# Exam: Ops 401 Entrance Exam

**Due** Dec 17 at 11:59pm **Points** 25 **Questions** 25
**Available** after Dec 15 at 8am **Time Limit** None

## Instructions

Welcome to the Ops 401 Entrance Exam. Please read these instructions carefully.

- This is an individual test: you may NOT collaborate with others.
- A score of 80% or higher is required to pass the exam.
- As you prepare to take this test, think of it as a quiz covering all of the Ops 301 topics.
- You are not expected to solve these challenges just by looking over the choices.
- You are expected to use your professional tools and problem-solving skills to empirically find the answers.

## Attempt History

| | Attempt | Time | Score |
|---|---|---|---|
| **LATEST** | Attempt 1 | 42 minutes | 24 out of 25 |

ⓘ Correct answers are hidden.

Score for this quiz: **24** out of 25
Submitted Dec 15 at 12:52pm
This attempt took 42 minutes.

### Question 1 1 / 1 pts

You recently deployed a Linux-based web server on Rackspace cloud in order to host your company's ecommerce storefront site. The site runs BigCommerce. When you purchased the domain and web server from Rackspace, you did not purchase any additional security protection. Recently, Rackspace has been reporting a high volume of suspicious traffic to and from the site, affecting server performance. What security solution would best protect the web server?

- BGP
- Firewall
- Proxy
- Cloudflare

## Question 2

**1 / 1 pts**

A highly aggressive, politically-motivated DDoS attack is taking place against the web server your company hosts in the AWS cloud. After analyzing system logs, you determine the attacker is overwhelming the web server with HTTP GET requests from multiple bot systems. Banning the IP of individual bot systems is ineffective; the botnet computers can change IP addresses and resume the attack within minutes. Your contracted web administrator, Angela, is on the phone with you asking what type of DDoS

- "This appears to be a layer 7 attack, and we should implement a CAPTCHA challenge."
- "This appears to be a layer 3 attack, and we should implement a URL filter."

- "This appears to be a layer 2 attack, and we should implement a web application
- "This appears to be a layer 4 attack, and we should implement a proxy."

## Question 3

1 / 1 pts

You are the sysadmin for a company that utilizes Active Directory (AD) for identity management and pfSense for routing. Your security operations center (SOC) is dealing with a high volume of security alerts caused by wired endpoints utilizing your company's CAT6 ethernet wallports. Your manager is requesting stricter authentication processes around how

- [x] Require an additional factor of authentication, such as a Yubikey
- [ ] Minimize what wired network hosts are allowed to do on the network
- [x] Implement a captive portal referencing FreeRADIUS integrated with AD
- [ ] Reconfigure FreeRADIUS to generate more verbose system logs of user activities on

## Question 4

1 / 1 pts

Your WSUS server is throwing the error "Message ID 6703 - WSUS Synchronization Failed" and your attempts to access the WSUS administration website fails with HTTP Error 503. According to Microsoft documentation, what is the best action to take?

- Restart the Windows Server Update Service by accessing WSUSService.exe
- Increase the Private Memory Limit and restart the Application Pool
- Reseat network cables
- Reduce the Private Memory Limit and restart the Application Pool

## Question 5

**1 / 1 pts**

You've just executed the following operation on a Kali Linux system.

```
$ nmap -p21-100 10.0.2.8
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-23 18:17 PST
Nmap scan report for 10.0.2.8
Host is up (0.00057s latency).
Not shown: 98 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
```

Which of the below ports have been scanned by Nmap? Select ALL that apply.

- [ ] 123
- [x] 21

443

100

## Question 6

1 / 1 pts

When you arrive at the datacenter where you work, you find a HP Proliant DL360 G6 Server, configured with RAID-5, has a failed hard drive. The

- Replace the malfunctioning drive with a new drive, and allow the system to rebuild
- Replace the failed drive, re-create the array, and restore from a backup.
- Contact HP and open a ticket.
- Replace the all the drives in the array, and restore from backup.

