Dirty Dog Labs Network Lab Report

Prepared by:
Ernie Johnson - Cybersecurity Specialist
ernie@erniejohnson.ca

1. Introduction

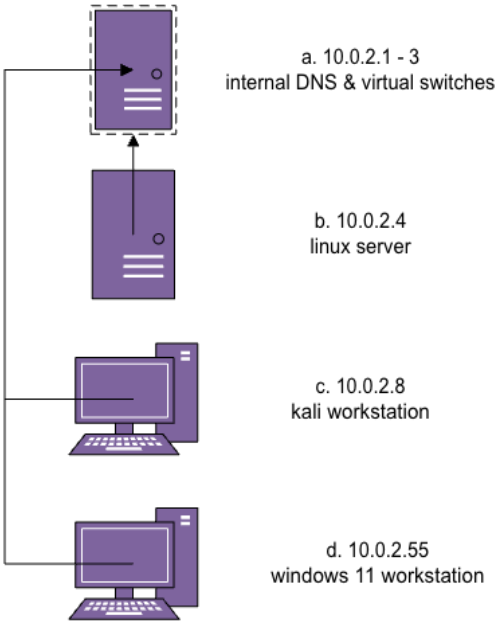
a. Executive Summary

This executive summary report presents the key findings from our basic network analysis of Dirty Dog Lab. The analysis aimed to assess their current security posture and identify areas for improvement.

Our security assessment identified minimal vulnerabilities, such as unused web servers, open ports, and outdated software. These findings pose a low immediate threat, but there are opportunities to further enhance your security posture. We recommend prioritising the following actions:

- Immediate: Complete software updates and conduct user education on security best practices.
- Long-term: Redesign the network architecture to isolate sensitive areas and implement continuous monitoring of infrastructure and services.

b. Initial Network Topography



2. Network Devices Information

a. Devices 10.0.2.1 - 3

i. These devices have been identified as the internal DNS server and virtual machine switches created by Oraclebox. They will be excluded from this report for clarity as they do not pose any security concerns.

b. Device 10.0.2.4 (ref. Image 1)

Hostname: LINUX-SERVER
Running:
Apache 2.4.52 (port 80 web server)
OpenSSH 8.9p1 (port 22)
Details:
MAC: 08:00:27:CB:20:4A
OS: Ubuntu 22.04.4 with Kernel 6.5.0-41
(device confirmed as nmap reported different)
ARP Ping Scan Time: 0.04s

c. Device 10.0.2.8 (ref. Image 2)

Hostname: KALI
Running:
OpenSSH 9.71p1 (port 22)
Details:
MAC: 08:00:27:1B:76:B0
OS: Debian with Kernel 6.8.11-amd64 (device confirmed)
ARP Ping Scan Time: na (host device)

d. Device 10.0.2.55 (ref. Image 3)

Hostname: WINDOWS11-DESKT
Running:
PRTG Network Monitor (port 80)
Details:
MAC: 08:00:27:CB:20:4A
OS: Windows 11 23H2 (device confirmed)
ARP Ping Scan Time: 0.04s

3. Information Collection Methodology

a. Data Collection Techniques

i. Data was collected on this network via several methods including a simple nmap (Ref. Image 6) scan across the entire IP range while under admin rights. `sudo nmap -T4 -A -v 10.0.2.0/24`
(Paranoid timing template, Aggressive Scanning and verbose output)
ii. Process was started 2024-06-27 @ 2241hEDT and completed scanning 256 IP addresses, finding 6 hosts, in 226.44 seconds.
iii. On device confirmations were individually performed via SSH access into each end-point from the Windows 11 workstation and individual device confirmations completed with `uname`, `hostname` and other command line tools built for aggregating different system commands (`winfetch`, `neofetch` being the primary used in this situation).
iv. OS and application information was referenced with various OSINT techniques to determine potential vulnerabilities
v. Wireshark packet analysis was conducted and compared to nmap data. (ref. Image 4 & Image 5).
vi. Results were then analysed and assembled into this report.

b. Tools and Software Used

i. Wireshark traffic analysis (ref. Image 4, Image 5)
ii. Nmap (ref. Image 6), ifconfig,
iii. Varied other command line utilities to obtain device details

