Exploring TCP Port Vulnerabilities in Metasploitable2 Using Kali Linux

by

Vibhuti Naik
Intern ID - 2046

Exploring TCP Port Vulnerabilities in Metasploitable2 Using Kali Linux

Port Scan

Description:

A port scan is a technique used by network administrators and attackers alike to discover which "doors" are open on a networked device. By sending packets to specific ports—such as Port 80 for web traffic or Port 21 for FTP—and analyzing the responses, the scanner determines the state of those ports: open, closed, or filtered. This process provides a blueprint of the target system, identifying active services, potential vulnerabilities, and the underlying operating system. While administrators use it for security auditing and troubleshooting, for an attacker, it is the essential first step in mapping out an attack surface before launching an exploit.

Impact:

- **Information Disclosure:** Reveals exactly which services are running (e.g., an outdated version of Apache or MySQL), giving attackers a starting point for their exploits.
- **Service Identification**: Advanced scanning can perform "banner grabbing" to identify the specific software version and OS, allowing for highly targeted attacks.
- **Network Resource Consumption**: Intense or "noisy" scans can consume significant bandwidth and CPU cycles, potentially leading to a degradation in network performance or a Denial of Service (DoS).
- **Bypassing Security**: It helps attackers identify misconfigured firewalls or "shadow IT" devices that were mistakenly left exposed to the public internet.

Severity: Critical

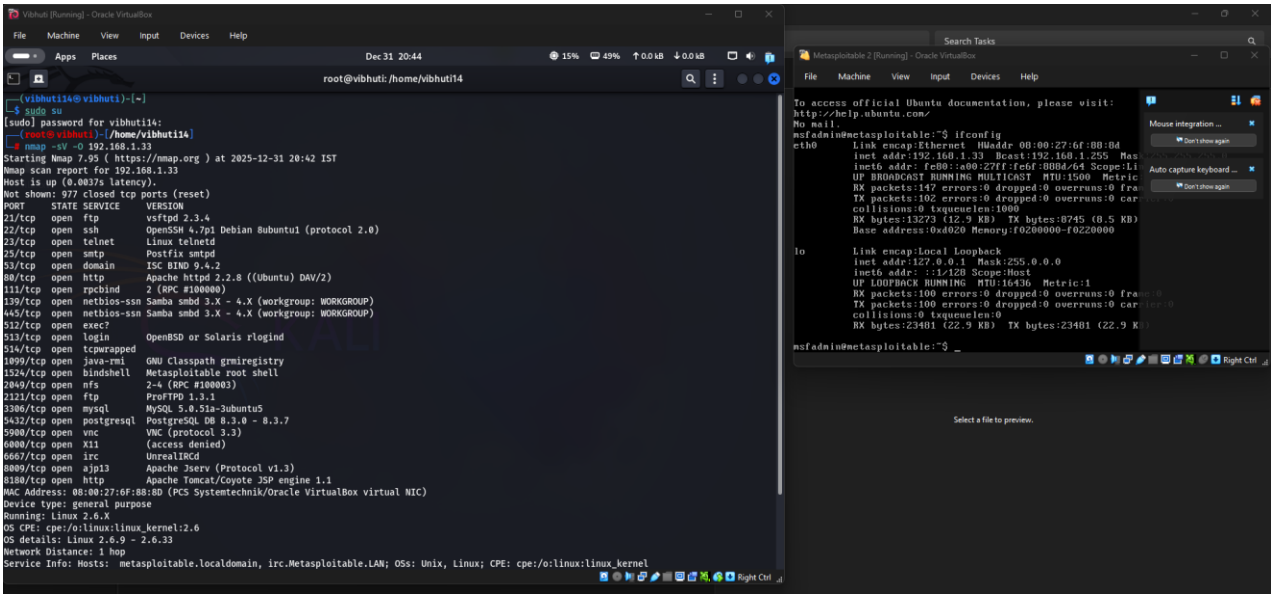
Remedial:

To protect your infrastructure from unauthorized scanning, implement the following:

- **Strict Firewall Rules:** Adopt a "deny-all" default stance. Only open ports that are strictly necessary for business operations and close all unused ports.
- **Intrusion Detection/Prevention Systems (IDS/IPS):** Deploy tools like Snort or Suricata that can detect patterns of rapid port hits and automatically drop traffic from the scanning IP.
- **Disable ICMP Responses:** Configure your edge devices to not respond to "ping" requests (ICMP Echo), making the network harder to discover during initial sweeps.

- **Regular Vulnerability Scanning:** Perform your own authorized scans (using tools like Nmap or Nessus) to identify and close gaps before an attacker finds them.

POC:



FTP Port 21

Description:

Port 21 is the default port used by the FTP protocol for control signaling. In a typical FTP session, the client connects to Port 21 on the server to issue commands (such as login credentials, folder navigation, and file deletion). It is important to note that Port 21 handles the "conversation," while a separate port (usually Port 20 or a random high port) is used to actually move the data. By default, FTP is an unencrypted, clear-text protocol, meaning all information sent over this port—including usernames and passwords—is visible to anyone capable of sniffing the network traffic.

Impact:

Leaving Port 21 open and using standard FTP carries several operational and security risks:

- **Cleartext Transmission:** FTP does not encrypt traffic. Credentials and data sent via Port 21 can be easily intercepted using "packet sniffing" tools.
- **Man-in-the-Middle (MitM) Attacks:** Attackers can intercept the control stream to modify commands or redirect file transfers to malicious destinations.
- **Brute Force Entry:** Because Port 21 is a well-known port, it is a constant target for automated bots attempting to guess passwords.

Severity: Critical

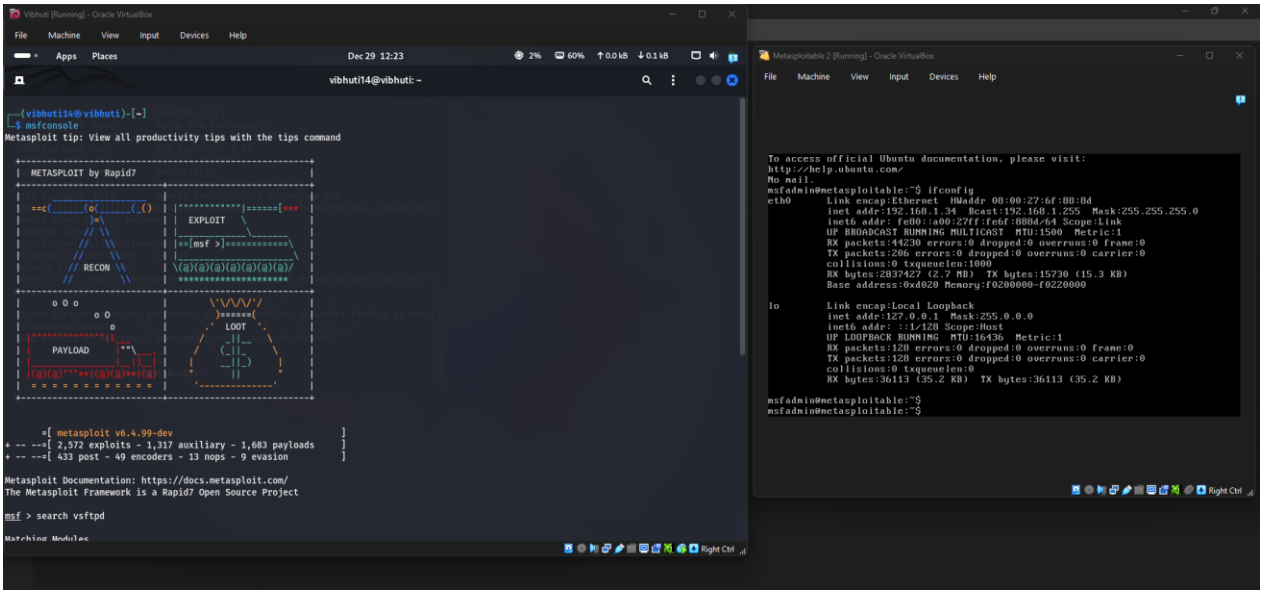
Remedial Actions:

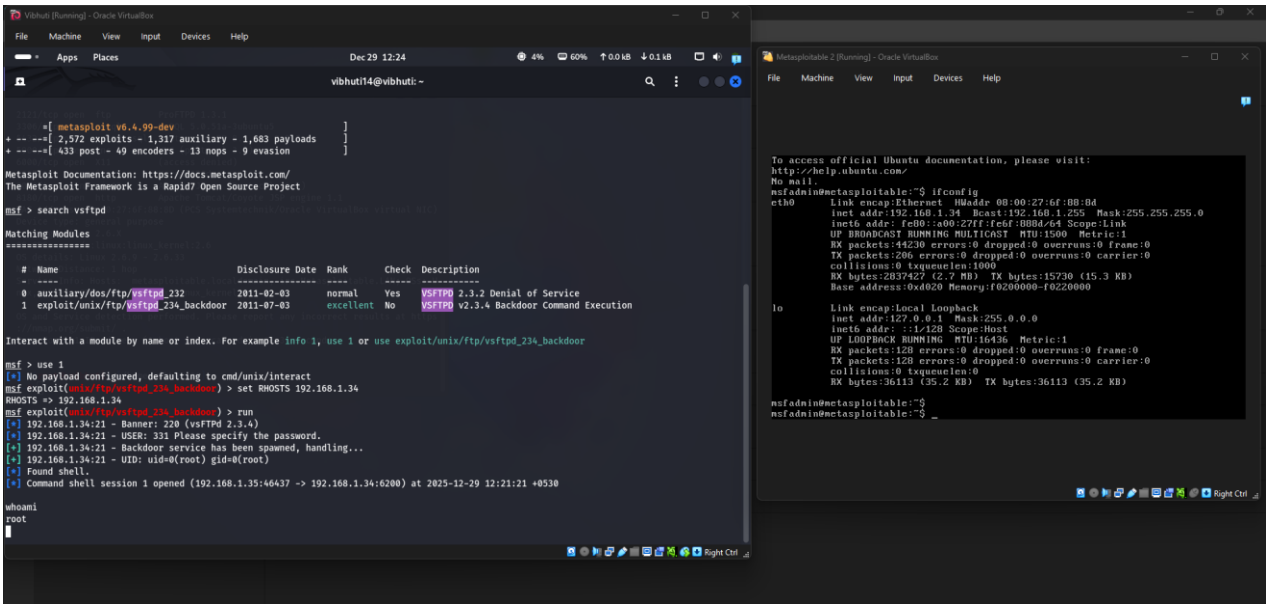
To secure your environment, consider the following steps:

- **Switch to SFTP (Port 22):** Replace FTP with SSH File Transfer Protocol. It provides full encryption for both commands and data through a single secure tunnel.
- **Implement FTPS:** If you must stay within the FTP family, use FTP over TLS/SSL. This upgrades the connection on Port 21 to an encrypted session (Explicit FTPS) or uses Port 990 (Implicit FTPS).
- **Disable Anonymous Access:** Ensure the server configuration explicitly denies logins without valid, unique user credentials.
- **Enforce Strong Password Policies:** Implement account lockout mechanisms and complex passwords to mitigate the risk of brute-force attacks.

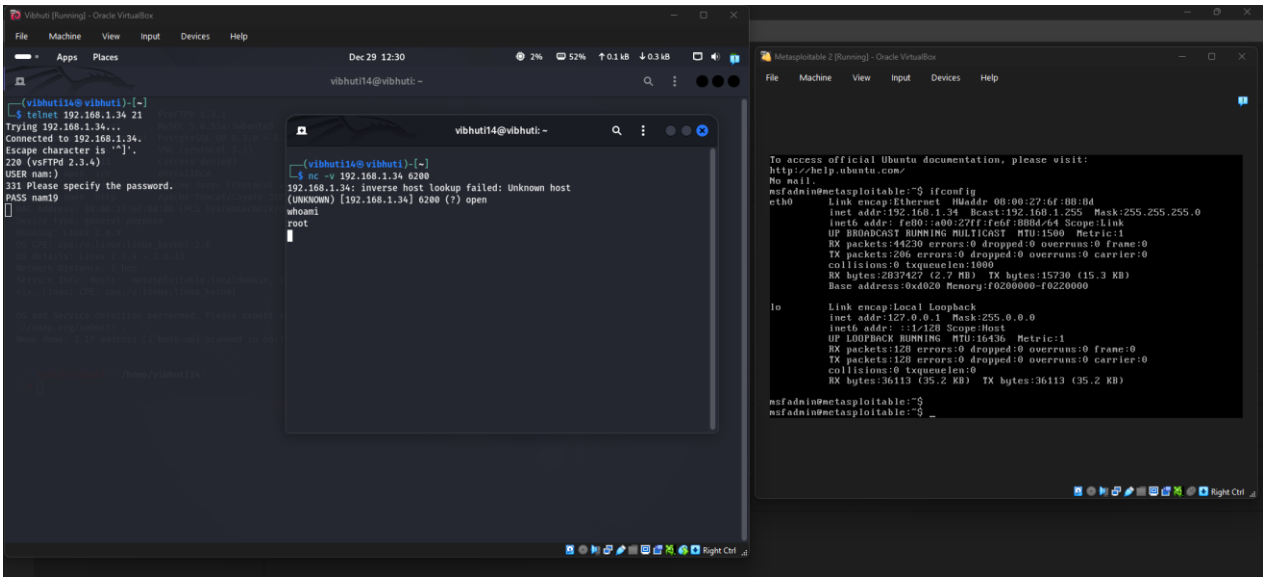
PUC:

Method 1: Using Metasploit (Automated)

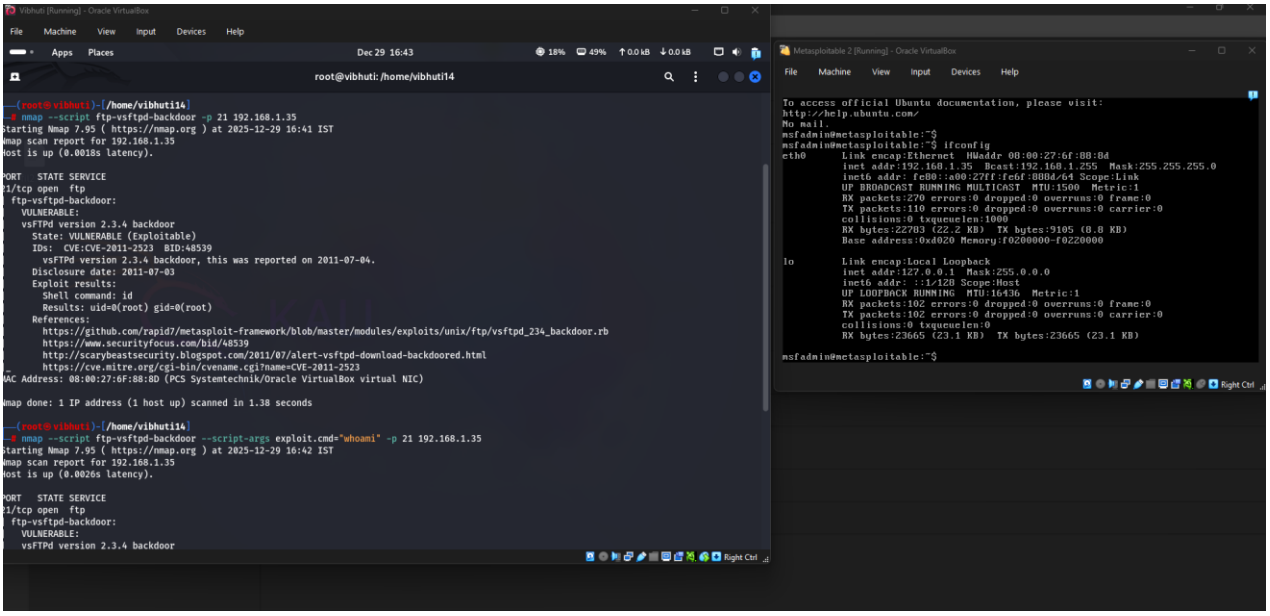


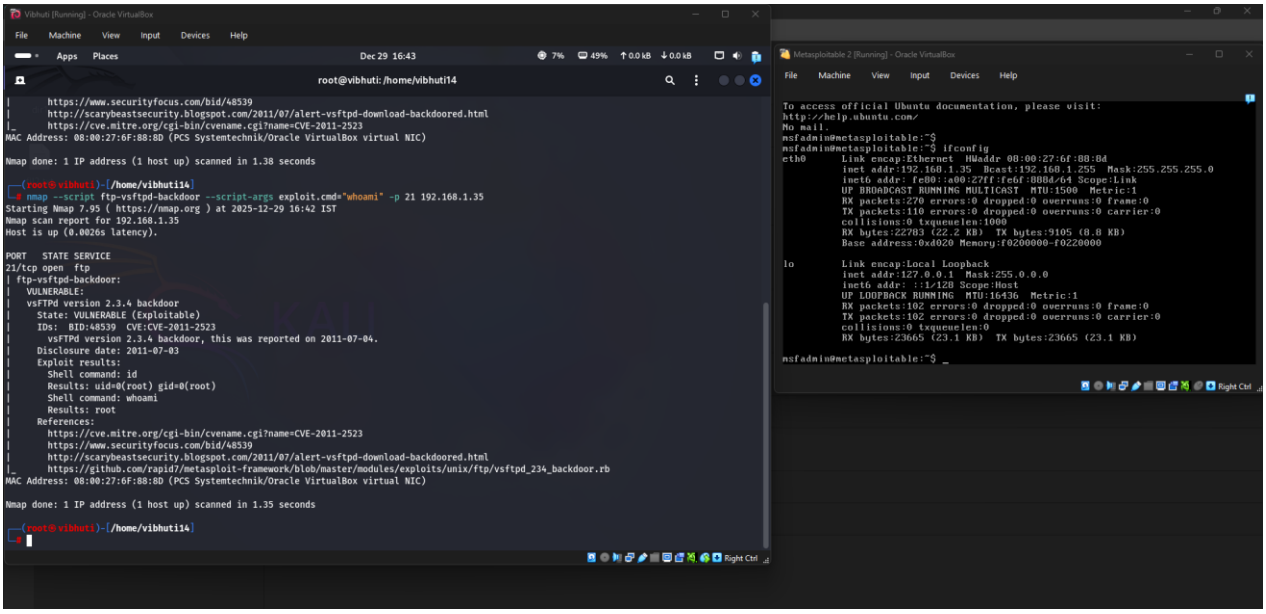


Method 2: Manual Exploitation (The "Smiley Face" Bug)



Method 3: Using Nmap (Scripting Engine)





SSH Port 22

Description:

Secure Shell (SSH) uses Port 22 as the standard channel for secure remote login and other network services between two computers. Unlike its predecessor Telnet, which transmitted data in plain text, SSH provides a cryptographically secure connection. When a client connects to a server on Port 22, it establishes an encrypted tunnel that protects session integrity and confidentiality. This port is the foundation for several critical services, including remote command-line access, SFTP (SSH File Transfer Protocol), and SCP (Secure Copy).