## Question 7

1 / 1 pts

A manager at the retail store your MSP supports accidentally downloaded a worm by plugging in his Samsung Galaxy S7 phone into his office computer. What security solution would you recommend to your client to prevent future malware infections like this one?

- Implement a URL filter, such as Trend Micro Worry-Free Business.

- Implement an endpoint antimalware agent, like Windows Defender
- Implement a DLP solution, such as Symantec Data Loss Prevention.
- Implement a USB firewall antimalware filter, such as Sonicwall USB4600 Deep

## Question 8

1 / 1 pts

Python method walk() generates the file names in a directory tree by "walking" the tree. The script below, intended to be a standalone executable, attempts to perform a bottom-to-top traversal of the directory tree, but it's incorrectly written.

```
for root, dirs, files in os.walk(".", topdown=True):
  for name in files:
    print(os.path.join(root, name))
  for name in dirs:
    print(os.path.join(root, name))
```

- [ ] Add `followlinks=True`
- [x] Add `#!/usr/bin/python` to the top of the script
- [x] Change the `topdown` setting from `True` to `False`
- [x] Add `import os`

## Question 9

1 / 1 pts

You are deploying a private web server that will host an internal web app that is available over SSL-encrypted connections. The web server administrator will only need command line access. Assuming you are utilizing well-known ports, select ALL ports that should be opened.

- [x] 22
- [ ] 3389
- [x] 443
- [ ] 80

## Question 10

1 / 1 pts

Jamie works for a local electric power company as its network systems administrator. Jamie needs to separate IT from OT systems in order to mitigate security risks on the network. What commercial product would help with this?

- ( ) All of these methods conform to the immutability concept.
- ( ) AWS S3

Guardicore

Okta

Cisco SD-WAN

## Question 11

1 / 1 pts

Which network addressing scheme allows for the largest number of host addresses per subnet?

IPv4

MAC Addressing

VLAN Addressing

IPv6

## Question 12

1 / 1 pts

What layer of the OSI model does the NETGEAR GS105 belong to?

Layer 4

Layer 3

Layer 2

Layer 1

## Question 13

1 / 1 pts

Jamala would like to apply a uniform set of permissions for the directory ~/Documents and all it contains. The owner should be able to read, write, and execute; the group should be able to read and execute; and the user should only be able to read. What command should he execute from the Ubuntu Linux terminal?

chmod 754 ~/Documents

chmod -R 755 ~/Documents

chmod +r world ~/Documents

chmod -R 754 ~/Documents

Partial

## Question 14

0.5 / 1 pts

Which of the following might be handled by the DNS server configuration file? Select all that apply:

- [ ] To specify which server should handle email sent to the company's domain.
- [x] To store resource records for different services exposed via domain names.
- [ ] To configure network interfaces and IP addresses for the DNS server.
- [ ] To define the behavior and settings of the DNS server.
- [x] To allow zone transfers between DNS servers.

## Question 15

**1 / 1 pts**

A forest can have multiple domain controllers. In Gideon's environment, any AD changes in domain controller 1 (DC1) will automatically replicate to domain controller 2 (DC2). This morning, Gideon compared the two DC configurations and noticed that DC1 had failed to replicate a recent change to DC2. Looking at system logs, DC1 showed an error "Status 8451: The replication operation encountered a database error" around the time of the most recent AD change. Gideon reviewed internal documentation and noted

