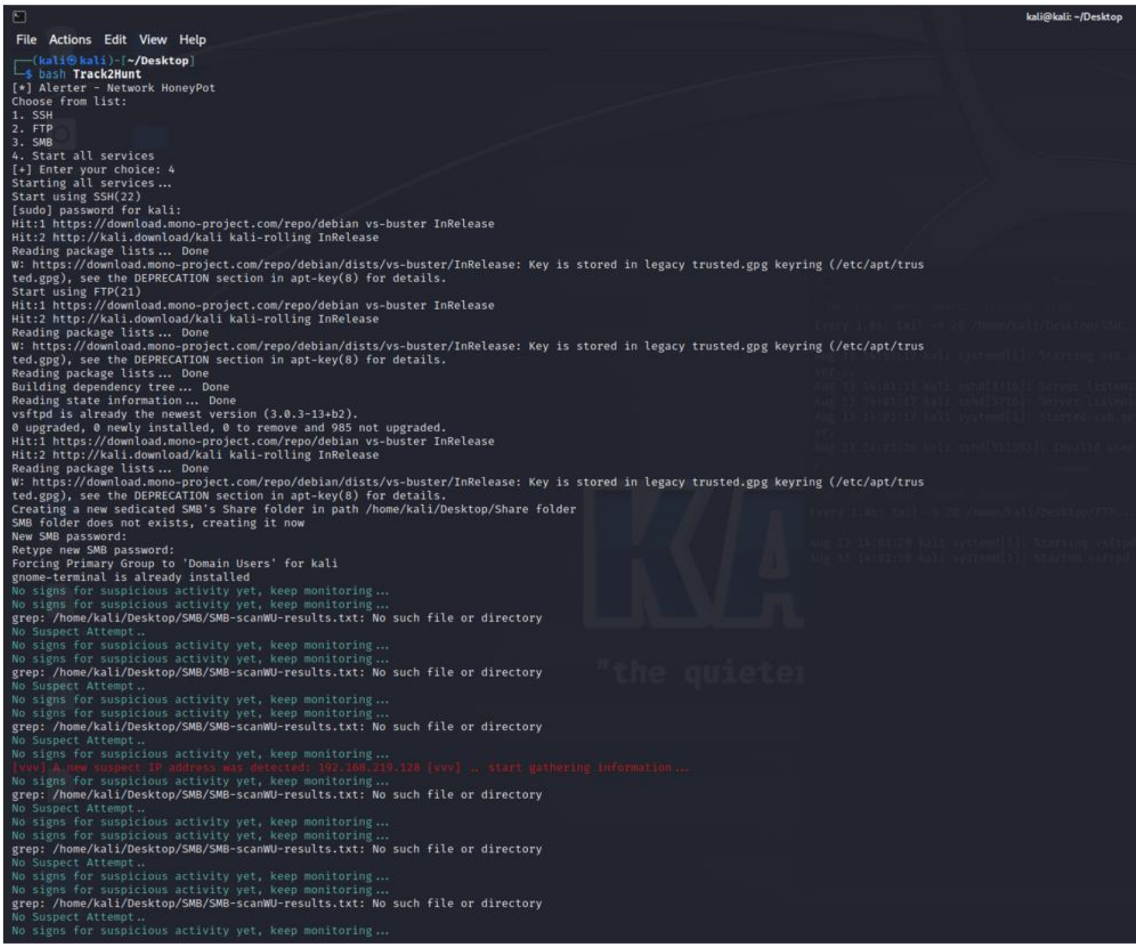
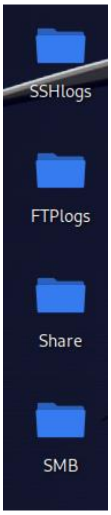
Bash it:)



