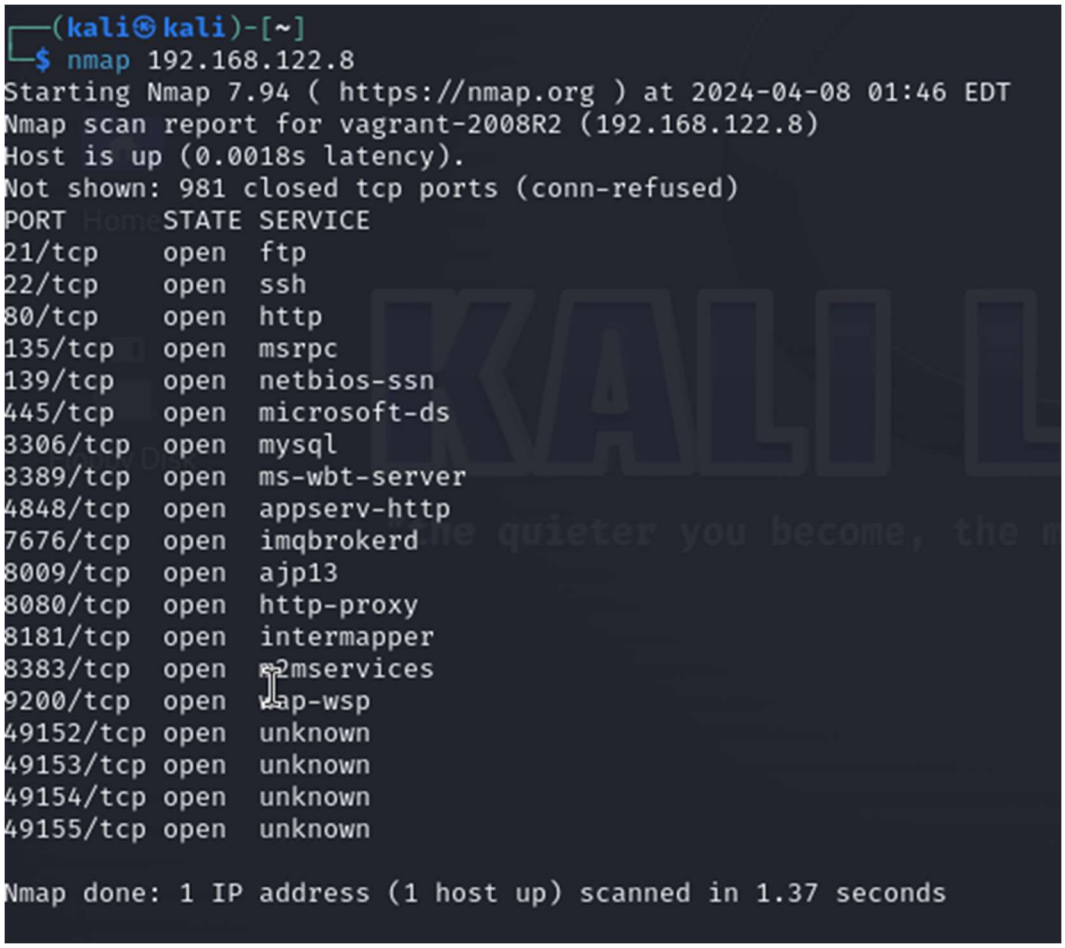

Figure 25: Initiating an Nmap Discovery on 192.168.122.8.

After finding the open ports, in the next subsection, we'll use Enum4Linux to further our investigation.

4.3.2. Details Section Three – Subsection Two

Target 3 reveals much from the Enum4Linux scan, revealing Nbtstat information.

