Advanced Network Security

Lab 2 – Reconnaissance

Overview

Reconnaissance is the first phase of attacking a network. The aim of reconnaissance is to identify information that may aid the exploitation of a system. At a non-technical level awareness of how members of an organisation communicate or interact is useful for phishing attacks.

At a basic level an organisation may not wish to publish the contact details or CEO's or directors, however if we consider the logical approach to assigning email address and telephone numbers, we may be able to infer this information.

At a technical level we can also infer information about an organisation's security posture or the OS version and patch level of machines by carrying out reconnaissance. In this tutorial you will be introduced to port scanners. Port scanners provide information about which ports are open on machines and correlate this information along with information about the timing of responses to infer which OS is being used on a host. Once a vulnerability has identified the OS version, they can identify vulnerabilities and determine if exploits exist.

Tips, Tricks & Terminology

- VM is short hand for virtual machine
- The password for Kali is root backwards ("toor")

Task 1 – Deployment and documentation

1. Deploy the virtual infrastructure from lab session 1, document the process thoroughly as this is part of the assignment. Document the reasons you are deploying your penetration testing platform on virtual infrastructure, taking the security of the university network into account. Assign 4GB of RAM to the Kali VM as this tutorial requires more RAM than the previous tutorial.

Task 2 – Basic Reconnaissance

1. Research the TCP handshake online, and become familiar with the process, it is of crucial importance to your understanding of port scanning.
2. Read the man pages for nmap, use the command "man nmap" to view the pages
3. Review the nmap documentation https://nmap.org/book/man.html, become familiar with the various scanning techniques, and pay particular attention to SYN scans.
4. Research & document how the TCP handshake is misused by port scanners to identify open ports. This research is required as part of the portfolio.
5. Use nmap on your Kali VM to scan the Metasploitable VM using each of the following scan types, document the strengths and weakness of each approach and describe the results: a. TCP connect()
    b. TCP SYN
    c. TCP FIN
6. Use nmap to perform OS detection and record the results

7. Use Zenmap to accomplish the above tasks, document the results and include screen captures.

Task 2 – Introduction to Metasploitable

1. Metasploitable is a framework used to identify and exploit vulnerable hosts. Review the information gathering section of the Metasploitable website:
   - https://www.offensive-security.com/metasploit-unleashed/information-gathering/
2. Carry out port scanning against the Metasploitable VM using the information from the metasploit website:
   - https://www.offensive-security.com/metasploit-unleashed/port-scanning/
3. Use the SMB scanner to identify which OS the target system is running, use the information from the following link:
   - https://www.offensive-security.com/metasploit-unleashed/scanner-smb-auxiliary-modules/
4. From the nmap results we know that the target is running an FTP server, if we can determine more information about the server, we may be able to exploit it. Review the information at the link below, determine name and version of the FTP server running on the target.
   - https://www.offensive-security.com/metasploit-unleashed/scanner-ftp-auxiliary-modules/
5. Document each of the sub tasks for your portfolio.

Task 3 – Wireshark Reconnaissance

1. Load Wireshark on the Kali VM.
2. Select Captures -> Interfaces
3. Start capturing data on eth0
4. Run a TCP SYN port scan from Kali using any of the tools from the previous tasks.
5. Stop the capture in Wireshark and analyse the packet capture you have created:
6. Can you identify the port scan taking place?
7. Describe how you identified the attack, referring to the TCP handshake

8. Review the documentation on Wireshark filters from the link below and conduct your own research on filtering. Then use Wireshark to filter the capture to show open ports.

- https://wiki.wireshark.org/CaptureFilters

Extended Task

1. Explore the reconnaissance, information gathering & vulnerability scanning tools Kali has to offer e.g Sparta, Armitage, etc . Use one or more of the tools to gather information about the target machine. Document the process as part of your assignment. It is probably best to run through the process once before trying to document it.