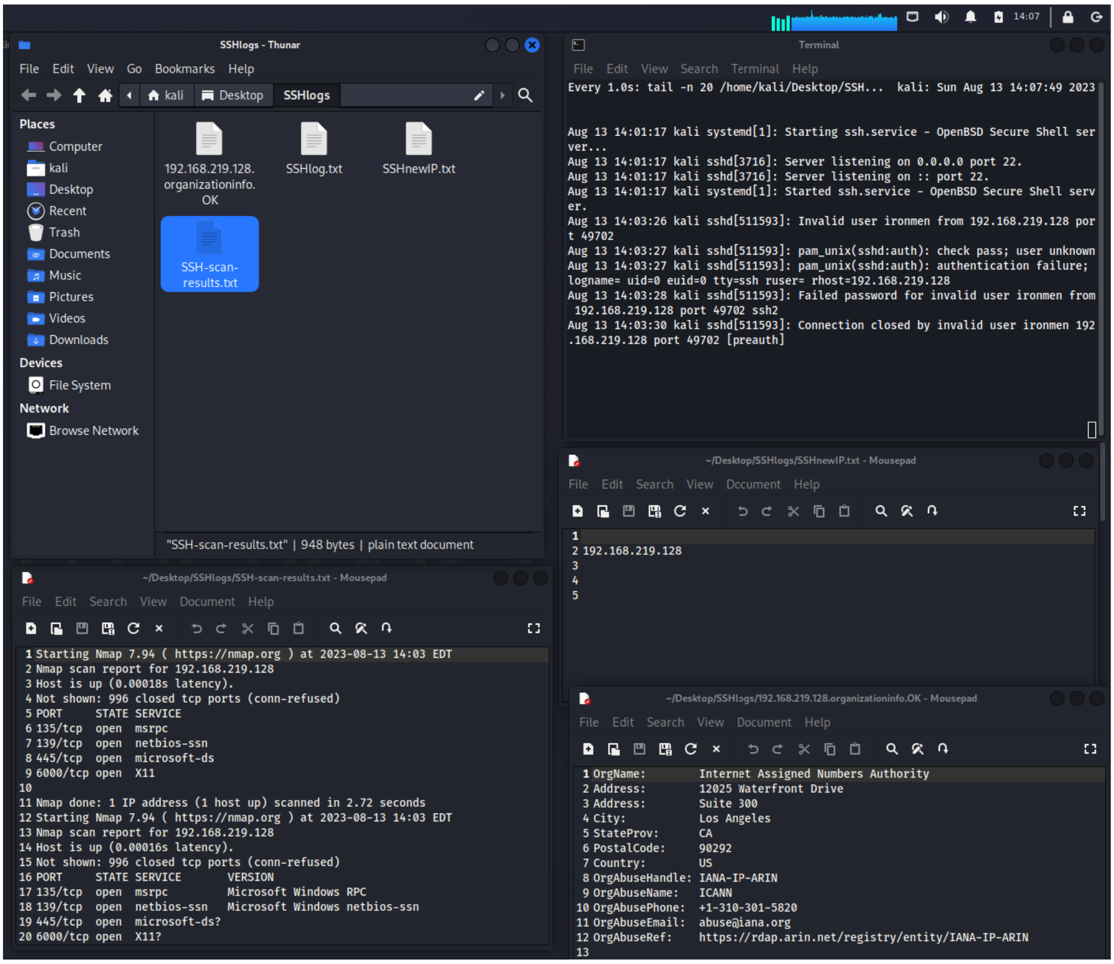
```
┌──(kali㉿kali)-[~/Desktop]
└─$ bash Track2Hunt
[*] Alerter - Network HoneyPot
Choose from list:
1. SSH
2. FTP
3. SMB
4. Start all services
[+] Enter your choice: 4
Starting all services ...
Start using SSH(22)
[sudo] password for kali:
Hit:1 https://download.mono-project.com/repo/debian vs-buster InRelease
Hit:2 http://kali.download/kali kali-rolling InRelease
Reading package lists ... Done
W: https://download.mono-project.com/repo/debian/dists/vs-buster/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trus
ted.gpg), see the DEPRECATION section in apt-key(8) for details.
Start using FTP(21)
Hit:1 https://download.mono-project.com/repo/debian vs-buster InRelease
Hit:2 http://kali.download/kali kali-rolling InRelease
Reading package lists ... Done
W: https://download.mono-project.com/repo/debian/dists/vs-buster/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trus
ted.gpg), see the DEPRECATION section in apt-key(8) for details.
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
vsftpd is already the newest version (3.0.3-13+b2).
0 upgraded, 0 newly installed, 0 to remove and 985 not upgraded.
Hit:1 https://download.mono-project.com/repo/debian vs-buster InRelease
Hit:2 http://kali.download/kali kali-rolling InRelease
Reading package lists ... Done
W: https://download.mono-project.com/repo/debian/dists/vs-buster/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trus
ted.gpg), see the DEPRECATION section in apt-key(8) for details.
Creating a new sedicated SMB's Share folder in path /home/kali/Desktop/Share folder
SMB folder does not exists, creating it now