Impact:

If Port 22 is left exposed to the public internet without proper hardening, the potential impacts include:

- **Full System Takeover:** Since SSH provides a remote command-line interface, a successful login can give an attacker total control over the operating system.
- **Brute-Force & Dictionary Attacks:** Attackers use automated tools to try thousands of common username and password combinations every minute against open Port 22 instances.
- **Data Exfiltration:** Using SFTP over Port 22, an unauthorized user can silently download sensitive databases, configuration files, and private user data.
- **Lateral Movement:** Once an attacker compromises one server via SSH, they can use it as a "jump box" to attack other internal systems that are not directly exposed to the internet.

Severity: Critical

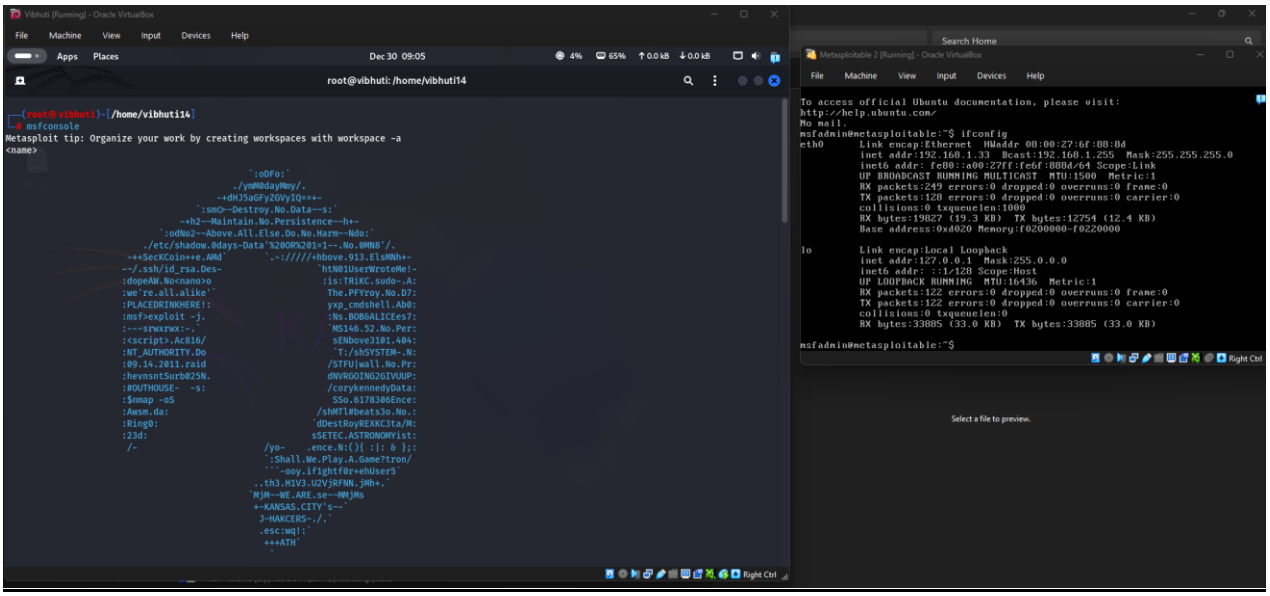
Remedial:

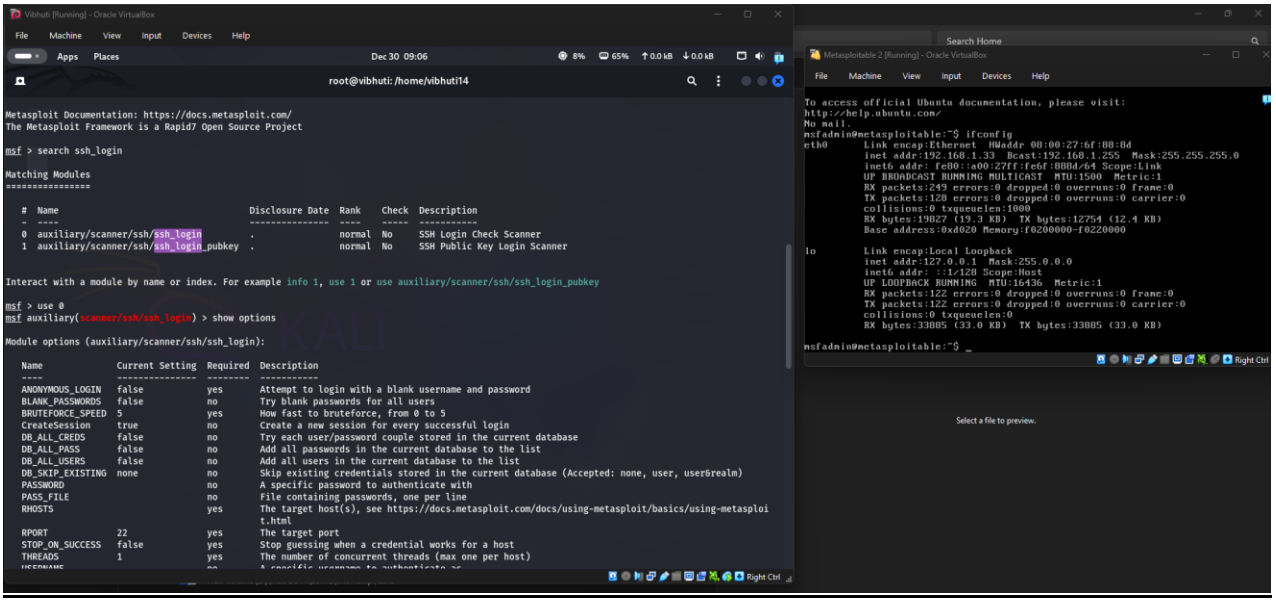
To secure Port 22, implement the following industry-standard hardening steps:

- **Disable Root Login:** Edit the SSH configuration file (/etc/ssh/sshd_config) and set PermitRootLogin no. This forces users to log in as a standard user and then use sudo for administrative tasks.
- **Enforce Key-Based Authentication:** Disable password logins entirely and require SSH Keys (RSA or Ed25519). This renders brute-force attacks useless as there is no password to guess.
- **Restrict Access via Firewall:** Use an Access Control List (ACL) or Security Group to allow Port 22 traffic only from specific, trusted IP addresses (your office or home VPN).
- **Implement Multi-Factor Authentication (MFA):** Add an extra layer of security by requiring a TOTP code (like Google Authenticator) in addition to an SSH key.

POC:

Method 1: Using Metasploit (Automated)





Telnet Port 23

Description:

Telnet is a legacy network protocol that enables a user on one computer to log into another computer on the same network or over the internet. Operating primarily on Port 23, it provides a text-based, bidirectional communication channel, allowing administrators to execute commands and manage devices—such as routers, switches, and old mainframe systems—remotely. Unlike modern protocols, Telnet was designed in an era before widespread cybersecurity threats, meaning it transmits all information, including usernames and passwords, in cleartext.

Impact:

The continued use of Port 23 on modern networks presents several critical risks:

- **Credential Theft:** Since data is unencrypted, login details are visible in "plain text" to anyone performing a Man-in-the-Middle (MitM) attack or packet sniffing.
- **Session Hijacking:** Attackers can intercept an active Telnet session, inject malicious commands, or take over the terminal entirely without the user's knowledge.
- **Full System Compromise:** Telnet often provides administrative Command Line Interface (CLI) access; once an attacker logs in, they have the power to delete data, install malware, or reconfigure network hardware.
- **Botnet Targeting:** Port 23 is a primary target for IoT botnets (like Mirai), which scan the internet for devices using default Telnet credentials to recruit them into massive DDoS networks.

Severity: Critical

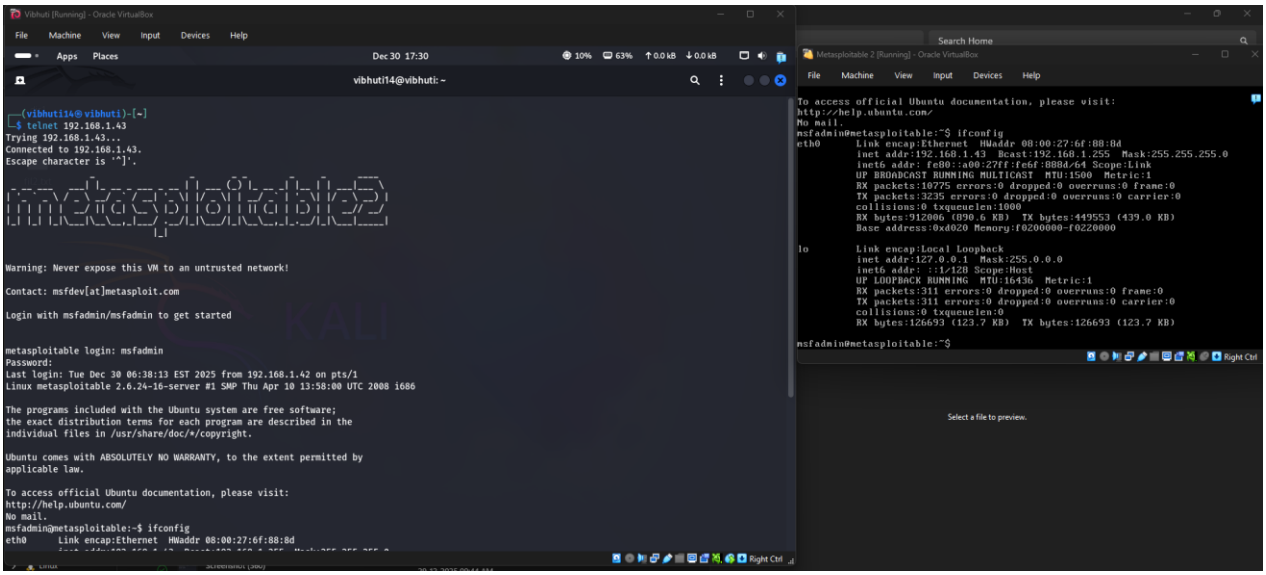
Remedial:

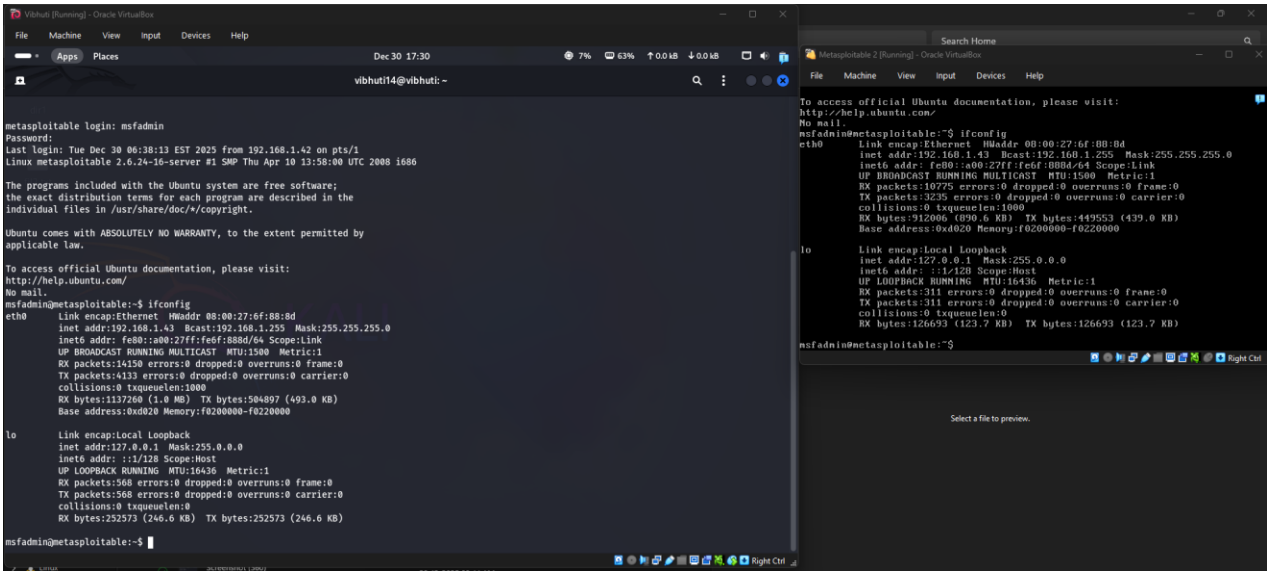
To secure your network and eliminate the risks associated with Telnet, follow these steps:

- **Disable Telnet:** The most effective remedy is to completely disable the Telnet service on all servers and network equipment.
- **Block Port 23 at the Firewall:** Ensure that your perimeter firewall and internal Access Control Lists (ACLs) are configured to drop all traffic directed at Port 23.
- **Change Default Credentials:** If you are in the process of migrating and must temporarily use Telnet, ensure that default manufacturer passwords are changed to complex, unique strings immediately.

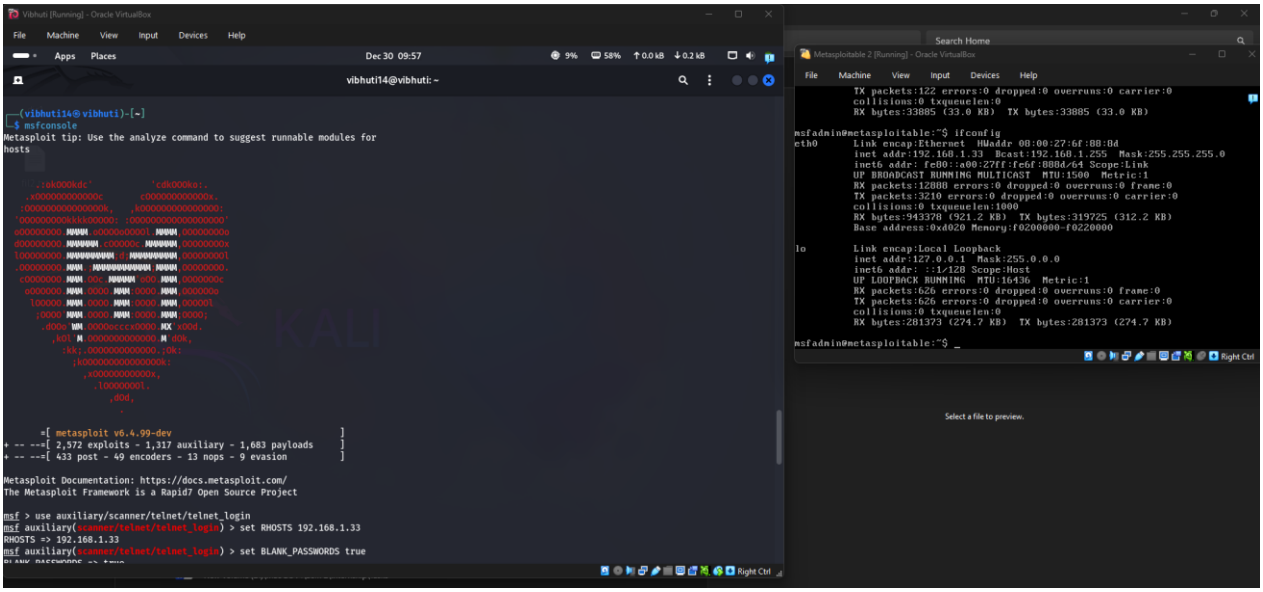
POC:

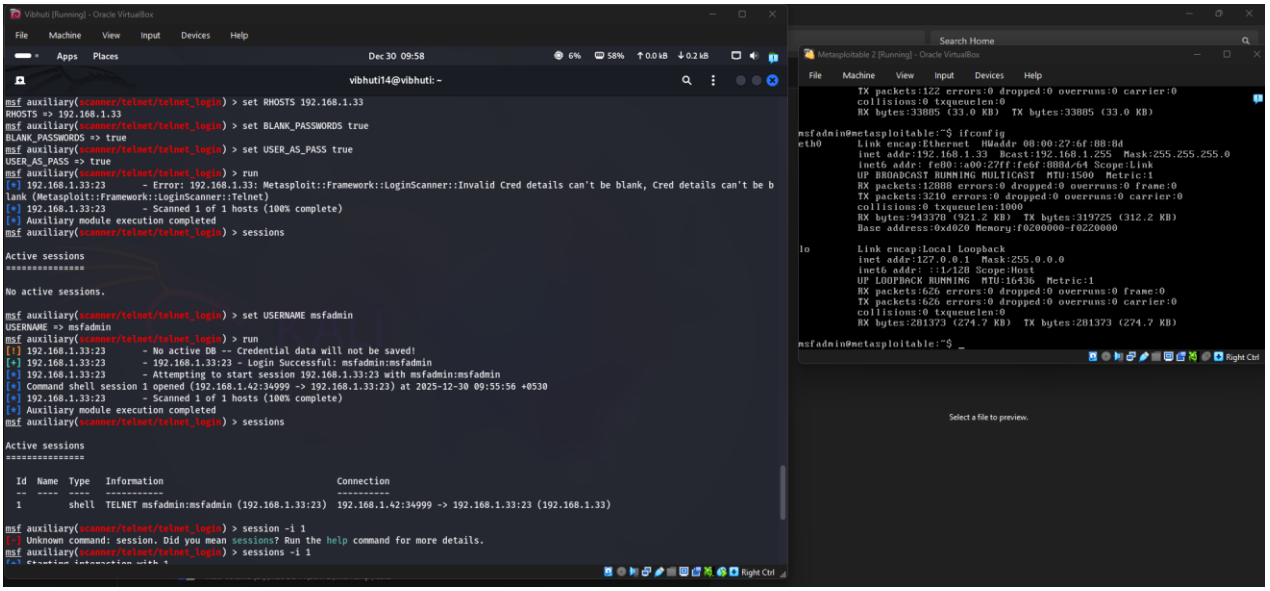
Method 1. Packet Sniffing (Wireshark/Ettercap)