4. Analysis and Findings

a. Potential Vulnerabilities and Risks Identified

i. **10.0.2.4**
   1. CVE-2024-24795. (NIST, 2024) Apache web server 2.4.52 has an http response issue which can lead to malicious response headers being injected causing http desync attacks. Suggested to upgrade Apache version ASAP.
   2. The web server on this device does not appear to be in use. It should be retired and uninstalled if there are no plans for operation.
   3. CVE-2023-51385. (NIST, 2024) OpenSSH 8.91p1 - incorrectly handles user names and could allow malicious command injection. Suggested to update the OpenSSH service.
   4. No other operating system/kernel vulnerabilities found. (Canonical Ubuntu, n.d.)

ii. **10.0.2.8**
    1. No widespread security concerns are reported on this device (Debian GNU/Linux, n.d.)

iii. **10.0.2.55**
    1. No widespread security concerns are reported in Windows 11 23H2 on this device (Microsoft Corp., n.d.)
    2. WNPA-SEC-2024-07. (Wireshark, 2024) Wireshark vulnerability - no active exploits - recommend software update.

b. Recommendations for Mitigation

i. Close access to any ports not-in-use
ii. Disable server functions if not in use.
iii. Implement pushed update policies to ensure software and operating systems are kept up to date

5. Conclusion

a. Summary of Key Findings

i. Dirty Dog Lab network appears to be in reasonably safe condition at the time of this report. Minor updates are required to install service patches to ensure no known vulnerabilities exist on this network.

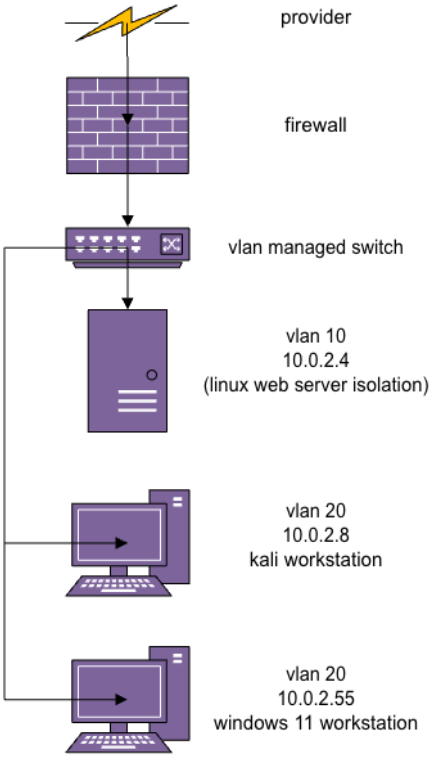
b. Final Recommendations

i. Implement update policies across the network. If unable to push these policies to devices, implement a manual software update plan.
ii. Educate users of end-points in the importance of software updates, create and publish training materials to aid in this
iii. Implement regular log and systems monitoring.
iv. Develop policies and procedures on acceptable use of company equipment. Ensure training and enforcement of policies is followed.
v. Develop an Information Security Continuous Monitoring plan (ISCM). (NIST, 2011)
vi. Develop cybersecurity incident SOP to follow in case of a breach.
vii. Regularly audit system and server log(s) to establish baseline usage and monitor for abnormalities.

c. Future Steps

i. Upgrading your network topology is vital to prevent major security breaches or lessen their impact. This involves segmenting your network with VLANs to isolate critical systems and data, and implementing a firewall to act as a security checkpoint to filter traffic and block unauthorised access. This layered approach will significantly strengthen your network defences.

Suggested new network topology:



6. References

Canonical Ubuntu. (n.d.). *CVEs*. Ubuntu. Retrieved June 27, 2024, from https://ubuntu.com/security/cves/

Debian GNU/Linux. (n.d.). *Security Information*. Debian. Retrieved June 27, 2024, from https://www.debian.org/security/

Microsoft Corp. (n.d.). *Security Update Guide*. Microsoft Security Response Center. Retrieved June 27, 2024, from https://msrc.microsoft.com/update-guide/vulnerability/

NIST. (2024, March 13). *NVD - CVE-2023-51385*. NVD. Retrieved June 27, 2024, from https://nvd.nist.gov/vuln/detail/CVE-2023-51385

NIST. (2024, June 10). *NVD - CVE-2024-24795*. NVD. Retrieved June 27, 2024, from https://nvd.nist.gov/vuln/detail/CVE-2024-24795

