

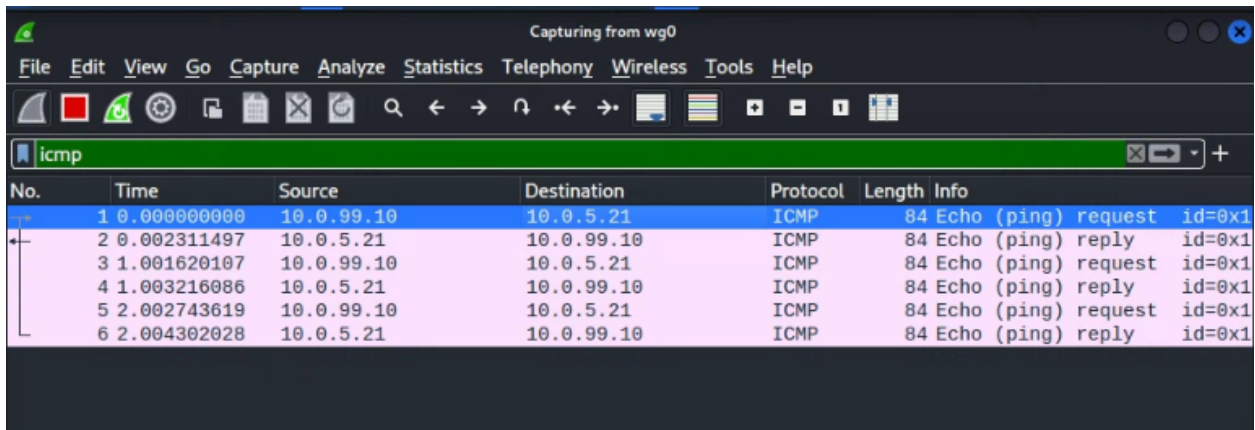
Activity 2.1 Host Discovery

In this activity you are going to enumerate the hosts in our target network 10.0.5.0/24 using various techniques beginning with "living-off-the-land techniques" and then by adding tools to the mix. You may work with your teammates to come up with the solution but you will execute the solution in your own environment and submit your own results as deliverables.

- There are live systems on 10.0.5.2,21,22,23 (there may be some more as well).
- Use Wireshark on Kali to begin capture on the **eth0** interface. Go ahead and manually ping 10.0.5.21 and make sure to capture the ICMP echo request and reply.

ping

Deliverable 1. Provide a screenshot similar to the one below that shows 1 outbound ping and the captured request and reply.



The screenshot shows a Wireshark packet capture on the 'wg0' interface. The filter is set to 'icmp'. The packet list shows six packets: an outbound ping request from 10.0.99.10 to 10.0.5.21 (packet 1), followed by its reply (packet 2), and then four more requests and replies (packets 3-6). The packet details pane shows the selected packet (packet 1) as an ICMP Echo (ping) request with ID 0x1.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.99.10	10.0.5.21	ICMP	84	Echo (ping) request id=0x1
2	0.002311497	10.0.5.21	10.0.99.10	ICMP	84	Echo (ping) reply id=0x1
3	1.001620107	10.0.99.10	10.0.5.21	ICMP	84	Echo (ping) request id=0x1
4	1.003216086	10.0.5.21	10.0.99.10	ICMP	84	Echo (ping) reply id=0x1
5	2.002743619	10.0.99.10	10.0.5.21	ICMP	84	Echo (ping) request id=0x1
6	2.004302028	10.0.5.21	10.0.99.10	ICMP	84	Echo (ping) reply id=0x1

Deliverable 2. Collaborate with your teammates from Module 1 to write either a bash script or one liner to ping ip's in the range of 10.0.5.2 - 10.0.5.50 your script should output a list of "up ip addresses" into a file called sweep.txt. Submit a screenshot similar to the redacted one below that shows either your 1 liner command or source code, followed by a cat of sweep.txt.

Hints

- 1 Ping
- Set timeout to something low
- Look for unique text in a positive response
- Pull the IP out of that response (grep, cut and or awk might be useful)
- Append the IP to sweep.txt

```
(champuser@kali)-[~/sec335/tech-journal/SEC335/week2]
$ for ip in $(seq 2 50); do ping -c 1 10.0.5.2 10.0.5.20 10.0.5.22; done
```

fping

Deliverable 3. Now, do the same thing with fping. Investigate the switches that allow you to provide a range of ip addresses as well as reporting the "up" hosts. You may need to throw out error messages. Provide a screenshot similar to the one below.

```
(champuser@kali)-[~/sec335/tech-journal/SEC335/week2]
$ sudo fping >> sweep2.txt

(champuser@kali)-[~/sec335/tech-journal/SEC335/week2]
$ cat sweep2.txt
10.0.5.2
10.0.5.20
10.0.5.22
```

nmap

- refer to <https://nmap.org/book/man-host-discovery.html>

Deliverable 4. Use nmap's -sn switch to scan 10.0.5.21, it should report that it is up. Execute nmap with this exercise. Capture traffic on eth0 using Wireshark. Provide a screenshot of your wireshark output.

Deliverable 5. Closely examine What destination ports and protocols were used in the use case? What observations do you have when comparing this to the ping and fping tests?

💡 Nmap sometimes behaves differently when running as a non privileged user. Be very careful. In the case of scans you should preface them with sudo because many operations and options run by nmap will need elevated privileges. If you use output files, they will be written and owned by root so you may need to tweak permissions in order to edit.

Updated Jan 23, 2023

Deliverable 6. Write a bash one liner or script that conducts an nmap -sn scan of 10.0.5.2-50 and outputs the list of ip addresses to sweep.txt similarly to the code written for ping and fping. Take a screenshot that shows the execution and output.

```
(champuser@kali)-[~/sec335/tech-journal/SEC335/week2]
$ sudo nmap -n -vv -sn 10.0.5.2-50 > sweep3.txt

(champuser@kali)-[~/sec335/tech-journal/SEC335/week2]
$ cat sweep3.txt
10.0.5.2
10.0.5.20
10.0.5.22

(champuser@kali)-[~/sec335/tech-journal/SEC335/week2]
$
```

Deliverable 7. Tech Journal - Technical

Document all of this work in a host-discovery section of your tech-journal. Make sure that the commands are appropriately formatted as bash and that any source code is included and referenced in the journal. Here's an example of that in markdown. Provide link(s) to this content.

```
```bash
echo helloworld
```
```

Deliverable 8. Tech Journal - Reflections include trials, tribulations and commentary that will be useful to your future self. Example (Don't use this one):

It took me forever to debug why the nmap scan wasn't returning the results I expected. It turned out that I neglected to run the scan as sudo.