Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Batch: B1 Roll No.: 16010121045

Experiment No. 3

Title: Perform Network Scanning using NMAP

Objective:
Perform Network Scanning using NMAP

CO	Outcome
CO1	Understand penetration testing with scope of its ethical implications, documentation and reporting

Books/ Journals/ Websites referred:

- https://nmap.org/
- https://nmap.org/book/man.html

Introduction:
Network scanning is a critical aspect of cybersecurity, allowing professionals to assess the security posture of a network by identifying open ports, services running on those ports, and potential vulnerabilities within those services. Nmap (Network Mapper) stands out as one of the most widely used and powerful network scanning tools available today. It enables security analysts, administrators, and ethical hackers to gather comprehensive information about network hosts, services, and their configurations.

Nmap's versatility allows for the detection of open ports, services running on those ports, and potential vulnerabilities associated with those services. The study delves into specific services commonly found in networks, including SSH, SMB, FTP, VNC, and MySQL, highlighting how Nmap can be leveraged to assess their security posture. By utilizing Nmap's extensive range of scanning techniques and scripts, organizations can proactively identify and mitigate security risks, thus enhancing their overall cybersecurity posture.

SSH (Secure Shell):
SSH is a cryptographic network protocol used for secure remote access to systems. Nmap can detect SSH services running on a network by scanning for open port 22, the default port for SSH. Additionally, Nmap can identify the version of SSH running, aiding in determining potential vulnerabilities associated with specific versions.

SMB (Server Message Block):
SMB is a network protocol used for providing shared access to files, printers, and other resources between nodes on a network. Nmap can identify SMB services by scanning for open ports 445 (SMB over TCP) and 139 (NetBIOS over TCP), allowing for the detection of potential vulnerabilities such as unauthenticated access, misconfigured shares, or outdated software versions.

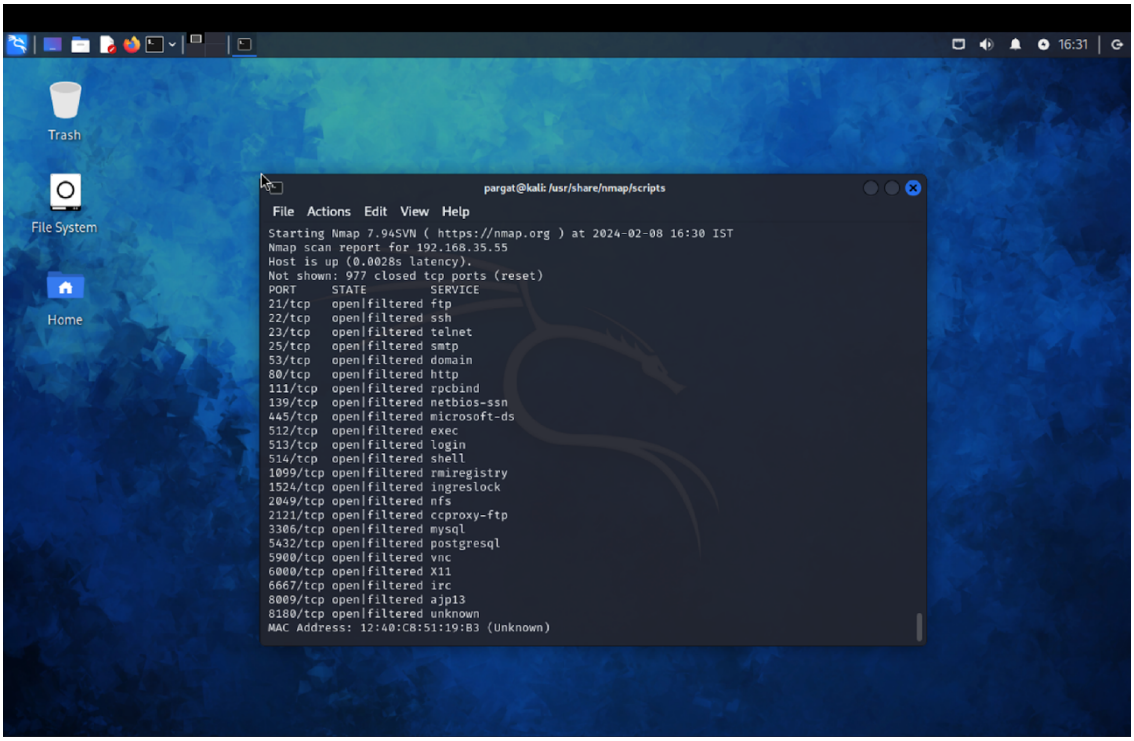
FTP (File Transfer Protocol):
FTP is a standard network protocol used for transferring files between a client and a server on a computer network. Nmap can detect FTP services by scanning for open port 21, the default port for FTP. Through banner grabbing and version detection, Nmap can identify FTP server software and potential vulnerabilities such as weak authentication mechanisms or outdated software versions.

VNC (Virtual Network Computing):
VNC is a graphical desktop sharing system that allows users to remotely control another computer. Nmap can detect VNC services by scanning for open ports such as 5900, the default port used by VNC servers. By identifying VNC services and their associated versions, Nmap helps in assessing the security posture of remote desktop access and detecting potential vulnerabilities.