NIST.gov. (2011, September 01). *NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. NIST Technical Series Publications. Retrieved June 27, 2024, from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf

Wireshark. (2024, May 15). *Wireshark • wnpa-sec-2024-07*. Wireshark. Retrieved June 27, 2024, from https://www.wireshark.org/security/wnpa-sec-2024-07.html

7. Images & Screen Captures

Image 1. neofetch of 10.0.2.4

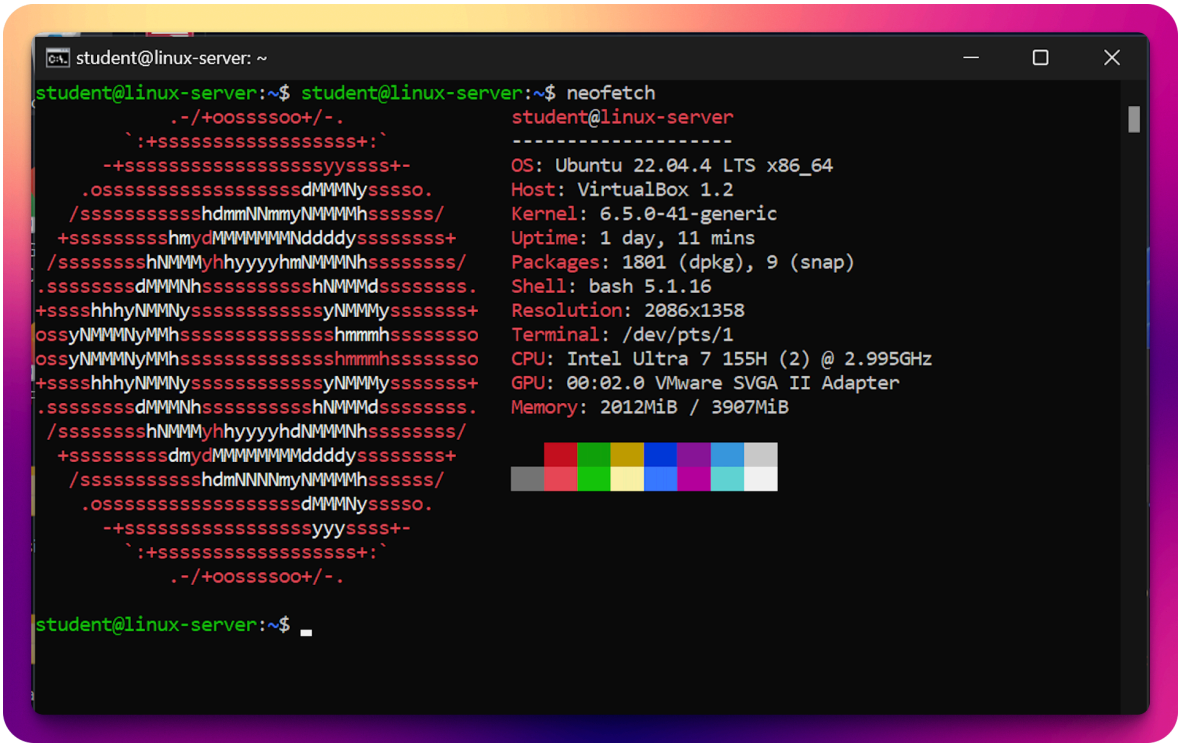


Image 2. neofetch of 10.0.2.8

