PassQueen
a.k.a dumpsqueen.com

FCSS - Security Operations 7.4 Analyst

Fortinet FCSS_SOC_AN-7.4

Version Demo

Total Demo Questions: 4

Total Premium Questions: 45

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, FortiAnalyzer Deployment	1
Topic 2, FortiAnalyzer Administration	1
Topic 3, Logs and Reports	5
Topic 4, Event Management	31
Topic 5, FortiAnalyzer Fabric	5
Topic 6, Mix Questions	2
Total	45

QUESTION NO: 1

An investigation confirms that a cloud-service user account has been compromised. The account has active authenticated sessions, and the analyst must immediately limit the adversary's ability to continue using the account while preserving evidence for investigation.

Which two actions are appropriate containment actions? (Choose two.)

A. Disable the account or require a credential reset.

B. Revoke active sessions and authentication tokens.

C. Delete available audit evidence from the cloud service.

D. Restore unrelated systems from backup.

ANSWER: A B

Explanation:

Disabling the account or requiring a credential reset prevents continued authentication with the compromised credentials. Revoking active sessions and authentication tokens limits the adversary's ability to continue using already established access. Deleting available evidence impairs the investigation, while restoring unrelated systems does not contain the compromised cloud account.

QUESTION NO: 2

Which two statements about the FortiAnalyzer Fabric topology are true? (Choose two.)

A. Downstream collectors can forward logs to Fabric members.

B. Logging devices must be registered to the supervisor.

C. The supervisor uses an API to store logs, incidents, and events locally.

D. Fabric members must be in analyzer mode.

ANSWER: A D

Explanation:

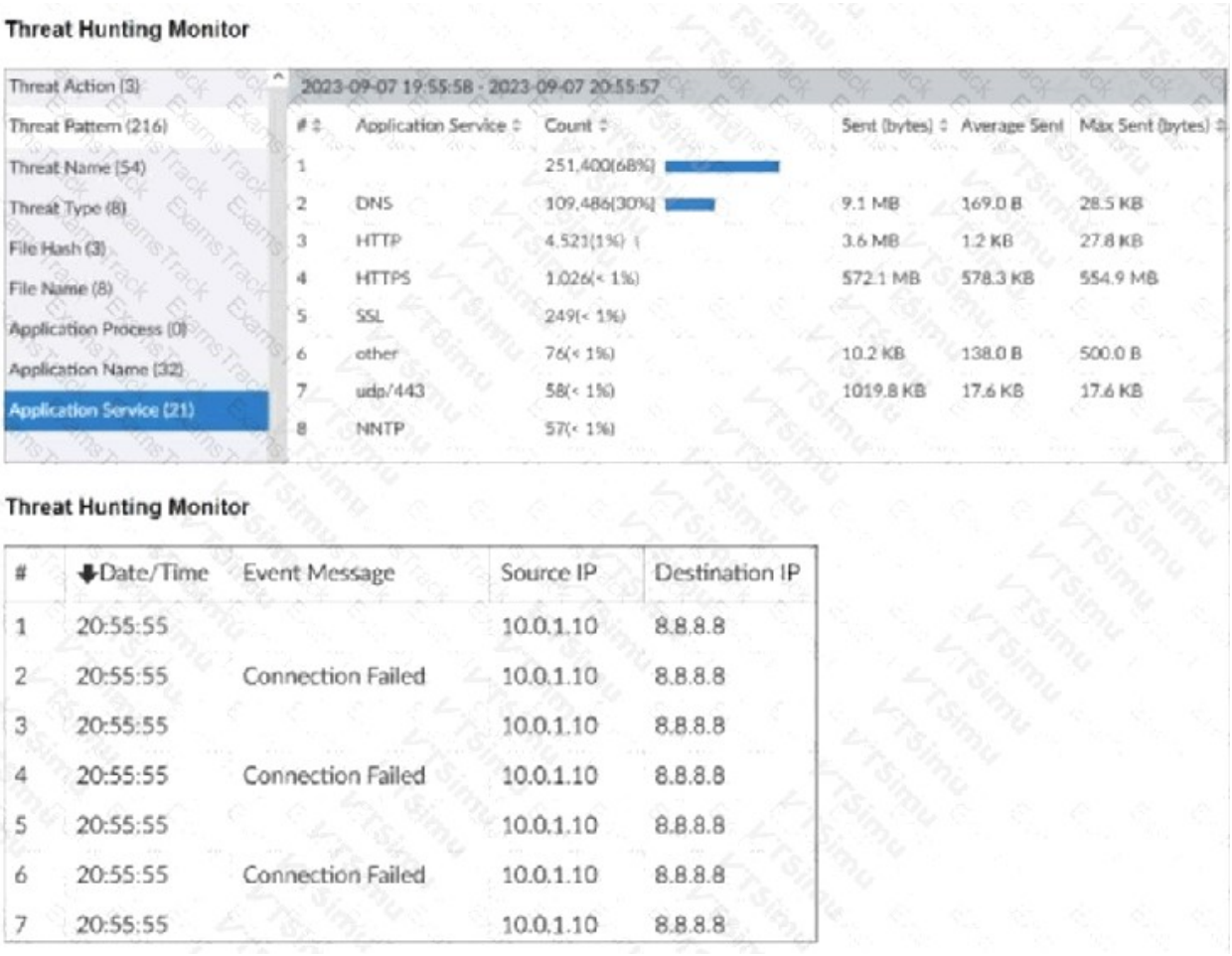
In a FortiAnalyzer Fabric deployment, downstream collectors can forward logs to Fabric members. This supports a scalable, distributed logging design: collectors accept log traffic from devices and relay the raw logs to an analyzer-tier FortiAnalyzer member, where the logs are indexed, retained, and made available for analysis. The Fabric architecture then allows the supervisor to provide centralized visibility and management across the distributed FortiAnalyzer environment without requiring every logging source to send directly to a single unit.

