



Cisco

642-544

Implementing Cisco Security Monitoring, Analysis and Response

Referring to the rule shown on the MARS GUI screen, which two of the following statements are correct?(Choose two.)

Rule Name:		System Rule: Backdoor, Connect-Dub02.04.15/0110410								Status:	Active	
Action:		None								Time Range:	04:14:30m	
Description:		This correlation rule detects a connection to a backdoor server or a response from a backdoor server in your network - there may or may not be any follow-up activity on the destination host. Backdoors (e.g. Rootkits, Trojan Horse programs) and commands shells provide extensive remote control of a host and may be left by an attacker on a compromised host to maintain future remote access.										
Offset	Open (Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	Close	Operation
1	<	ANY	\$TARGET01, ANY	ANY	Penetrate/Backdoor/Kernel/Connect, Penetrate/Backdoor/Trojan/Connect, Penetrate/Backdoor/Trojan/SYN, Penetrate/Backdoor/RemoteControlApp/Connect, Penetrate/Backdoor/CoincidentShell	ANY	None	ANY	ANY	1		FOLLOWED BY:
2		\$TARGET01, ANY	ANY	ANY	Penetrate/Backdoor/RemoteControlApp/Response, Penetrate/Backdoor/Trojan/Response, Penetrate/Backdoor/Trojan/SYN-ACK	ANY	None	ANY	ANY	1		OR
3		\$TARGET01, ANY	ANY	ANY	Penetrate/Backdoor/Trojan/Response, Penetrate/Backdoor/Trojan/SYN-ACK, Penetrate/Backdoor/RemoteControlApp/Response	ANY	None	ANY	ANY	1		

- A. This rule will fire if the offset 1 condition occurs "OR" if the offset 2 condition occurs.
- B. This rule will fire if the offset 3 condition occurs.
- C. The expressions between cells are "AND' while the expressions between items in the same cell are "OR".
- D. This is a user-defined rule.
- E. This rule can be deleted after changing its status to "inactive."

Answer: B, C

QUESTION: 42

Referring to the System Inspection Rule shown on the MARS GUI screen, which one of the following statements is correct?

Inspection Rules:

View: Inactive

Rule Name:		System Rule: Client Exploit - Mass Mailing Worm								Status:	Inactive	
Action:		None								Time Range:	04:02m	
Description:		This signature detects excessive amount of e-mail (at least 20/min) from a single host. To sharpen this rule for non-mail server hosts; create a group of mail server hosts and then create an exception by excluding these hosts in the source of this rule.										
Offset	Open (Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	Close	Operation
1		\$TARGET01, ANY	ANY	smtp (src port: ANY, dst port: 25, proto: UDP), smtp (src port: ANY, dst port: 25, proto: TCP), smtps (src port: ANY, dst port: 465, proto: TCP)	ANY	ANY	None	ANY	ANY	20		

- A. Click on "Add" to activate the rule.
- B. Click on "Activate" to activate the rule.
- C. Click on "Change Status" to activate the rule.
- D. Click on "Edit." Then you can apply and activate the rule.
- E. Click on "Duplicate" to archive the rule to a remote NAS.

Answer: C

QUESTION: 43

Referring to the diagram shown on the MARS GUI screen, why is the Push function not enabled (grayed out)?

Enforcement Device: HQ-FW-1 [a], Alternate

Default gateway: 172.30.1.1

Enforcement Device Information

Device	Type	Manager	Children	Log To	Collects From
HQ-FW-1 [a]	Cisco PIX 6.2	PN-MARS on demo3		PN-MARS on demo3	

Interface Information

Direction	IP Address	Interface Name	DNS Name	MAC Address	MAC Update Time
Inbound	10.33.10.2	inside	None / not found.	N/A	N/A
Outbound	192.168.1.1	DMZ-slot:1	None / not found.	N/A	N/A