New SMB password:
Retype new SMB password:
Forcing Primary Group to 'Domain Users' for kali
gnome-terminal is already installed
No signs for suspicious activity yet, keep monitoring ...
No signs for suspicious activity yet, keep monitoring ...
grep: /home/kali/Desktop/SMB/SMB-scanWU-results.txt: No such file or directory
No Suspect Attempt ..
No signs for suspicious activity yet, keep monitoring ...
No signs for suspicious activity yet, keep monitoring ...
grep: /home/kali/Desktop/SMB/SMB-scanWU-results.txt: No such file or directory
No Suspect Attempt ..
No signs for suspicious activity yet, keep monitoring ...
No signs for suspicious activity yet, keep monitoring ...
grep: /home/kali/Desktop/SMB/SMB-scanWU-results.txt: No such file or directory
No Suspect Attempt ..
No signs for suspicious activity yet, keep monitoring ...
[vvv] A new suspect IP address was detected: 192.168.219.128 [vvv] .. start gathering information ...
No signs for suspicious activity yet, keep monitoring ...
grep: /home/kali/Desktop/SMB/SMB-scanWU-results.txt: No such file or directory
No Suspect Attempt ..
No signs for suspicious activity yet, keep monitoring ...
No signs for suspicious activity yet, keep monitoring ...
grep: /home/kali/Desktop/SMB/SMB-scanWU-results.txt: No such file or directory
No Suspect Attempt ..
No signs for suspicious activity yet, keep monitoring ...
No signs for suspicious activity yet, keep monitoring ...
grep: /home/kali/Desktop/SMB/SMB-scanWU-results.txt: No such file or directory
No Suspect Attempt ..
No signs for suspicious activity yet, keep monitoring ...
```

