



Department of
Bachelor of Computer Applications

Information Security & Mobile Applications – Section <A>

Ethical Hacking Fundamentals
Activity #01

LinkedIn Learning Certification Course
[Part-VII: Evading IDS, Firewalls, & Honeypots]

Subject Code: 19BCA4C02
Class: IInd Year IInd Semester

Submitted On:

23-12-2022

By:

Suman Garai
20BCAR0246

Signature

Faculty In-Charge:

Dr. Ajay Shriram
Khushwaha

A handwritten signature in blue ink, appearing to read 'Dr. Khushwaha', is written over a horizontal line.

Signature



Certificate

This is to certify that Mr./Ms. Suman Garai with USN 20BCAR0246 has satisfactorily completed the Activity I Part 1 LinkedIn Course Name: Evading IDS, Firewalls, & Honeypots Hours: 2 hours 12 minutes prescribed by Department of BCA, School of Computer Science & IT, Jain (Deemed-to-be-University), Bengaluru for the partial fulfilment of fifth semester BCA Degree Course in the year 2021-2022, and has secured _____ out of 10.

23-12-2022

Date of Submission

Signature of Student

A handwritten signature in blue ink, likely belonging to the Faculty In-Charge.

Signature of Faculty
In-Charge



JAIN
DEEMED-TO-BE UNIVERSITY

SCHOOL OF
COMPUTER
SCIENCE AND IT

Evaluation Criteria

Sr. No.	Criteria / Parameters	Total Marks	Marks Obtained
1	On-time submission Certification	05	
2	Certification of Completion	05	
3	Report (with Assessment Screenshots test attempted)	05	
4	Conclusion [Minimum one page without any kind of plagiarism]	10	
	TOTAL	25	
	CONVERT	10	

Table of Contents

Sl. No.	Title	Page No.
1	Introduction to the Course	5
2	Screenshots with name and section	6-8
3	Conclusion	9
4	Certificate	10

Introduction to the Course

While many cyber-attacks may start with social engineering, the actual breach occurs after the malware or an intruder has got inside the perimeter. Consequently, businesses place a lot of emphasis on using firewalls, intrusion detection systems, and sometimes Honeypots to protect the perimeter. In this course, he'll cover the major perimeter protection devices. I'll start by explaining and demonstrating the basics of firewall technology. We'll take a look at web application firewalls and API gateway threat mitigation solutions, and we'll learn about the carrier Honeypot and how operational security teams use security onion for intrusion detection and alerting. We'll then take a look at the evasion techniques used by malware and intruders, and we'll demonstrate some evasive attacks. This course teaches us about perimeter defences and how our adversaries evade them. The topics covered in this course are drawn from the Evading IDS, Firewalls, and Honeypots competency in the Certified Ethical Hacker (CEH) body of knowledge.

Learning objectives

- Applying the basics of the Windows Firewall
- Using advanced features in the Windows Firewall
- Reviewing firewall logs
- Linux iptables
- Setting up an iptables firewall
- Managing rules with Firewall Builder
- Setting up a Cisco PIX firewall
- Installing GNS3
- How web application firewalls protect web servers
- Protecting API services with the WS02 gateway
- Running the Cowrie honeypot
- Detecting intrusions with Security Onion