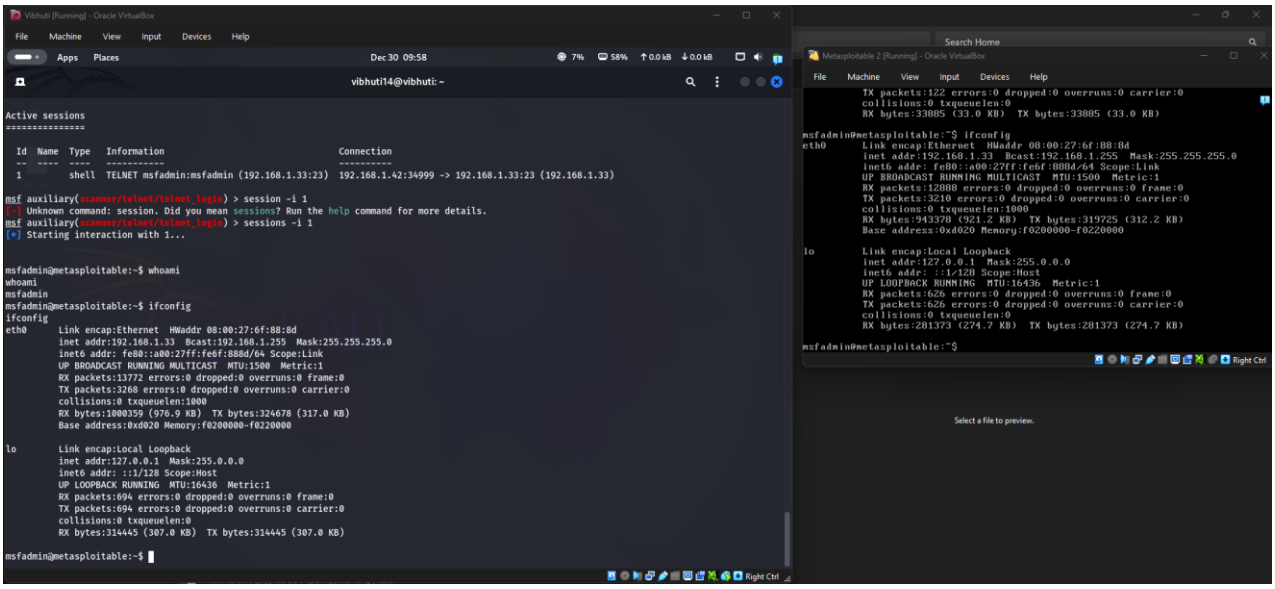




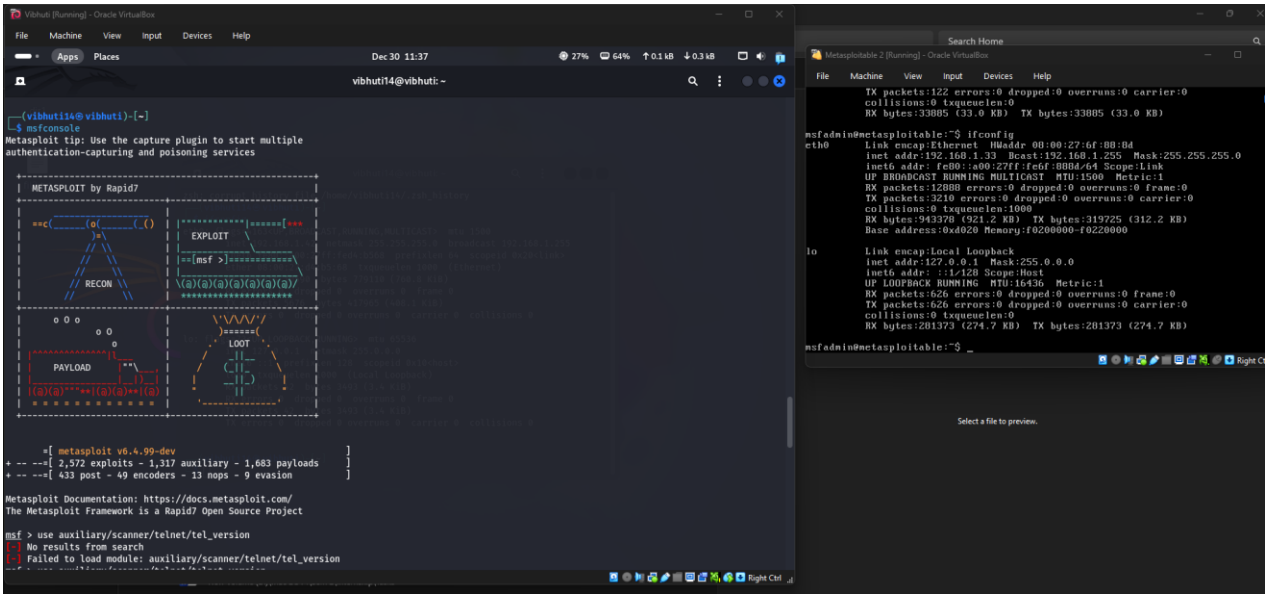
Method 2. Exploiting "Environmental Variables" (Metasploit)

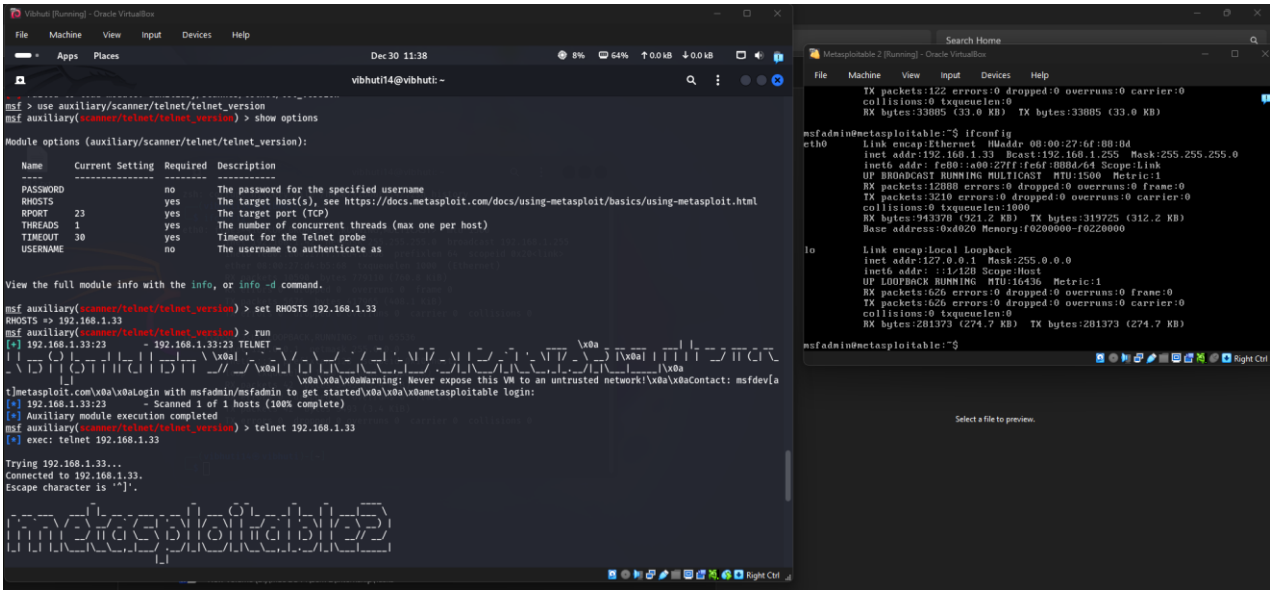






Method 3. Exploiting "Environmental Variables" (Metasploit)





SMTP Port 25

Description:

Simple Mail Transfer Protocol (SMTP) is the foundational protocol for email routing, and it traditionally operates on Port 25. Unlike Port 587 (used for client-to-server submission) or Port 465 (SMTPS), Port 25 is primarily used for server-to-server relaying. When one Mail Transfer Agent (MTA) sends an email to another, it establishes a connection via Port 25 to hand off the message. Historically, Port 25 was designed without built-in encryption or mandatory authentication, meaning that messages and credentials can be sent in "plain text."

Impact:

The risks of an unhardened or exposed Port 25 include:

- **Open Relay Abuse:** If not properly restricted, any attacker can use your server to send millions of spam emails, leading to your IP address being blacklisted globally.
- **Email Spoofing:** Because Port 25 often lacks strict authentication, attackers can forge the "From" address to send phishing emails that appear to come from your domain.
- **Cleartext Interception:** Traffic sent over Port 25 without STARTTLS can be read by anyone on the network path, exposing sensitive communication or internal data.
- **Denial of Service (DoS):** Misconfigured mail servers can be flooded with connection requests, crashing the email service and preventing legitimate business mail from flowing.

Severity: High

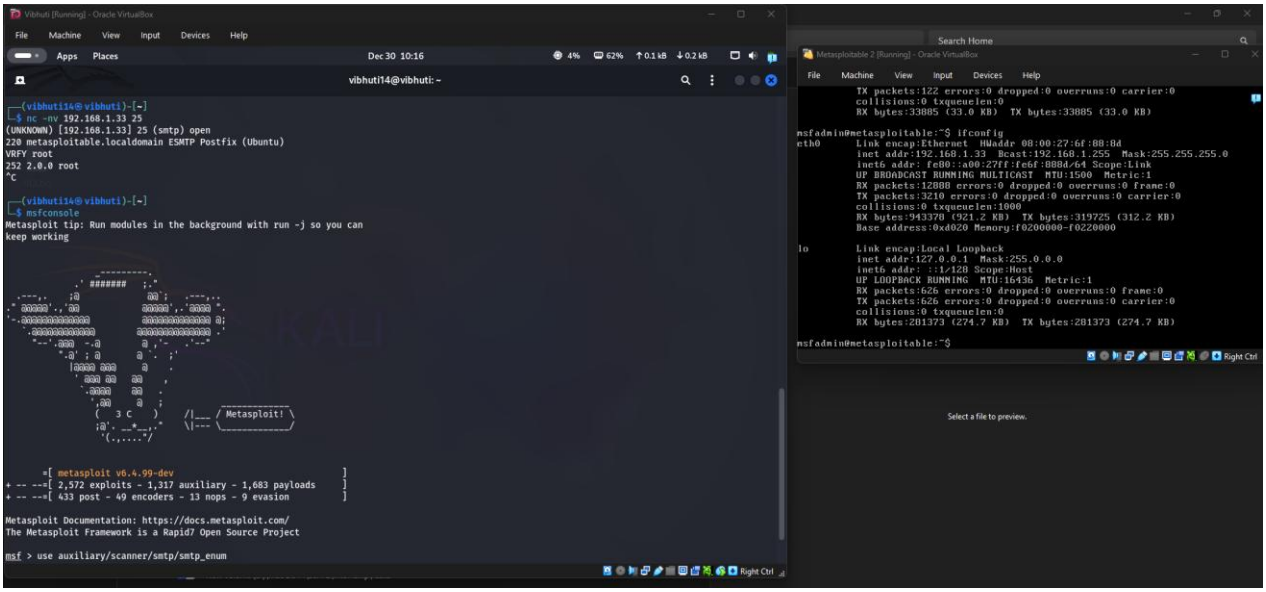
Remedial:

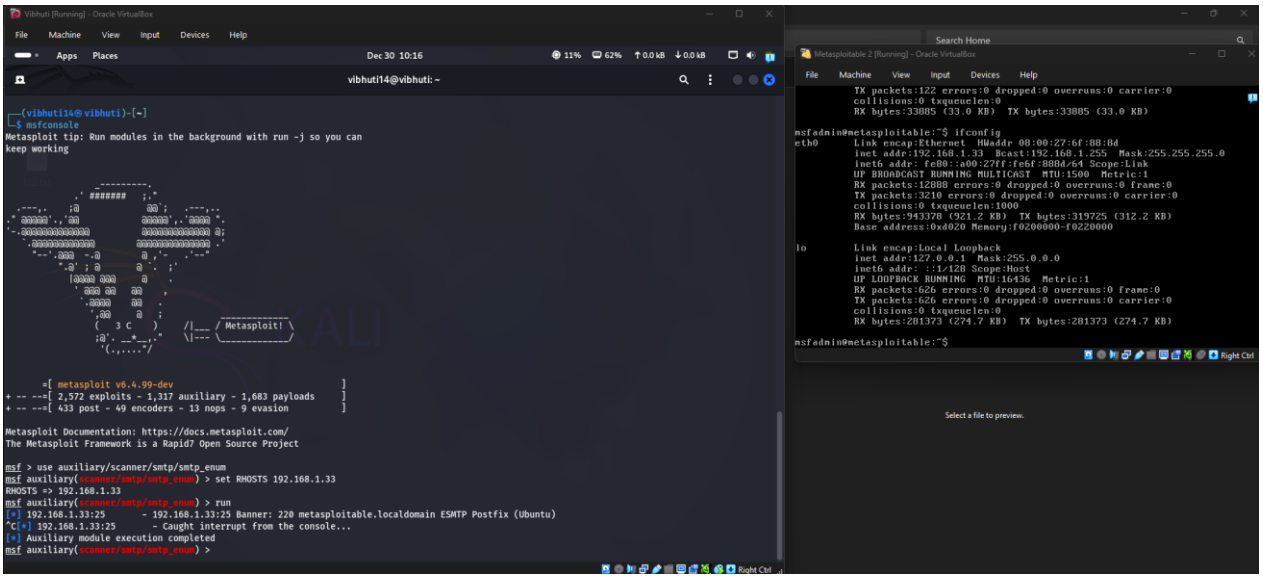
To secure Port 25, administrators should implement the following "defense-in-depth" measures:

- **Disable Open Relay:** Configure your MTA (Postfix, Exim, Sendmail, etc.) to only accept mail for your own domains or from authenticated/trusted IP addresses.
- **Enforce STARTTLS:** Use the STARTTLS command to upgrade unencrypted connections to secure SSL/TLS sessions, ensuring that server-to-server traffic is encrypted.
- **Use Alternative Ports for Clients:** Force end-users and applications to use **Port 587** (SMTP Submission) with mandatory authentication, reserving Port 25 strictly for incoming mail from other servers.
- **Implement SPF, DKIM, and DMARC:** Deploy these DNS-based authentication records to verify that emails coming from your server are legitimate and have not been tampered with.

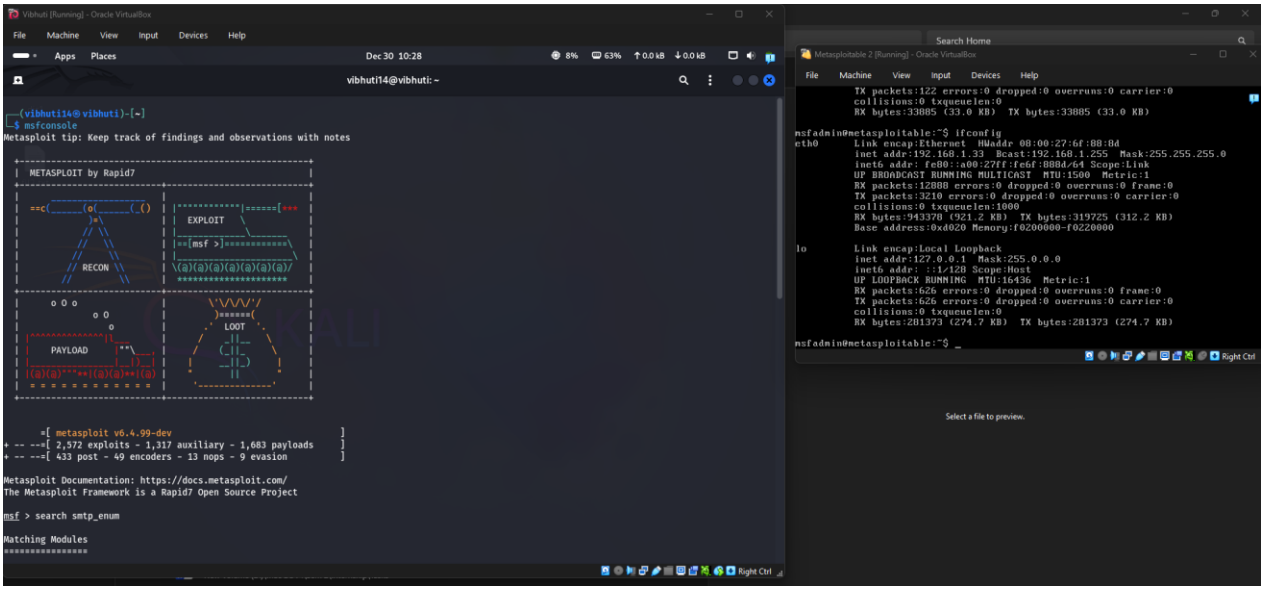
POC:

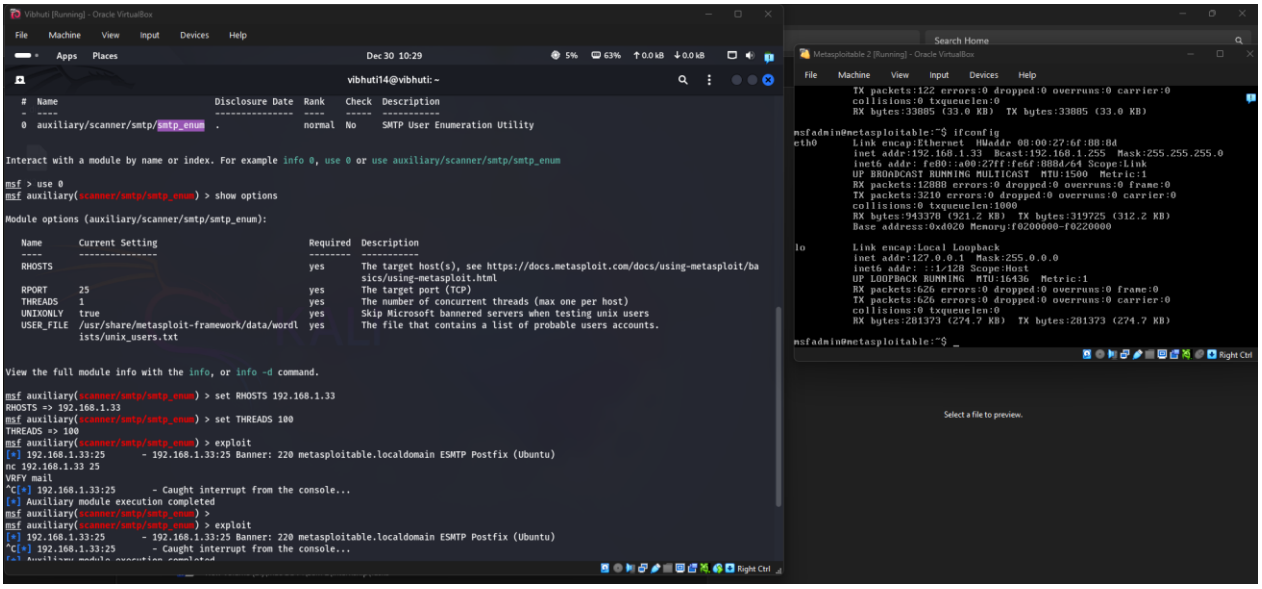
Method 1. User Enumeration (VRFY and EXPN)