- ( ) Defragment the database on DC2
- ( ) Demote and repromote DC2

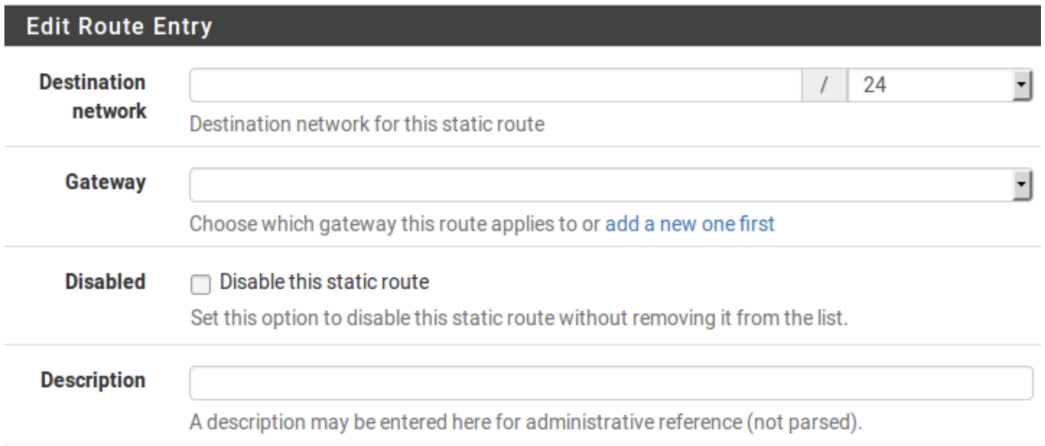
Demote and repromote DC1

Defragment the database on DC1

## Question 16

1 / 1 pts

You are configuring a new static route on a pfSense device (10.1.1.9), from it to another router (10.1.1.2), then to a subnet (192.168.2.0/24) behind the other router. What values should be entered in “Destination Network” and “Gateway?”


Destination Network: 10.1.1.2 Gateway: 10.1.1.9

Destination Network: 192.168.2.0 Gateway: 10.1.1.2

Destination Network: 10.1.1.2 Gateway: 192.168.2.0

Destination Network: 192.168.2.0 Gateway: 10.1.1.9

## Question 17

1 / 1 pts

Behold this powershell script:

```
$ServerList = Get-ADComputer -Filter * -Properties OperatingSystem, DnsHostNar
$MasterList = @()
foreach ($Server in $ServerList) {
    $MyObject = New-Object PSObject -Property @{
        ServerName = $Server.DnsHostName
        OS = (Get-CimInstance -ComputerName $Server.DnsHostName -ClassName '
        RAM = (Invoke-Command $Server.DnsHostName {(systeminfo | Select-String
        CFreeGB = (Invoke-Command $Server.DnsHostName {(Get-WmiObject win32
        CTotalGB = (Invoke-Command $Server.DnsHostName {(Get-WmiObject win3
    }
    $MasterList += $MyObject
}
$MasterList | Select ServerName, OS, RAM, CTotalGB, CFreeGB |
Export-csv C:\Users\$env:username\Desktop\ServerOverview.csv -NoTypeInform
```

What is accomplished by the line `$MasterList += $MyObject` ?

Append `$MasterList` to `$MyObject`

Overwrite `$MyObject` with `$MasterList`

Overwrite `$MasterList` with `$MyObject`

Append `$MyObject` to `$MasterList`

## Question 18

1 / 1 pts

Krysta's company has acquired a subsidiary, and she is evaluating the subsidiary's network configuration for the first time on the Sonicwall router/firewall appliance. What network segmentation technique is being used on the WLAN zone?

| Name | Zone | Group | IP Address | Subnet Mask | IP Assignment |
|---|---|---|---|---|---|
| X0 | LAN | | 10.150.253.1 | 255.255.255.0 | Static |
| X1 | WAN | Default LB Group | 173.240.215.253 | 255.255.255.0 | Static |
| X2 | N-Series | | 192.168.19.1 | 255.255.255.0 | Static |
| X3 | Unassigned | | 0.0.0.0 | 0.0.0.0 | N/A |
| X4 | WAN | | 10.254.254.6 | 255.255.255.252 | Static |
| X5 | WLAN | | 192.168.253.1 | 255.255.255.240 | Static |
| X5:V201 | WLAN Staff | | 192.168.253.129 | 255.255.255.192 | Static |
| X5:V202 | WLAN Guests | | 192.168.253.193 | 255.255.255.192 | Static |
| X6 | POS | | 192.168.253.97 | 255.255.255.224 | Static |
| X7 | IoT | | 192.168.253.65 | 255.255.255.224 | Static |

Physical subnetting

WLAN Guests

Airgap

VLAN

## Question 19

1 / 1 pts

Fernando's company manages identities on its computer systems using role-based access control. A month ago, he was transferred internally from Marketing Analyst to NOC Technician. Curious about how the company systems worked, he logged into a marketing department computer and was

Roaming profiles

Privilege creep

Identity duplication

Single sign-on

Partial

## Question 20

0.5 / 1 pts

Choose which of the following IPv4 addresses would be a part of the same subnet as 192.168.1.1/27. Only choose options that correctly explain why.