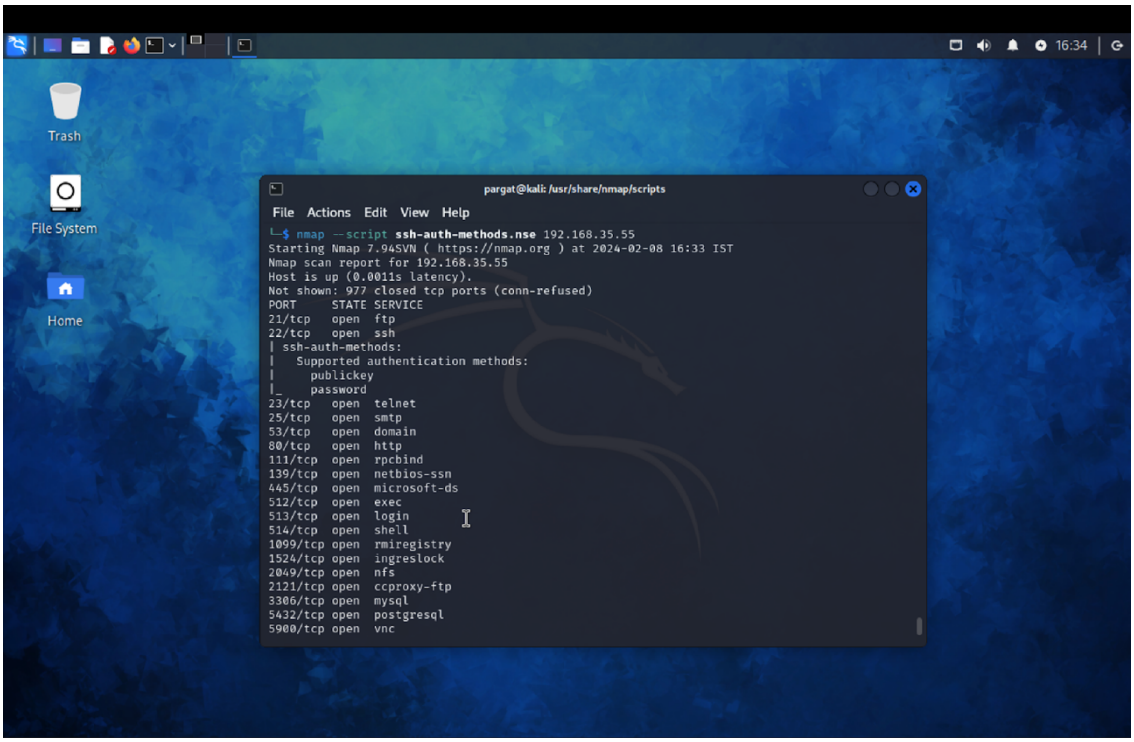
MySQL:
MySQL is a popular open-source relational database management system. Nmap can identify MySQL services by scanning for open port 3306, the default port for MySQL. Furthermore, Nmap can enumerate MySQL server information and versions, aiding in the identification of potential vulnerabilities such as weak authentication mechanisms, misconfigurations, or outdated software versions.

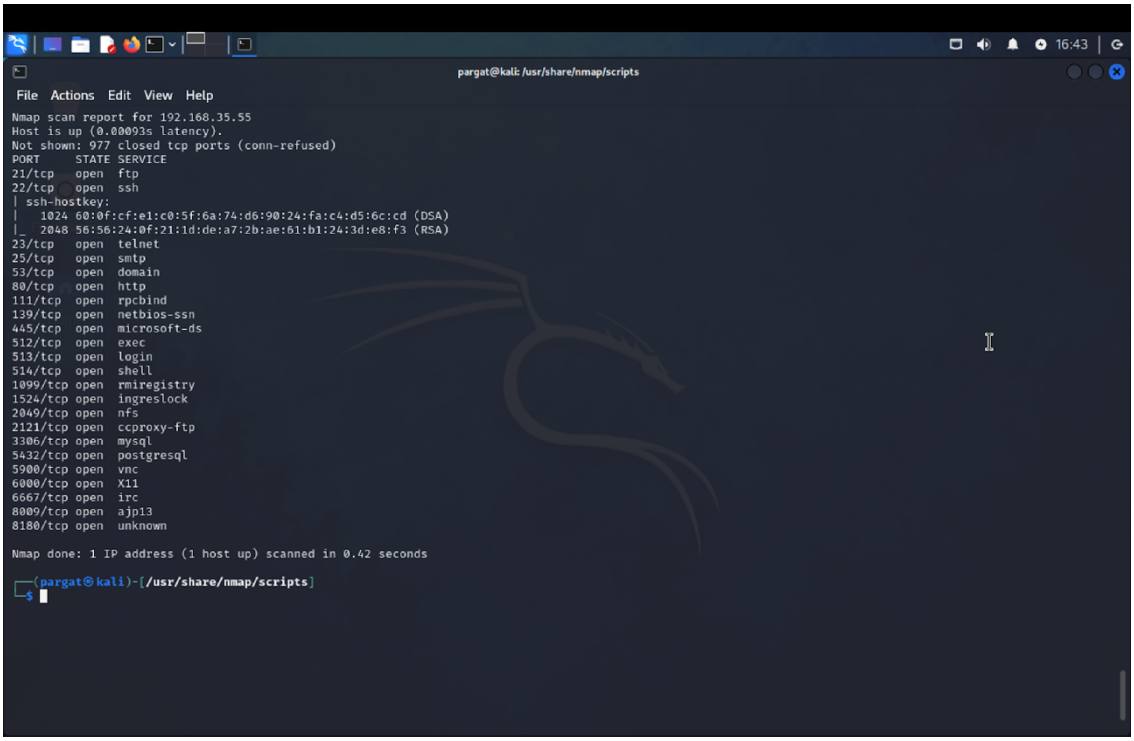
Implementation details:

The following screenshots depict the exploited vulnerabilities identified through lab experiments using Nmap:

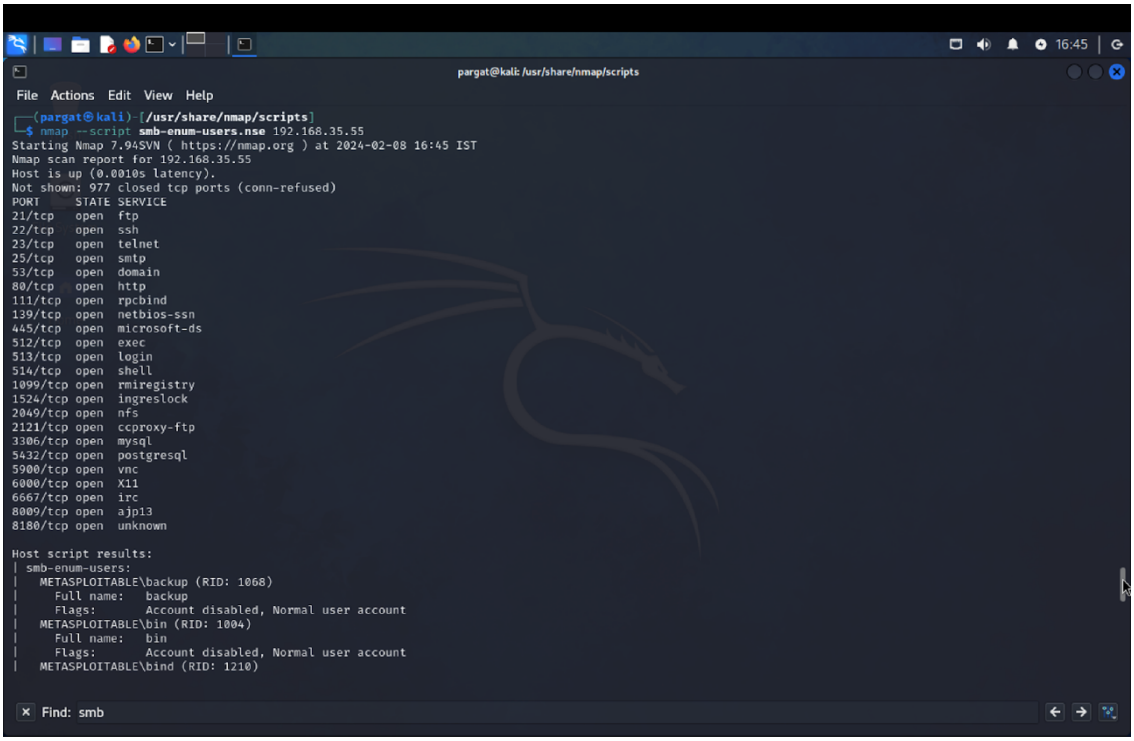


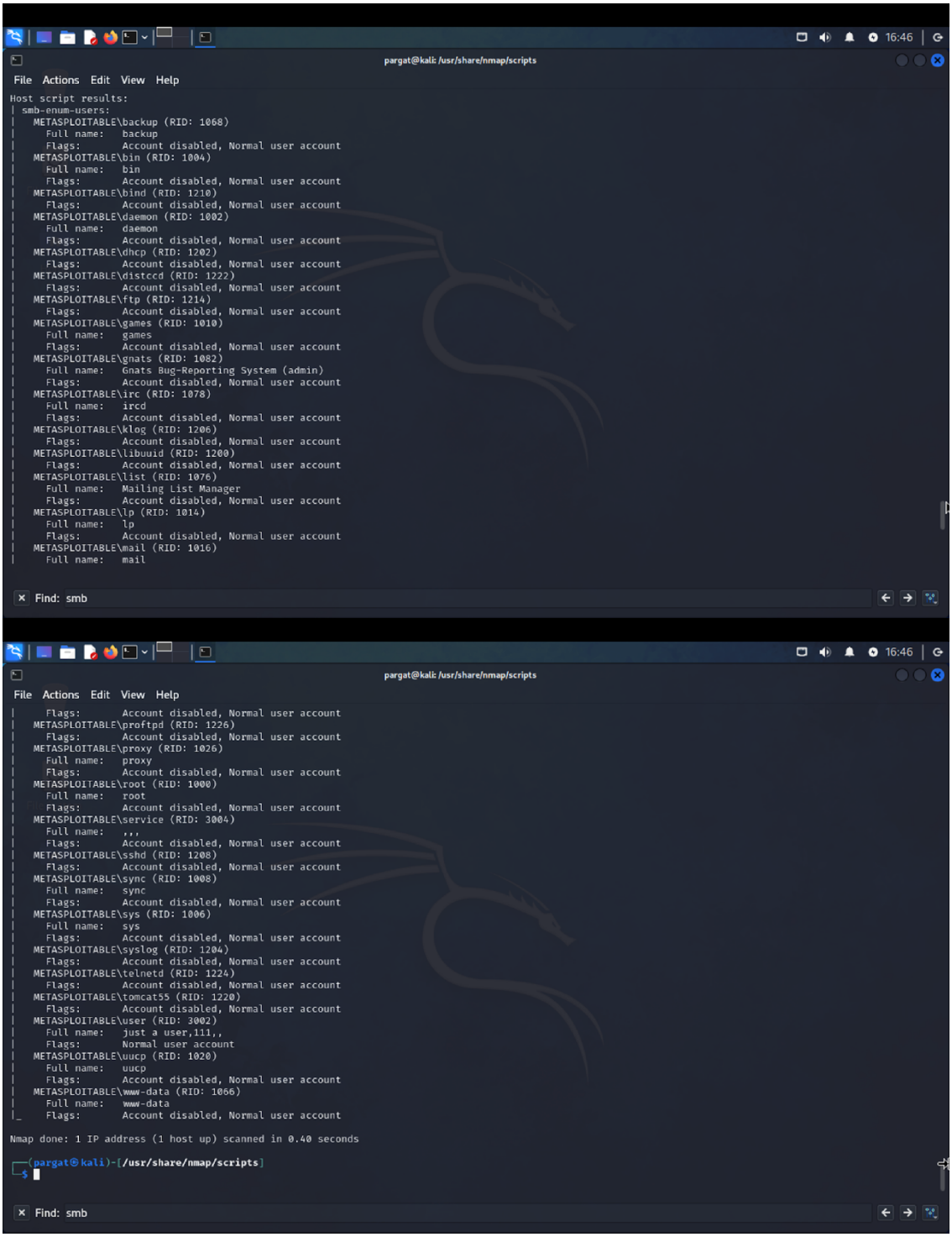
SSH

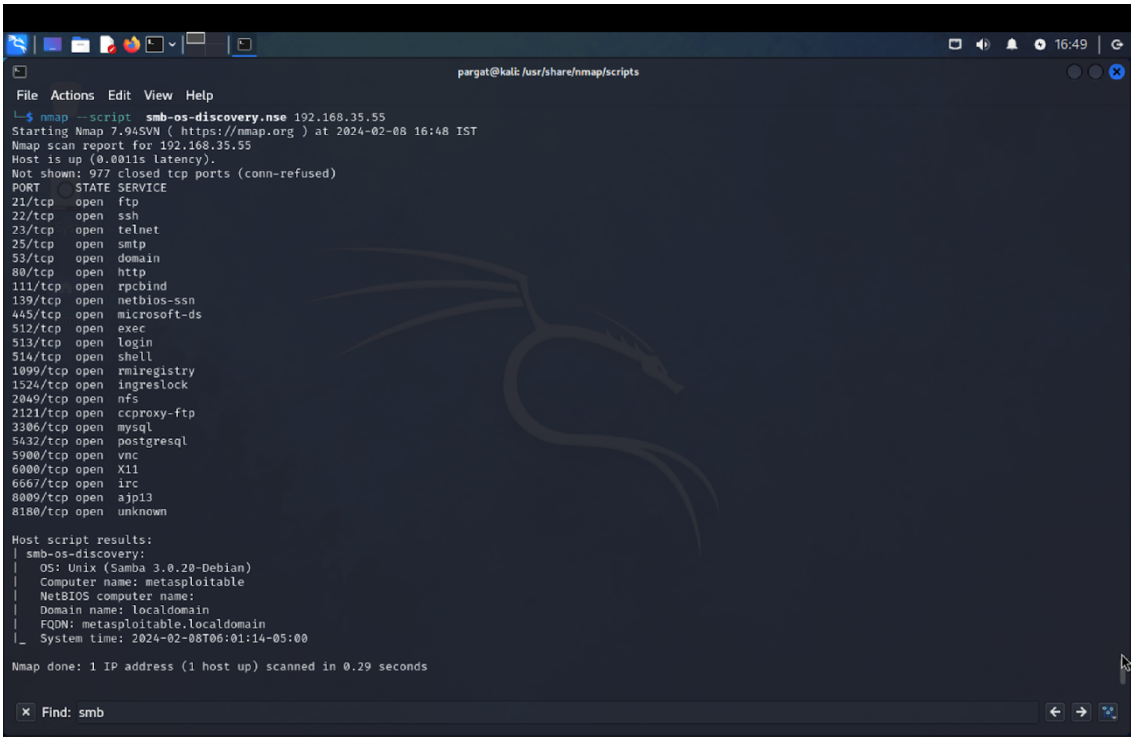



pargat@kali: /usr/share/nmap/scripts
File Actions Edit View Help
Nmap scan report for 192.168.35.55
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
| ssh-hostkey:
| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
(pargat㉿kali)-[/usr/share/nmap/scripts]
$