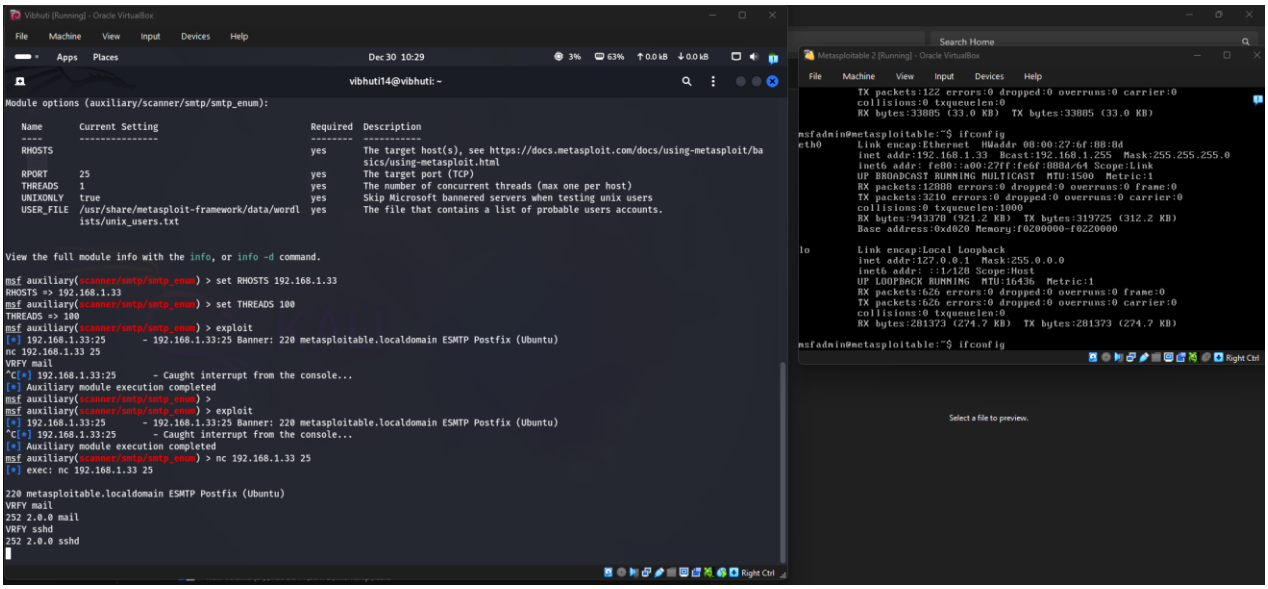




Method 2. SMTP Enumeration in Metasploit







HTTP Port 80

Description:

Hypertext Transfer Protocol (HTTP) is the foundational protocol of the World Wide Web, and it traditionally communicates over Port 80. It is a stateless, application-layer protocol used to request and transmit web pages, images, and other resources between a client (web browser) and a server. When you enter a URL starting with http://, your browser connects to the server's Port 80 to retrieve data. Unlike its secure successor, HTTPS, Port 80 does not use encryption. This means that all data—is sent in "plain text," making it visible to anyone positioned between the user and the server.

Impact:

The lack of encryption on Port 80 creates several critical vulnerabilities:

- **Data Eavesdropping:** Any sensitive information entered into a web form (passwords, credit card numbers, or personal details) can be captured by attackers using network sniffers.
- **Session Hijacking:** Attackers can "sniff" session cookies sent over Port 80, allowing them to impersonate a logged-in user and gain unauthorized access to accounts.
- **Content Injection:** Since the connection is unauthenticated, a Man-in-the-Middle (MitM) attacker can modify the web content in transit, injecting malicious scripts (XSS) or fraudulent advertisements into the user's browser.

Severity: High

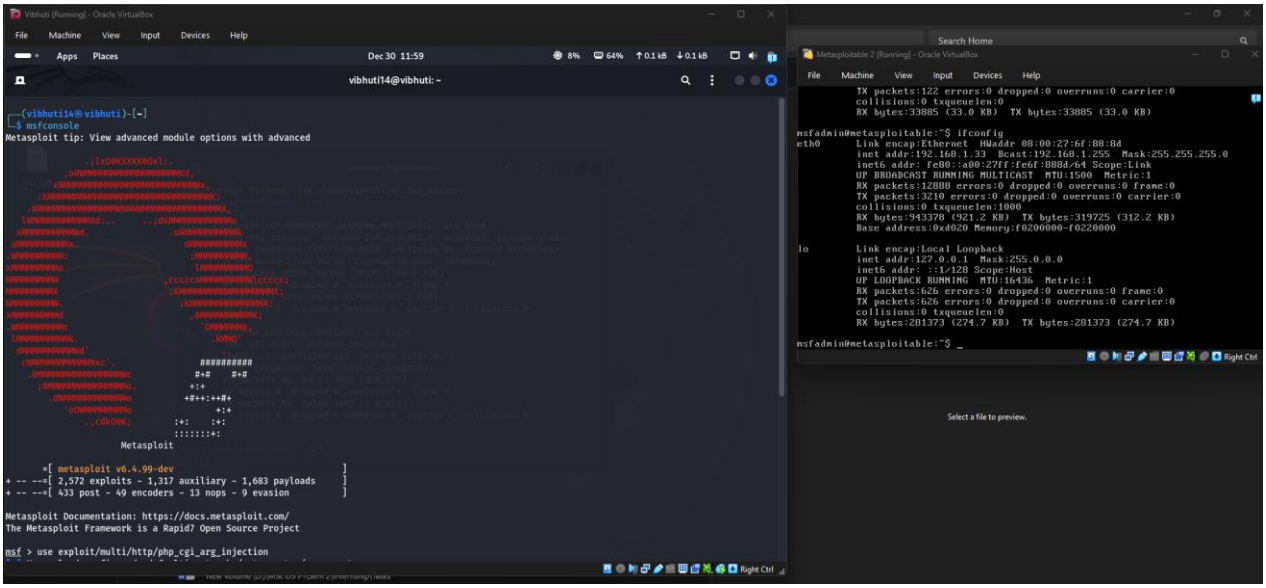
Remedial:

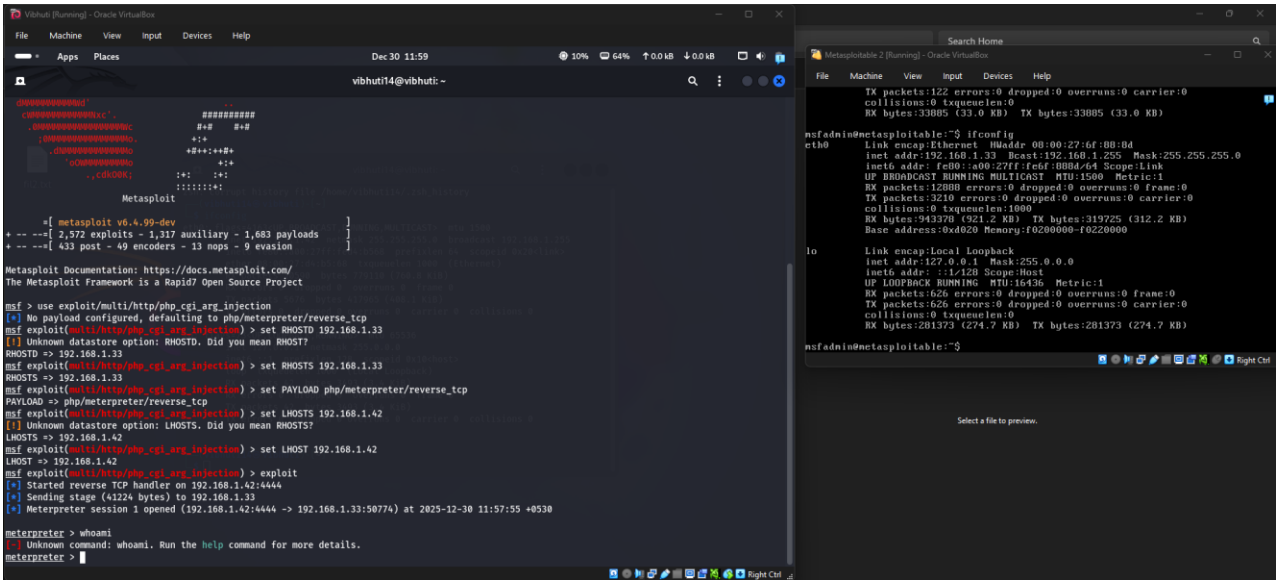
To secure web traffic and move away from unprotected Port 80 usage:

- **Implement HTTPS (Port 443):** Install an SSL/TLS certificate (e.g., from Let's Encrypt) to encrypt all traffic between the server and the client.
- **Enable HSTS (HTTP Strict Transport Security):** Use the HSTS header to instruct browsers to *only* communicate with your server over HTTPS, preventing "protocol downgrade" attacks.
- **Secure Cookies:** Set the Secure and HttpOnly flags on all session cookies to ensure they are never transmitted over an unencrypted Port 80 connection.
- **Use a Web Application Firewall (WAF):** Deploy a WAF to filter out malicious traffic and automated bot scans targeting Port 80.

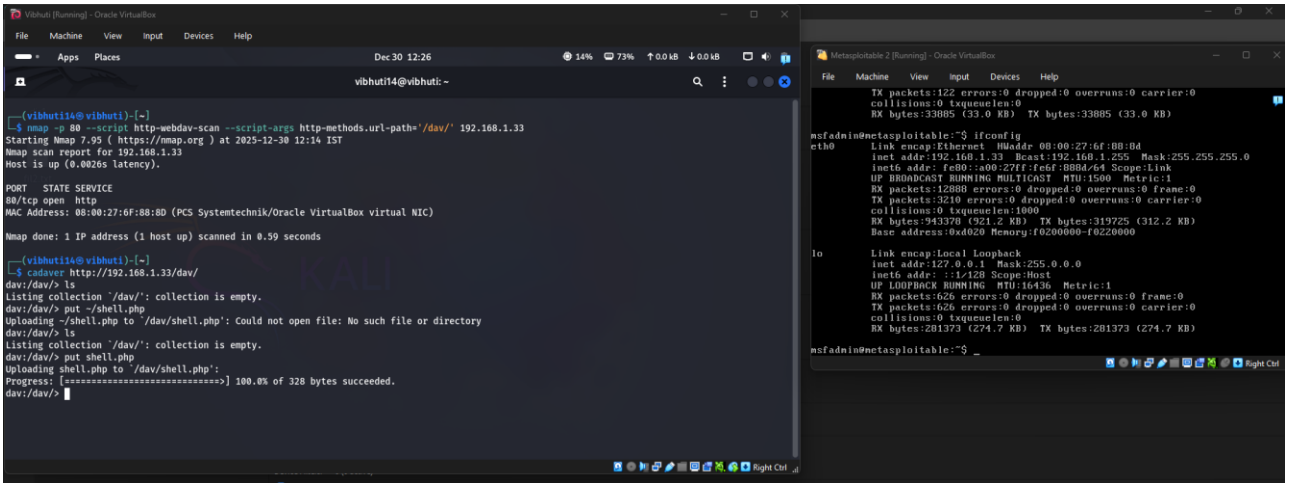
POC:

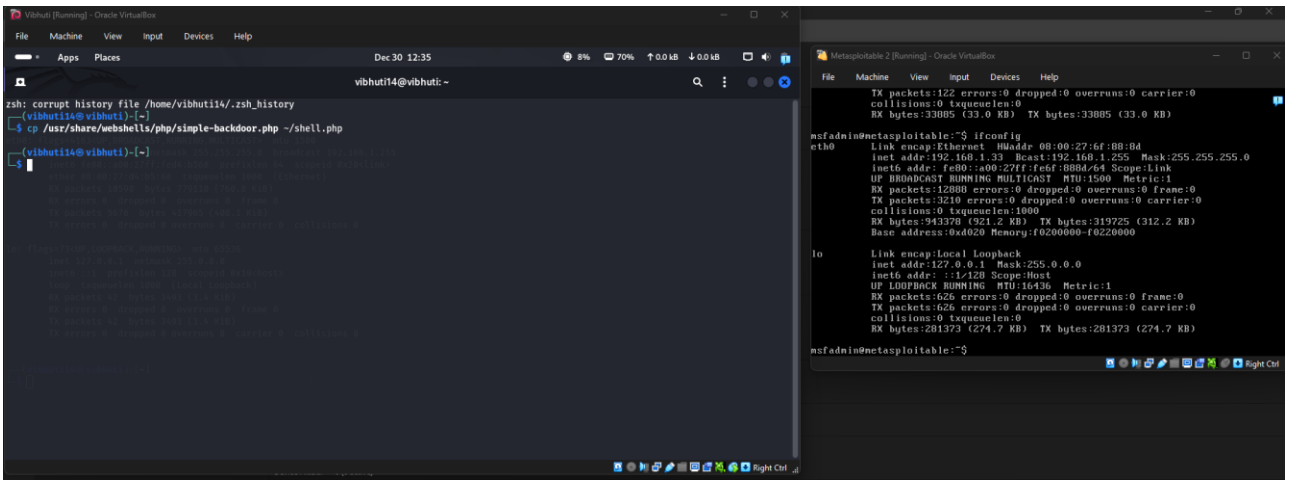
Method 1. PHP_CGI Remote Code Execution (CVE-2012-1823)

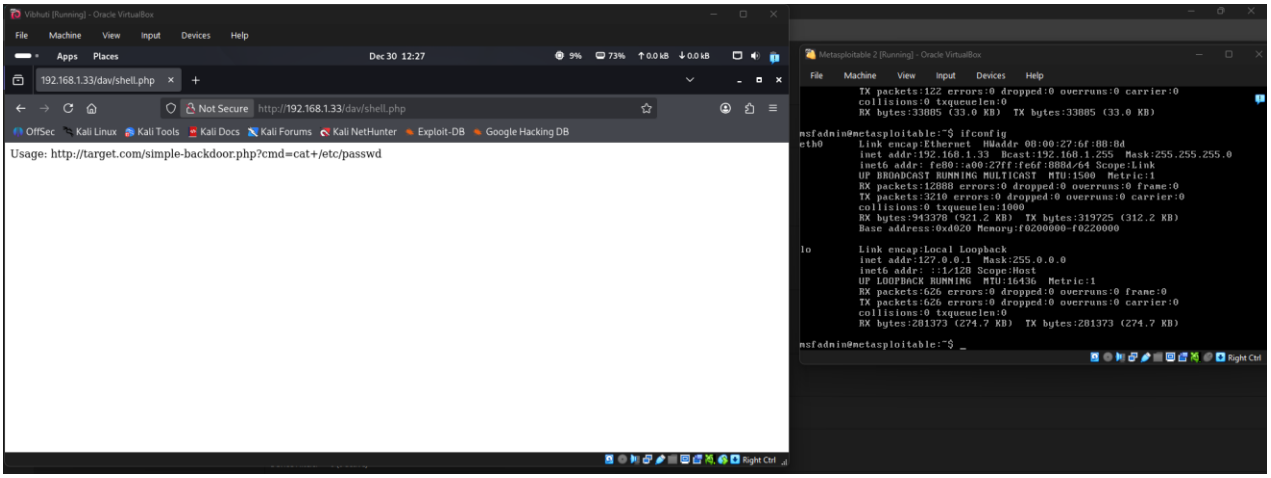




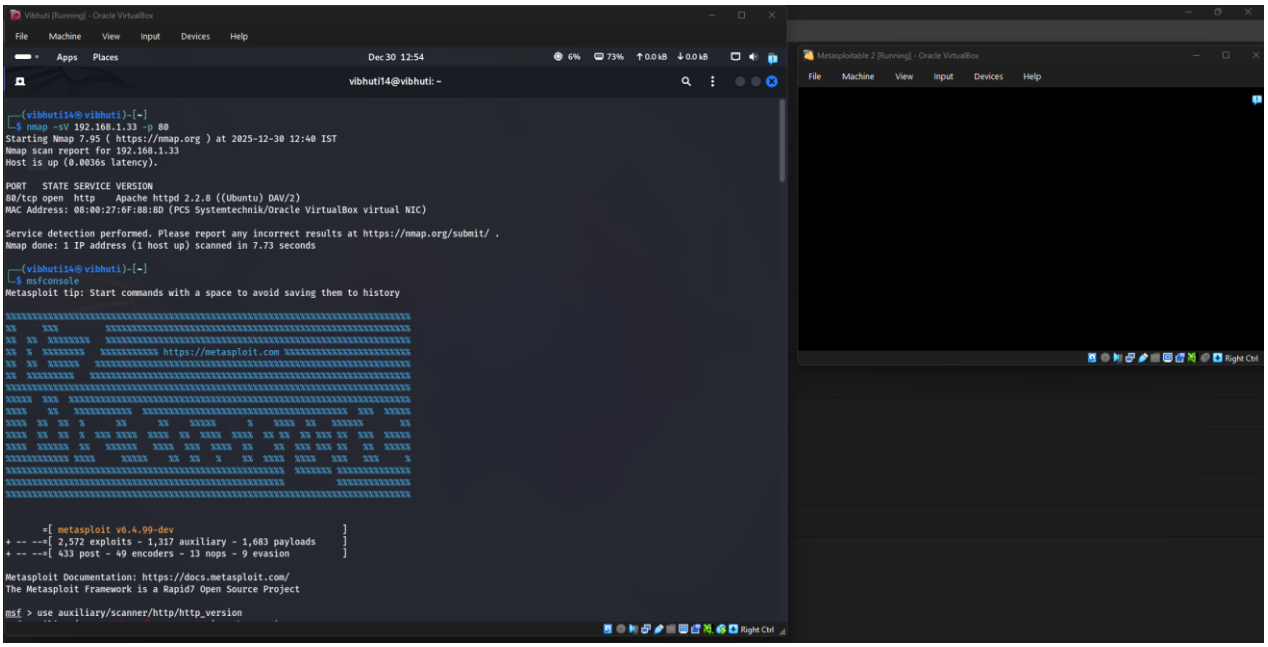
Method 2. WebDAV Exploitation (Cadaver)