There was an attempt to access our system via SSH.

# Destination directories:



SSH-results


14:07
SSHlogs - Thunar
File Edit View Go Bookmarks Help
kali
Desktop
SSHlogs
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
192.168.219.128.organizationinfo.OK
SSHlog.txt
SSHnewIP.txt
SSH-scan-results.txt
Terminal
File Edit View Search Terminal Help
~/Desktop/SSHlogs/SSHnewIP.txt - Mousepad
File Edit Search View Document Help
~/Desktop/SSHlogs/SSH-scan-results.txt - Mousepad
~/Desktop/SSHlogs/192.168.219.128.organizationinfo.OK - Mousepad

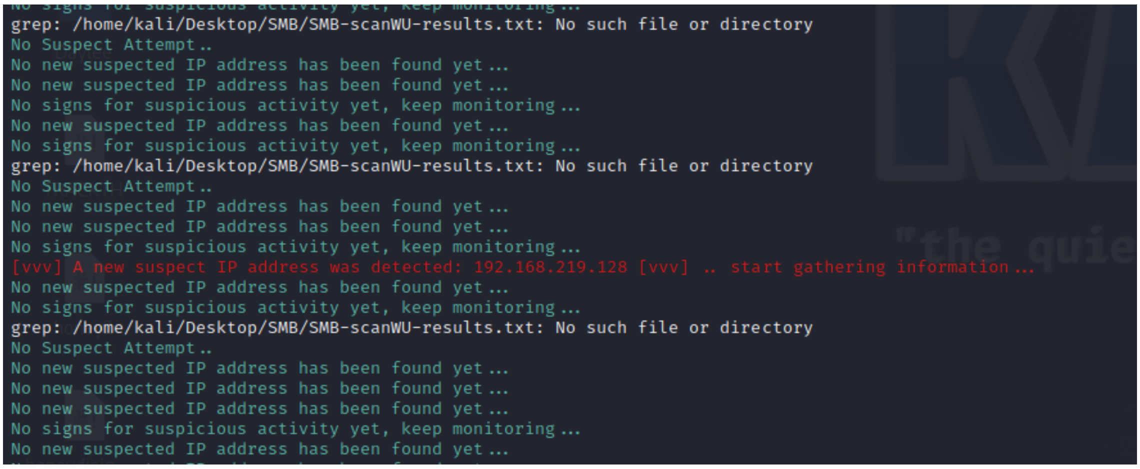
"SSH-scan-results.txt" | 948 bytes | plain text document

```
Every 1.0s: tail -n 20 /home/kali/Desktop/SSH...  kali: Sun Aug 13 14:07:49 2023


Aug 13 14:01:17 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell ser
ver...
Aug 13 14:01:17 kali sshd[3716]: Server listening on 0.0.0.0 port 22.
Aug 13 14:01:17 kali sshd[3716]: Server listening on :: port 22.
Aug 13 14:01:17 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell serv
er.
Aug 13 14:03:26 kali sshd[511593]: Invalid user ironmen from 192.168.219.128 por
t 49702
Aug 13 14:03:27 kali sshd[511593]: pam_unix(sshd:auth): check pass; user unknown
Aug 13 14:03:27 kali sshd[511593]: pam_unix(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.219.128
Aug 13 14:03:28 kali sshd[511593]: Failed password for invalid user ironmen from
 192.168.219.128 port 49702 ssh2
Aug 13 14:03:30 kali sshd[511593]: Connection closed by invalid user ironmen 192
.168.219.128 port 49702 [preauth]
```

```

192.168.219.128



```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-13 14:03 EDT
Nmap scan report for 192.168.219.128
Host is up (0.00018s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6000/tcp open  X11

Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-13 14:03 EDT
Nmap scan report for 192.168.219.128
Host is up (0.00016s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
6000/tcp open  X11?
```

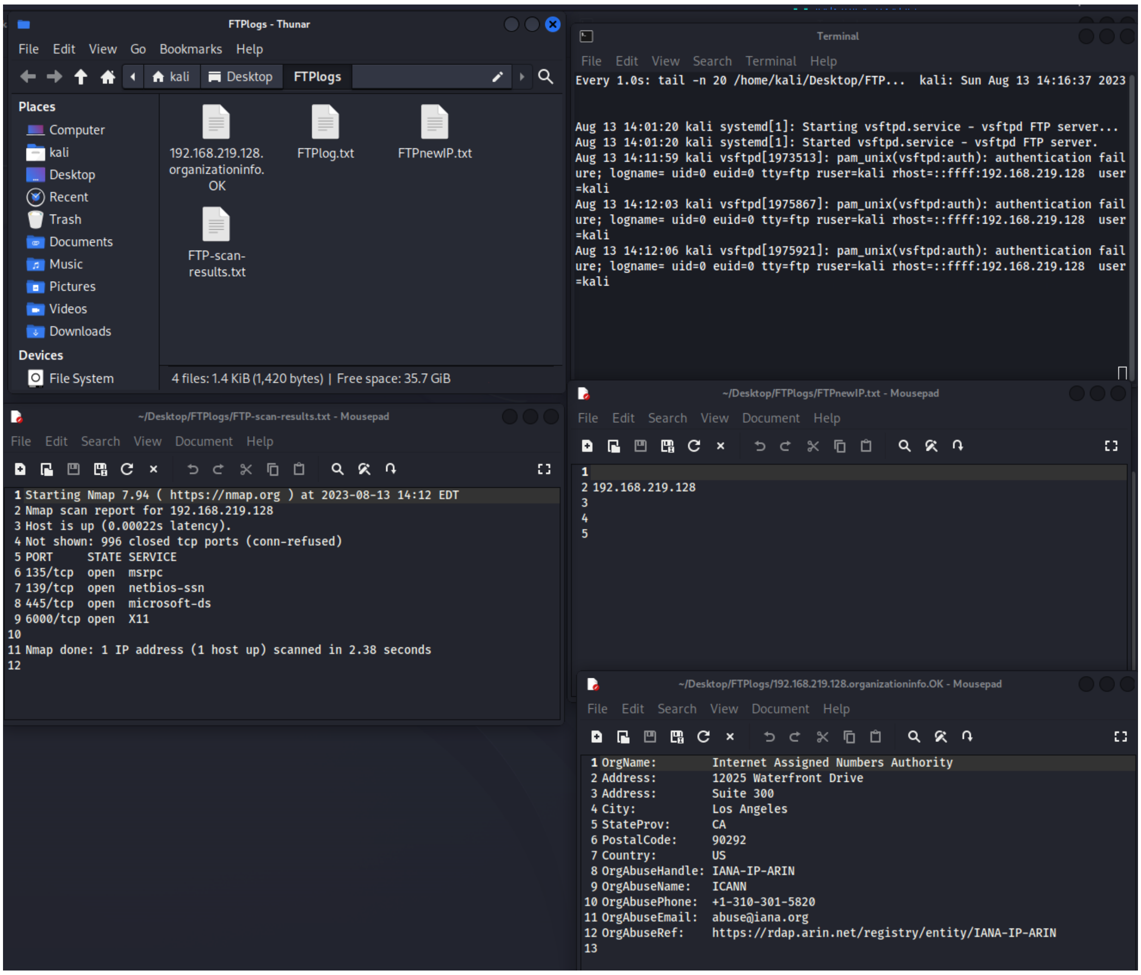
```
OrgName:        Internet Assigned Numbers Authority
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

```



```
No signs for suspicious activity yet, keep monitoring...
grep: /home/kali/Desktop/SMB/SMB-scanWU-results.txt: No such file or directory
No Suspect Attempt..
No new suspected IP address has been found yet...
No new suspected IP address has been found yet...
No signs for suspicious activity yet, keep monitoring...
No new suspected IP address has been found yet...
No signs for suspicious activity yet, keep monitoring...
grep: /home/kali/Desktop/SMB/SMB-scanWU-results.txt: No such file or directory
No Suspect Attempt..
No new suspected IP address has been found yet...
No new suspected IP address has been found yet...
No signs for suspicious activity yet, keep monitoring...
[vvv] A new suspect IP address was detected: 192.168.219.128 [vvv] .. start gathering information...
No new suspected IP address has been found yet...
No signs for suspicious activity yet, keep monitoring...
grep: /home/kali/Desktop/SMB/SMB-scanWU-results.txt: No such file or directory
No Suspect Attempt..
No new suspected IP address has been found yet...
No new suspected IP address has been found yet...
No new suspected IP address has been found yet...
No signs for suspicious activity yet, keep monitoring...
No new suspected IP address has been found yet...
```

There was an attempt to access our system via FTP.

FTP- results

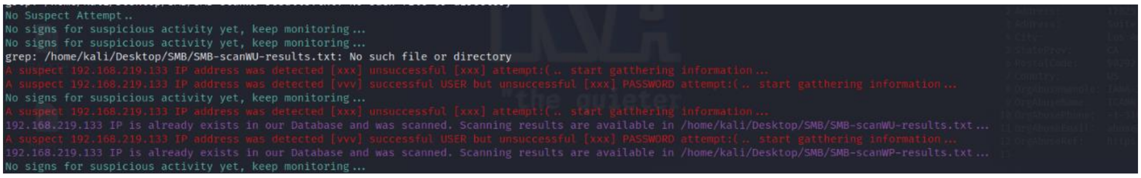

FTPlogs - Thunar
File Edit View Go Bookmarks Help
kali Desktop FTPlogs
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
192.168.219.128.organizationinfo.OK
FTPlog.txt
FTPnewIP.txt
FTP-scan-results.txt
4 files: 1.4 KiB (1,420 bytes) | Free space: 35.7 GiB
Terminal
File Edit View Search Terminal Help
~/Desktop/FTPlogs/FTPnewIP.txt - Mousepad
~/Desktop/FTPlogs/FTP-scan-results.txt - Mousepad
~/Desktop/FTPlogs/192.168.219.128.organizationinfo.OK - Mousepad
File Edit Search View Document Help