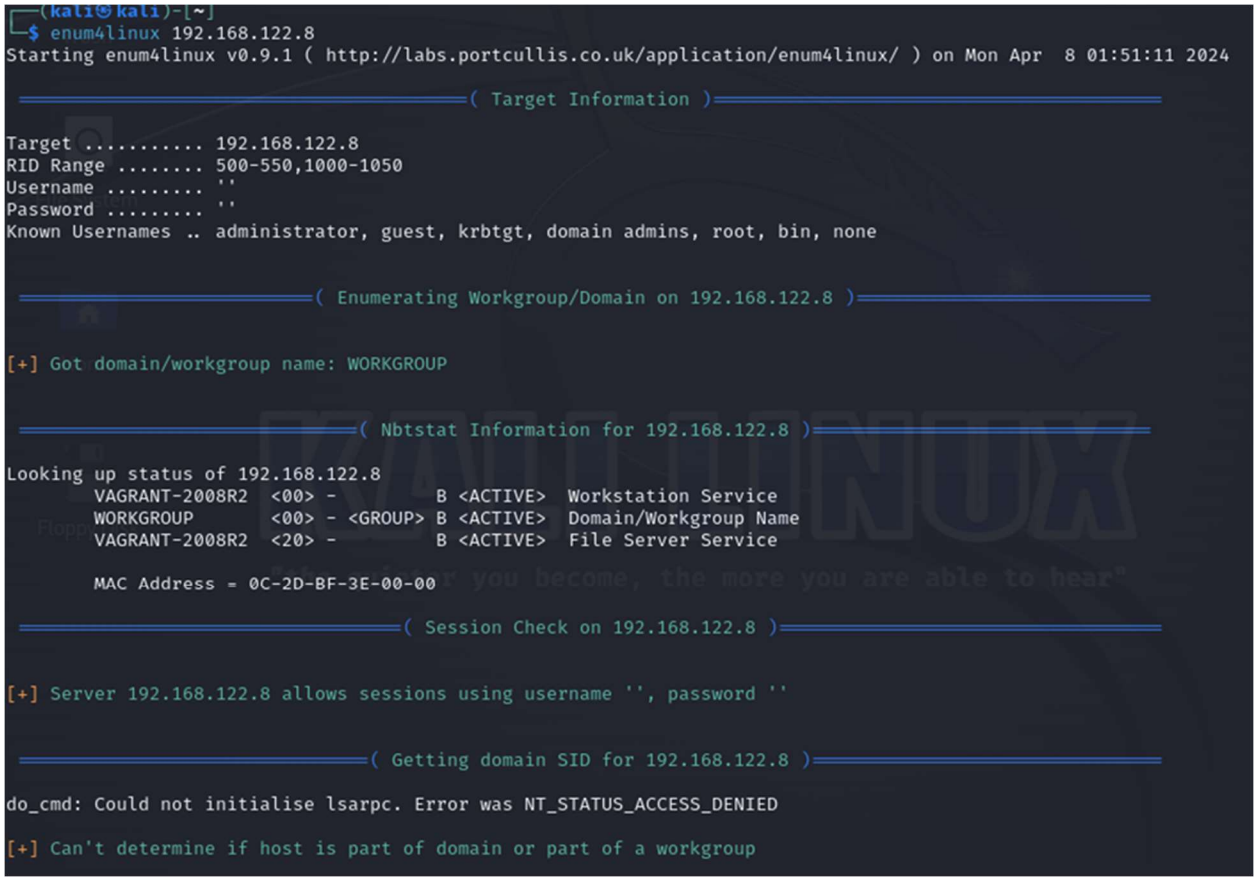

Figure 26: Extracting System Insights with Enum4Linux.

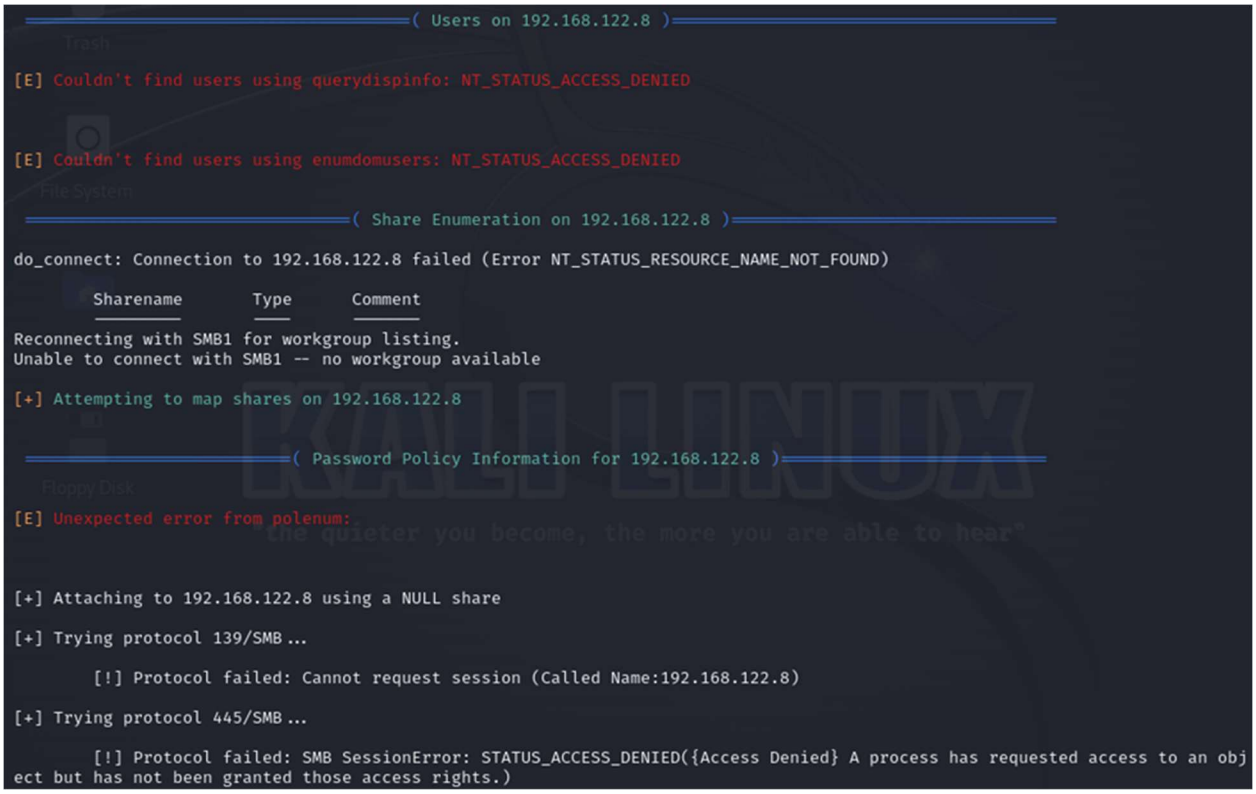

Figure 27: Thwarted Enumeration on a Secure Network.