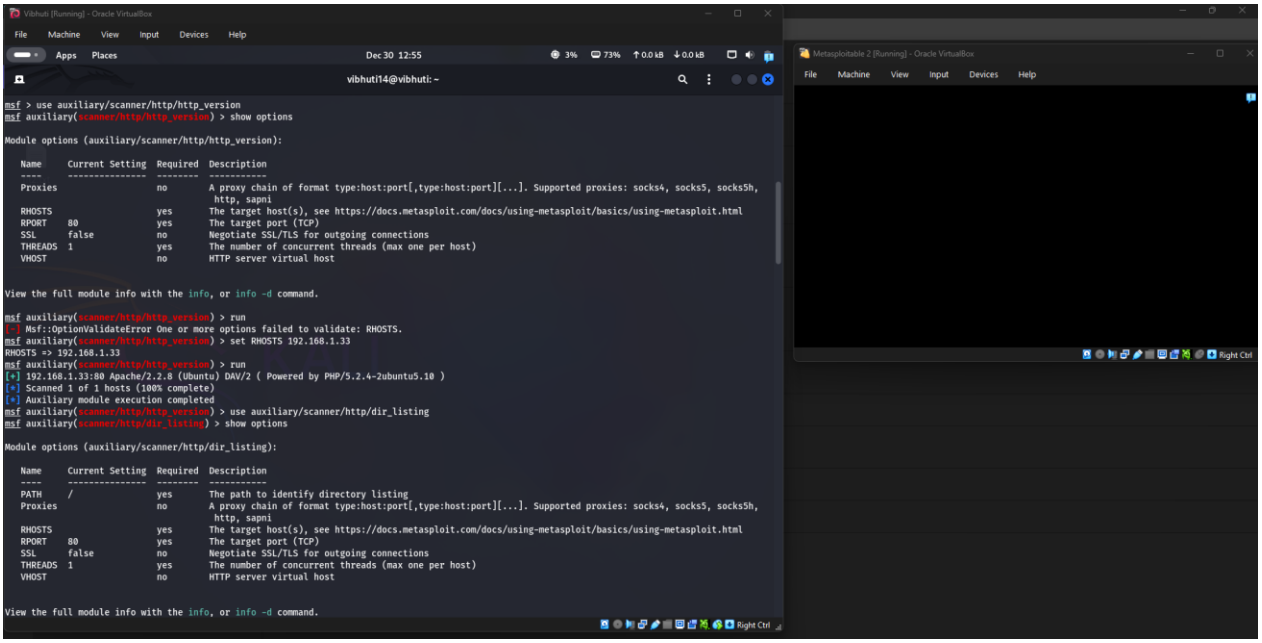


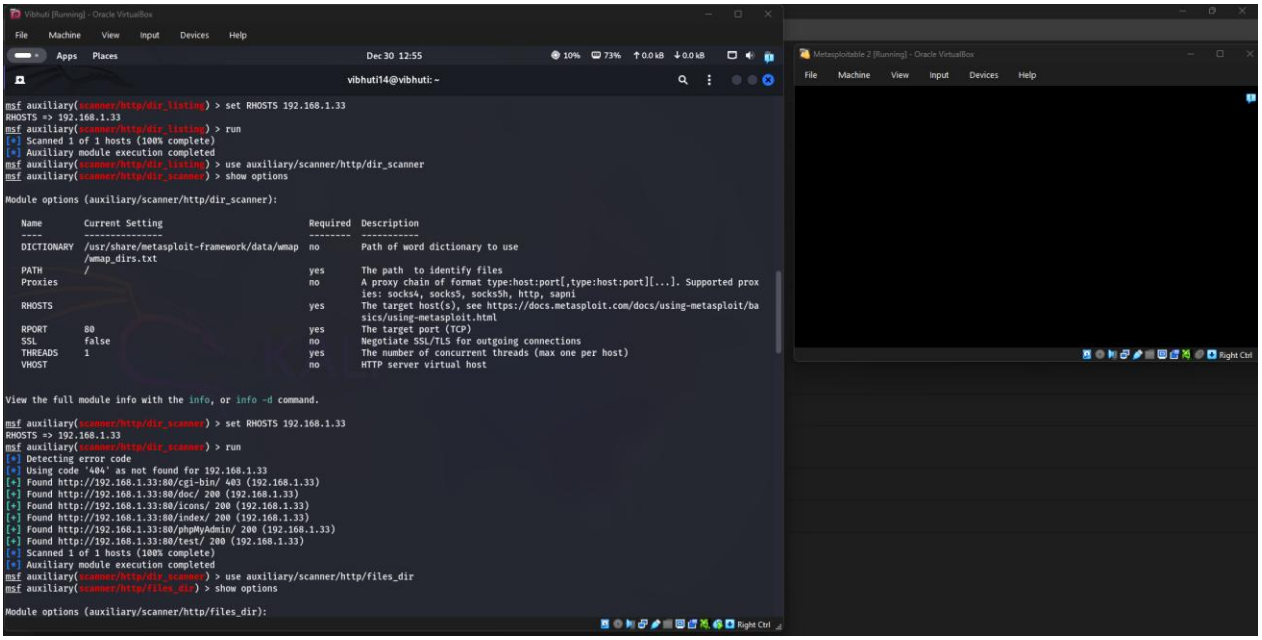


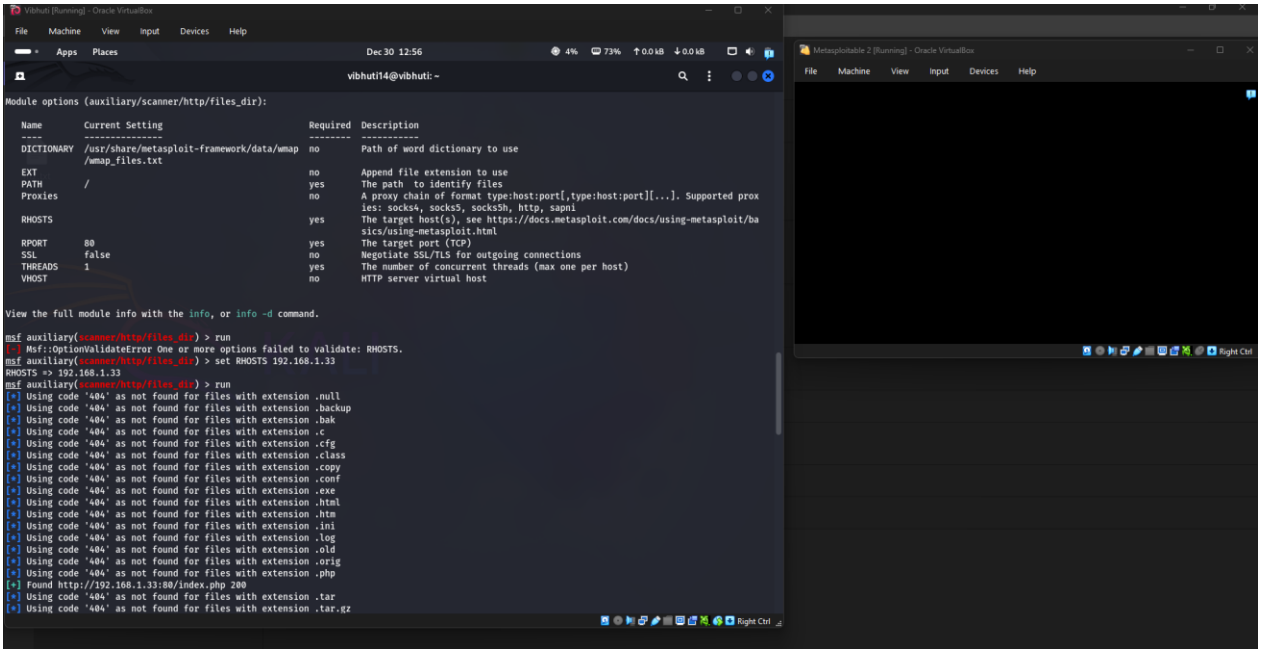


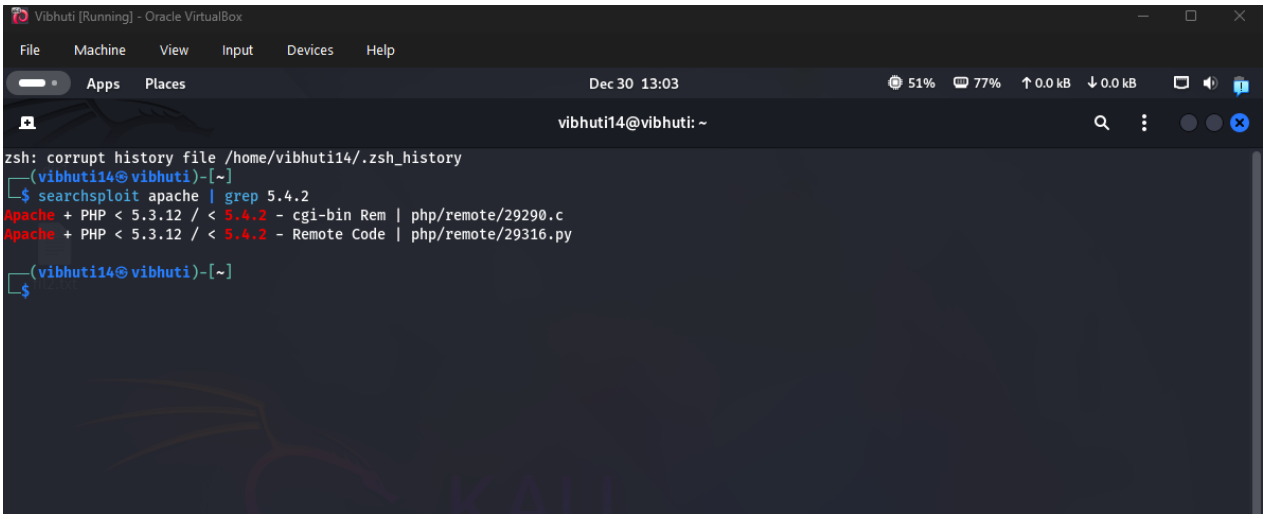
Method 3. Using Metasploit (Automated)

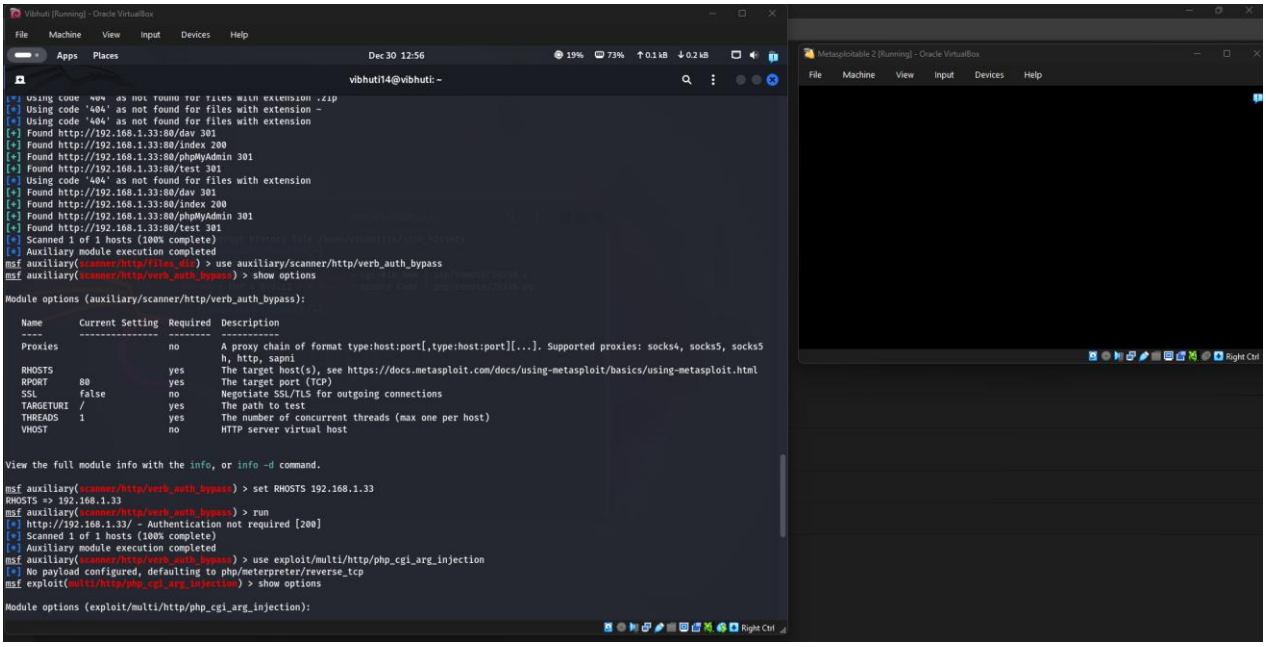


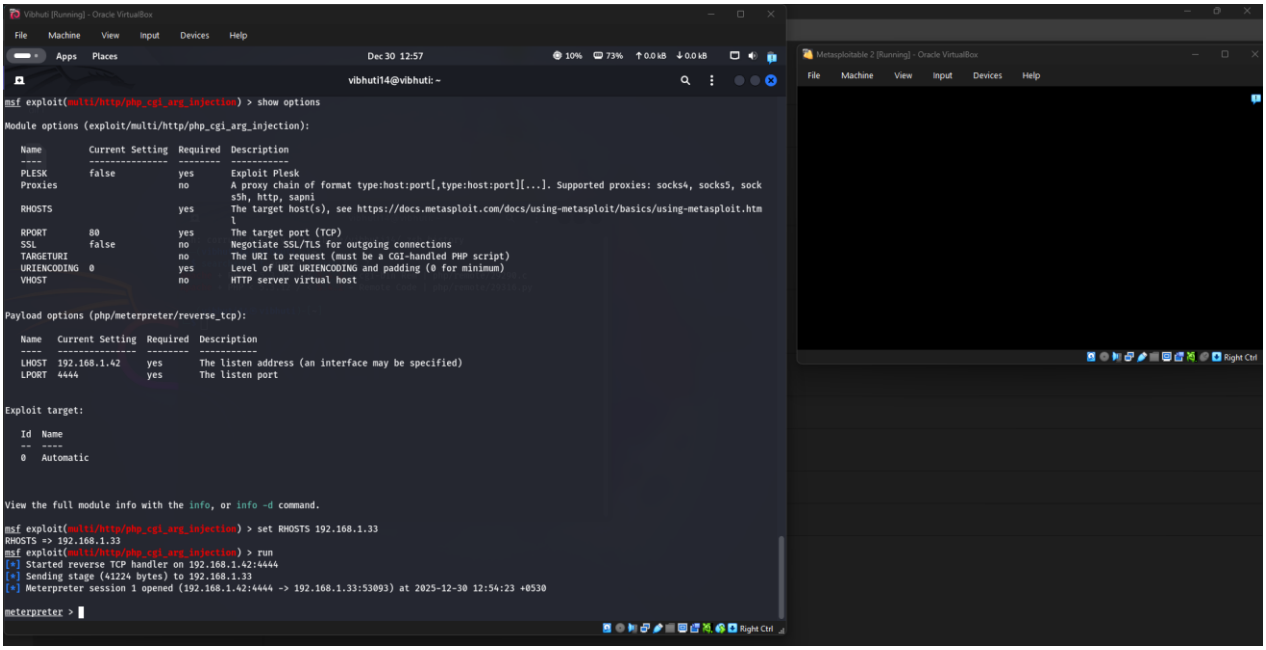



Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places Dec 30 12:55
vibhuti14@vibhuti: ~
msf auxiliary(scanner/http/dir_listing) > set RHOSTS 192.168.1.33
RHOSTS => 192.168.1.33
msf auxiliary(scanner/http/dir_listing) > run
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/dir_listing) > use auxiliary/scanner/http/dir_scanner
msf auxiliary(scanner/http/dir_scanner) > show options
Module options (auxiliary/scanner/http/dir_scanner):
Name Current Setting Required Description
DICTIONARY /usr/share/metasploit-framework/data/wmap /wmap_dirs.txt no Path of word dictionary to use
PATH / yes The path to identify files
Proxies no A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, socks5h, http, sapni
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 yes The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host
View the full module info with the info, or info -d command.
msf auxiliary(scanner/http/dir_scanner) > set RHOSTS 192.168.1.33
RHOSTS => 192.168.1.33
msf auxiliary(scanner/http/dir_scanner) > run
[*] Detecting error code
[*] Using code '404' as not found for 192.168.1.33
[+] Found http://192.168.1.33:80/cgi-bin/ 403 (192.168.1.33)
[+] Found http://192.168.1.33:80/doc/ 200 (192.168.1.33)
[+] Found http://192.168.1.33:80/icons/ 200 (192.168.1.33)
[+] Found http://192.168.1.33:80/index/ 200 (192.168.1.33)
[+] Found http://192.168.1.33:80/phpMyAdmin/ 200 (192.168.1.33)
[+] Found http://192.168.1.33:80/test/ 200 (192.168.1.33)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/dir_scanner) > use auxiliary/scanner/http/files_dir
msf auxiliary(scanner/http/files_dir) > show options
Module options (auxiliary/scanner/http/files_dir):
Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Right Ctrl


Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places Dec 30 12:56
vibhuti14@vibhuti: ~
Module options (auxiliary/scanner/http/files_dir):
Name Current Setting Required Description
DICTIONARY /usr/share/metasploit-framework/data/wmap /wmap_files.txt no Path of word dictionary to use
EXT no Append file extension to use
PATH / yes The path to identify files
Proxies no A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, socks5h, http, sapni
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 yes The number of concurrent threads (max one per host)
VHOST no HTTP server virtual host
View the full module info with the info, or info -d command.
msf auxiliary(scanner/http/files_dir) > run
[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf auxiliary(scanner/http/files_dir) > set RHOSTS 192.168.1.33
RHOSTS => 192.168.1.33
msf auxiliary(scanner/http/files_dir) > run
[*] Using code '404' as not found for files with extension .null
[*] Using code '404' as not found for files with extension .backup
[*] Using code '404' as not found for files with extension .bak
[*] Using code '404' as not found for files with extension .c
[*] Using code '404' as not found for files with extension .cfg
[*] Using code '404' as not found for files with extension .class
[*] Using code '404' as not found for files with extension .copy
[*] Using code '404' as not found for files with extension .conf
[*] Using code '404' as not found for files with extension .exe
[*] Using code '404' as not found for files with extension .html
[*] Using code '404' as not found for files with extension .htm
[*] Using code '404' as not found for files with extension .ini
[*] Using code '404' as not found for files with extension .log
[*] Using code '404' as not found for files with extension .old
[*] Using code '404' as not found for files with extension .orig
[*] Using code '404' as not found for files with extension .php
[+] Found http://192.168.1.33:80/index.php 200
[*] Using code '404' as not found for files with extension .tar
[*] Using code '404' as not found for files with extension .tar.gz
Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Right Ctrl


Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places Dec 30 13:03
51% 77% 0.0 kB 0.0 kB
vibhuti14@vibhuti: ~
zsh: corrupt history file /home/vibhuti14/.zsh_history
┌──(vibhuti14㉿vibhuti)-[~]
└─$ searchsploit apache | grep 5.4.2
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Rem | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code | php/remote/29316.py
┌──(vibhuti14㉿vibhuti)-[~]
└─$





RPCBIND Port 111

Description:

The rpcbind utility (formerly known as portmap) serves as a central directory for Remote Procedure Call (RPC) services, operating primarily on Port 111. In a distributed network environment, different RPC-based services (like NFS, NIS, or quota) run on various high-numbered, dynamic ports. When a client wants to access one of these services, it first contacts the rpcbind service on Port 111 to "look up" which port the specific service is currently using. Essentially, Port 111 acts as a switchboard or traffic controller, mapping RPC program numbers to the actual TCP/UDP ports listening on the machine.