```
Every 1.0s: tail -n 20 /home/kali/Desktop/FTP...  kali: Sun Aug 13 14:16:37 2023


Aug 13 14:01:20 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Aug 13 14:01:20 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.
Aug 13 14:11:59 kali vsftpd[1973513]: pam_unix(vsftpd:auth): authentication fail
ure; logname= uid=0 euid=0 tty=ftp ruser=kali rhost=::ffff:192.168.219.128  user
=kali
Aug 13 14:12:03 kali vsftpd[1975867]: pam_unix(vsftpd:auth): authentication fail
ure; logname= uid=0 euid=0 tty=ftp ruser=kali rhost=::ffff:192.168.219.128  user
=kali
Aug 13 14:12:06 kali vsftpd[1975921]: pam_unix(vsftpd:auth): authentication fail
ure; logname= uid=0 euid=0 tty=ftp ruser=kali rhost=::ffff:192.168.219.128  user
=kali
```

```

192.168.219.128
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-13 14:12 EDT
Nmap scan report for 192.168.219.128
Host is up (0.00022s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6000/tcp open  X11

Nmap done: 1 IP address (1 host up) scanned in 2.38 seconds
```

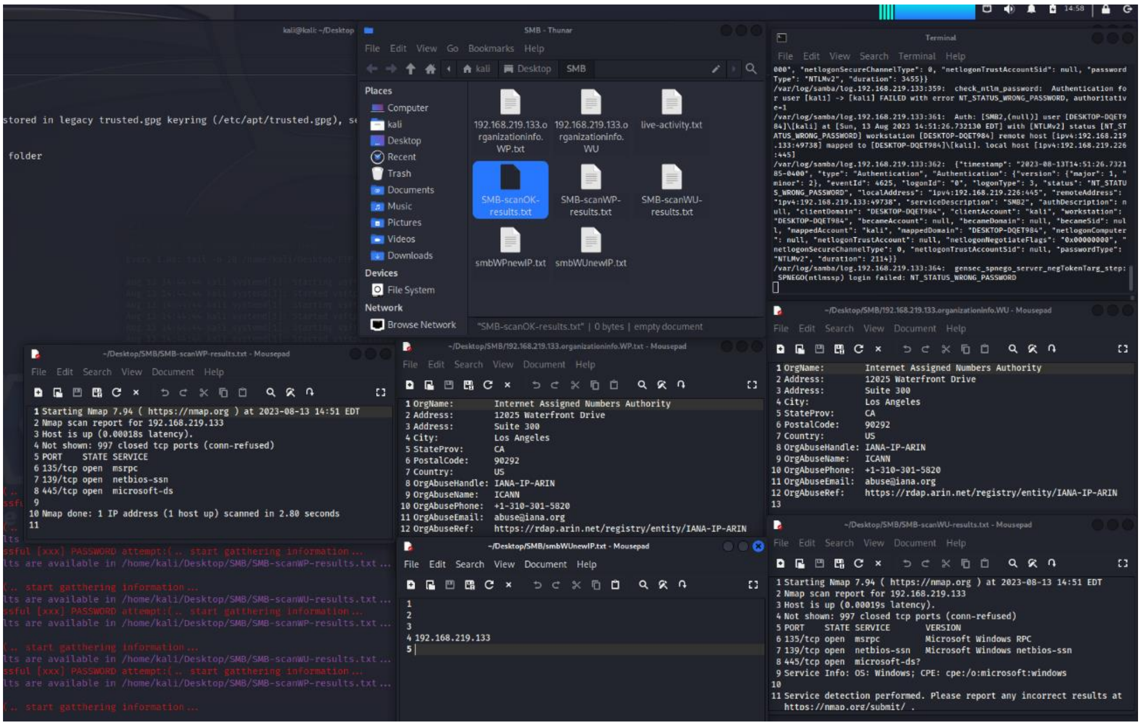
```
OrgName:        Internet Assigned Numbers Authority
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN
```



