QuickStart

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

## Deliverables

To successfully complete this project, you must perform the following:

1. Complete all project tasks.
2. Answer the 10 exam questions in written form and submit to your coach.

3. Provide an executive presentation to your coach via Zoom. The presentation will be done using PowerPoint (or similar product), followed by a live demonstration of your working network. The PowerPoint presentation must have a design of your choice and have at least 7 slides to include:
    a. Executive Summary at beginning
    b. Description of vulnerabilities found
    c. Exploits conducted
    d. Recommendations and closing remarks at the end

Project Grading

The project is worth 100 points. A passing grade is 70 or more points. Points are distributed as follows:

- Discovery of vulnerabilities – 30 pts
- Successful exploitation of vulnerabilities – 30 pts
- Written exam answers – 20 pts
- Presentation development – 10 pts
- Presentation execution – 10 pts
- Cracking passwords (bonus) – 10 pts

Exam Questions

1. What specific tools and commands did you use to discover vulnerabilities of the servers?
2. List 4 vulnerabilities you found on the servers.
3. What specific tools did you use to exploit the vulnerabilities?
4. How did you prove you had root access to the servers?
5. Describe the risk associated with an attacker using an exploit to gain root access.
6. Why did you create your own account on the server?
7. Describe any interesting files you found on the servers.
8. What is meant by the phrase “covering your tracks”?
9. Provide some recommendations for improving security on the servers.
10. How would **you** financially gain from using such exploits on a server?

Project Accounts

| System | Username | Password |
|---|---|---|
| Production Server | msfadmin | msfadmin |
| Router-FW | admin | pfsense |
| DNS Server | root | password |
| Web Server | admin<br>root | $eclab!2<br>$eclab!3 |
| CEO PC | user<br>root | $eclab!2<br>$eclab!3 |

Project C
Network Diagram