There is no workgroup information or user information from the Enum4Linux scan. In the next section, we'll scan for vulnerabilities using the Nessus Basic Network Scan.

4.3.3. Details Section Three – Subsection Three

On the scan template page, we do the Basic Network Scan using Nessus.

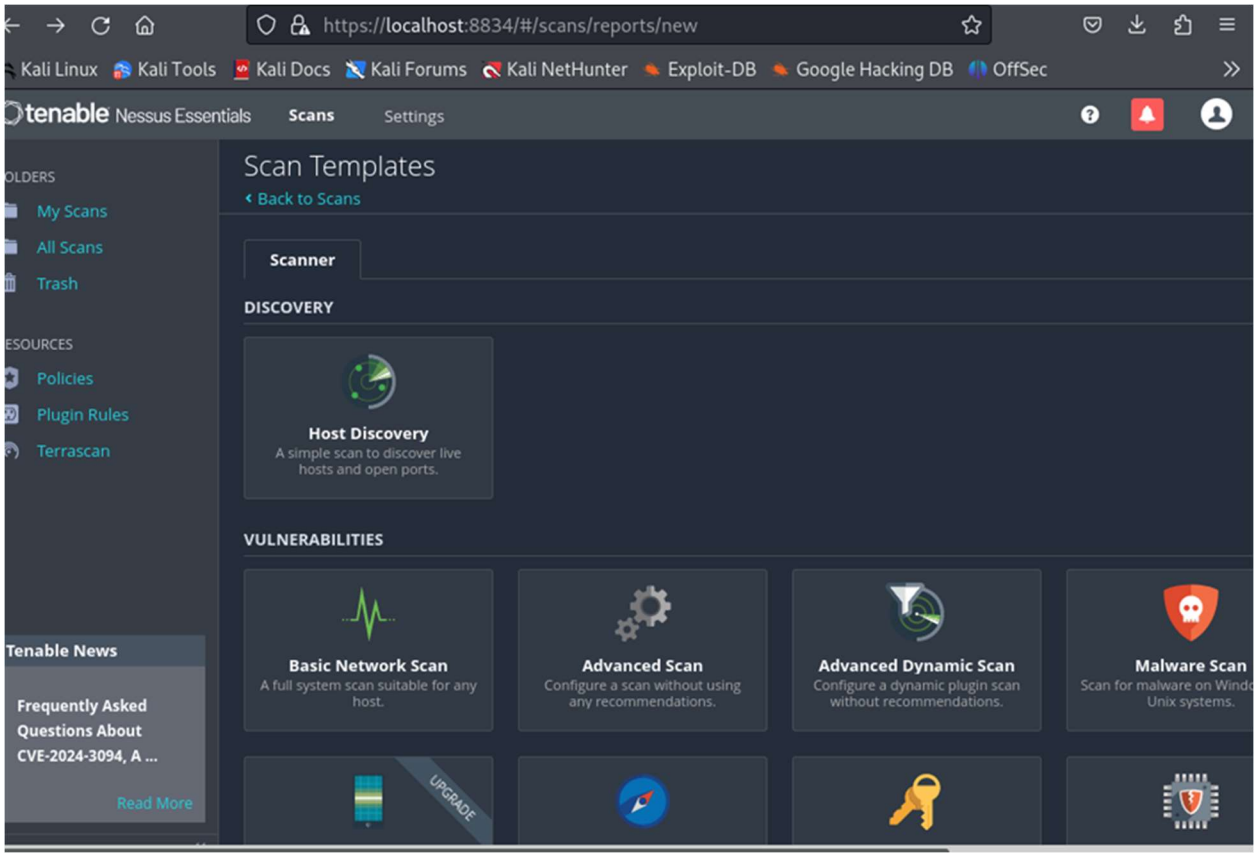

Figure 28: Nessus prepares for a basic network scan vulnerability assessment.

The scan alerts us of several critical vulnerabilities.