Recommended Policies/Commands

access-list inside-acl
deny tcp host 10.1.1.10 host 192.168.1.10 eq 21

Or

access-list inside-acl
deny tcp host 10.1.1.10 any

Or

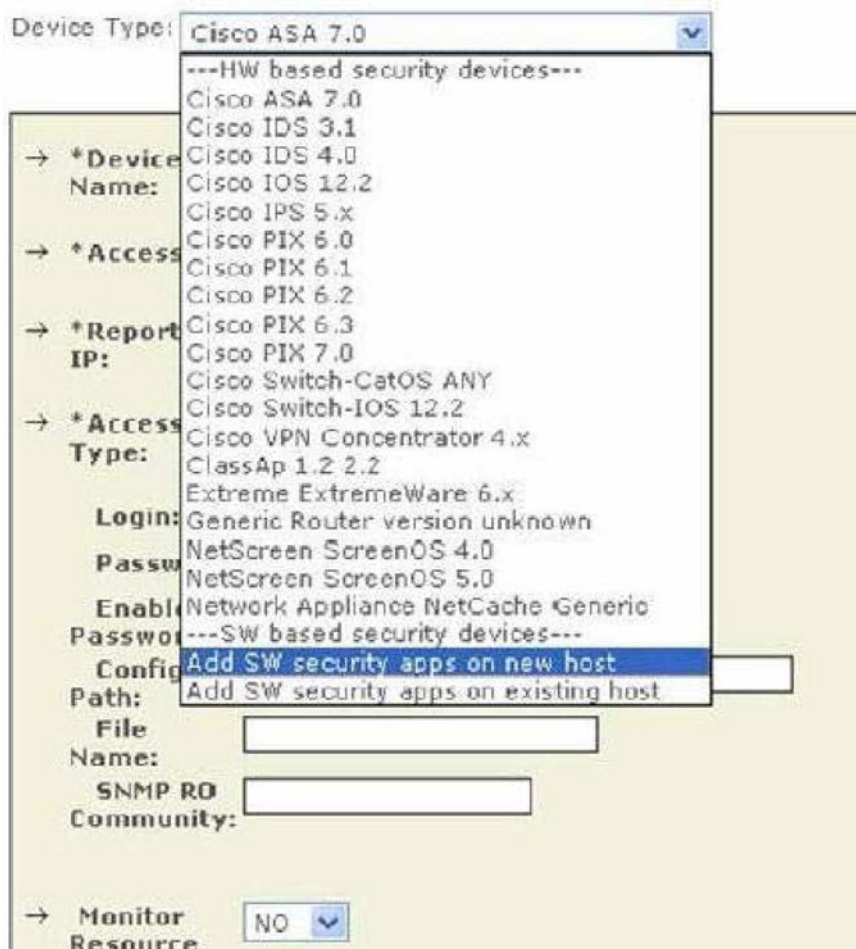
shun 10.1.1.10 192.168.1.10 4002 21 tcp

- A. Because the HQ-FW-1 device is the alternate choke point for mitigating this attack.
- B. Because MARS cannot push commands to Layer 3 devices.
- C. Because the Incident has not been confirmed by the administrator.
- D. Because the Incident is a false positive.
- E. Because MARS is operating at level 2 and not at level 3.
- F. Because the selected mitigation command is not supported on the HQ-FW-1 device.

Answer: B

QUESTION: 44

Which three of the following reporting devices can be added to the MARS appliance using the "Add SW security apps on new host?" (Choose three.)

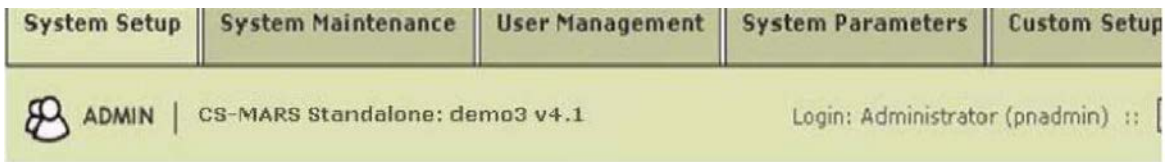


- A. Cisco ACS
- B. Netflow
- C. SNORT
- D. FWSM
- E. Generic web server.

Answer: A, C, E

QUESTION: 45

After manually adding the BR-FW-1 device shown in the MARS GUI screen, what additional steps do you need to perform?



Note:

1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * is denotes a required field.

Device Type: Cisco PIX 6.1

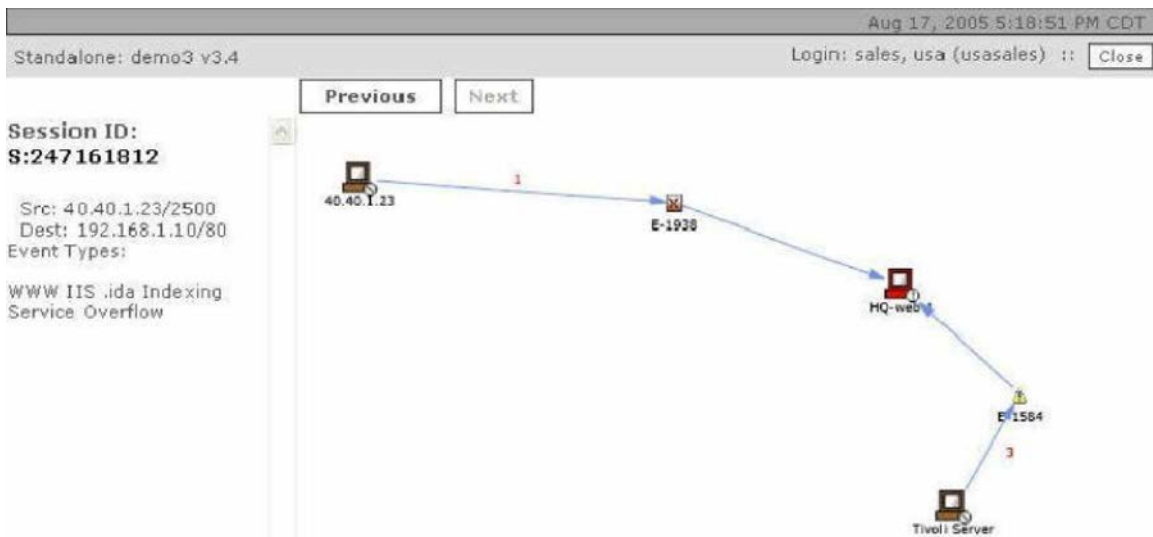
→ *Device Name:	<input type="text" value="BR-FW-1"/>
→ *Access IP:	<input type="text" value="10"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="8"/>
→ *Reporting IP:	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
→ *Access Type:	<input type="text" value="TELNET"/>
Login:	<input type="text"/>
Password:	<input type="text"/>
Enable Password:	<input type="text"/>
Config Path:	<input type="text" value="demoTopo"/>
File Name:	<input type="text" value="BR-FW-1.config"/>
SNMP RO Community:	<input type="text" value="criscnl"/>