Impact:

- **Information Disclosure**: Attackers can query the rpcbind service using tools like rpcinfo to list all registered RPC services, versions, and ports, revealing the server's internal architecture.
- **DDoS Amplification**: Port 111 is frequently abused in UDP Reflection/Amplification attacks. A small request to the rpcbind service can trigger a much larger response, allowing attackers to flood a third-party target with massive amounts of traffic.
- **Vulnerability Mapping**: By identifying specific RPC services (like an old version of NFS), an attacker can identify exactly which exploits to use for a deeper compromise.
- **Service Disruption**: If the rpcbind service is flooded or crashed, other critical dependent services (like Network File System) may become unreachable.

Severity: High

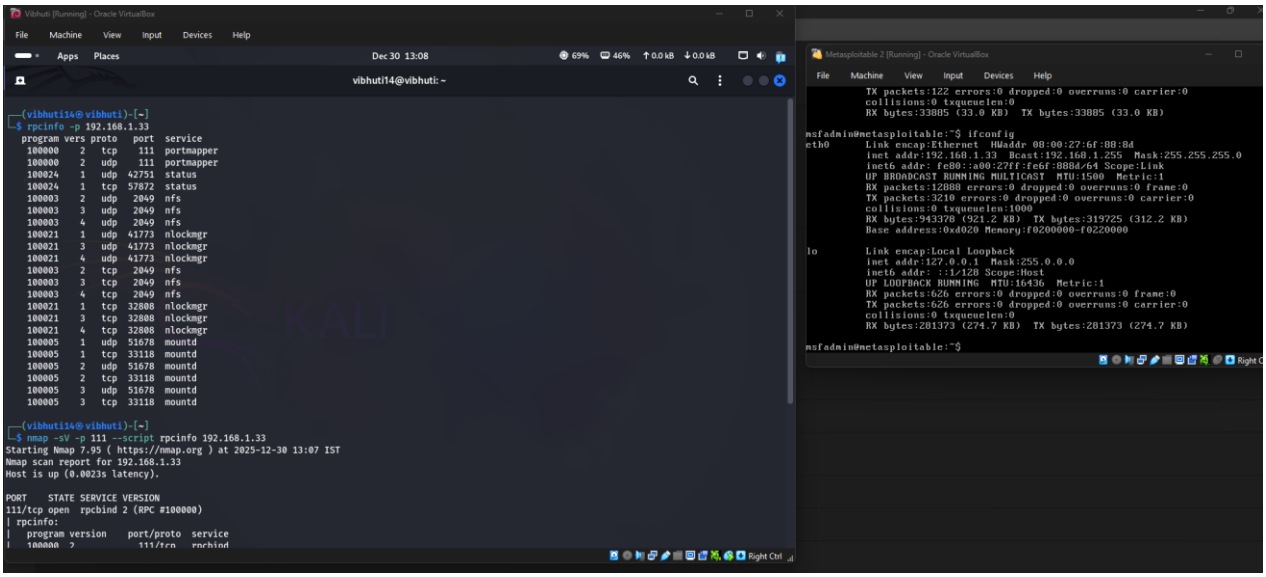
Remedial:

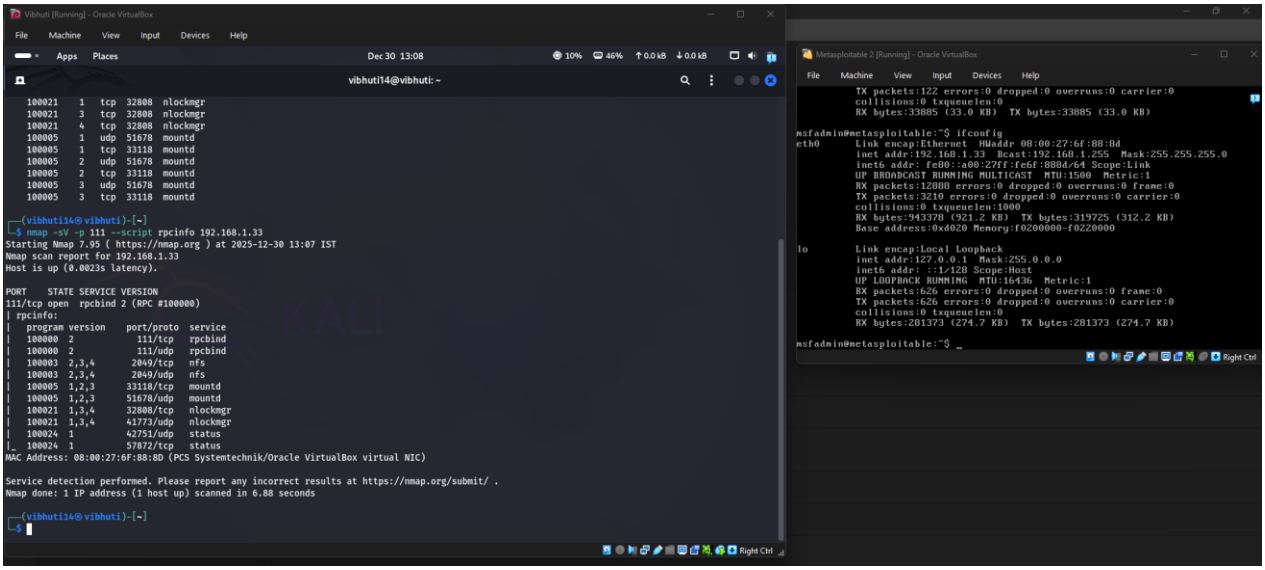
To secure rpcbind and Port 111, the following measures are recommended:

- **Restrict Access via Firewall:** Block Port 111 (both TCP and UDP) at the network perimeter. Access should only be allowed from trusted internal IP addresses that strictly require RPC services.
- **Use TCP Wrappers:** Configure /etc/hosts.allow and /etc/hosts.deny to limit which specific hosts are permitted to query the rpcbind service.
- **Disable Unnecessary RPC Services:** If the server does not need to act as an NFS server or use other RPC-based protocols, disable the rpcbind service entirely using systemctl stop rpcbind.
- **Implement Network Segmentation:** Keep RPC-dependent servers in a dedicated, isolated VLAN that is not directly reachable from the general user network or the internet.

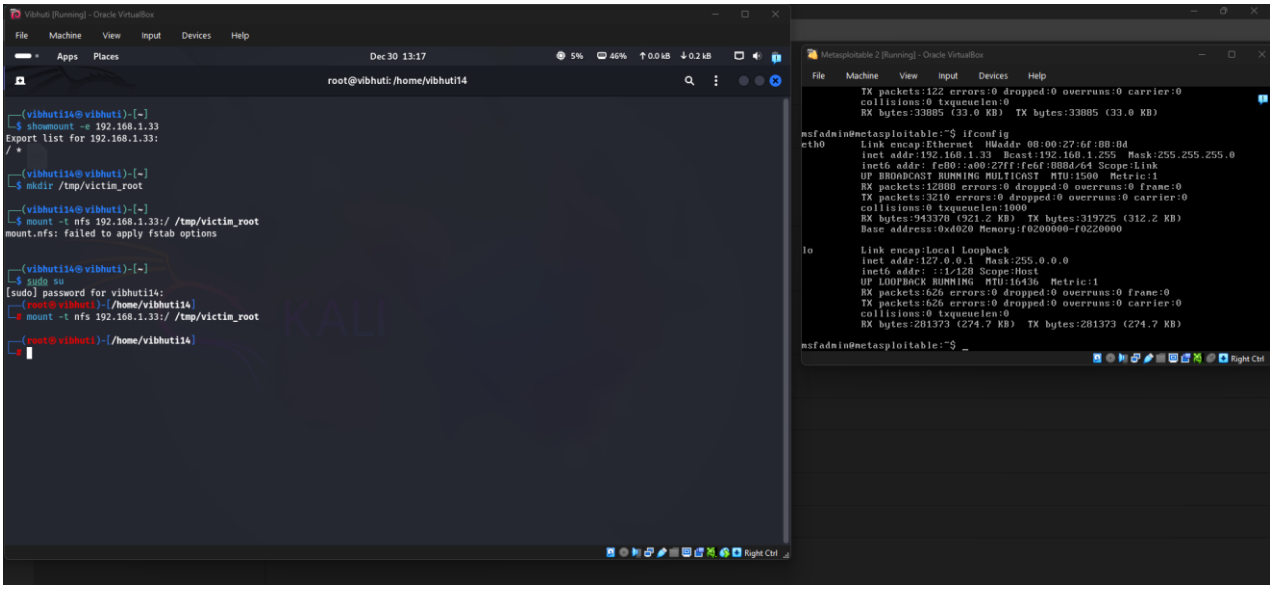
POC:

Method 1. RPC Service Enumeration (Fingerprinting)

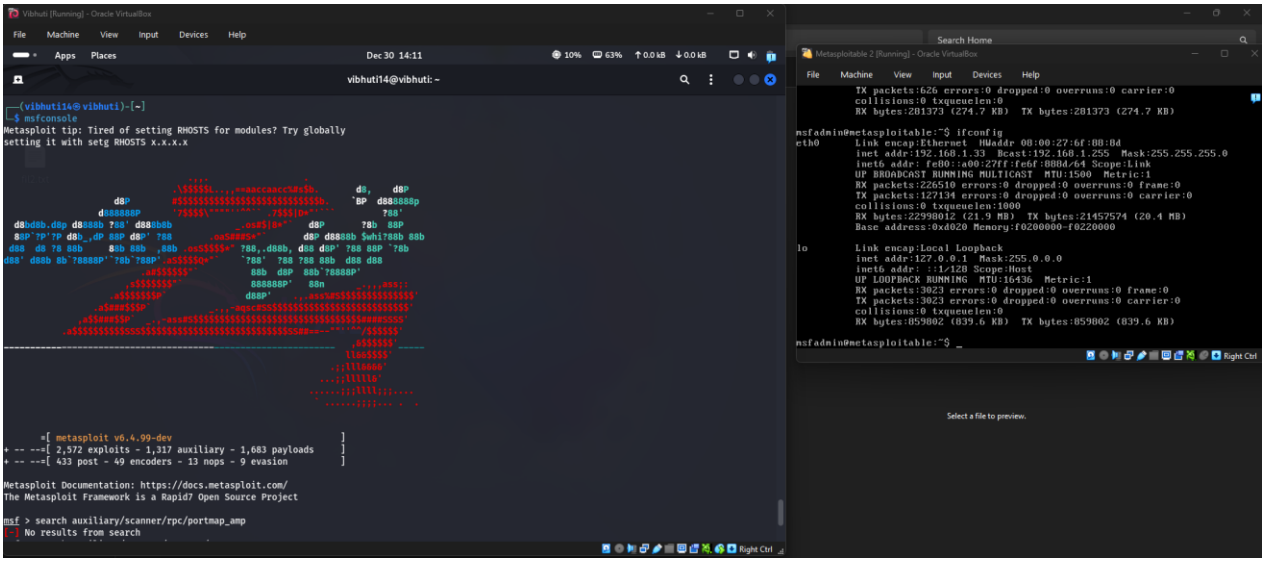


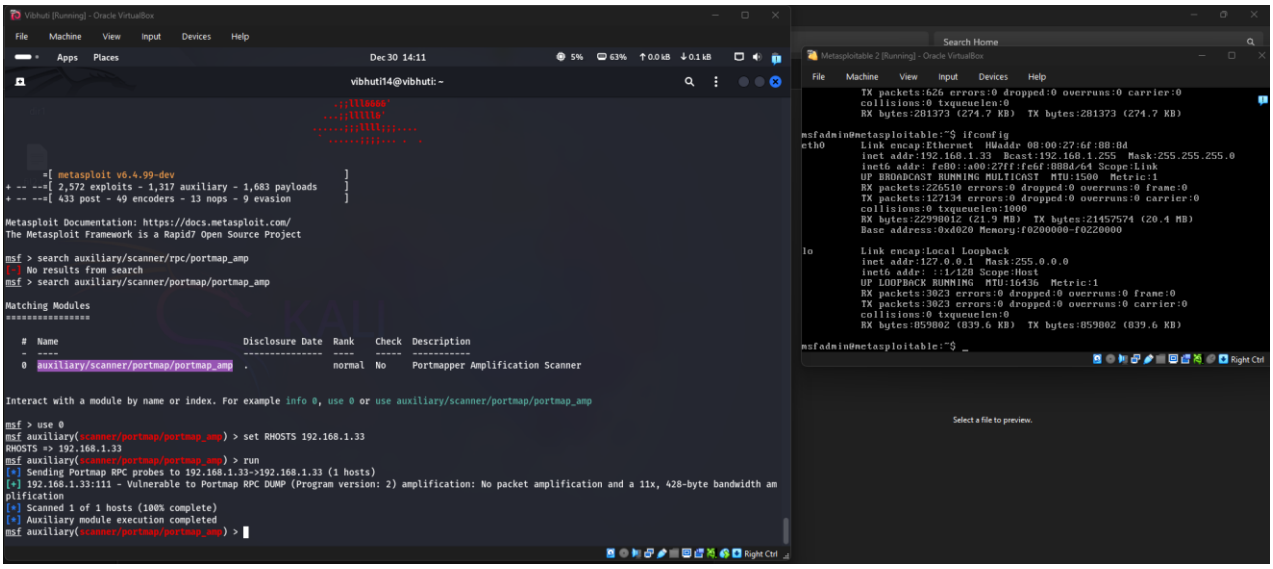


Method 2. Information Disclosure via NFS Mounts



Method 3. RPC DUMP Analysis (Metasploit)





NetBIOS-SSN Port 139 & 445

Description:

NetBIOS Session Service (Port 139) and Direct-Host SMB (Port 445) are the primary ports used by Windows for file and printer sharing. Historically, the Server Message Block (SMB) protocol relied on NetBIOS over TCP/IP (NBT) to function, using Port 139 to establish a session between two computers on a local network. With the release of Windows 2000, Microsoft introduced the ability to run SMB directly over TCP/IP without the legacy NetBIOS layer, moving this traffic to Port 445. While Port 139 is now considered a legacy port kept for backward compatibility with older devices, Port 445 is the modern standard for network resource access.

Impact:

- **Remote Code Execution (RCE)**: Vulnerabilities in the SMB service (most notably EternalBlue) allow attackers to execute arbitrary code with system-level privileges without any user interaction.
- **Ransomware Propagation**: Because SMB is "wormable," malware like WannaCry and NotPetya uses Port 445 to spread automatically from one computer to another across an entire network in minutes.
- **Data Exfiltration**: An attacker who gains access to an open SMB share can read, modify, or delete sensitive company files, databases, and backups.
- **Credential Harvesting**: Attackers can perform "SMB Relay" attacks, where they intercept NTLM authentication hashes and reuse them to log into other systems on the network.