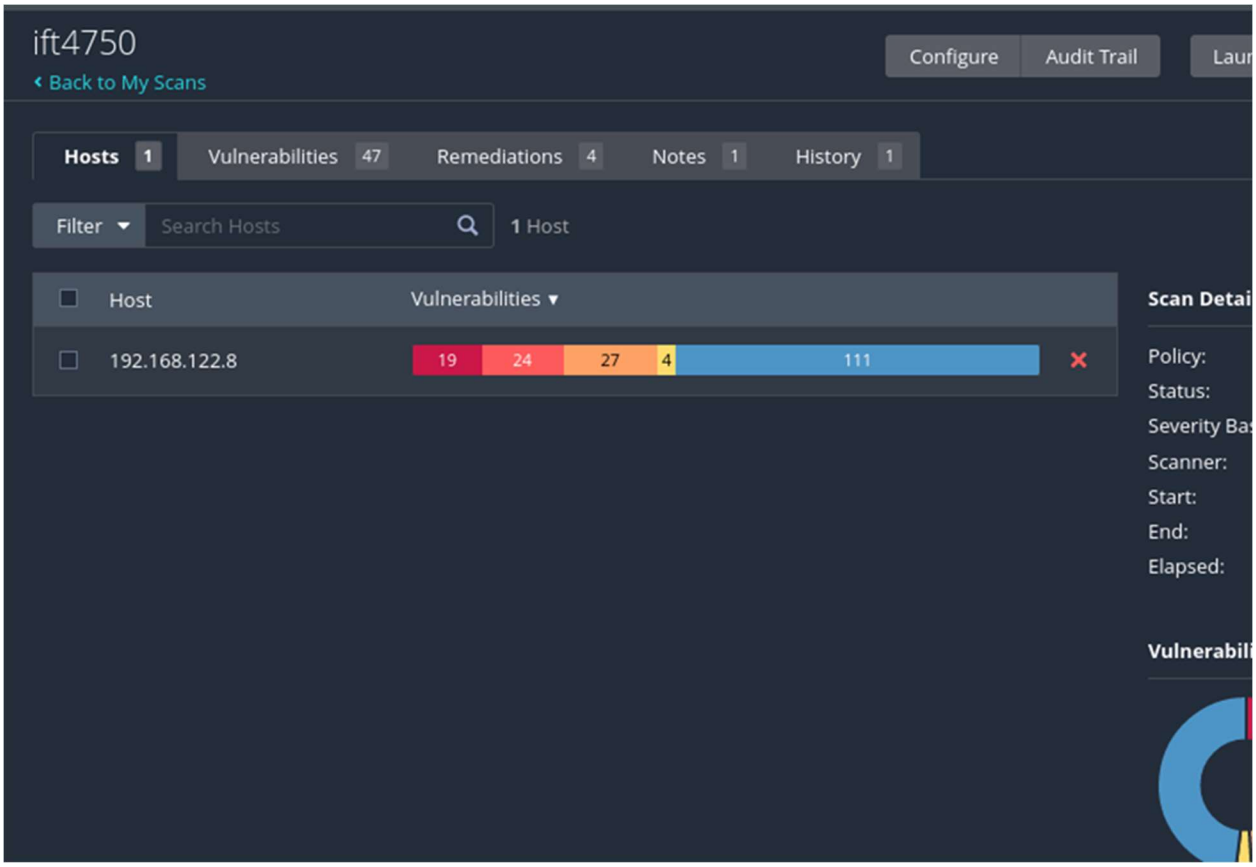

Figure 29: Vulnerability exposed: A comprehensive Nessus Scan Report.

