

Lab 04 Requirements

- Internet connectivity & VMware Workstation version 15.5.7 or above
- VM snapshots from previous labs
- All VMs on INFO6065 LAN Segment
- Confirm VM connectivity

Part 01: Scanning Networks

We will conduct two quick network scans to demonstrate a method of comparing scan results and highlighting any changes using **ndiff**

On Kali, use **mkdir** to create a new directory in **/home/kali** called **scripts**. Change into the newly created directory and install **ndiff**:

```
apt install ndiff
```

Turn on the Windows 7 and Windows 10 VMs and confirm connectivity to Kali

From Kali, start an **nmap** scan that will ping sweep the 10.0.0.0 network and save the output in XML format into a file named **scan1**

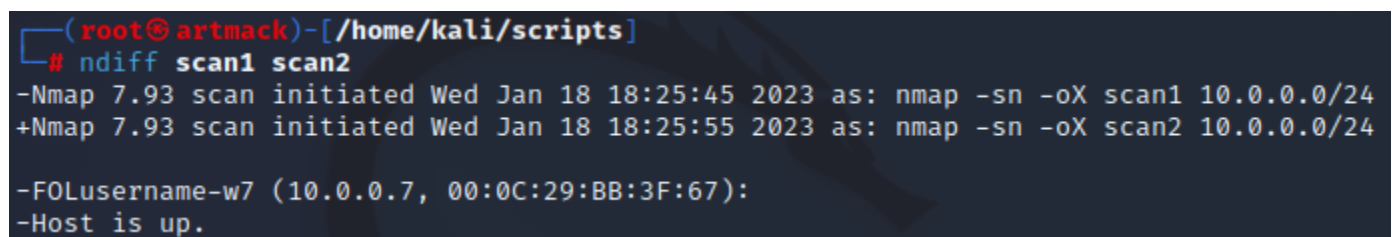
```
sudo nmap -sn 10.0.0.0/24 -oX scan1
```

Turn off the Windows 7 VM and issue the same scan saving this scan in XML to a file named **scan2**

```
sudo nmap -sn 10.0.0.0/24 -oX scan2
```

The two scans you have done should differ in the sense that the Windows 7 host is offline during the second scan. We can compare these results using **ndiff** as shown below:

```
ndiff scan1 scan2
```



```
(root@artmack)-[/home/kali/scripts]
# ndiff scan1 scan2
-Nmap 7.93 scan initiated Wed Jan 18 18:25:45 2023 as: nmap -sn -oX scan1 10.0.0.0/24
+Nmap 7.93 scan initiated Wed Jan 18 18:25:55 2023 as: nmap -sn -oX scan2 10.0.0.0/24

-FOLusername-w7 (10.0.0.7, 00:0C:29:BB:3F:67):
-Host is up.
```

Slide 01:


- Take a screenshot of the **ndiff** comparison results as shown above


Angry IP Scanner

Download **LAB04_files.7z** from this week's content on FOL, use 7zip with **info6076** as the password to extract the contents

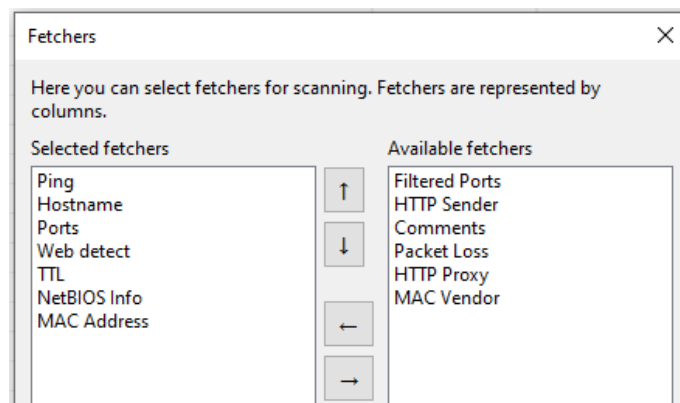
Copy the two extracted files over to your W10 VM

Note: You may need to install VM tools on your W10 VM or connect a NAT adapter in order to download/transfer the files properly

On your Windows 10 VM, install  OpenJDK11U-jdk_x86-32_windows_hotspot_11.0.8_10.msi

Accept the terms and use the defaults. Once completed, run the  ipscan-3.7.2-setup.exe file to install the Angry IP Scanner

Ensure all of your VMs are turned on. On the W10 VM, run Angry IP Scanner and select the following from the **Tools** → **Fetchers...** options listed below:



Run the scan using **IP Range: 10.0.0.0 to 10.0.0.255**

Are you able to tell what the computer names are for the clients?

