iSEC
information security inc.

Windows Lateral Movement 3

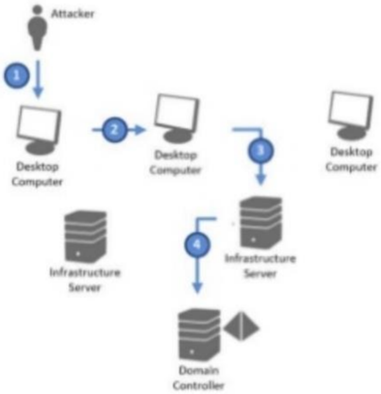
Information Security Inc.

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

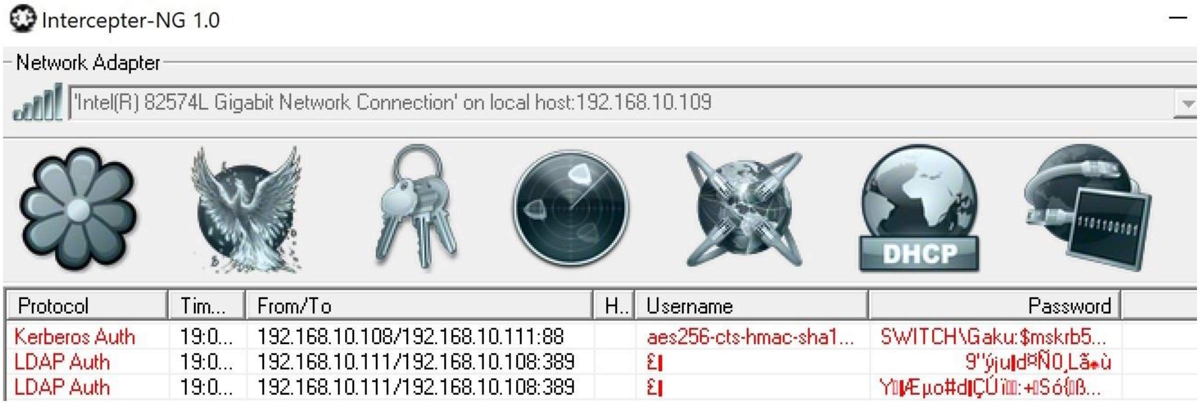


On the network without credentials
=> identify the network

- 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



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

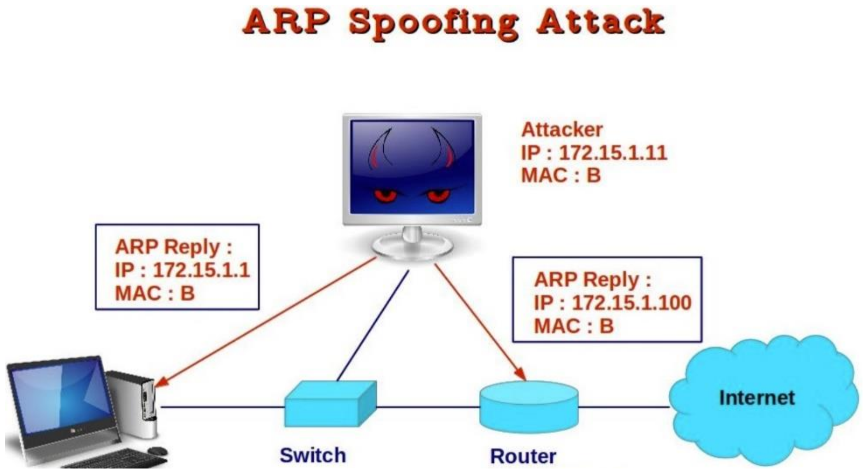
Protocol	Tim...	From/To	H..	Username	Password
Kerberos Auth	19:0...	192.168.10.108/192.168.10.111:88		aes256-cts-hmac-sha1...	SWITCH\Gaku:$mskrb5...
LDAP Auth	19:0...	192.168.10.111/192.168.10.108:389		£▌	9"ýju▌d¤Ñ0¸Lã•ù
LDAP Auth	19:0...	192.168.10.111/192.168.10.108:389		£▌	Y▯▌Æµo#d▌ÇÚï▯▯:+▯Só{▯ß...