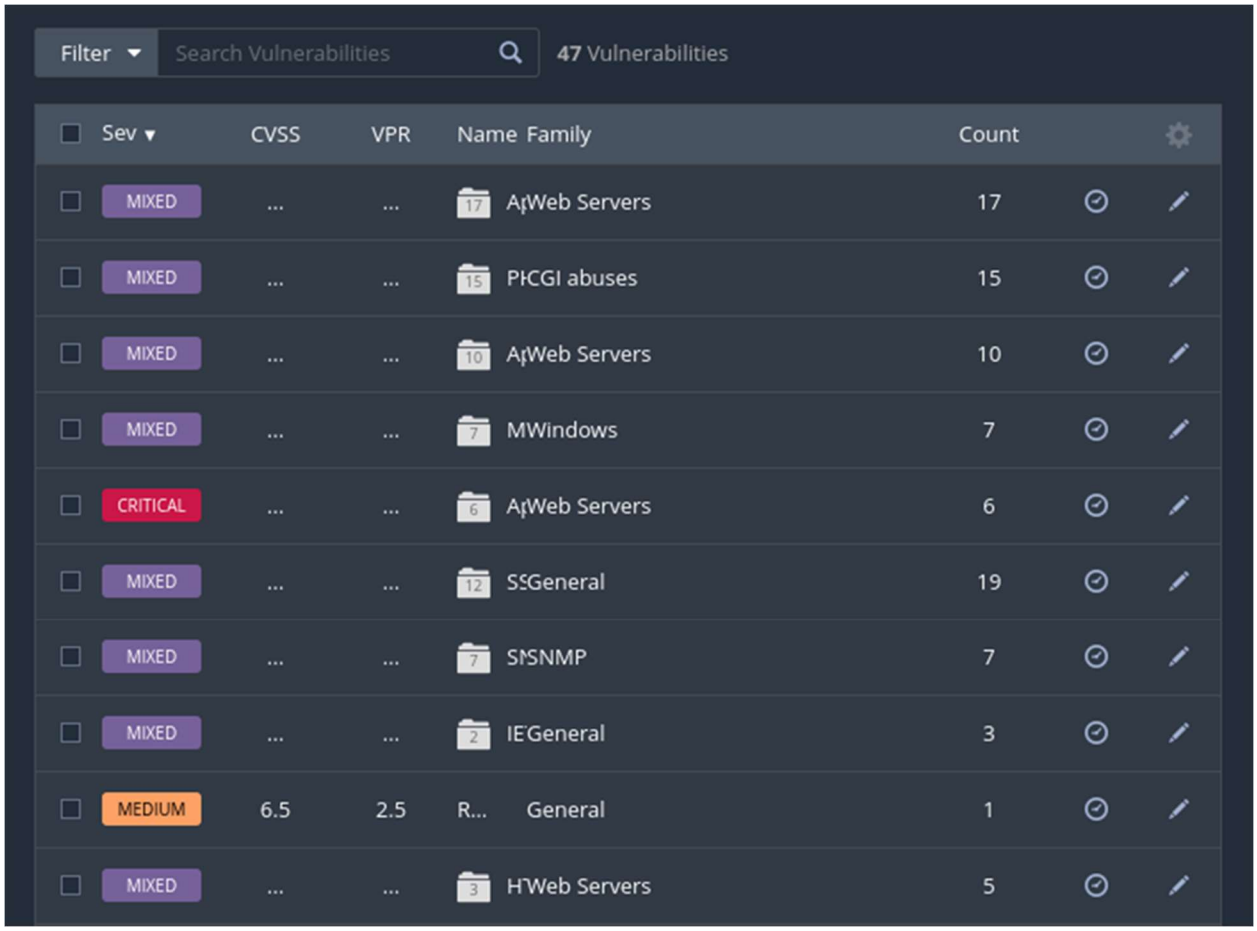

Figure 30: Filtering through the Web of vulnerabilities, finding an attack vector.

Furthering our research, we investigate one of the critical vulnerabilities of CVE-2019-0708 which is in Remote Desktop Protocol (RDP) which is a BlueKeep alert.

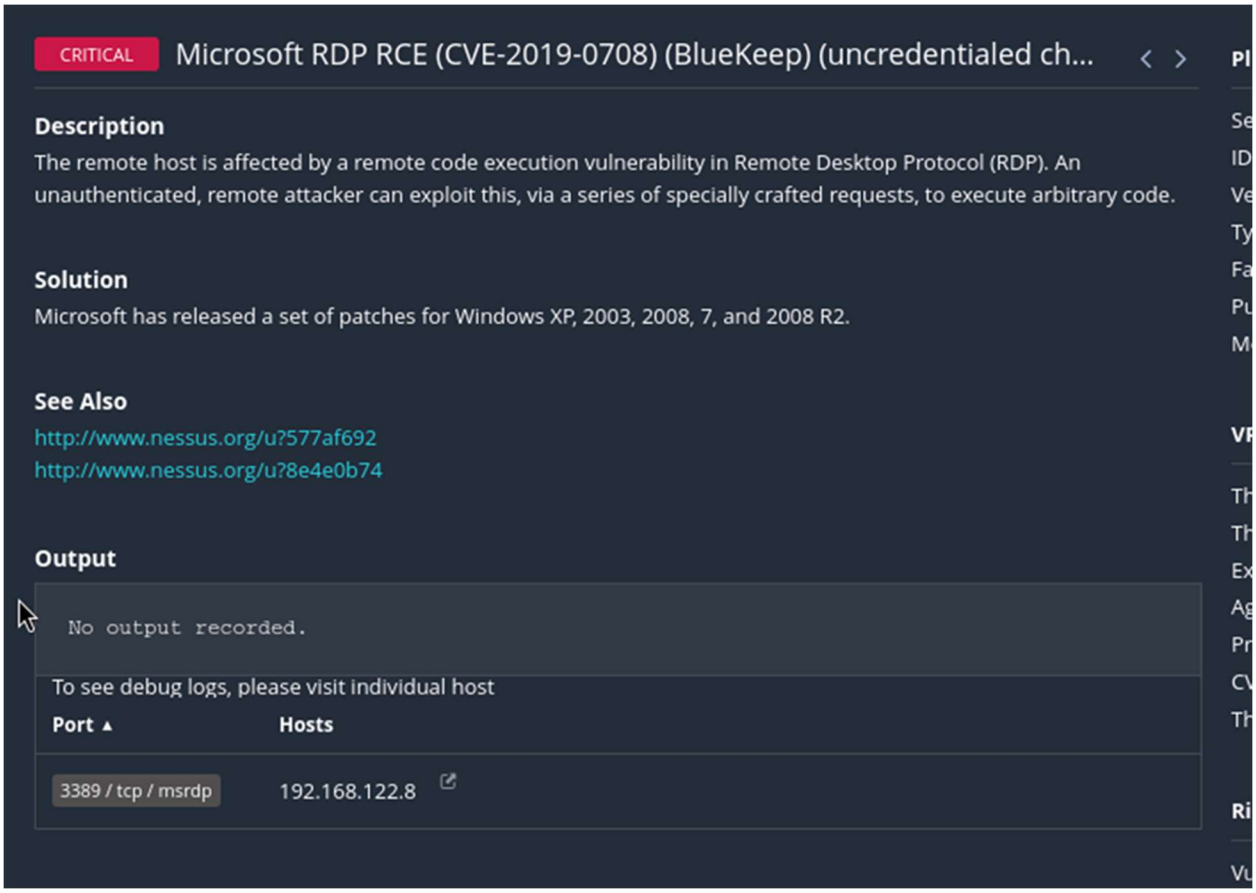

Figure 31: BlueKeep Alert: details of the vulnerability, our attack vector (NIST, 2021).

Switching gears, we quickly do a netcat scan to see if the target system is vulnerable.