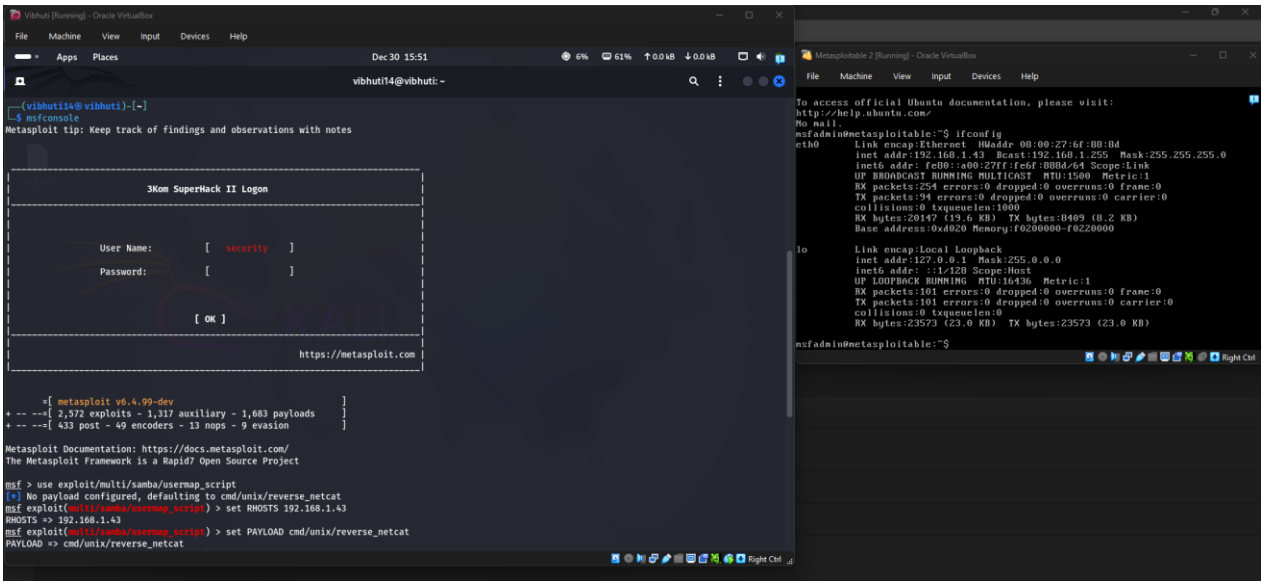
Severity: Critical

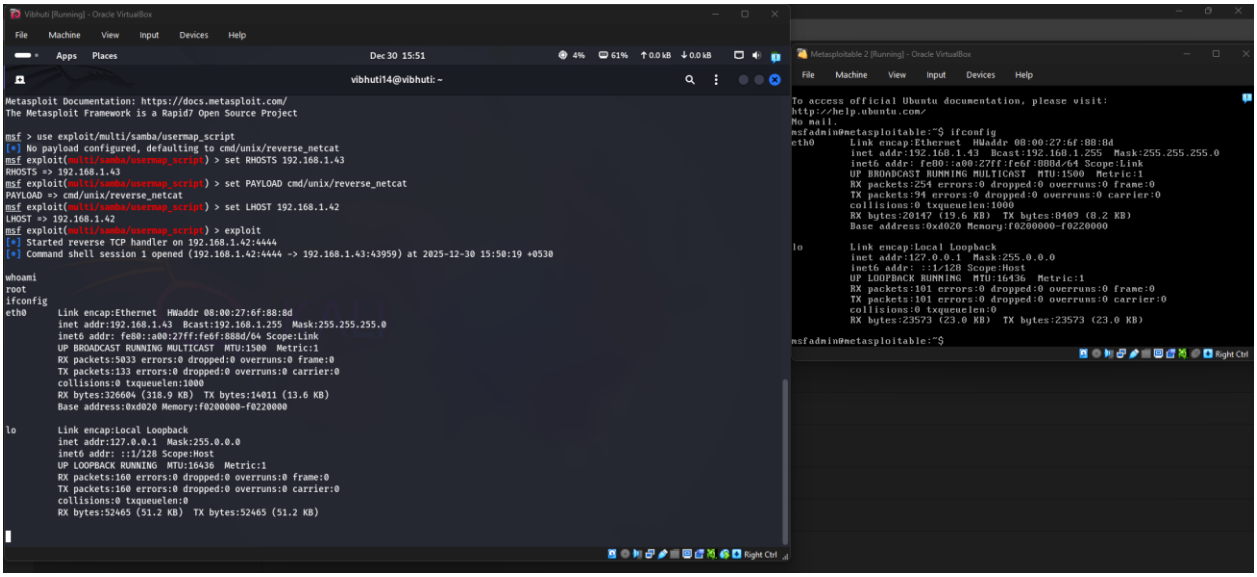
Remedial:

- **Block at the Perimeter:** Configure your firewall to drop all incoming and outgoing traffic on Ports 139 and 445 from the internet. These should only ever be accessible via a secure VPN.
- **Disable SMBv1:** Legacy SMBv1 is highly insecure and was the primary vector for EternalBlue. Ensure it is disabled on all systems via Windows Features or PowerShell: Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
- **Enforce SMB Signing:** Require digital signatures for all SMB traffic to prevent "Man-in-the-Middle" and relay attacks.
- **Restrict Share Permissions:** Follow the "Principle of Least Privilege." Audit all network shares and remove "Everyone" or "Guest" access, replacing them with specific user groups.

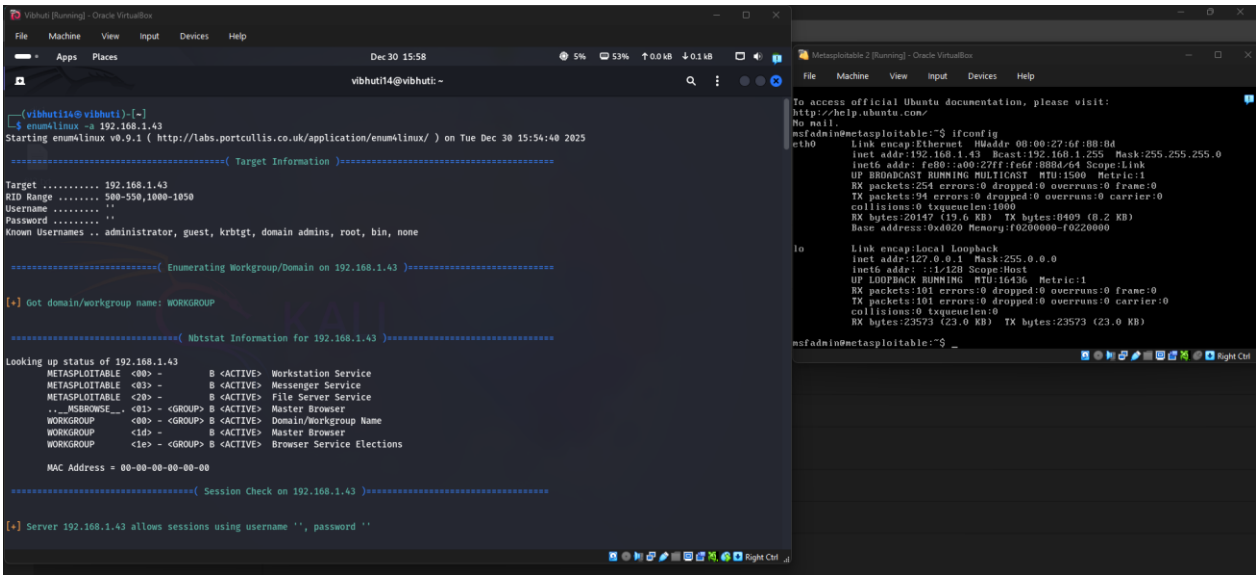
POC:

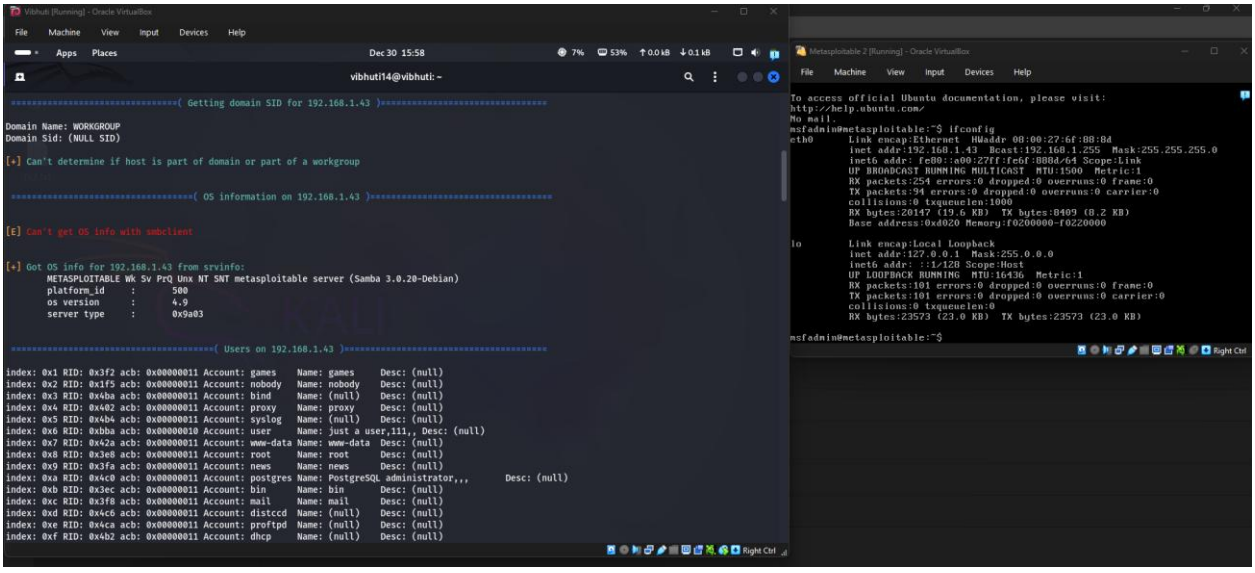
Method 1. Username Map Script (CVE-2007-2447)

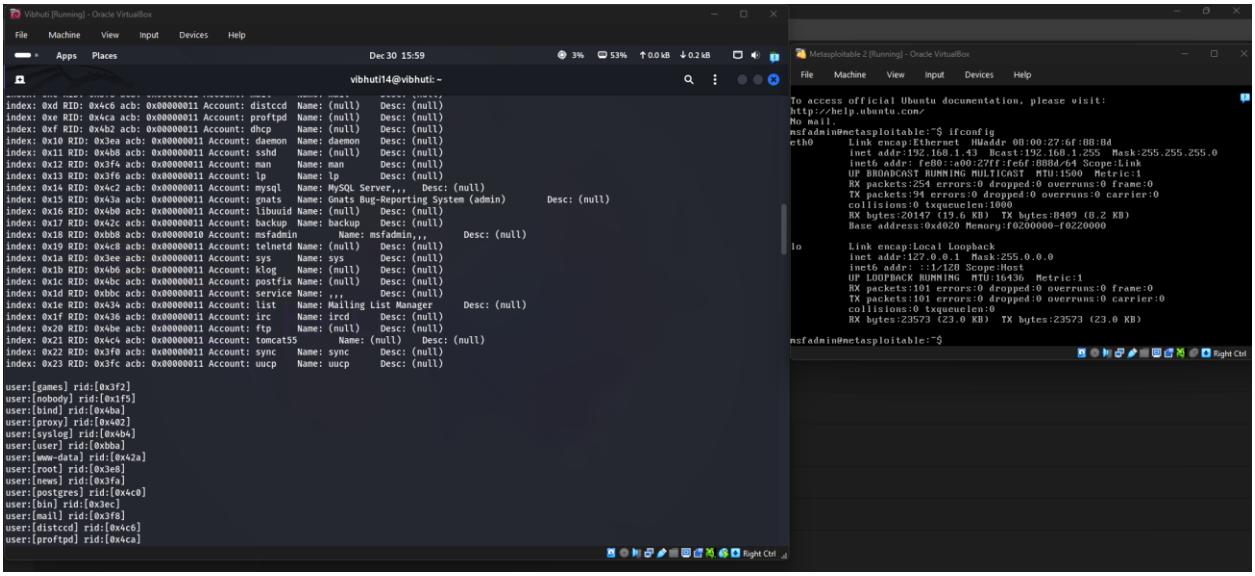


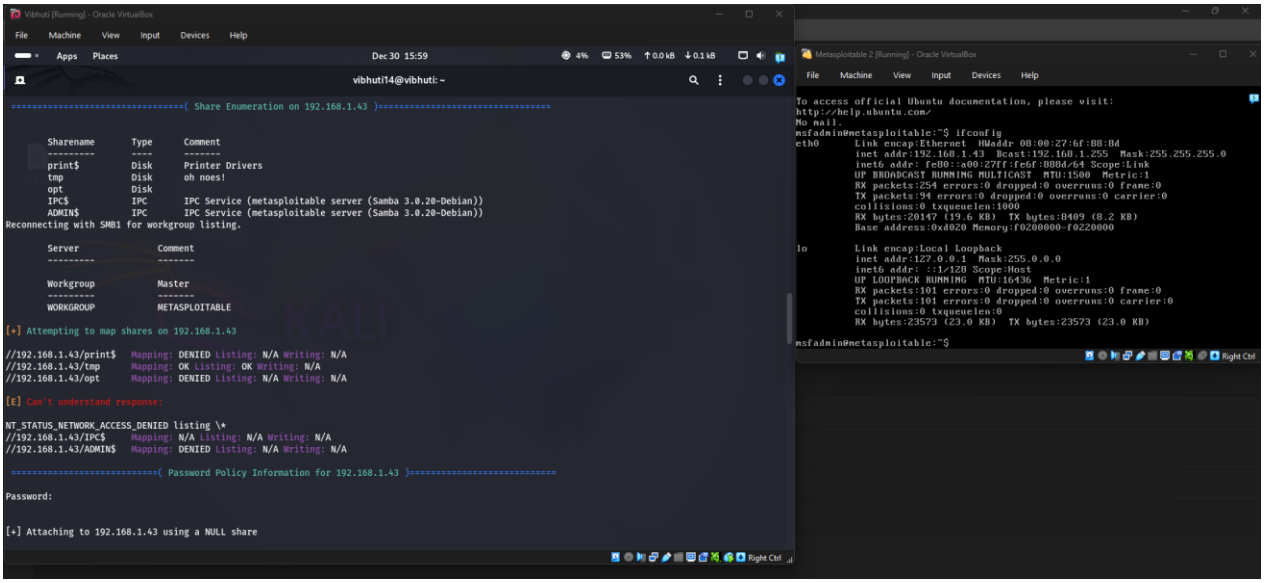


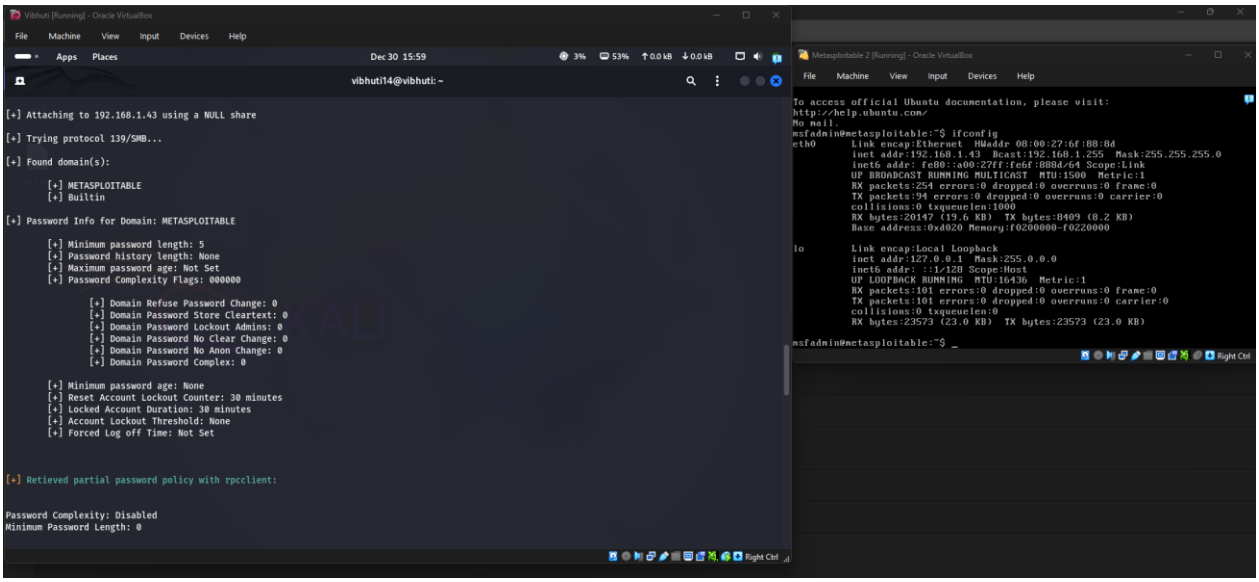
Method 2. Manual SMB Enumeration and Null Session

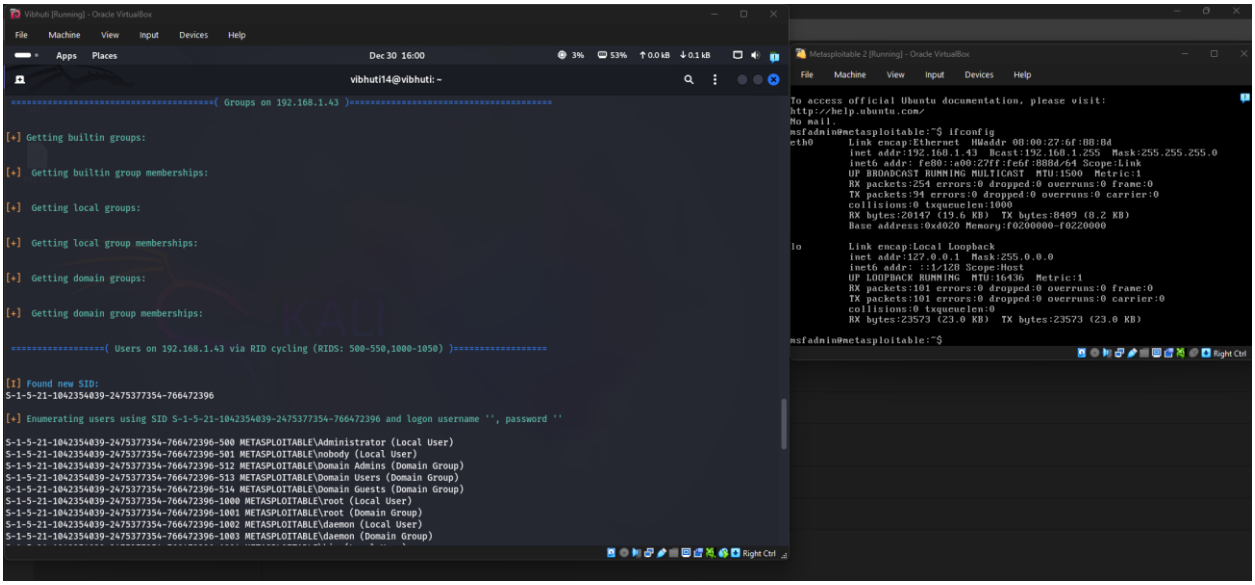


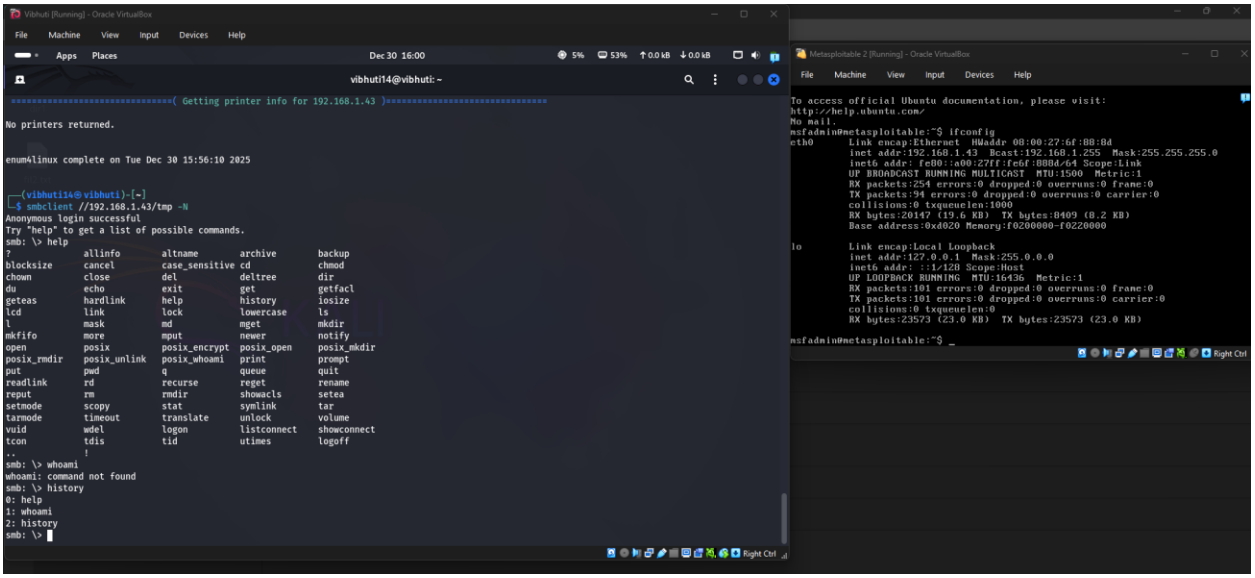



Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places Dec 30 15:59
vibhuti14@vibhuti: ~
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon Name: daemon Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man Name: man Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp Name: lp Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql Name: MySQL Server,,, Desc: (null)
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid Name: (null) Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)
index: 0x18 RID: 0xbb8 acb: 0x00000010 Account: msfadmin Name: msfadmin,,, Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null) Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog Name: (null) Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null) Desc: (null)
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service Name: ,,, Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc Name: ircd Desc: (null)
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp Name: (null) Desc: (null)
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55 Name: (null) Desc: (null)
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync Name: sync Desc: (null)
index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp Name: uucp Desc: (null)
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
Right Ctrl
Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:6f:88:8d
inet addr:192.168.1.43 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:254 errors:0 dropped:0 overruns:0 frame:0
TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:20147 (19.6 KB) TX bytes:8409 (8.2 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:101 errors:0 dropped:0 overruns:0 frame:0
TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23573 (23.0 KB) TX bytes:23573 (23.0 KB)
msfadmin@metasploitable:~$
Right Ctrl

