Quick Start Cybersecurity Bootcamp

Project C – Ethical Hacking

Scenario

After successfully installing a network upgrade for your company's client, you have been asked to perform another cybersecurity service for that client. The client hired a consultant to install and configure a new server in their internal network to support production and operations. You are tasked with determining the vulnerabilities of the new Production server and provide specific examples of how any vulnerabilities could be exploited. You are also asked to perform the same service on the Webserver in their DMZ.

Project Tasks

A network diagram is attached to this document showing the installation of the new Production server. Use this as a guide for completing this project, and feel free to use it in your presentation if you wish. This project adds to the VirtualBox network you created in Project A. If you removed that network, you will be responsible for restoring it to full functionality.

By successfully completing this project, you will have demonstrated your ability to scan a computer for vulnerabilities, analyze those vulnerabilities for exploitability, execute exploits against a target computer, and create persistence.

Project tasks are as follows:

1. Install the supplied Production server VM into the Trusted network in VirtualBox.
2. Use tools within Kali Linux to enumerate possible vulnerabilities on the Production server.
3. Use tools within Kali Linux to enumerate possible vulnerabilities on the Web server.
4. Exploit at least 2 vulnerabilities on the Production server, one of which must give you root access to the server.
5. Exploit at least 2 vulnerabilities on the Web server, one of which must give you root access to the server.
6. Create your own account on the Production server that has root permissions
7. Look for any interesting files on the Production and Web servers
8. Bonus: crack the passwords for the users configured on the Production server
9. Provide recommendations to improve server security

Questions/Answers

Exam Questions

1. What specific tools and commands did you use to discover vulnerabilities of the servers?
   a) Nmap -A -T4 192.168.0.18 for services on hosts (non-credentialed)
   b) Nmap 10.200.0.9/32 for all host on network range (non-credentialed)
   c) Nessus to enumerate entire network and hosts (yet to complete)
2. List 4 vulnerabilities you found on the servers.
   a) VNC TCP/port 5900
   b) NetBIOS (metasploitable)
   c) Shell (CVE 9.3) CVE -2012-1527/1528
   d) Blindshell (metasploitable) TCP/ port 1524
   e) SMTP (metasploitable) TCP/port 25
   f) http TCP/port 80 (metasploitable)
3. What specific tools did you use to exploit the vulnerabilities?
   a) Metasploit
4. How did you prove you had root access to the servers?
   a) whoami
5. Describe the risk associated with an attacker using an exploit to gain root access.
   a) An attacker can easily create a user id/password with escalated admin privileges which can use to hack into the system, down sensitive documents or install backdoor rootkit or even keylogger malware to gather key struck.

6. Why did you create your own account on the server?

   a) To continually have access to the system even if the vulnerability is found and patched. This way I can launch a continuous persistent attack on the production server, thereby compromising the organization's services.

7. Describe any interesting files you found on the servers.
   a) Lost + Found file is the largest file with only 2 root users.

8. What is meant by the phrase "covering your tracks"?

   a) It means hacking into a system covertly without leaving fingerprints or erasing evidence of your presence in a system.

9. Provide some recommendations for improving security on the servers.

   a) Closing the VNC service, closing unused ports, running frequently run vulnerability assessments and patch software while updating the firewall too.

10. How would you financially gain from using such exploits on a server?

    a) Become a Pen Tester to help companies discover vulnerabilities in their systems so as to patch them earlier before the Blackhat hackers find them which could be financially and reputationally damaging to the company.