Test Setup

```
•     ------------------                                        -------------
     | Attacker      |        |  +++++++++++++++  | Gateway | 192.168.10.105
     | 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

- ARP poisoning; Used as either resort or for a very specific test
- There is generally a good chance that you will affect end users

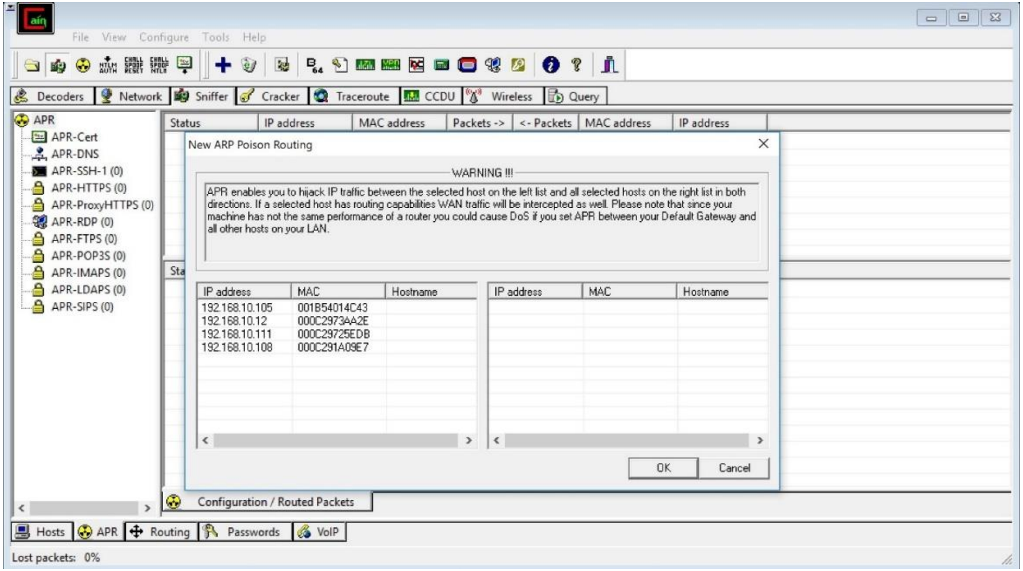


A variety of attacks to comprise the systems

- ARP poisoning tools
- Cain and Abel

A variety of attacks to comprise the systems

- Scanning MAC Addresses and listing IPs



New ARP Poison Routing

WARNING !!!

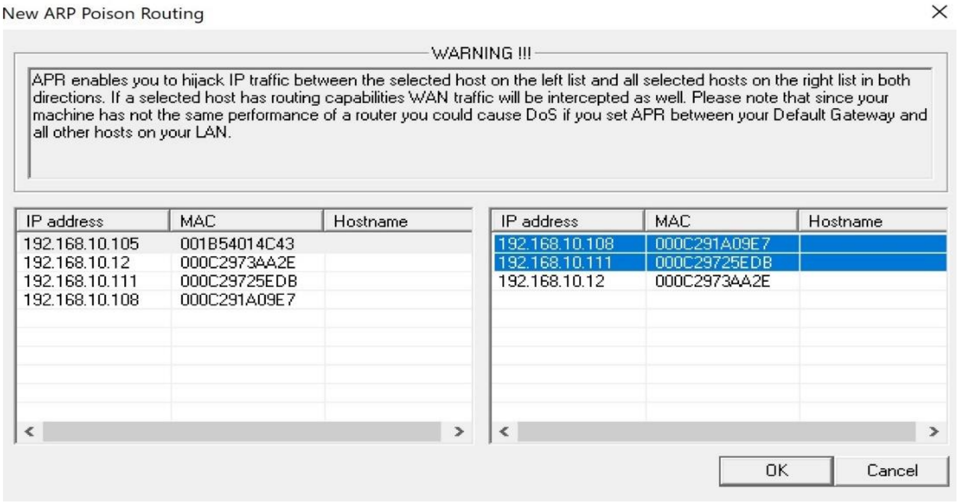
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
192.168.10.105	001B54014C43	
192.168.10.12	000C2973AA2E	
192.168.10.111	000C29725EDB	
192.168.10.108	000C291A09E7	

IP address	MAC	Hostname

A variety of attacks to comprise the systems

- Click on the gateway on the right (192.168.10.105) and select the Hosts you want to attack on the left