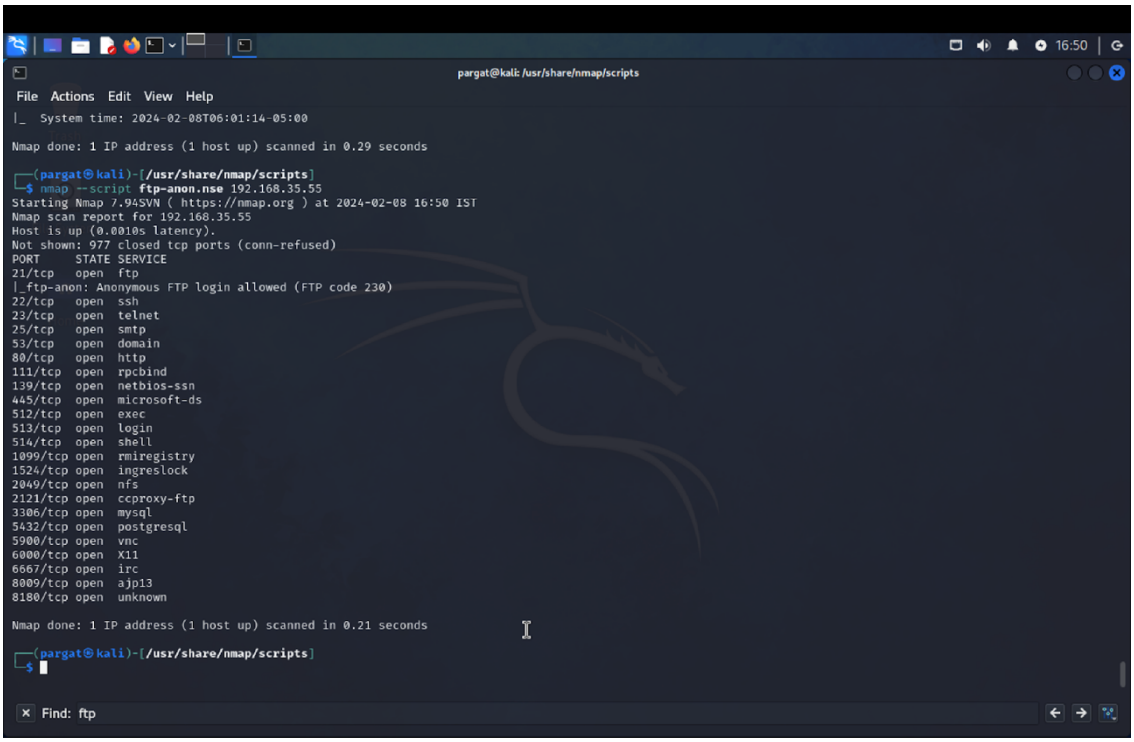
SMB

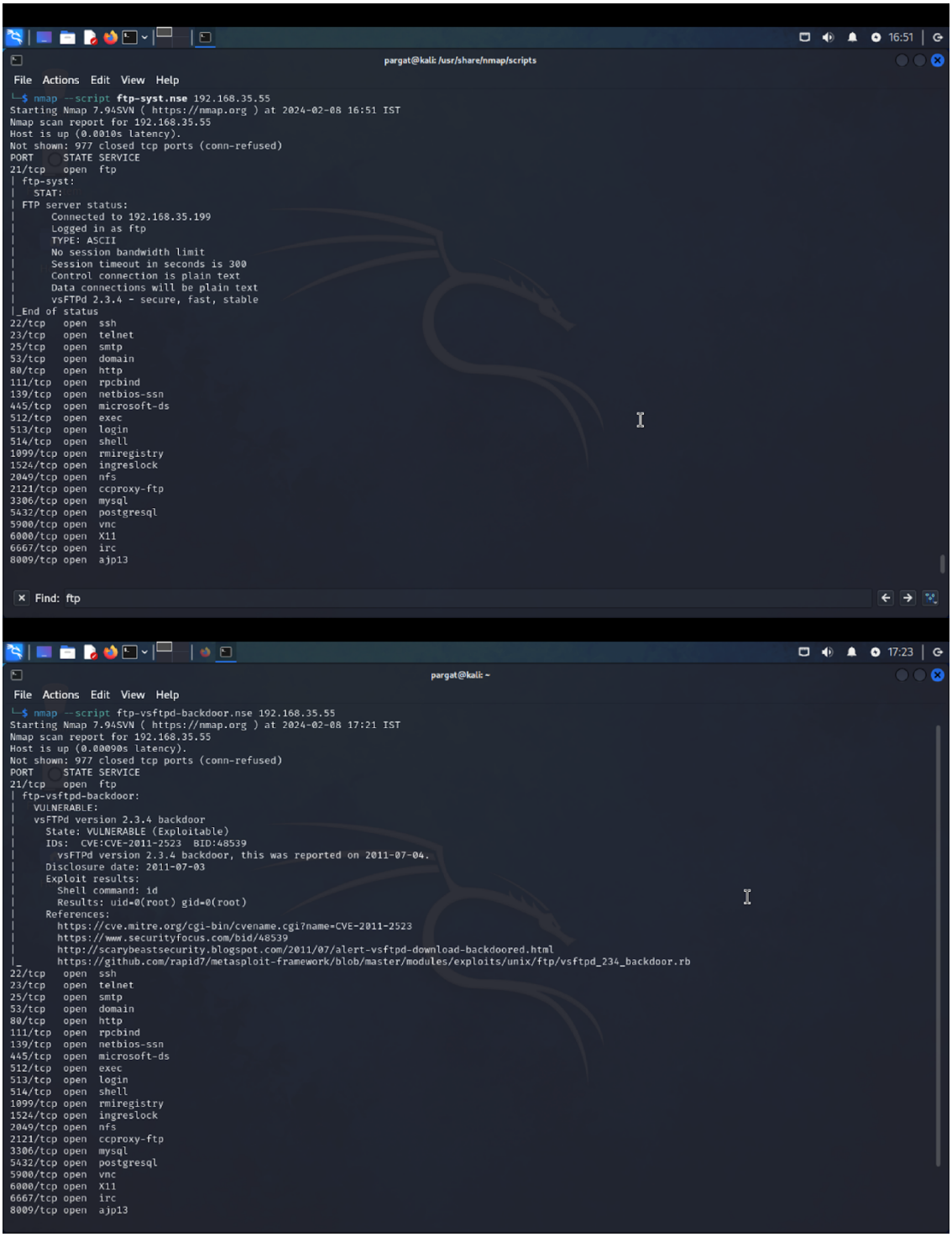

pargat@kali: /usr/share/nmap/scripts
File Actions Edit View Help
(pargat㉿kali)-[/usr/share/nmap/scripts]
$ nmap --script smb-enum-users.nse 192.168.35.55
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-08 16:45 IST
Nmap scan report for 192.168.35.55
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Host script results:
| smb-enum-users:
| METASPLOITABLE\backup (RID: 1068)
| Full name: backup
| Flags: Account disabled, Normal user account
| METASPLOITABLE\bin (RID: 1004)
| Full name: bin
| Flags: Account disabled, Normal user account
| METASPLOITABLE\bind (RID: 1210)
Find: smb


pargat@kali: /usr/share/nmap/scripts
File Actions Edit View Help
Host script results:
| smb-enum-users:
| METASPLOITABLE\backup (RID: 1068)
| Full name: backup
| Flags: Account disabled, Normal user account
| METASPLOITABLE\bin (RID: 1004)
| Full name: bin
| Flags: Account disabled, Normal user account
| METASPLOITABLE\bind (RID: 1210)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\daemon (RID: 1002)
| Full name: daemon
| Flags: Account disabled, Normal user account
| METASPLOITABLE\dhcp (RID: 1202)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\distccd (RID: 1222)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\ftp (RID: 1214)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\games (RID: 1010)
| Full name: games
| Flags: Account disabled, Normal user account
| METASPLOITABLE\gnats (RID: 1082)
| Full name: Gnats Bug-Reporting System (admin)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\irc (RID: 1078)
| Full name: ircd
| Flags: Account disabled, Normal user account