Screenshots

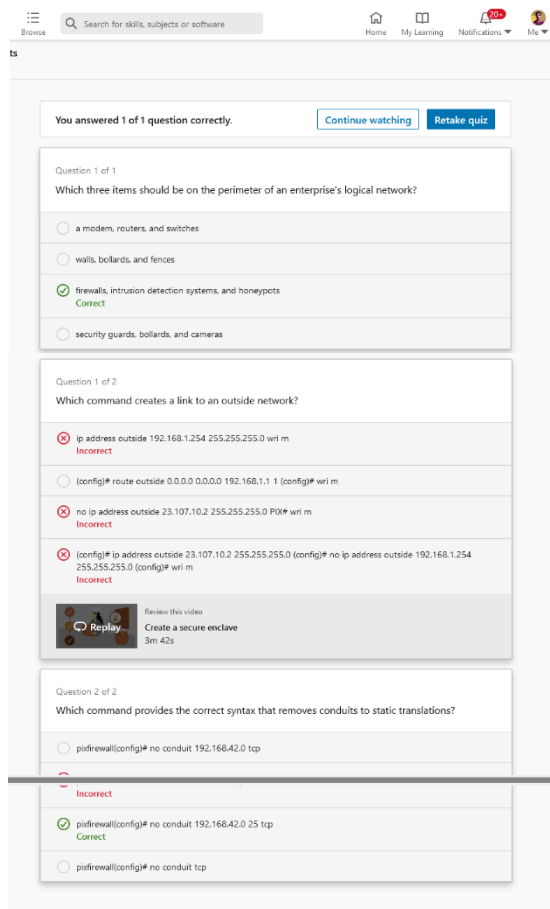


Figure: Section 01 – Firewall

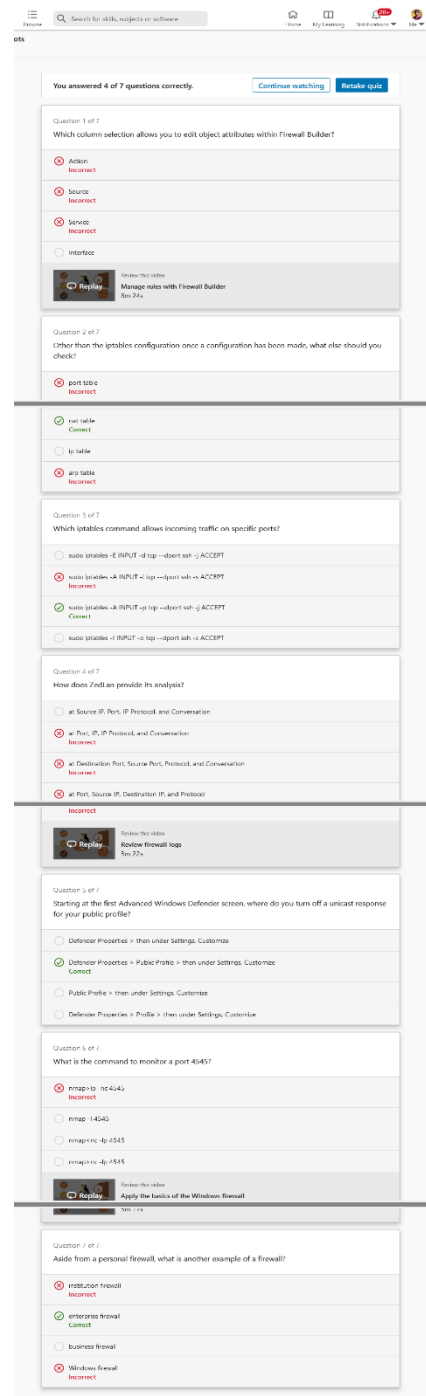


Figure: Section 02- Hardware Firewalls

ts


Search for skills, subjects or software

Home My Learning Notifications Me

You answered 2 of 4 questions correctly. [Continue watching](#) [Retake quiz](#)


Question 1 of 4
"User A" installed Kali on a VM housed in Windows Virtual PC and is trying to connect to GNS3, but is unable to do so. Why?

- ☐ The IP scheme for the network is not set up correctly.
- ☒ The firewall on the workstation with GNS3 is on. **Incorrect**
- ☐ Windows Virtual PC is not supported by GNS3.
- ☒ The GNS3 configuration is incorrect. **Incorrect**

 Review this video
Integrate Kali into GNS3
4m 46s

Question 2 of 4
What does the following configuration entry convert the key into?
jrichrton-mac~ john\$ cd .ssh
jrichrton-mac~ ssh\$ ssh-keygen -e -f id_rsa.pub

- ☐ SSH
- ☐ PKF format
- ☒ SSH2 **Incorrect**
- ☒ RSA **Incorrect**

 Review this video
Simulate the ASA firewall
6m 38s

Question 3 of 4
Here is part of the router configuration Miguel used: user:j someone nhash 1 0529575903696f2c492143375828267c7a760e1113734624452725707c0108065b Why isn't anything returned?

- ☒ He should not have nhash after his username. **Incorrect**
- ☐ He needs to reboot either the router or the switch.
- ☐ He forgot his password.
- ☒ His permission level is too low. **Correct**

Question 4 of 4
A switch has an IP of 192.168.10.25 on a /25 network. A host has an IP of 192.168.10.129, and the email server is 192.168.10.111. Why can't the host ping anything?

- ☒ The issue is the firewall on the host. **Incorrect**
- ☒ The host's IP is outside the IP range of the switch. **Correct**
- ☐ The switch's e5 port is shut down.
- ☒ The email server's IP is outside the IP range of the switch. **Incorrect**

Figure: Section 04 – Special Purpose Perimeter Devices

ots

Search for skills, subjects or software

Home My Learning Notifications Me

You answered 3 of 4 questions correctly. [Continue watching](#) [Retake quiz](#)

Question 1 of 4
Which file tells Cowrie the passwords to use?

- ☐ data/user.txt
- ☐ data/usedb.txt
- ☐ data/rootdb.txt
- ☒ data/userdb.txt **Correct**

Question 2 of 4
_____ is a type of honeypot.

- ☒ Honeycomb **Incorrect**
- ☒ Honeyrat **Correct**
- ☐ Medium Interaction
- ☐ Moderate Interaction

Question 3 of 4
What are the tiers for WSO2's API Cloud?

- ☒ Bronze, Silver, Gold **Correct**
- ☒ Unlimited, Gold, Silver, Bronze **Incorrect**
- ☐ Unauthorized, Authorized, Authentic
- ☐ Unlimited, 50PerMin, 20PerMin, 10PerMin

Question 4 of 4
Which protocol does a web application firewall monitor by default?

- ☒ TCP/IP **Incorrect**
- ☒ SHTTP **Incorrect**
- ☐ HTTP
- ☒ HTTPS **Incorrect**


 Review this video
Understand Web Application Firewalls
3m 50s

Figure: Section 05 – Protection from intrusion

Conclusion

Ethical hacking—testing to see if an organization's network is vulnerable to outside attacks—is a desired skill for many IT security professionals. In this course, cybersecurity expert prepares us to take our first steps into testing client defences. He provides us with an overview of firewall technology, detailing how firewalls work in both Windows and Linux, as well as how to set up a firewall simulation in a GNS3 network. Next, he goes over web application firewalls, API gateway threat mitigation solutions, and how to use honeypots to detect intruders. Finally, he covers the main ways to manage a suspected intrusion, including how to use the Security Onion intrusion detection system (IDS).

Certificate