WARNING !!!

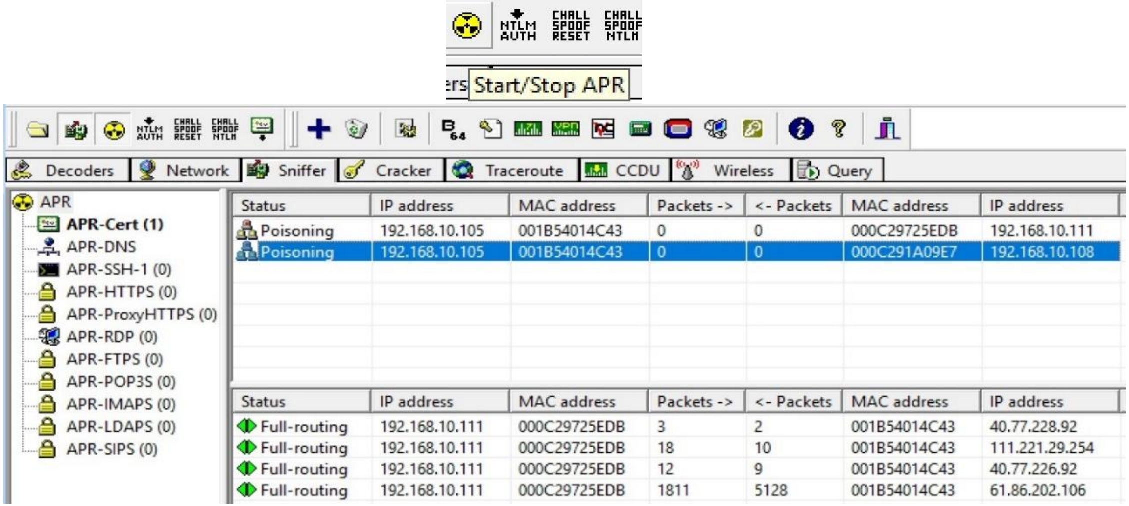
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
192.168.10.105	001B54014C43	
192.168.10.12	000C2973AA2E	
192.168.10.111	000C29725EDB	
192.168.10.108	000C291A09E7	

IP address	MAC	Hostname
192.168.10.108	000C291A09E7	
192.168.10.111	000C29725EDB	
192.168.10.12	000C2973AA2E	

A variety of attacks to comprise the systems

- Starting MiTM attack

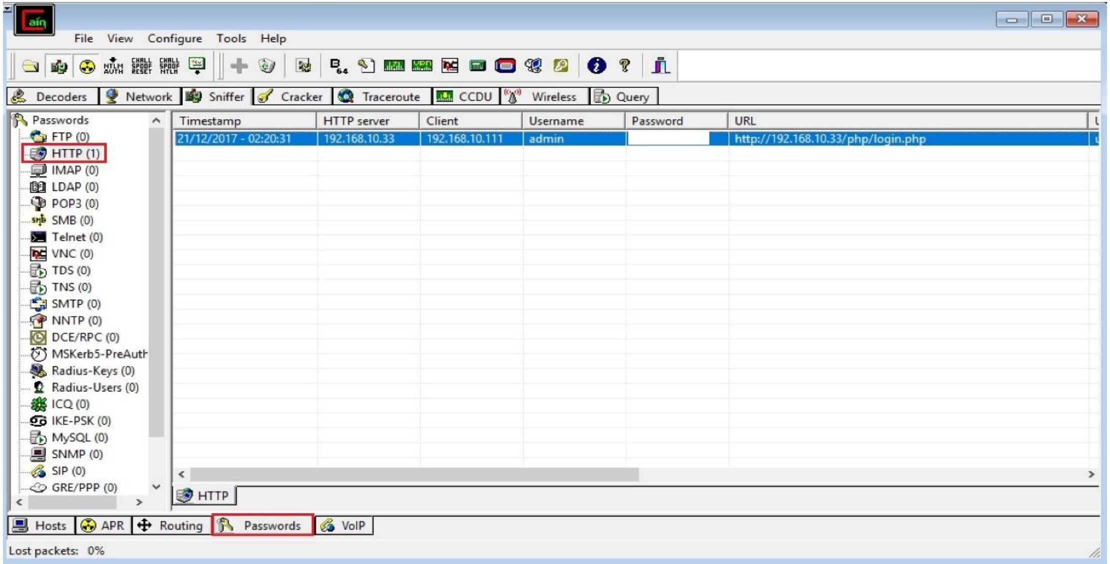


Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.10.105	001B54014C43	0	0	000C29725EDB	192.168.10.111
Poisoning	192.168.10.105	001B54014C43	0	0	000C291A09E7	192.168.10.108

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	192.168.10.111	000C29725EDB	3	2	001B54014C43	40.77.228.92
Full-routing	192.168.10.111	000C29725EDB	18	10	001B54014C43	111.221.29.254
Full-routing	192.168.10.111	000C29725EDB	12	9	001B54014C43	40.77.226.92