| METASPLOITABLE\klog (RID: 1206)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\libuuid (RID: 1200)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\list (RID: 1076)
| Full name: Mailing List Manager
| Flags: Account disabled, Normal user account
| METASPLOITABLE\lp (RID: 1014)
| Full name: lp
| Flags: Account disabled, Normal user account
| METASPLOITABLE\mail (RID: 1016)
| Full name: mail
Find: smb
pargat@kali: /usr/share/nmap/scripts
File Actions Edit View Help
| Flags: Account disabled, Normal user account
| METASPLOITABLE\proftpd (RID: 1226)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\proxy (RID: 1026)
| Full name: proxy
| Flags: Account disabled, Normal user account
| METASPLOITABLE\root (RID: 1000)
| Full name: root
| Flags: Account disabled, Normal user account
| METASPLOITABLE\service (RID: 3004)
| Full name: ,,,
| Flags: Account disabled, Normal user account
| METASPLOITABLE\sshd (RID: 1208)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\sync (RID: 1008)
| Full name: sync
| Flags: Account disabled, Normal user account
| METASPLOITABLE\sys (RID: 1006)
| Full name: sys
| Flags: Account disabled, Normal user account
| METASPLOITABLE\syslog (RID: 1204)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\telnetd (RID: 1224)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\tomcat55 (RID: 1220)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\user (RID: 3002)
| Full name: just a user,111,,
| Flags: Normal user account
| METASPLOITABLE\uucp (RID: 1020)
| Full name: uucp
| Flags: Account disabled, Normal user account
| METASPLOITABLE\www-data (RID: 1066)
| Full name: www-data
|_ Flags: Account disabled, Normal user account
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
(pargat㉿kali)-[/usr/share/nmap/scripts]
$
Find: smb