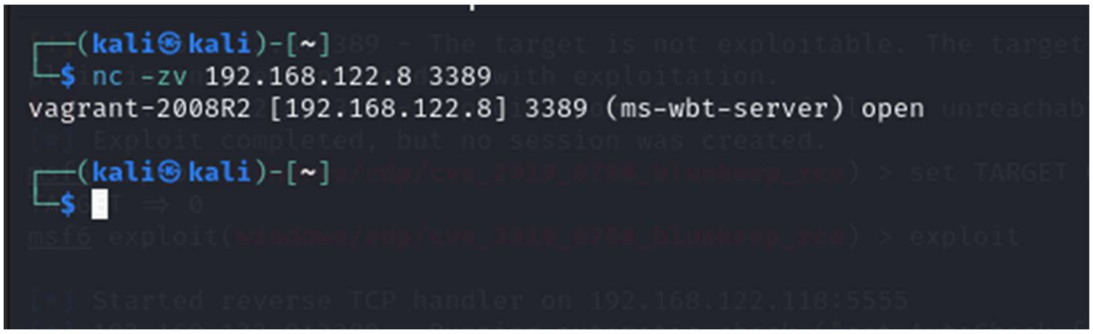

Figure 32: Netcat probes the network services to see if the target system is vulnerable.

4.3.4. Details Section Three – Subsection Four

Our final scan involves using the Metasploit console to provide more details about the BlueKeep vulnerability.

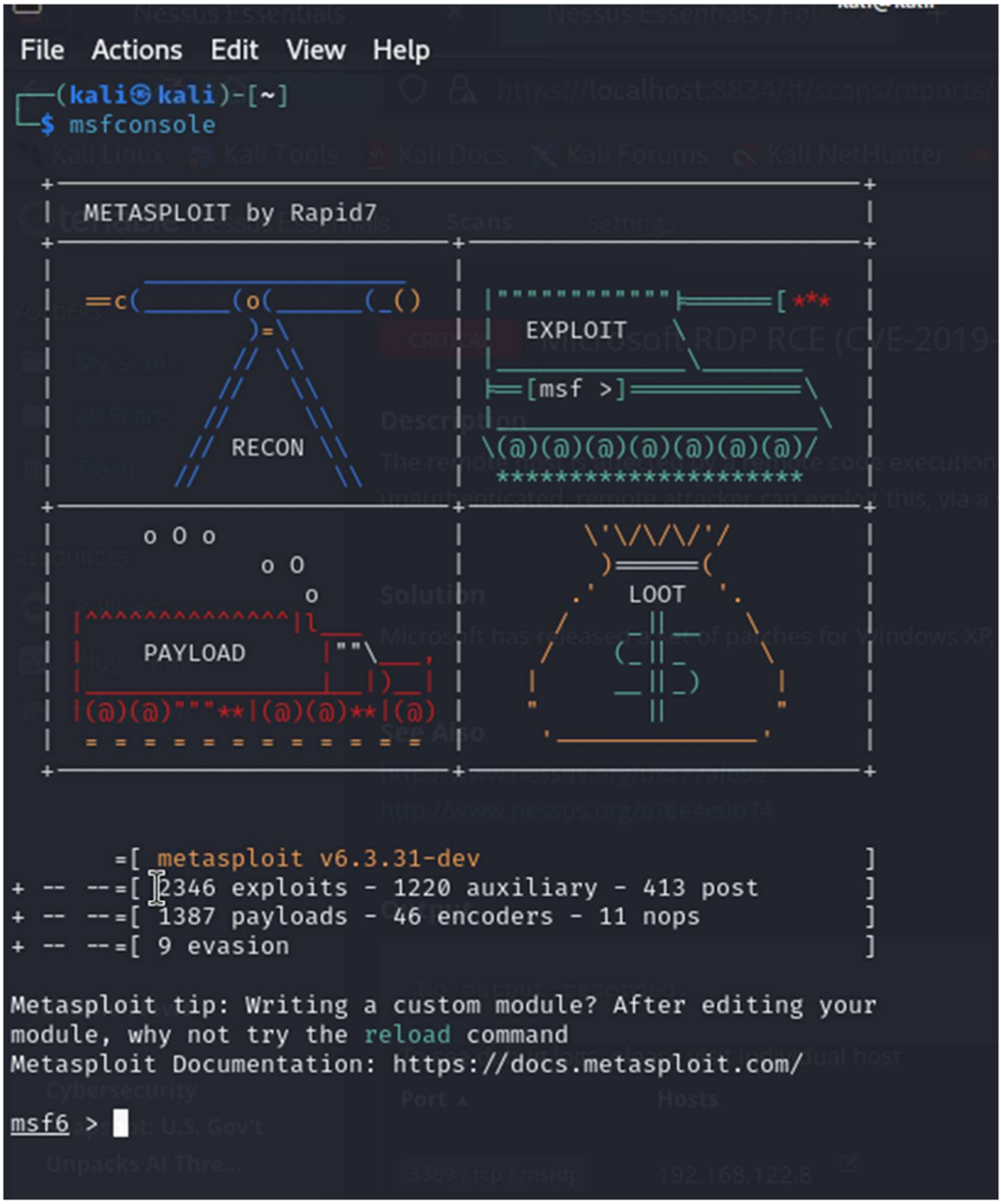

Figure 33: The Metasploit framework is ready to exploit.