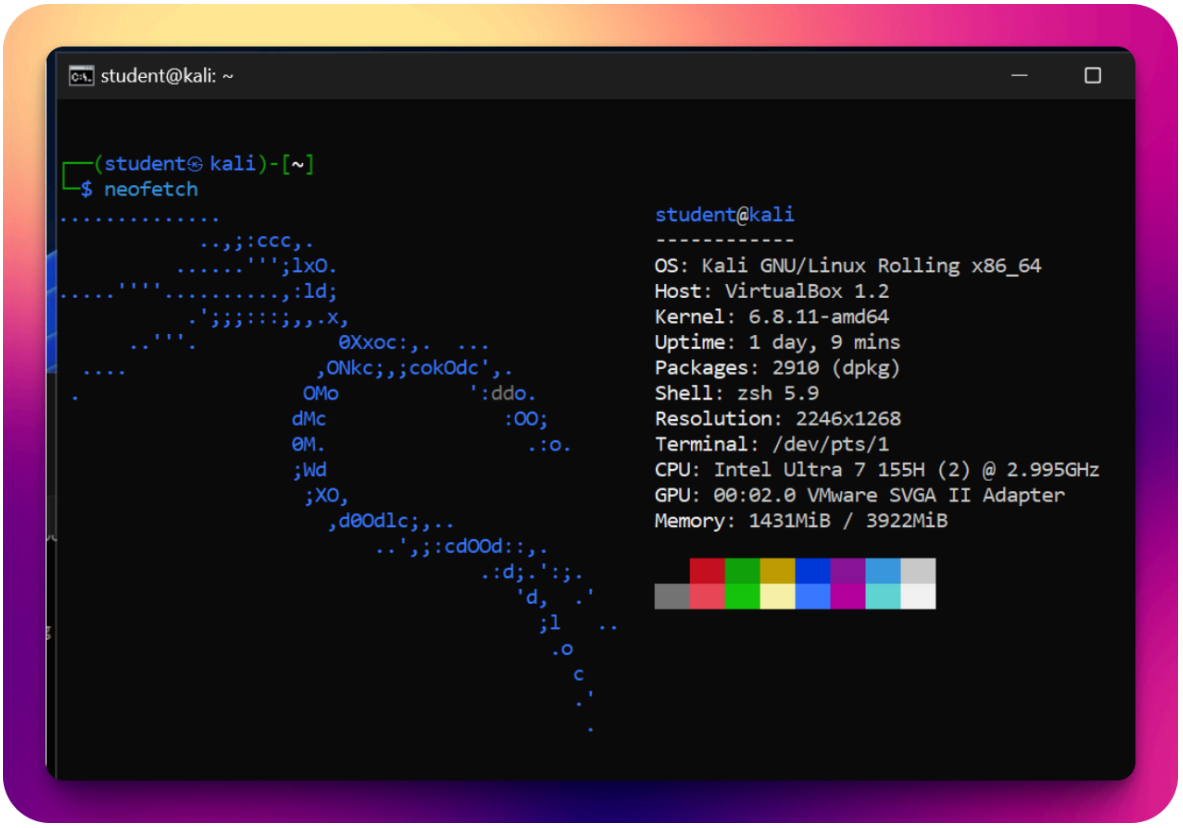


Image 3. winfetch of 10.0.2.55

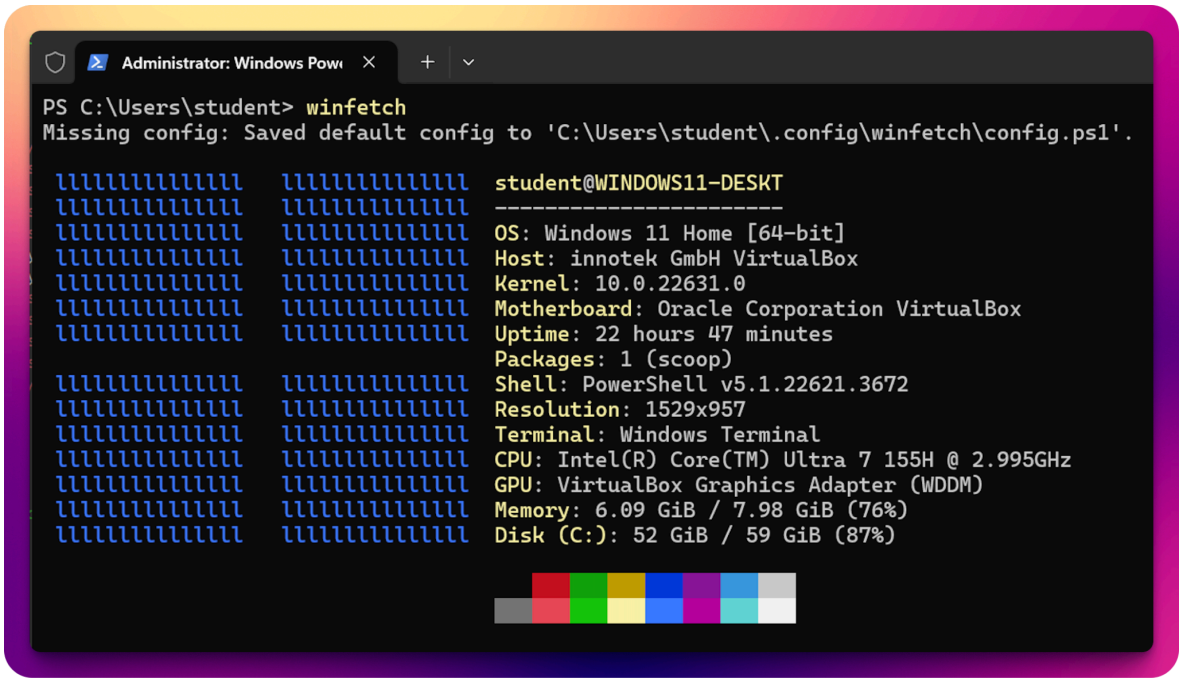


Image 4. Wireshark capture showing filtering by port

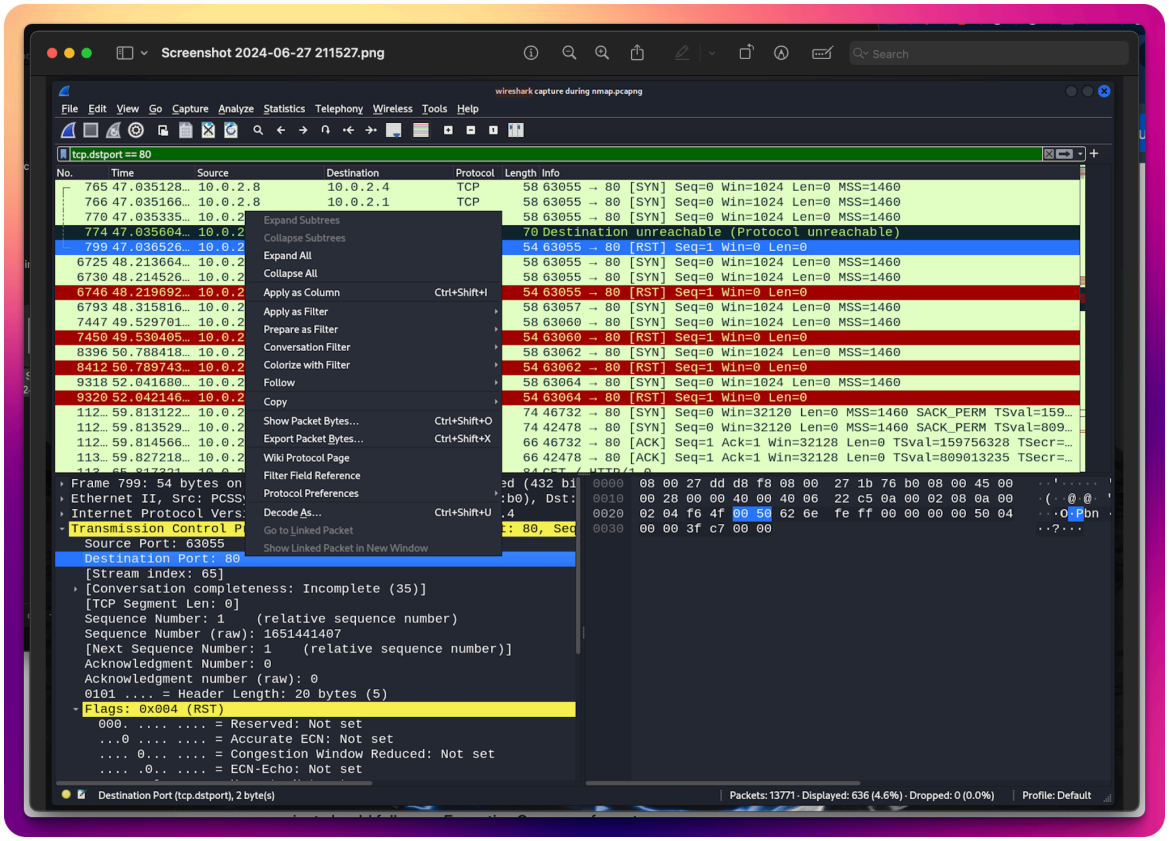
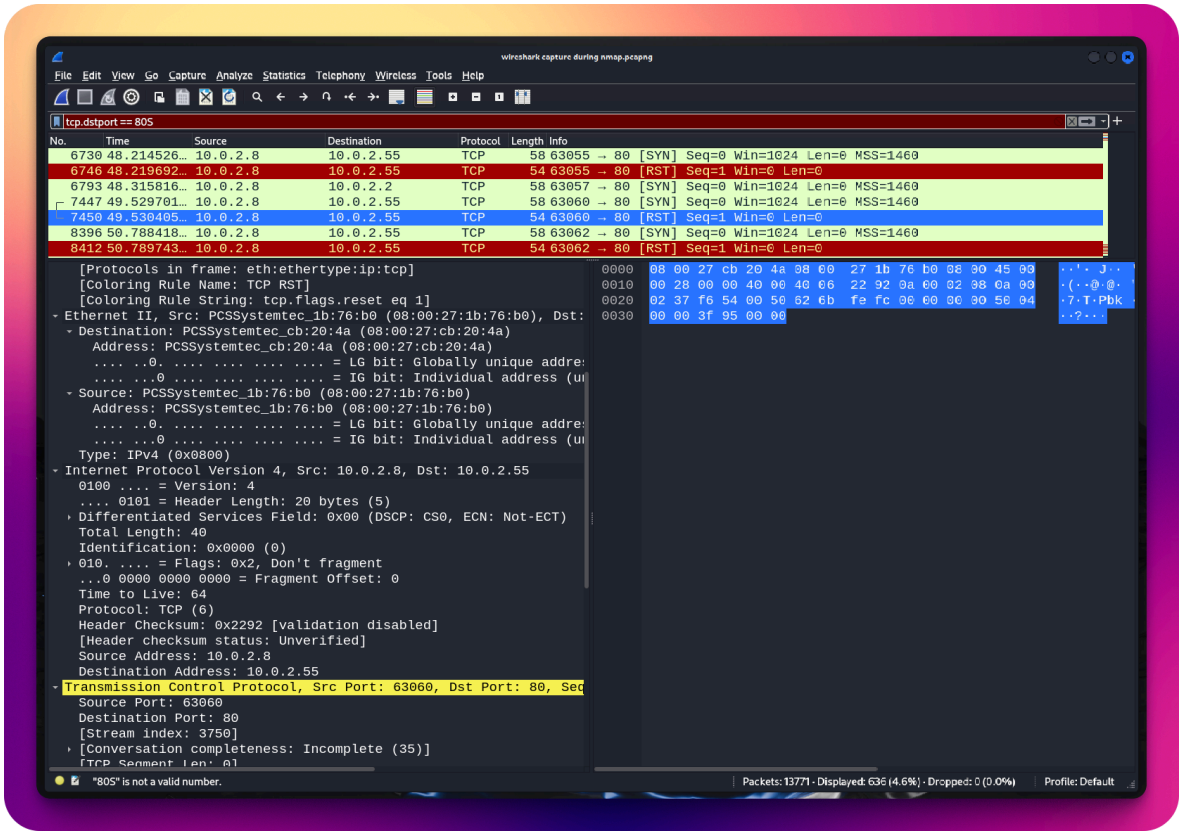