```
No Suspect Attempt..
No signs for suspicious activity yet, keep monitoring...
No signs for suspicious activity yet, keep monitoring...
grep: /home/kali/Desktop/SMB/SMB-scanWU-results.txt: No such file or directory
A suspect 192.168.219.133 IP address was detected [xxx] unsuccessful [xxx] attempt:(.. start gatthering information...
A suspect 192.168.219.133 IP address was detected [vvv] successful USER but unsuccessful [xxx] PASSWORD attempt:(.. start gatthering information...
No signs for suspicious activity yet, keep monitoring...
A suspect 192.168.219.133 IP address was detected [xxx] unsuccessful [xxx] attempt:(.. start gatthering information...
192.168.219.133 IP is already exists in our Database and was scanned. Scanning results are available in /home/kali/Desktop/SMB/SMB-scanWU-results.txt...
A suspect 192.168.219.133 IP address was detected [vvv] successful USER but unsuccessful [xxx] PASSWORD attempt:(.. start gatthering information...
192.168.219.133 IP is already exists in our Database and was scanned. Scanning results are available in /home/kali/Desktop/SMB/SMB-scanWP-results.txt...
No signs for suspicious activity yet, keep monitoring...
```

There was an attempt to access our system via FTP.

SMB- results



kali@kali: ~/Desktop
SMB - Thunar
File Edit View Go Bookmarks Help
kali Desktop SMB
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
192.168.219.133.organizationinfo.WP.txt
192.168.219.133.organizationinfo.WU
live-activity.txt
SMB-scanOK-results.txt
SMB-scanWP-results.txt
SMB-scanWU-results.txt
smbWPnewIP.txt
smbWUnewIP.txt
"SMB-scanOK-results.txt" | 0 bytes | empty document
14:58
Terminal
File Edit View Search Terminal Help
~/Desktop/SMB/SMB-scanWP-results.txt - Mousepad
~/Desktop/SMB/192.168.219.133.organizationinfo.WP.txt - Mousepad
~/Desktop/SMB/smbWUnewIP.txt - Mousepad
~/Desktop/SMB/192.168.219.133.organizationinfo.WU - Mousepad
~/Desktop/SMB/SMB-scanWU-results.txt - Mousepad
File Edit Search View Document Help

```
stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), s

folder
```

```
000", "netlogonSecureChannelType": 0, "netlogonTrustAccountSid": null, "password
Type": "NTLMv2", "duration": 3455}}
/var/log/samba/log.192.168.219.133:359:  check_ntlm_password:  Authentication fo
r user [kali] -> [kali] FAILED with error NT_STATUS_WRONG_PASSWORD, authoritativ
e=1
/var/log/samba/log.192.168.219.133:361:  Auth: [SMB2,(null)] user [DESKTOP-DQET9
84]\[kali] at [Sun, 13 Aug 2023 14:51:26.732130 EDT] with [NTLMv2] status [NT_ST
ATUS_WRONG_PASSWORD] workstation [DESKTOP-DQET984] remote host [ipv4:192.168.219
.133:49738] mapped to [DESKTOP-DQET984]\[kali]. local host [ipv4:192.168.219.226
:445]
/var/log/samba/log.192.168.219.133:362:  {"timestamp": "2023-08-13T14:51:26.7321
85-0400", "type": "Authentication", "Authentication": {"version": {"major": 1, "
minor": 2}, "eventId": 4625, "logonId": "0", "logonType": 3, "status": "NT_STATU
S_WRONG_PASSWORD", "localAddress": "ipv4:192.168.219.226:445", "remoteAddress":
"ipv4:192.168.219.133:49738", "serviceDescription": "SMB2", "authDescription": n
ull, "clientDomain": "DESKTOP-DQET984", "clientAccount": "kali", "workstation":
"DESKTOP-DQET984", "becameAccount": null, "becameDomain": null, "becameSid": nul
l, "mappedAccount": "kali", "mappedDomain": "DESKTOP-DQET984", "netlogonComputer
": null, "netlogonTrustAccount": null, "netlogonNegotiateFlags": "0x00000000", "
netlogonSecureChannelType": 0, "netlogonTrustAccountSid": null, "passwordType":
"NTLMv2", "duration": 2114}}
/var/log/samba/log.192.168.219.133:364:  gensec_spnego_server_negTokenTarg_step:
 SPNEGO(ntlmssp) login failed: NT_STATUS_WRONG_PASSWORD
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-13 14:51 EDT
Nmap scan report for 192.168.219.133
Host is up (0.00018s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 2.80 seconds

```