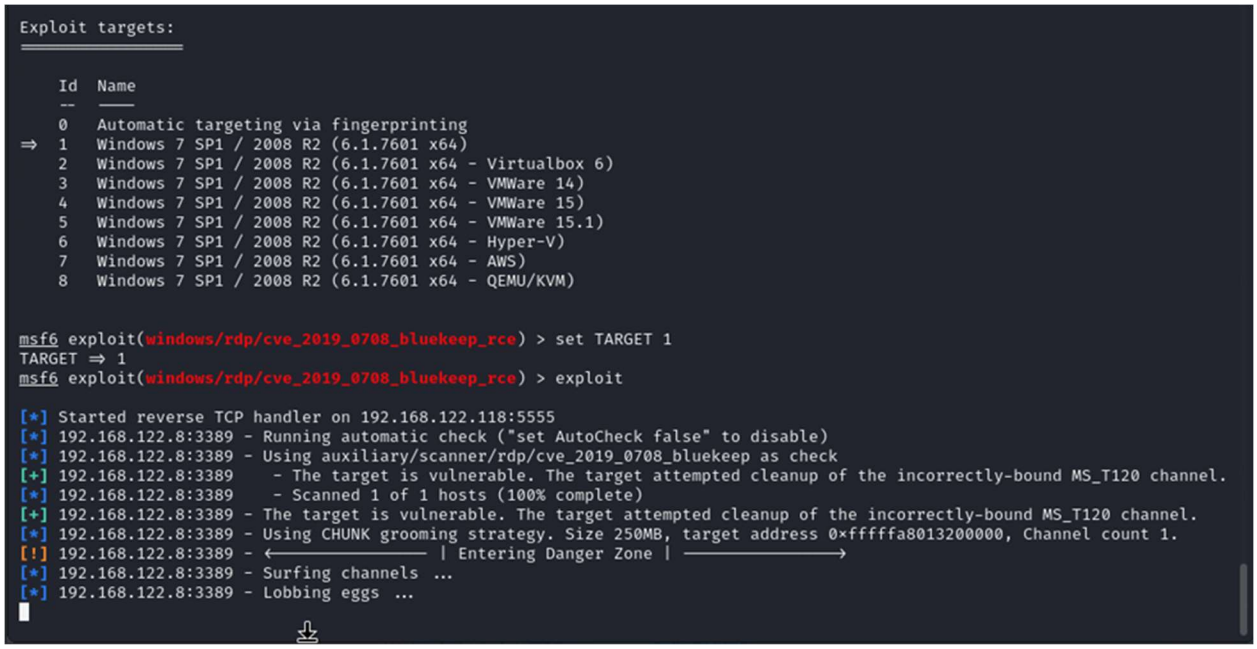

Figure 34: Configuring an the BlueKeep exploit in Metasploit's arsenal.

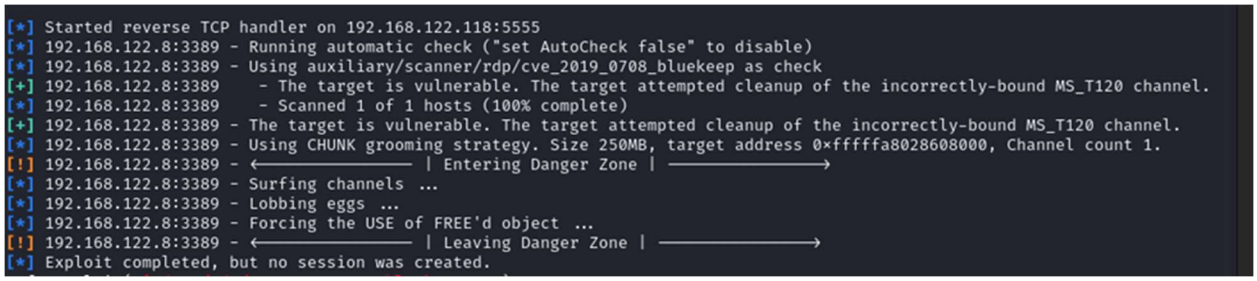

Figure 35: Attempting to gain access with a remote session.

