QuickStart

Cybersecurity Bootcamp

Project D – Cybersecurity Analyst

Scenario

Based upon your previous work with your client, they have asked you to improve the security of their network. They specifically wish to implement a way to identify and log attacks against their web and production servers. After some research, you decide that installing an IDS/IPS would meet their needs.

Project Tasks

By successfully completing this project, you will have demonstrated your understanding of firewalls and your ability to install and configure an IDS/IPS.

Project tasks are as follows:

1. Download and install Snort on the pfSense firewall.
2. Configure Snort to log suspicious activity on the Untrusted and DMZ interfaces.
3. Configure Snort to alert to the types of exploits you performed in the previous ethical hacking project.
4. Create firewall rules to block FTP traffic from the Untrusted network to the DMZ

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 solutions. 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. Description of how you used Snort.
    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:

- Successful installation of Snort – 20 pts
- Configuration of Snort – 20 pts
- Creation of firewall rules – 20 pts
- Written exam answers – 20 pts
- Presentation development – 10 pts
- Presentation execution – 10 pts

Exam Questions

1. Write an example of a firewall rule that will allow only HTTPS traffic to enter the DMZ.
2. Write an example of a firewall rule that will block FTP traffic originating from the Untrusted network.
3. Does the order of rule placement in a firewall matter and if so, why?
4. Which Linux distribution is pfSense based on?
5. Which logs would be useful in monitoring traffic on the firewall and why?
6. How could you block users from accessing inappropriate websites?
7. How would you implement secure file transfer between the Trusted network and the web server in the DMZ?
8. Given that you have an IT administrator workstation with an address of 192.168.0.30/24, write an example of a firewall rule to allow only that workstation to access the webserver using HTTPS and FTPS.
9. What would you recommend to improve the security of the DMZ and the Trusted network, and why?
10. List and briefly describe 3 commercial IDS/IPS products you would recommend to a client.

Project Accounts

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

Project D
Network Diagram