What version of Apache is MS2 running?

What can you tell based on the MAC Address field?

IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range: 10.0.0.0 to 10.0.0.255 IP Range [gear icon]

Hostname: FOLusername-W10 IP↑ /24 [Start button] [menu icon]

| IP | Ping | Hostname | Ports [3+] | Web detect | TTL | NetBIOS Info | MAC Address |
|------------|------|-----------------|------------|------------------------|-----|---|-------------------|
| 10.0.0.7 | 0 ms | FOLUSERNAME-W7 | [n/a] | [n/a] | 10 | WORKGROUP\FOLUSERNAME-W7 [00-0C-29-BB-3F-67] | 00:0C:29:BB:3F:67 |
| 10.0.0.10 | 0 ms | FOLusername-W10 | [n/a] | [n/a] | 10 | [n/a] | 00:0C:29:74:2F:18 |
| 10.0.0.99 | 0 ms | [n/a] | 80 | Apache/2.4.54 (Debian) | 10 | [n/a] | 00:0C:29:46:E1:1B |
| 10.0.0.200 | 0 ms | [n/a] | 80 | Apache/2.4.29 (Ubuntu) | 10 | [n/a] | 00:0C:29:4B:C3:69 |
| 10.0.0.216 | 0 ms | WIN-6E2FPEJ0QPN | [n/a] | [n/a] | 10 | WORKGROUP\WIN-6E2FPEJ0QPN [00-0C-29-6A-45-66] | 00:0C:29:6A:45:66 |

Slide 02:

- Sort the results by **Ping**
- Ensure that your FOLusername appears in at least one of the Hostnames
- Show your results for all 5 of your VMs as per the example above

Manual/Targeted Scans

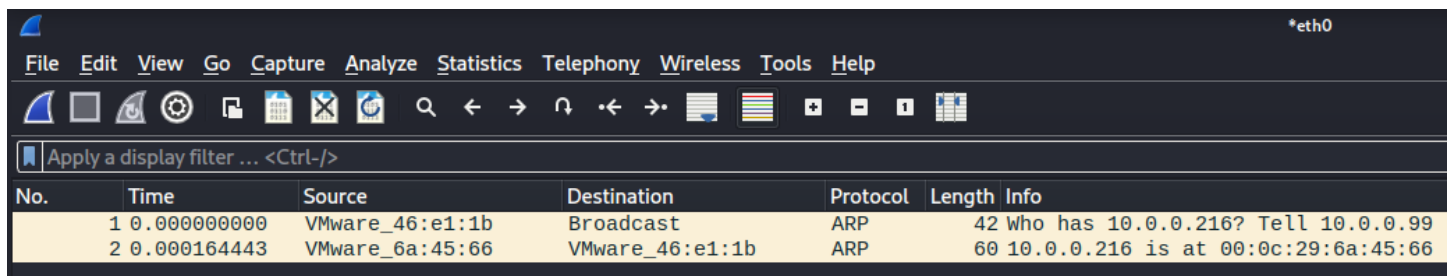
Now that we have done a number of automated scans we are going to see the difference that manual targeted scans can make

If you have been paying close attention to the nmap options previously used, you might have noticed that the **-sn** option tells nmap to perform a ping scan

- Start a new Wireshark capture on Kali and do a ping scan of your S2016 VM
- How many “packets” did this generate?
- Did nmap send a ping to discover if the S2016 VM is up and running?

If nmap knows it is being asked to do a ping scan on the local LAN segment, it is smart enough to know that it can do the scan a layer 2 using an ARP request. The reason it knows to use an ARP should make sense...

Example output shown below:



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-----------------|-----------------|----------|--------|------------------------------------|
| 1 | 0.000000000 | VMware_46:e1:1b | Broadcast | ARP | 42 | who has 10.0.0.216? Tell 10.0.0.99 |
| 2 | 0.000164443 | VMware_6a:45:66 | VMware_46:e1:1b | ARP | 60 | 10.0.0.216 is at 00:0c:29:6a:45:66 |

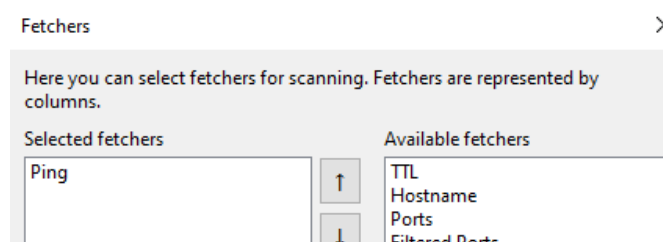


Explanation – If someone has blocked ICMP traffic on their machine, you can tell if that machine is up and running on the network just by using layer 2 ARP instead of layer 3 ICMP. This can be used to get around layer 3 traffic filters.