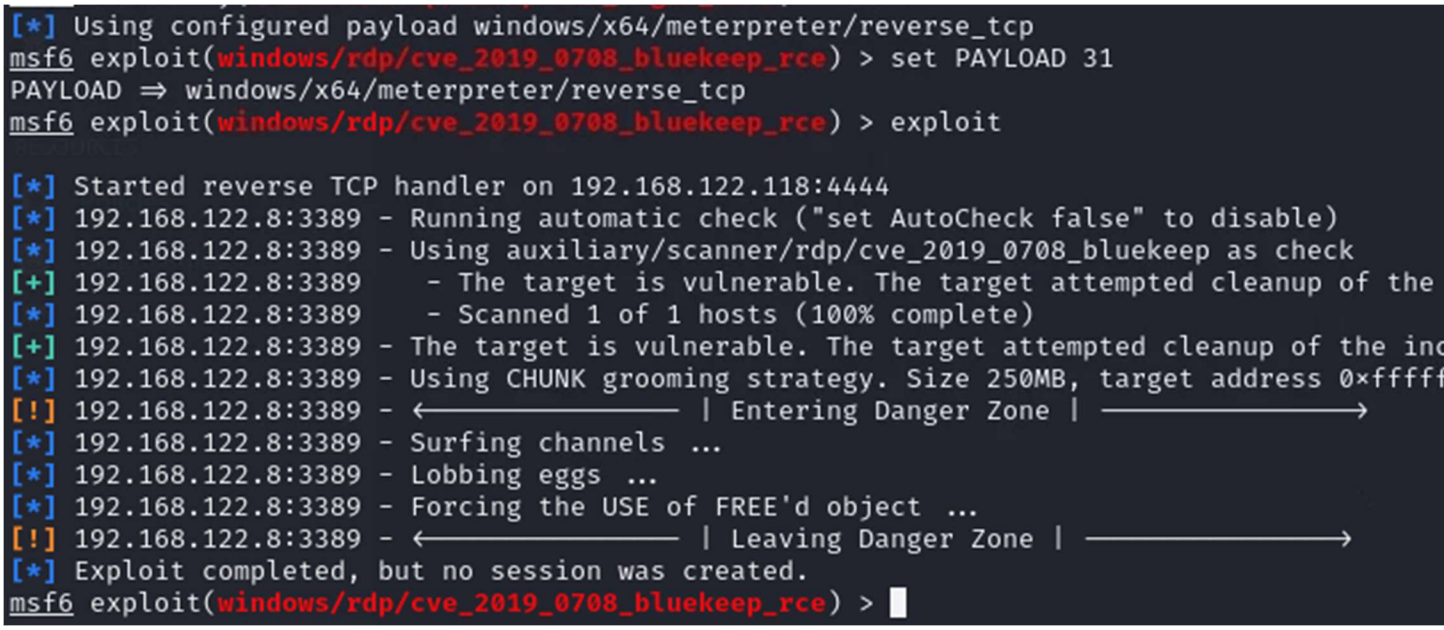

Figure 36: Payload precision: Crafting the delivery of a Metasploit Exploit.

SUMMARY

The findings of the pen testing vary with the three targets. Target 1, 192.168.122.243, seems to be more secured down than the other two targets. No vulnerabilities were found that were critical from Nessus, or user information from Enum4Linux. Target 2 shows more vulnerabilities on 192.168.122.44. There are more open ports that were discovered using Nmap ARP Ping Scan. The Nmap comprehensive scan shows more server and network vulnerabilities with accessible information for the host to be exploited. Using Enum4Linux, there are workgroups with the users account information. Nessus finds twelve critical vulnerabilities, and six high-risk. Target 2 shows vulnerabilities with Backdoors, RPC, and gaining a shell remotely. Target 3 shows vulnerabilities like Target 2 in the Nmap scans with named open ports. The Nessus scans revealed various vulnerabilities across the network hosts. Notably, a critical Remote Code Execution (RCE) vulnerability, identified as BlueKeep (CVE-2019-0708).

The systems that need security fixes include the web servers, Windows OS services, and patching to reduce backdoor injections and remote vulnerabilities.

RECOMMENDATIONS

Our original goals involve aiding Upwork with strengthening their cyber security landscape by finding vulnerabilities with three targets. Target 1's recommendations involve seeing what open ports are needed to remain open and closed, based on business practices. Target 2's recommendations involve patch management on both the servers and network. Target 3's recommendations are that all detected vulnerabilities be remediated immediately, following best practices and vendor guidelines. This includes applying patches, reviewing security configurations, and monitoring for any unusual system behavior. Regular security assessments should be scheduled to ensure continued resilience against new and evolving threats.

Additional recommendations overall involve a patching policy where all systems should have the latest security patches applied. This is especially critical for the services identified with known exploits listed in our three target findings. There should be a configuration review since misconfigurations were identified in web servers and general services should be reviewed and rectified. Security best practices, such as the principle of least privilege, should be enforced. Security Hardening, where services like SNMP should be configured with strong community strings, and default credentials across all services should be changed to strong, unique passwords. There should be continuous monitoring to implement a robust intrusion detection system (IDS) and regular monitoring protocols to detect and respond to malicious activities in real time. Finally, staff training should be instilled in conducting regular security awareness training for staff to prevent potential security breaches due to human error.

CONCLUSION

The pen test findings on Upwork were done and concluded on April 19, 2024, and summarized in this report. Four skilled security professionals from Arizona State University conducted the tests using Kali Linux, Nmap, Enum4Linux, netcat, Nessus Vulnerability Scanning, Metasploit, and CrackMapExec. Pen tests are important for identifying any critical vulnerabilities in security and systems. The key findings from the three targets were open ports with little firewall structure, RPC, remote, and backdoor vulnerabilities. There are recommendations for vulnerability categorization, improved patching policies, configuration review, continuous monitoring, and further staff training.

Simulating real-world cyber-attacks aids in finding and identifying potential vulnerabilities that were not caught during the OSINT phase, along with other weaknesses. The goals of any security professional who partakes in pen testing should assess effectiveness of current security, identify any hidden risks, and strengthen cyber defenses.

ANNEXES

A. References

Apporto Virtual Lab.
CrackMapExec.
Enum4Linux.
Kali Linux.
Metasploit.
Nessus Vulnerability Scanning.
Netcat.
NIST. (2021, June 3). *NVD - CVE-2019-0708*. https://nvd.nist.gov/vuln/detail/CVE-2019-0708
Nmap.

B. Acronoyms

ARP- Address Resolution Protocol.
HTTP- Hypertext Transfer Protocol
IDS- Intrusion Detection System.
OS- Operating System.
OSINT- Open-Source Intelligence.
RDP- Remote Desktop Protocol.
SMB- Server Message Block.
SNMP- Simple Network Management Protocol