CONFIABILIDADE E SEGURANÇA CIBERNÉTICA
(DACYS)
PL02
*Jorge Pinto Leite (**JPL**)*
*Pedro Sousa Rodrigues (**DCR**), Nuno Peralta* (**NSP**)
{@isep.ipp.pt}

Exercise 1: Port Scanning

With the entrypoints enumerated the attacker now needs to enumerate what ports are reachable from its position. This enumeration is paramount since not all services are HTTP and other vulnerable services might be exposed on different ports.

1. Explain how a **TCP handshake** [1] works.
2. How does the **NMAP SYN Connect Scan** [2] port scan work?
3. What is the difference between **TCP Full Connect Scan** and the **SYN Scan** (Stealth) scan?
4. What is an **ICMP Scan** (ping scan)?
5. Why a Windows 2019 Server doesn't show on an ICMP Scan NMAP Scan?
6. What is the role of a Firewall and how can it improve security at this attack stage?
7. How many ports exist on a TCP/IP computer stack?
8. Gather information regarding **Suricata** [3] (or other IDS/IPS solution). What is the role of an IDS/IPS system?
9. What is the difference between IDS and IPS?
10. Connect to the VPN provided by your instructor:
    - (i) What is the route pushed to your machine?
    - (ii) Perform a **TCP Scan** using NMAP.
        - (I) What machines were found?
        - (II) How many services did you find on each machine?
    - (iii) Redo the last scan, but now, without using the **ICMP alive check**. Why did the values change?
    - (iv) Perform a **UDP scan**.
        - (I) Why is it taking so long?
        - (II) How does the port enumeration works in this mode?

Exercise 2: Service Enumeration

Enumerated our targets we need to enumerate the service running on their ports. Not always is a service running on the default port. An administrator can change the default port to obscure the exposure of a service. For instance, the default port for HTTP is TCP/80, however, you might find the same service on port TCP/5000, therefore it is essential to optimize our scan to determine what service is running on each port.

1. Perform a scan with **banner-grabbing** capabilities using NMAP. What changed?
2. What services exist? Describe them and their purpose.
3. Did you find the flag (format: **flag{TEXT}**)?

Exercise 3: Scripting

After identifying the service itself, NMAP gives you additional capabilities to detect vulnerabilities using scripts readily available. This method is helpful in a first engagement to gather information on potentially vulnerable services to be exploited at a first glance of the infrastructure.

1. Perform a scan with the scripting engine enabled. What are the defaults? Why not all scripts run?
2. Run a bruteforce on the FTP service using the RockYou wordlist [4]. What is the password? Hint: use **root** as the username.
3. Enumerate the found share. What is the **flag** presented in it? What does the trailing "$" represents on the SMB protocol?

References

[1] RFCs.io, “Tcp rfcs.” [Online]. Available: https://rfcs.io/tcp

[2] G. Lyon, “Port scanning techniques: Nmap network scanning.” [Online]. Available: https://nmap.org/book/man-port-scanning-techniques.html

[3] “Suricata.io,” Aug 2022. [Online]. Available: https://suricata.io/

[4] “Rockyou,” Aug 2022. [Online]. Available: https://en.wikipedia.org/wiki/RockYou