Netdiscover

Something that all the scans we have performed so far is that they are active scans. You should know what that means. Now we are going to use netdiscover to **passively** scan the network at layer 2

- Use **netdiscover -h** to determine what options are required to start **passively** scanning the LAN segment for any live hosts
 - The command will have two options and one argument
- Start Wireshark
- Once the netdiscover is listening and Wireshark is capturing, use Angry IP Scanner with just the Ping option set in **Tools → Fetchers...** to simulate normal network activity on the 10.0.0.0 subnet



| No. | Time | Source | Destination | Protocol | Length | Info |
|------|--------------|-----------------|-----------------|----------|--------|--|
| 1538 | 63.294949306 | 10.0.0.99 | 10.0.0.7 | TCP | 54 | 8888 → 50413 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 1537 | 63.294932314 | 10.0.0.7 | 10.0.0.99 | TCP | 62 | 50413 → 8888 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| 1077 | 10.390543326 | 10.0.0.216 | 10.0.0.10 | ICMP | | |
| 1076 | 10.390502509 | 10.0.0.10 | 10.0.0.216 | ICMP | | |
| 1075 | 10.390220900 | 10.0.0.216 | 10.0.0.10 | ICMP | | |
| 1074 | 10.390171247 | 10.0.0.10 | 10.0.0.216 | ICMP | | |
| 1073 | 10.389805660 | 10.0.0.216 | 10.0.0.10 | ICMP | | |
| 1072 | 10.389697708 | 10.0.0.10 | 10.0.0.216 | ICMP | | |
| 854 | 8.514284867 | 10.0.0.200 | 10.0.0.10 | ICMP | | |
| 853 | 8.514247938 | 10.0.0.10 | 10.0.0.200 | ICMP | | |
| 852 | 8.513985145 | 10.0.0.200 | 10.0.0.10 | ICMP | | |
| 851 | 8.513900956 | 10.0.0.10 | 10.0.0.200 | ICMP | | |
| 850 | 8.513541502 | 10.0.0.200 | 10.0.0.10 | ICMP | | |
| 849 | 8.513458095 | 10.0.0.10 | 10.0.0.200 | ICMP | | |
| 246 | 3.516174423 | 10.0.0.99 | 10.0.0.10 | ICMP | | |
| 245 | 3.516168742 | 10.0.0.10 | 10.0.0.99 | ICMP | | |
| 244 | 3.515840416 | 10.0.0.99 | 10.0.0.10 | ICMP | | |
| 243 | 3.515834114 | 10.0.0.10 | 10.0.0.99 | ICMP | | |
| 242 | 3.515406641 | 10.0.0.99 | 10.0.0.10 | ICMP | | |
| 241 | 3.515385021 | 10.0.0.10 | 10.0.0.99 | ICMP | | |
| 16 | 0.219146005 | 10.0.0.7 | 10.0.0.10 | ICMP | | |
| 15 | 0.219105258 | 10.0.0.10 | 10.0.0.7 | ICMP | | |
| 14 | 0.218484052 | 10.0.0.7 | 10.0.0.10 | ICMP | | |
| 13 | 0.218360600 | 10.0.0.10 | 10.0.0.7 | ICMP | | |
| 12 | 0.217947134 | 10.0.0.7 | 10.0.0.10 | ICMP | | |
| 9 | 0.217695692 | 10.0.0.10 | 10.0.0.7 | ICMP | | |
| 1588 | 68.394304827 | VMware_bb:3f:67 | VMware_46:e1:1b | ARP | 60 | 10.0.0.7 is at 00:0c:29:bb:3f:67 |
| 1587 | 68.394175435 | VMware_46:e1:1b | VMware_bb:3f:67 | ARP | 60 | 10.0.0.7 is at 00:0c:29:bb:3f:67 |

root@artmack: /home/kali/scripts

File Actions Edit View Help

Currently scanning: (passive) | Screen View: Unique Hosts

1514 Captured ARP Req/Rep packets, from 4 hosts. Total size: 90840

| IP | Echo (ping) | At MAC Address | Count | Len | MAC Vendor / Hostname |
|------------|-------------|-------------------|-------|-------|-----------------------|
| 10.0.0.10 | | 00:0c:29:74:2f:18 | 1502 | 90120 | VMware, Inc. |
| 10.0.0.7 | | 00:0c:29:bb:3f:67 | 8 | 480 | VMware, Inc. |
| 10.0.0.200 | | 00:0c:29:4b:c3:69 | 2 | 120 | VMware, Inc. |
| 10.0.0.216 | | 00:0c:29:6a:45:66 | 2 | 120 | VMware, Inc. |