Full-routing	192.168.10.111	000C29725EDB	1811	5128	001B54014C43	61.86.202.106

A variety of attacks to comprise the systems

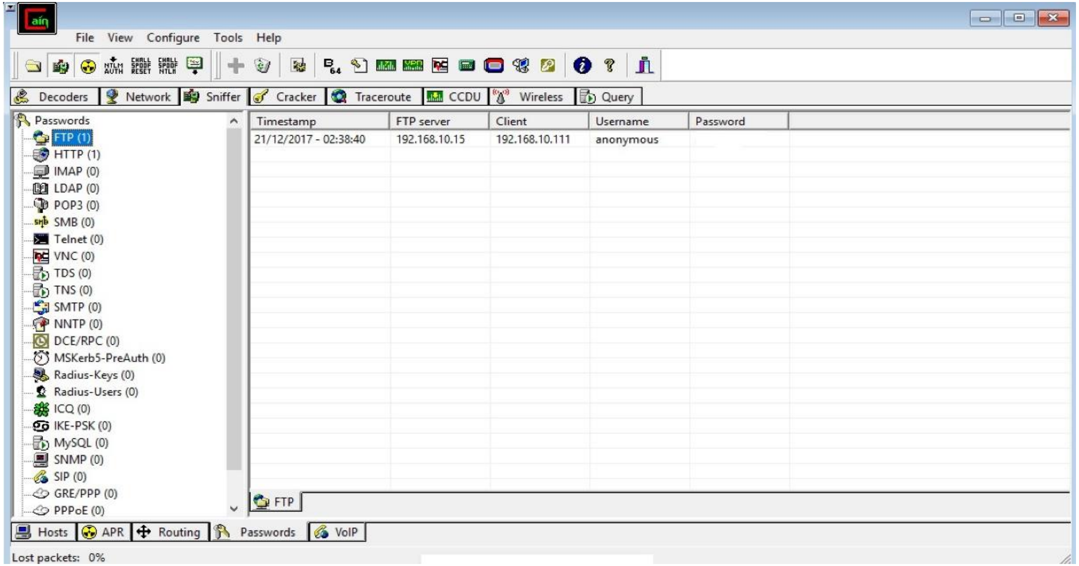
- Looking for clear text passwords, HTTP



Timestamp	HTTP server	Client	Username	Password	URL
21/12/2017 - 02:20:31	192.168.10.33	192.168.10.111	admin		http://192.168.10.33/php/login.php

A variety of attacks to comprise the systems

- Looking for clear text passwords, FTP

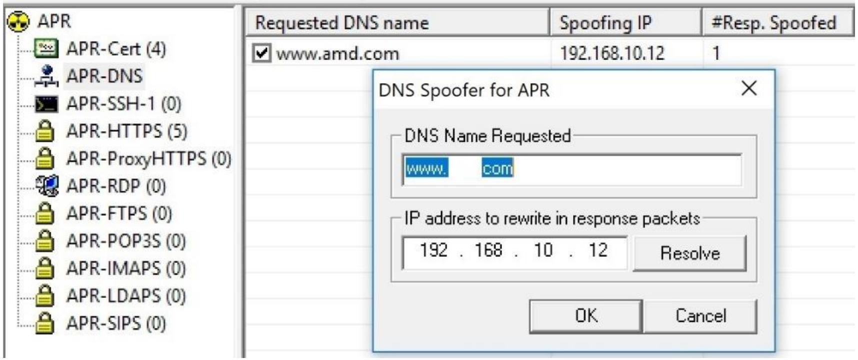


Timestamp	FTP server	Client	Username	Password
21/12/2017 - 02:38:40	192.168.10.15	192.168.10.111	anonymous	

Lost packets: 0%

A variety of attacks to comprise the systems

- DNS spoofing



Requested DNS name	Spoofing IP	#Resp. Spoofed
☑ www.amd.com	192.168.10.12	1

DNS Spoofer for APR

DNS Name Requested: www.   com

IP address to rewrite in response packets: 192 . 168 . 10 . 12

References

- Cain and Abel
http://www.oxid.it/cain.html

- Wikipedia ARP spoofing
https://en.wikipedia.org/wiki/ARP_spoofing