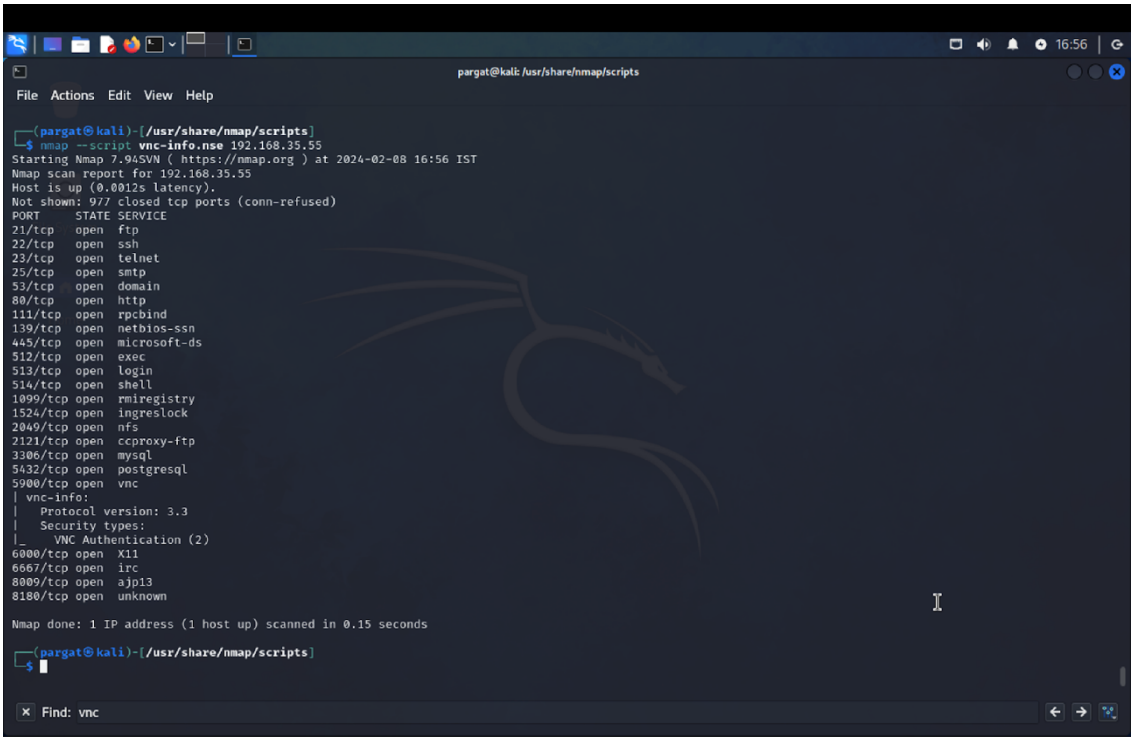

16:49
pargat@kali: /usr/share/nmap/scripts
File Actions Edit View Help
└─$ nmap --script smb-os-discovery.nse 192.168.35.55
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-08 16:48 IST
Nmap scan report for 192.168.35.55
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Host script results:
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: metasploitable
| NetBIOS computer name:
| Domain name: localdomain
| FQDN: metasploitable.localdomain
|_ System time: 2024-02-08T06:01:14-05:00
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
Find: smb

FTP

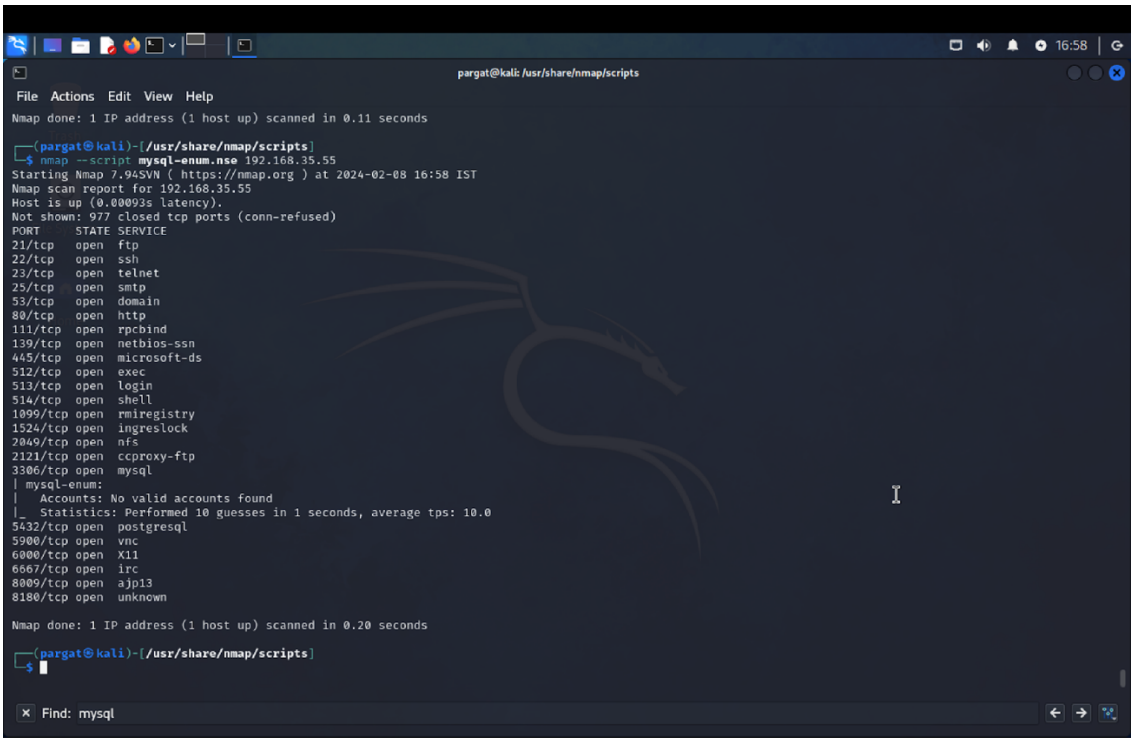

16:50
pargat@kali: /usr/share/nmap/scripts
File Actions Edit View Help
|_ System time: 2024-02-08T06:01:14-05:00
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
(pargat㉿kali)-[/usr/share/nmap/scripts]
$ nmap --script ftp-anon.nse 192.168.35.55
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-08 16:50 IST
Nmap scan report for 192.168.35.55
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
(pargat㉿kali)-[/usr/share/nmap/scripts]
$
Find: ftp