Slide 03:

- Take a screenshot showing the **netdiscover** results in the terminal, as well as the captured Wireshark ICMP traffic
- Use the up arrow to show me the command you used to run the **netdiscover** scan
- Ensure that your FOLusername is visible

Part 02: Bash Scripting

On your Kali VM, create a new bash script that will scan a host using their IP address. You will need your metasploitable2 VM running for this portion of the lab

Now that you have done a ping sweep of the 10.0.0.0/24 subnet, you should see what hosts are up and running on that network

Create a new file in **/home/kali/scripts** called **host_id.sh** and using a text editor enter the following into the script:

```

root@artmack: /home/kali/scripts
File Actions Edit View Help
GNU nano 6.4 host_id.sh
#!/bin/bash

if [ $# -ne 1 ]; then
    echo "Usage: ./host_id.sh TARGET-IP-ADDRESS"
    exit 1
fi

hostnames=$(hostname -I | sed -e 's/[[:space]]*$/' | tr " " ",")

echo ""
echo "Scanning IP ${1}"
echo "nmap -e eth1 -sn -n -v --reason --open ${1}"

nmap -e eth1 -sn -n -v --reason --open ${1}
  
```

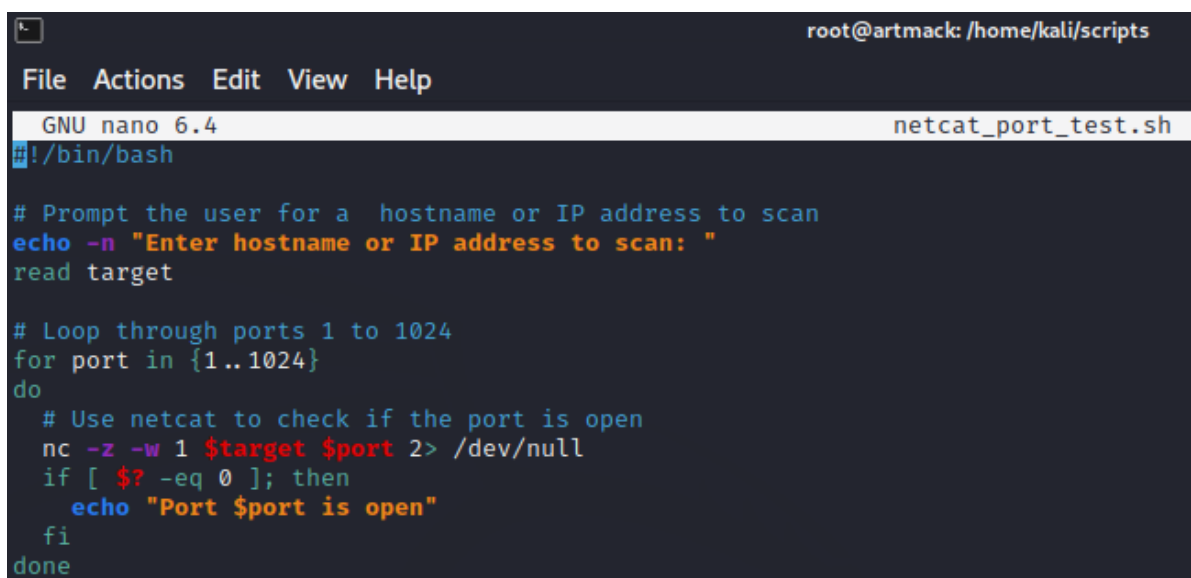
-sn tells nmap to scan using ARP, HTTP, ICMP, etc. The if statement at the beginning tells the use how to structure the command

Run the script using **./host_id.sh** You should have received an ARP response because the target host is on the same subnet as Kali

Did you receive any permission errors? You will need to fix that error before continuing...