192.168.1.37 is part of the same subnet, because the subnet mask is

192.168.1.27 is part of the same subnet, because the first 27 bits of the binary representation of both 192.168.1.27 and 192.168.1.1 are identical.

192.168.1.27 is part of the same subnet, because the number after the / always

192.168.1.17 is part of the same subnet, because the subnet mask is 255.255.255.224.

## Question 21

1 / 1 pts

Determine the VPN tunnel configuration based on the pfSense system logs captured here.

| | | |
|---|---|---|
| Aug 27 21:30:29 | charon | 15[CFG] leftid=192.168.122.139 |
| Aug 27 21:30:29 | charon | 15[CFG] right=192.168.122.179 |
| Aug 27 21:30:29 | charon | 15[CFG] rightsubnet=192.168.2.0/24 |
| Aug 27 21:30:29 | charon | 15[CFG] rightauth=psk |
| Aug 27 21:30:29 | charon | 15[CFG] rightid=192.168.122.179 |
| Aug 27 21:30:29 | charon | 15[CFG] ike=aes128-sha256-modp2048! |
| Aug 27 21:30:29 | charon | 15[CFG] esp=aes256-sha256-modp2048,aes192-sha256-modp2048,aes128-sha256-modp2048,aes256gcm128-sha256-modp2048,aes256gcm96-sha256-modp2048,aes256gcm64-sha256-modp2048! |

Local Router IP: 192.168.122.179; Remote Router IP: 192.168.122.139; Mutual PSK; Phase 1 AES-128 SHA256

Local Router IP: 192.168.122.179; Remote Router IP: 192.168.122.139; Mutual RSA; Phase 1 AES-256 SHA256

Local Router IP: 192.168.122.139; Remote Router IP: 192.168.122.179; Mutual PSK; Phase 1 AES-128 SHA256

Local Router IP: 192.168.122.139; Remote Router IP: 192.168.122.179; Mutual PSK; Phase 1 AES-256 SHA256

## Question 22

**1 / 1 pts**

Darlene is a consultant who helps configure networks for small to mid-sized companies in her area. While performing a site survey of a new client, she accesses the web portal for the building's Fortinet FortiGate 60E Network Security/Firewall Appliance to assess its network configuration. The primary subnet is listed with CIDR notation of 172.168.1.1/16. Determine the network class, subnet mask, and provide a valid example IP address within this subnet's range.

Class B, subnet mask 255.255.0.0, example IP 172.168.1.55.

Class C, subnet mask 255.255.0.0, example IP 172.168.1.55.

Class C, subnet mask 255.255.255.0, example IP 172.167.1.55.

Class B, subnet mask 255.255.0.0, example IP 172.167.1.55.

## Question 23

1 / 1 pts

Why are hubs vulnerable to passive sniffing?

- All ports on a hub share a collision domain
- Hubs are more susceptible to arp flooding
- Hubs direct network traffic with a switching model
- All ports on a hub are enabled by default

## Question 24

1 / 1 pts

The new HP ProLiant server blade your team recently purchased warns that all its hard drive bays are not hot-swappable. What does this mean?

Hard drives cannot be safely removed or reinserted while the server is running

The hard drives are capable of being striped with parity in RAID

Hard drives can be safely removed or reinserted while the server is running

A hard drive can fail without the server going down (single-drive fault tolerance)

## Question 25

**1 / 1 pts**

While investigating complaints from network users that their web browsers are malfunctioning, you discover that your DNS server's forward lookup table has several new records for popular sites like google.com. What type of attack is most likely taking place?

DNS tunneling

Random Subdomain Attack

DNS spoofing

DNS flood attack

Quiz Score: **24** out of 25