Fabric members must be in analyzer mode because the member role needs the local analytics and log-processing capabilities used by the Fabric. Analyzer-mode FortiAnalyzers can receive forwarded logs from collectors, maintain the log database, and provide the log, event, and incident information that is available through the Fabric's centralized workflow. This separation of collector and analyzer responsibilities enables organizations to scale log ingestion independently from log analysis and retention while maintaining a unified operational view.

Fortinet documents FortiAnalyzer deployment modes and centralized logging architecture in the FortiAnalyzer 7.4 Administration Guide. Additional FortiAnalyzer product and documentation resources are available from the Fortinet Documentation Library.

QUESTION NO: 3

Refer to the exhibits.



Threat Hunting Monitor

Threat Action (3)
Threat Pattern (216)
Threat Name (54)
Threat Type (8)
File Hash (3)
File Name (8)
Application Process (0)
Application Name (32)
Application Service (21)

2023-09-07 19:55:58 - 2023-09-07 20:55:57

#	Application Service	Count	Sent (bytes)	Average Sent	Max Sent (bytes)
1		251,400(68%)			
2	DNS	109,486(30%)	9.1 MB	169.0 B	28.5 KB
3	HTTP	4,521(1%)	3.6 MB	1.2 KB	27.8 KB
4	HTTPS	1,026(< 1%)	572.1 MB	578.3 KB	554.9 MB
5	SSL	249(< 1%)			
6	other	76(< 1%)	10.2 KB	138.0 B	500.0 B
7	udp/443	58(< 1%)	1019.8 KB	17.6 KB	17.6 KB
8	NNTP	57(< 1%)			

Threat Hunting Monitor

#	Date/Time	Event Message	Source IP	Destination IP
1	20:55:55		10.0.1.10	8.8.8.8
2	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
3	20:55:55		10.0.1.10	8.8.8.8
4	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
5	20:55:55		10.0.1.10	8.8.8.8
6	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
7	20:55:55		10.0.1.10	8.8.8.8

What can you conclude from analyzing the data using the threat hunting module?

A. Spearphishing is being used to elicit sensitive information.

B. DNS tunneling is being used to extract confidential data from the local network.

C. Reconnaissance is being used to gather victim identityinformation from the mail server.

D. FTP is being used as command-and-control (C&C) technique to mine for data.

ANSWER: B

Explanation:

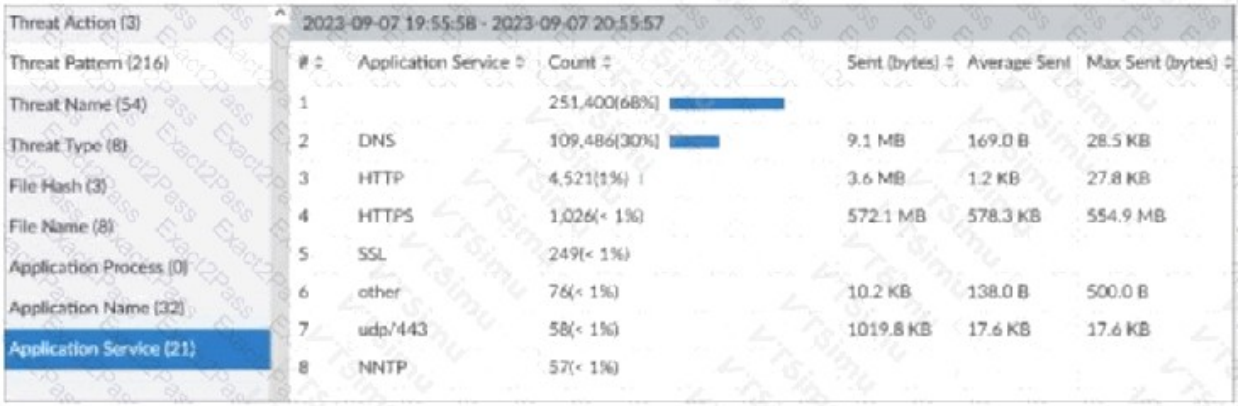
DNS tunneling is being used to extract confidential data from the local network. The threat-hunting data indicates an unusually large volume of DNS activity, including a very high DNS event count and substantial transmitted data. DNS normally carries relatively small query and response messages; a persistent pattern of high-volume DNS requests or unusually large DNS payloads is therefore an important hunting indicator. Attackers can encode data into DNS query names or other DNS fields and send those requests to an external DNS resolver or attacker-controlled authoritative domain. This enables data to leave the network while appearing to be ordinary DNS traffic.

The repeated activity involving the internal host and the public DNS address also supports investigation of DNS as the communication channel. In FortiAnalyzer threat hunting, analysts correlate application usage, byte counts, hosts, and connection events to identify outliers such as this host's abnormal DNS behavior. The observed DNS-centric pattern aligns with the MITRE ATT&CK technique *Application Layer Protocol: DNS*, which documents DNS as a protocol that adversaries can use for command-and-control communications and data transfer. Review the affected endpoint, its DNS query names, query lengths, request frequency, and the queried domains to validate the tunnel and scope the possible data exposure. See MITRE ATT&CK: Application Layer Protocol—DNS and FortiAnalyzer 7.4 documentation.

QUESTION NO: 4

Refer to the exhibits.

Threat Hunting Monitor



Threat Hunting Monitor

#	Date/Time	Event Message	Source IP	Destination IP
1	20:55:55		10.0.1.10	8.8.8.8
2	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
3	20:55:55		10.0.1.10	8.8.8.8
4	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
5	20:55:55		10.0.1.10	8.8.8.8
6	20:55:55	Connection Failed	10.0.1.10	8.8.8.8
7	20:55:55		10.0.1.10	8.8.8.8

What can you conclude from analyzing the data using the threat hunting module?

A. Spearphishing is being used to elicit sensitive information.

B. DNS tunneling is being used to extract confidential data from the local network.

C. Reconnaissance is being used to gather victim identity information from the mail server.

D. FTP is being used as command-and-control (C & C) technique to mine for data.

ANSWER: B

Explanation:

DNS tunneling is being used to extract confidential data from the local network. The threat-hunting results show an exceptionally large volume and count of DNS-related activity, including substantial outbound byte totals. This pattern is significant because normal DNS traffic generally consists of many small, short requests and responses. DNS tunneling instead encodes payload data into DNS query names or related DNS fields, allowing a host to move information through a protocol that is often permitted to leave the network.

The repeated activity associated with the internal source and external DNS destination adds useful context: the DNS service is being used in a way that warrants investigation as a possible covert communication or data-exfiltration channel. In a threat-hunting workflow, analysts correlate application usage, connection volume, byte statistics, source and destination addresses, and repetition over time to identify these deviations from an expected DNS baseline. The observed high-volume DNS behavior therefore supports the conclusion that confidential data may be leaving the local network through a DNS tunnel.

FortiAnalyzer provides threat-hunting and log-analysis capabilities for investigating anomalous traffic patterns and pivoting into relevant event details. See the FortiAnalyzer 7.4 Administration Guide and Fortinet's DNS tunneling overview.