```
ssful [xxx] PASSWORD attempt:(.. start gatthering information...
lts are available in /home/kali/Desktop/SMB/SMB-scanWP-results.txt...

(.. start gatthering information...
lts are available in /home/kali/Desktop/SMB/SMB-scanWU-results.txt...
ssful [xxx] PASSWORD attempt:(.. start gatthering information...
lts are available in /home/kali/Desktop/SMB/SMB-scanWP-results.txt...

(.. start gatthering information...
lts are available in /home/kali/Desktop/SMB/SMB-scanWU-results.txt...
ssful [xxx] PASSWORD attempt:(.. start gatthering information...
lts are available in /home/kali/Desktop/SMB/SMB-scanWP-results.txt...

(.. start gatthering information...
```

```
OrgName:        Internet Assigned Numbers Authority
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN
```

```



192.168.219.133

```

```
OrgName:        Internet Assigned Numbers Authority
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-13 14:51 EDT
Nmap scan report for 192.168.219.133
Host is up (0.00019s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
135/tcp open  msrpc       Microsoft Windows RPC
139/tcp open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
 https://nmap.org/submit/ .
```

Alerter - Network HoneyPot

Purpose: This script aims to detect and report suspicious network activities across various services such as SSH, FTP, and SMB. It captures logs, checks for unique IP addresses, and uses tools like `nmap` and `whois` to gather further information on suspicious IP addresses.

Define Colors

- RED: For highlighting errors or issues
- GREEN: For successful operations or checks
- PURPLE: For informative messages
- NC: No Color

Functions

1. **NODUPSSHLOG**

- Description: Logs SSH attempts without duplicates.
- Location: `/home/kali/Desktop/SSHlogs`
- File: `SSHlog.txt`

2. **SCANSSH**

- Description: This function actively scans and checks SSH logs for unique IP addresses, opens a live log view, and collects more information on the new IPs.

3. **NODUPFTPLOG**

- Description: Logs FTP attempts without duplicates.
- Location: `/home/kali/Desktop/FTPlogs`
- File: `FTPlog.txt`

4. **SCANFTP**

- Description: Similar to SCANSSH but specific to FTP logs.

5. **SMBWP**

- Description: Monitors SMB login attempts with correct usernames but incorrect passwords. Also logs suspicious IPs and gathers information about them.

6. **SMBOK**

- Description: Monitors successful SMB login attempts. Logs and collects information on associated IPs.

7. **SMBWU**

- Description: Monitors SMB login attempts with wrong usernames.

8. **SMB-activate**

- Description: An infinite loop activating the SMBWP function to constantly monitor suspicious SMB activities.

Execution

Upon running the script, the user is prompted to choose from a list of services (SSH, FTP, SMB, etc.) to monitor.

Notes:

- Make sure to run the script with appropriate permissions.
- This script heavily relies on journalctl, nmap, and whois, ensure they are installed and accessible.

- Logging directories are created on the desktop for easy access. Make sure to have enough storage for the logs.

Conclusion

The script provides an active way of monitoring your network for any suspicious activities. It provides instant feedback and detailed information on the intruder's IP, helping in threat analysis.