- A. Click "Activate" to enable the device.
- B. Click "Submit" to enable the device.
- C. Click "Submit" to test access to the device. When access is successful, click "Activate" to activate the device.
- D. Click "Activate" to activate the device, then click "Submit" to save the device configuration.
- E. Click "Discover" to initiate manual discovery. When discovery is completed, click "Submit," then "Activate."

Answer: E

QUESTION: 46

Referring to the incident Vector Graph shown on the MARS GUI screen, which three of the following statements are correct? (Choose three.)



- A. The port being attacked is port 80.
- B. This incident has two associated Event Types.
- C. You can mitigate this attack by clicking on the device being attacked.
- D. The device being attacked is the Tivoli Server.
- E. Click the Previous button to view any other Sessions related to this incident.

Answer: A, B, E

QUESTION: 47

Referring to the Rule shown on the MARS GUI screen, what is used to determine that there is a sudden traffic increase to a particular port, and which type of attack is this Rule useful for detecting? (Choose two.)

Rule Name:		System Rule: Sudden Traffic Increase To Port				
Action:		None				
Description:		This rule detects scans statistically significant increase in traffic to a particular port.				
Offset	Open (Source IP	Destination IP	Service Name	Event	Device
1		ANY	ANY	ANY	Sudden increase of traffic to a port	ANY

- A. Real-time queries
- B. CSA logs
- C. Netflow data
- D. Smp polling
- E. DoS attacks
- F. Access attacks
- G. Reconnaissance attacks
- H. Denial of service attacks.

Answer: C, E

QUESTION: 48

To configure the MARS appliance to send out an alert when the system rule fires, what should you do from the MARS GUI screen shown?

<input checked="" type="checkbox"/>	Rule Name:	System Rule: Network Activity: Windows Popup Spam				
	Action:	None				
	Description:	This correlation detects excessive traffic (likely pop up spam) from the same source to the Windows Me				
Offset	Open (Source IP	Destination IP	Service Name	Event	
1		\$TARGET01, ANY ANY		MSMessengerService_UDP (src.port: ANY, dst.port: 1026-1029, proto: UDP)	ANY	

- A. Click on "Active" in the "Status" field, select the appropriate alerts, then apply.
- B. Click on "None" in the "Action" field, select the appropriate alerts, then apply.
- C. Click "Edit" to edit the "Operation" field of the rule, select the appropriate alert option(s), then apply.
- D. Click "Edit" to edit the "Event" field of the rule, select the appropriate alert option(s), then apply.
- E. Click "Edit" to edit the "Reported User" field of the rule, select the appropriate alert option(s), then apply.

Answer: B

QUESTION: 49

Referring to the incident shown on the MARS GUI screen, which two of the following statements are correct? (Choose two.)

Rule Name:	Nimda Rule						
Action:	None						
Description:	Rule to capture Nimda virus						
Offset	Open (Source IP	Destination IP	Service Name	Event	Device	Repc
1		ANY	ANY	ANY	Penetrate/Nimdaworm	ANY	None

Incident ID: 227269460

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time
1	S:236785492, I:227269459, I:227269460	IIS DOT DOT EXECUTE IIS Dot Dot Crash WWW WinNT cmd.exe Exec	10.1.5.2 2010	10.10.1.243 80	TCP	Aug 9, 2005
1		IIS CGI Double Decode WWW IIS Unicode Directory traversal IIS DOT DOT EXECUTE IIS Dot Dot Crash WWW WinNT cmd.exe Exec	Groups: 4, Total: 5			

- A. This is a low-severity incident.

- B. This is a false positive incident.
- C. There are multiple events that correlate to the 236785492 session.
- D. The 236785492 session is related to both the 227269459 and the 227269460 Incidents.
- E. The Nimda rule triggered both the 227269459 and the 227269460 Incidents.

Answer: C, D

Download Full Version From <https://www.certkillers.net>



DON'T KNOW
OR NO PREFERENCE

Pass your exam at First Attempt....Guaranteed!