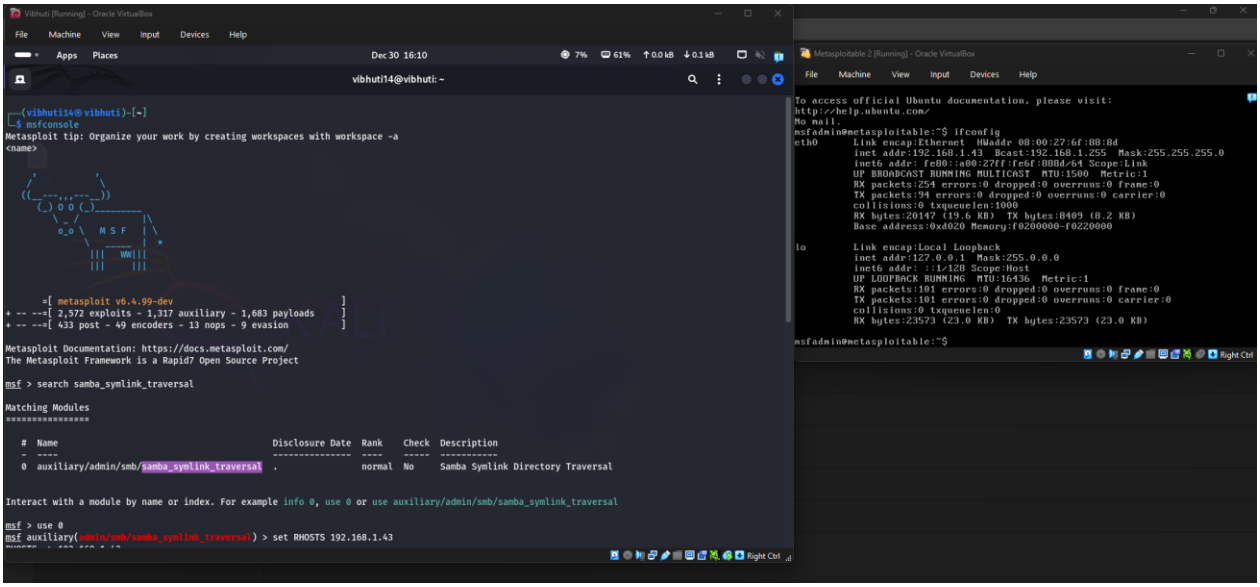

Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places Dec 30 15:59
vibhuti14@vibhuti: ~
========== Share Enumeration on 192.168.1.43 ==========
Sharename Type Comment
print$ Disk Printer Drivers
tmp Disk oh noes!
opt Disk
IPC$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Server Comment
Workgroup Master
WORKGROUP METASPLOITABLE
[+] Attempting to map shares on 192.168.1.43
//192.168.1.43/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.1.43/tmp Mapping: OK Listing: OK Writing: N/A
//192.168.1.43/opt Mapping: DENIED Listing: N/A Writing: N/A
[E] Can't understand response:
NT_STATUS_NETWORK_ACCESS_DENIED listing *
//192.168.1.43/IPC$ Mapping: N/A Listing: N/A Writing: N/A
//192.168.1.43/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A
========== Password Policy Information for 192.168.1.43 ==========
Password:
[+] Attaching to 192.168.1.43 using a NULL share
Right Ctrl
Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:6f:88:8d
inet addr:192.168.1.43 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:254 errors:0 dropped:0 overruns:0 frame:0
TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:20147 (19.6 KB) TX bytes:8409 (8.2 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:101 errors:0 dropped:0 overruns:0 frame:0
TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23573 (23.0 KB) TX bytes:23573 (23.0 KB)
msfadmin@metasploitable:~$
Right Ctrl

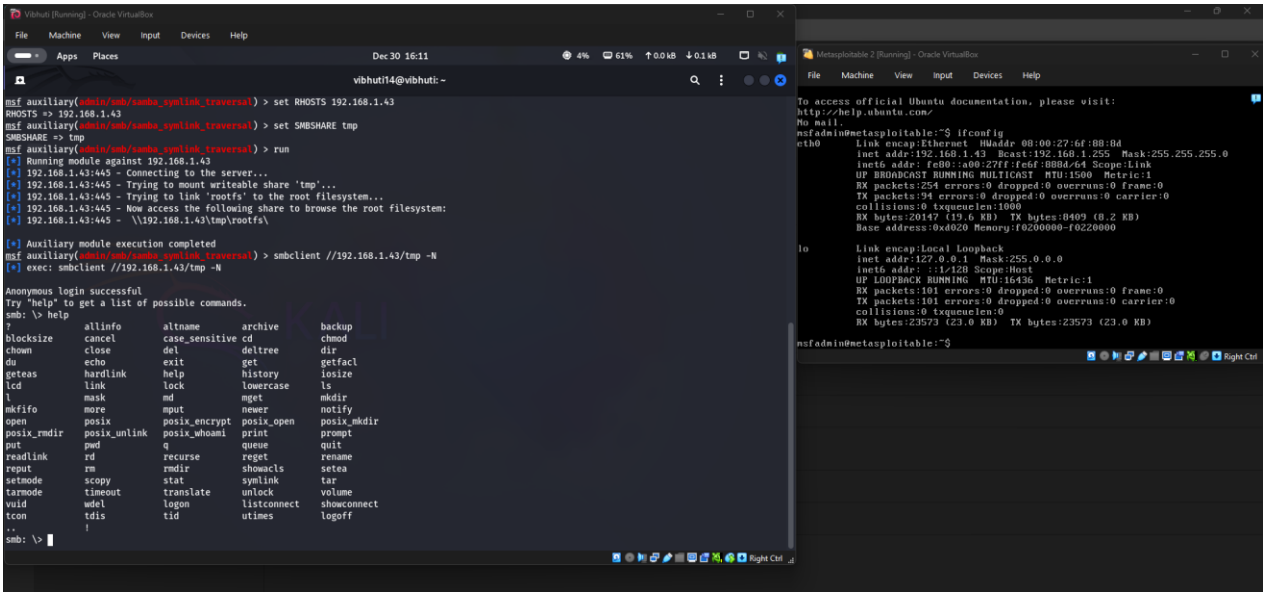

Vibhuti [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places Dec 30 15:59
vibhuti14@vibhuti: ~
[+] Attaching to 192.168.1.43 using a NULL share
[+] Trying protocol 139/SMB...
[+] Found domain(s):
[+] METASPLOITABLE
[+] Builtin
[+] Password Info for Domain: METASPLOITABLE
[+] Minimum password length: 5
[+] Password history length: None
[+] Maximum password age: Not Set
[+] Password Complexity Flags: 000000
[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 0
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 0
[+] Minimum password age: None
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set
[+] Retieved partial password policy with rpcclient:
Password Complexity: Disabled
Minimum Password Length: 0
Right Ctrl
Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:6f:88:8d
inet addr:192.168.1.43 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe6f:888d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:254 errors:0 dropped:0 overruns:0 frame:0
TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:20147 (19.6 KB) TX bytes:8409 (8.2 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:101 errors:0 dropped:0 overruns:0 frame:0
TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:23573 (23.0 KB) TX bytes:23573 (23.0 KB)
msfadmin@metasploitable:~$
Right Ctrl





Method 3. SMB Symlink Directory Traversal





Exec Port 512

Description:

The exec service, which operates on Port 512 (TCP), is a legacy "r-command" utility (Remote Execution) primarily found on Unix-like systems. It is designed to allow a user on one computer to execute commands on a remote host without needing to provide a password every time, provided the host is "trusted." When a request is sent to Port 512, the rexecd daemon handles the authentication, which is typically based on the source IP address and entries in files like .rhosts or /etc/hosts.equiv.

Impact:

- **Cleartext Credential Theft:** Similar to Telnet, the rexec protocol transmits usernames and passwords in plain text. Anyone monitoring the network can capture these credentials with ease.
- **IP Spoofing Attacks:** Since the service often trusts specific IP addresses, an attacker can "spoof" their source IP to trick the server into executing commands without any password at all.
- **Full Remote Command Execution:** A successful connection gives the attacker a shell on the target system. From here, they can install malware, delete data, or pivot to other systems on the network.

Severity: Critical

Remedial:

- **Disable the Service Immediately:** The primary remedy is to shut down the rexecd daemon. On most systems, this involves disabling it in inetd or xinetd configurations, or stopping the systemd service:

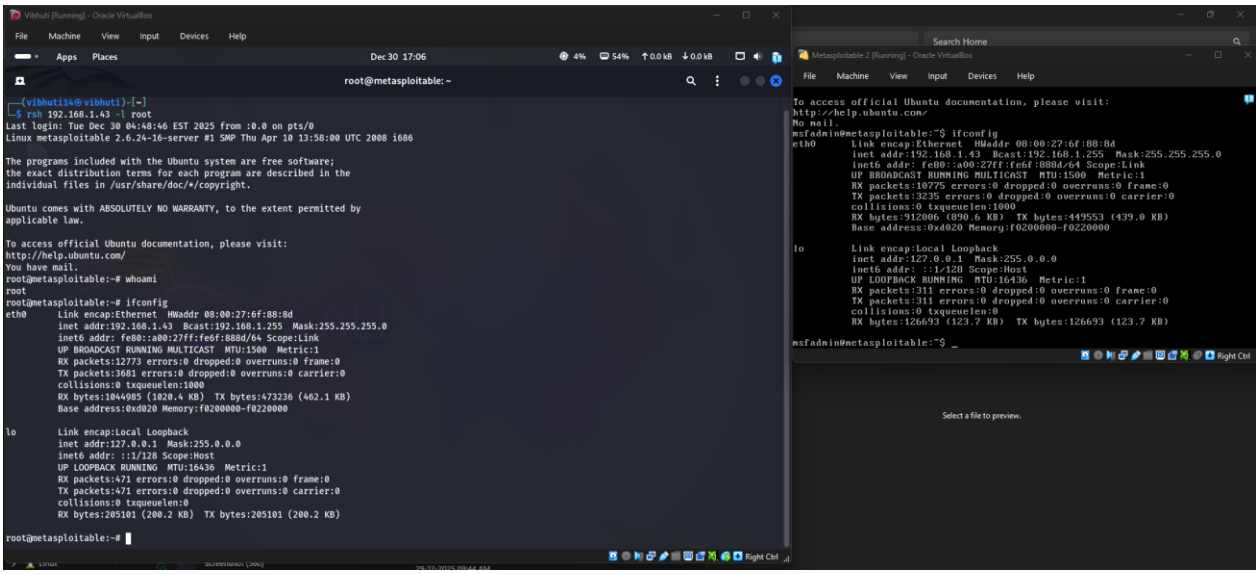
systemctl stop rexec

systemctl disable rexec

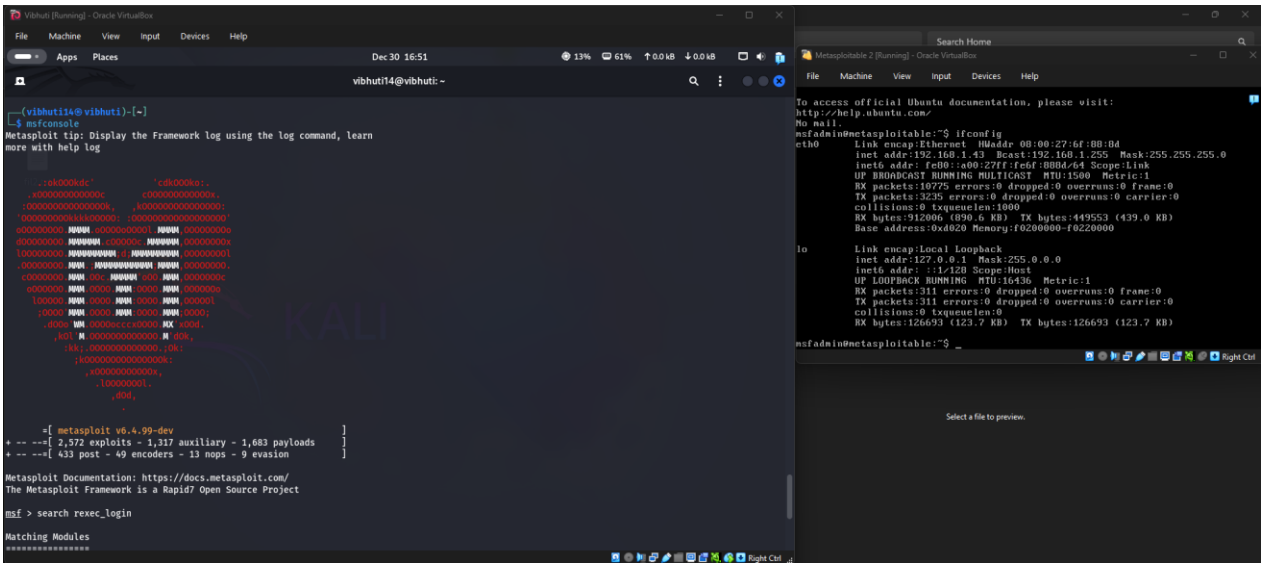
- **Migrate to SSH (Port 22):** SSH was specifically designed to replace the insecure "r-commands" (rexec, rsh, rlogin). It provides the same remote execution capability but with strong encryption and secure key-based authentication.
- **Block Port 512 at the Firewall:** Ensure your network firewall and host-based firewalls (like iptables or ufw) are configured to drop all traffic on Port 512.
- **Remove Trust Files:** Delete any .rhosts or /etc/hosts.equiv files found on the system, as these are used to bypass password prompts in the legacy r-command suite.

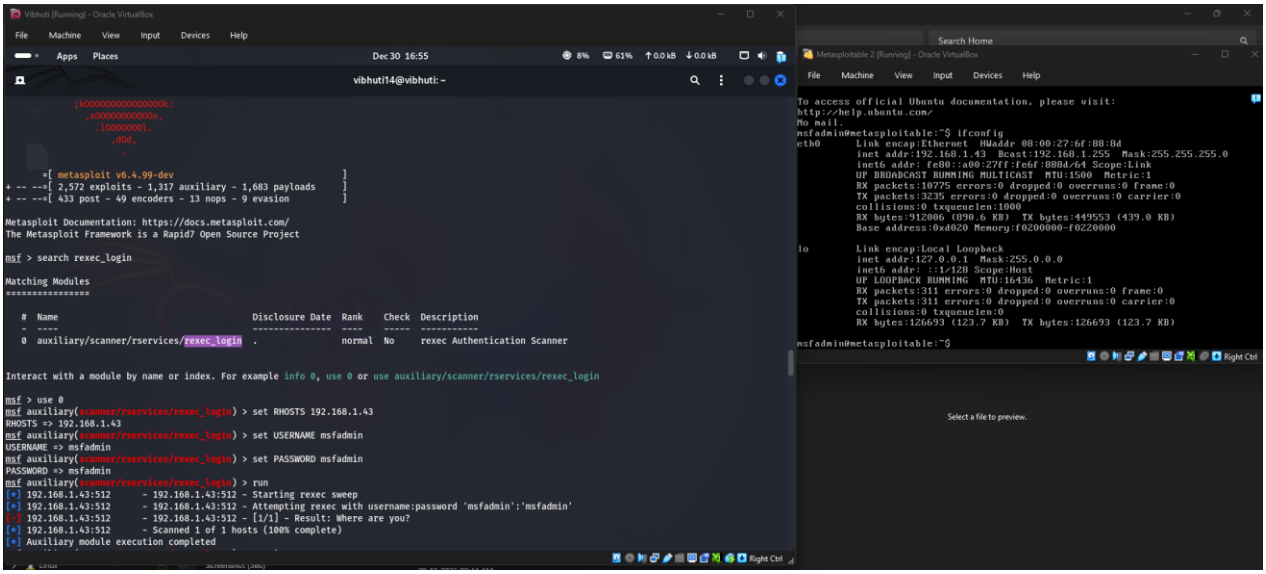
POC:

Method 1. Using the rsh client directly (manual exploitation)



Method 2. Automated Brute-Force (Metasploit)





Method 3. r-Service Trust Abuse (Information Disclosure)