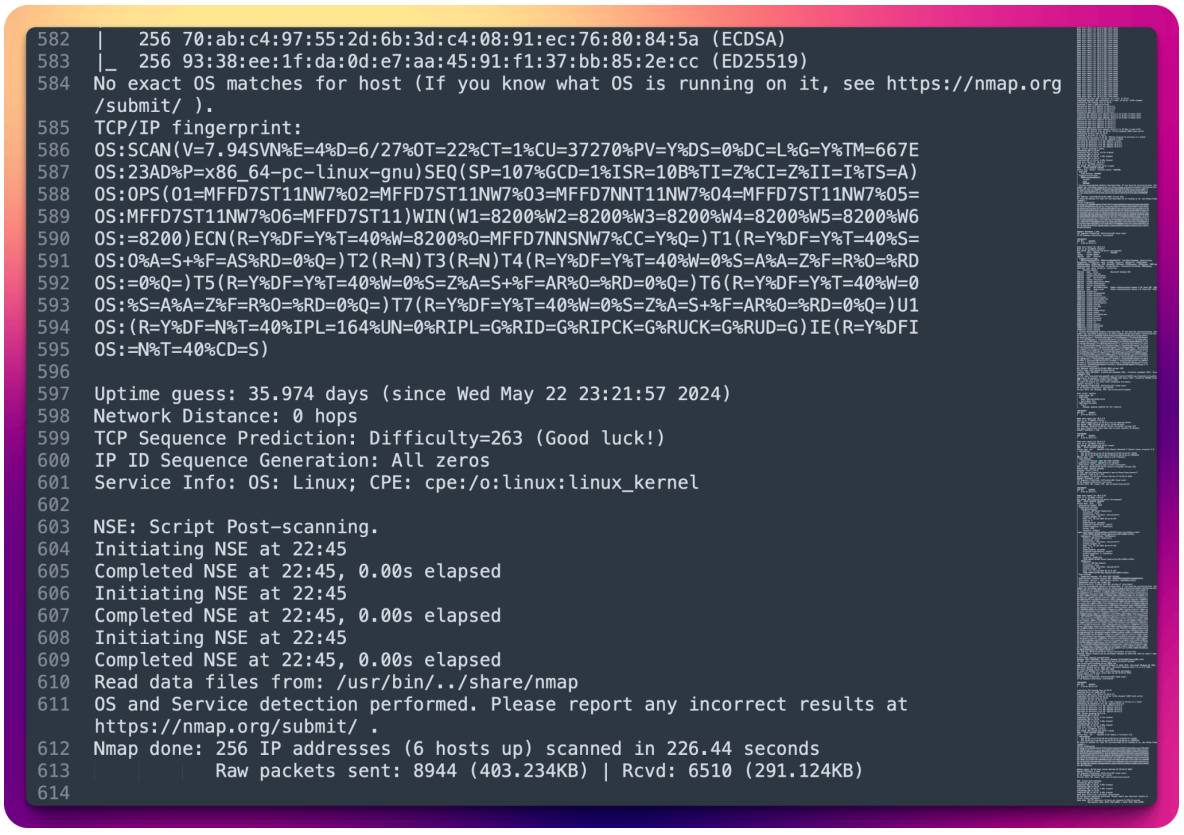
Image 5. Wireshark capture showing *some* sections of OSI model.



