CONFIABILIDADE E SEGURANÇA CIBERNÉTICA
(DACYS)
PL03
*Jorge Pinto Leite (**JPL**)*
*Pedro Sousa Rodrigues (**DCR**), Nuno Peralta* (**NSP**)
{@isep.ipp.pt}

Exercise 1: Vulnerability Scanning

Vulnerability Scanners provide a great deal of information. They are useful to gather information on large infrastructures regarding patching (using credential scans), or even exploitable services or misconfigurations (using non-credential scans). Focusing on the latter can provide a quick overview of the environment and help understand not only the attack surface but also how can an attacker gain a foothold into the organization.

1. Gather investigation on Vulnerability scanners such as Tenable [1] Nessus, Legion [2], and OpenVAS [3];
2. Scan the network using the Legion tool:
   (i) What tools did it run?
   (ii) What information could you collect using it?
   (iii) What attacks did it perform?
3. Install OpenVAS on your VM:
   (i) Scan the Lab Network (DO NOT scan other targets!);
   (ii) What information can you retrieve?
   (iii) If you were a malicious actor, what vulnerability would you choose to exploit and why?
   (iv) As a defender, how can you better protect yourself using this information? How would you prioritize to better protect your network?

Exercise 2: Metasploit

The time has come to exploit the service and start collecting data. One of the tools of the trade is Metasploit [4] [5]. You can use several exploits implemented in this framework to fully compromise a system.

1. Use Metasploit to compromise a service in the LAB environment;
2. What is Meterpreter and what advantages and disadvantages it offers?
3. What is the difference between a Reverse Shell, and a Bind shell?

Exercise 3: Pivoting

After getting a foothold into the infrastructure you might find some service that allows you to pivot even further on the network. An attacker will use pivoting to move laterally and reach new servers and services.

1. Perform pivoting on the Squid Server using proxychains [6] and Nmap;
2. Perform pivoting using a Meterpreter shell on a compromised host;
3. Repeat the pivoting using the SSH service;
4. Did you discover a new service? What is the secret flag?

References

[1] “Nessus vulnerability assessment: Nessus®.” [Online]. Available: https://www.tenable.com/products/nessus

[2] Govanguard, “Legion,” Dec 2018. [Online]. Available: https://github.com/GoVanguard/legion

[3] “Greenbone openvas.” [Online]. Available: https://openvas.org/

[4] “Penetration testing software, pen testing security.” [Online]. Available: https://www.metasploit.com/

[5] “Metasploit unleashed.” [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/

[6] Haad, “Haad/proxychains: Proxychains - a tool that forces any tcp connection made by any given application to follow through proxy like tor or any other socks4, socks5 or http(s) proxy. supported auth-types: ”user/pass” for socks4/5, ”basic” for http.” [Online]. Available: https://github.com/haad/proxychains