Parse NetCat output with Bash

Create a new script named **netcat_port_test.sh** that will scan a specific target IP for any services running on that server using *well known ports* (1-1024). Use a text editor to enter the following into the new script:

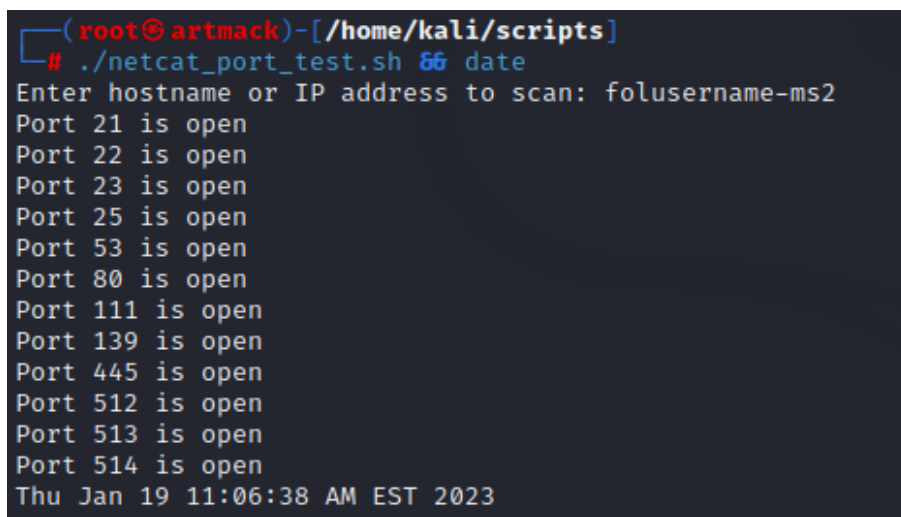


```
root@artmack: /home/kali/scripts
File Actions Edit View Help
GNU nano 6.4 netcat_port_test.sh
#!/bin/bash

# Prompt the user for a hostname or IP address to scan
echo -n "Enter hostname or IP address to scan: "
read target

# Loop through ports 1 to 1024
for port in {1..1024}
do
    # Use netcat to check if the port is open
    nc -z -w 1 $target $port 2> /dev/null
    if [ $? -eq 0 ]; then
        echo "Port $port is open"
    fi
done
```

Save the file and give it 744 permissions, then run the bash script against your FOLusername-ms2 host along with the **date** command



```
(root@artmack)-[/home/kali/scripts]
# ./netcat_port_test.sh && date
Enter hostname or IP address to scan: folusername-ms2
Port 21 is open
Port 22 is open
Port 23 is open
Port 25 is open
Port 53 is open
Port 80 is open
Port 111 is open
Port 139 is open
Port 445 is open
Port 512 is open
Port 513 is open
Port 514 is open
Thu Jan 19 11:06:38 AM EST 2023
```

Slide 04:

- Take a screenshot showing the output you receive in the terminal

Part 03: Challenge – Parse Bash script output

Modify your existing **netcat_port_test.sh** script so that it:

- Takes the original output and cuts out the port number then appends it to a new file with the following naming convention: *hostname.portnumber*

Here is an example using the S2016 server:

Original script output:

```
(root@artmack)-[/home/kali/scripts]
# ./netcat_port_test.sh
Enter hostname or IP address to scan: folusername-w2k16
Port 135 is open
Port 139 is open
Port 445 is open
```

Modified script will output parsed results in a file named after the host being scanned:

```
(root@artmack)-[/home/kali/scripts]
# ./netcat_port_test2.sh
Enter hostname or IP address to scan: folusername-w2k16

(root@artmack)-[/home/kali/scripts]
# ls -ail | grep folusername
2755361 -rw-r--r-- 1 root root 24 Jan 19 11:27 folusername-w2k16.portlist

(root@artmack)-[/home/kali/scripts]
# cat folusername-w2k16.portlist
135
139
445
135
139
445
```

Run your modified script against your FOLusername-ms2 target. You should get the same output as shown below:

```
(root@artmack)-[/home/kali/scripts]
# cat folusername-ms2.portlist && date
21
22
23
25
53
80
111
139
445
512
513
514
Thu Jan 19 11:37:34 AM EST 2023
```

Hints: Use **Cut** and **append**

For more information on how to use the cut command, enter **cut --help** in the Kali Linux terminal

Keep in mind that your modified script may look different from the example shown below and that's okay if the results are the same in the end.

```
(root@artmack)-[/home/kali/scripts]
# cat netcat_port_test2.sh
#!/bin/bash

# Prompt the user for a hostname or IP address to scan
echo -n "Enter hostname or IP address to scan: "
read target

# Loop through ports 1 to 1024
for port in {1..1024}
do
    # Use netcat to check if the port is open
    nc -z -w 1 $target $port 2> /dev/null
done
```

Slide 05:

- Take a screenshot showing the contents of your **modified** Bash Script

*** Take a snapshot of all the VMs named **After Lab 04** ***