Note:
This is but one small capture of data collected.

Data Link layer (2) information showing source and destination MAC addressing,
Network Layer (3) - IP addressing,
Transport Layer (4) - TCP protocol and port numbers of source and destination.

Image 6. Final segment of nmap dump



```
582 |   256 70:ab:c4:97:55:2d:6b:3d:c4:08:91:ec:76:80:84:5a (ECDSA)
583 |_  256 93:38:ee:1f:da:0d:e7:aa:45:91:f1:37:bb:85:2e:cc (ED25519)
584 No exact OS matches for host (If you know what OS is running on it, see https://nmap.org
    /submit/ ).
585 TCP/IP fingerprint:
586 OS:SCAN(V=7.94SVN%E=4%D=6/27%OT=22%CT=1%CU=37270%PV=Y%DS=0%DC=L%G=Y%TM=667E
587 OS:23AD%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)
588 OS:OPS(O1=MFFD7ST11NW7%O2=MFFD7ST11NW7%O3=MFFD7NNT11NW7%O4=MFFD7ST11NW7%O5=
589 OS:MFFD7ST11NW7%O6=MFFD7ST11)WIN(W1=8200%W2=8200%W3=8200%W4=8200%W5=8200%W6
590 OS:=8200)ECN(R=Y%DF=Y%T=40%W=8200%O=MFFD7NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=
591 OS:O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD
592 OS:=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0
593 OS:%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1
594 OS:(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI
595 OS:=N%T=40%CD=S)
596
597 Uptime guess: 35.974 days (since Wed May 22 23:21:57 2024)
598 Network Distance: 0 hops
599 TCP Sequence Prediction: Difficulty=263 (Good luck!)
600 IP ID Sequence Generation: All zeros
601 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
602
603 NSE: Script Post-scanning.
604 Initiating NSE at 22:45
605 Completed NSE at 22:45, 0.00s elapsed
606 Initiating NSE at 22:45
607 Completed NSE at 22:45, 0.00s elapsed
608 Initiating NSE at 22:45
609 Completed NSE at 22:45, 0.00s elapsed
610 Read data files from: /usr/bin/../share/nmap
611 OS and Service detection performed. Please report any incorrect results at
    https://nmap.org/submit/ .
612 Nmap done: 256 IP addresses (6 hosts up) scanned in 226.44 seconds
613            Raw packets sent: 8944 (403.234KB) | Rcvd: 6510 (291.124KB)
614
```