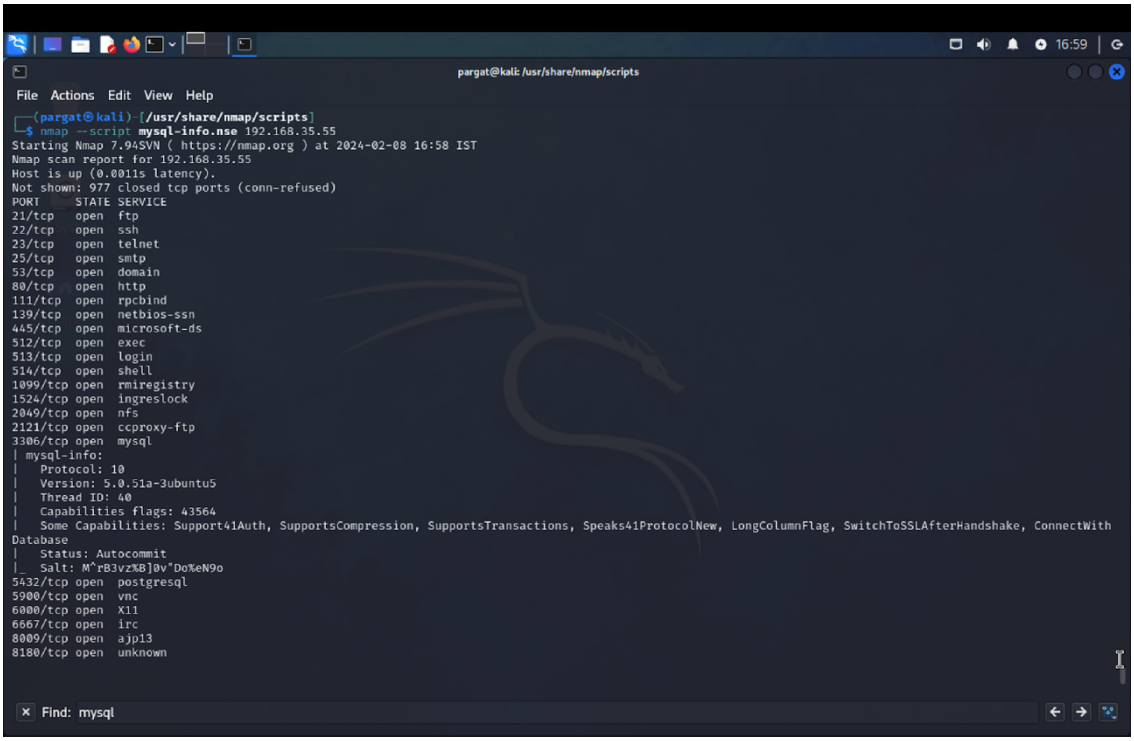

pargat@kali: /usr/share/nmap/scripts
File Actions Edit View Help
└─$ nmap --script ftp-syst.nse 192.168.35.55
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-08 16:51 IST
Nmap scan report for 192.168.35.55
Host is up (0.0010s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.35.199
| 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
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
Find: ftp
pargat@kali: ~
File Actions Edit View Help
└─$ nmap --script ftp-vsftpd-backdoor.nse 192.168.35.55
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-08 17:21 IST
Nmap scan report for 192.168.35.55
Host is up (0.00090s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
| ftp-vsftpd-backdoor:
| VULNERABLE:
| vsFTPd version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
| IDs: CVE:CVE-2011-2523 BID:48539
| vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
| Disclosure date: 2011-07-03
| Exploit results:
| Shell command: id
| Results: uid=0(root) gid=0(root)
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
| https://www.securityfocus.com/bid/48539
| http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_ https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13

VNC


pargat@kali: /usr/share/nmap/scripts
File Actions Edit View Help
(pargat㉿kali)-[/usr/share/nmap/scripts]
$ nmap --script vnc-info.nse 192.168.35.55
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-08 16:56 IST
Nmap scan report for 192.168.35.55
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
| vnc-info:
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
(pargat㉿kali)-[/usr/share/nmap/scripts]
$
Find: vnc

MYSQL


pargat@kali: /usr/share/nmap/scripts
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
(pargat㉿kali)-[/usr/share/nmap/scripts]
$ nmap --script mysql-enum.nse 192.168.35.55
Starting Nmap 7.94SVN (https://nmap.org) at 2024-02-08 16:58 IST
Nmap scan report for 192.168.35.55
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
| mysql-enum:
| Accounts: No valid accounts found
|_ Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
(pargat㉿kali)-[/usr/share/nmap/scripts]
$
Find: mysql



Conclusion:

Through NMAP's extensive scanning capabilities, we obtained crucial insights into the targeted network's structure and vulnerabilities. The scan revealed active hosts, open ports, and services running on those ports, offering valuable information for enhancing network security. NMAP's diverse scanning techniques enabled comprehensive analysis, empowering network administrators to prioritize security measures effectively.