IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

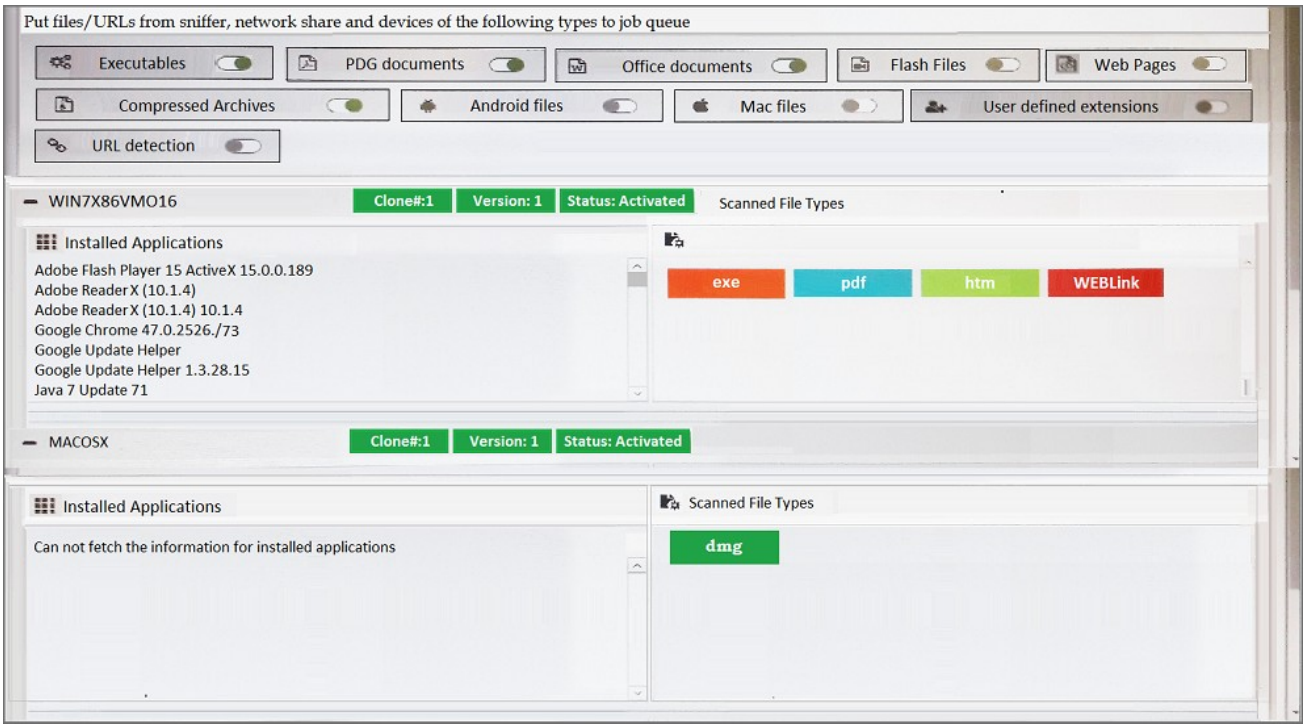
http://www.itrenzheng.com

Exam : **NSE7_ATP-2.5**

Title : Fortinet NSE 7 - Advanced Threat Protection 2.5

Version : DEMO

1.Examine the FortiSandbox Scan Profile configuration shown in the exhibit, and then answer the following question:



Based on the configuration, which of the following statements are true? (Choose two.)

A. PDF files will be inspected in the WIN7X86VM)16 VM.

B. URLs submitted using JSON API will not be inspected.

C. HTM files submitted using the management GUI will be inspected.

D. DMG files will be inspected in the MACOSX VM.

Answer: CD

2.Which samples can FortiClient submit to FortiSandbox for analysis? (Choose two.)

A. Downloads from emails

B. URLs from web requests

C. Command and control traffic

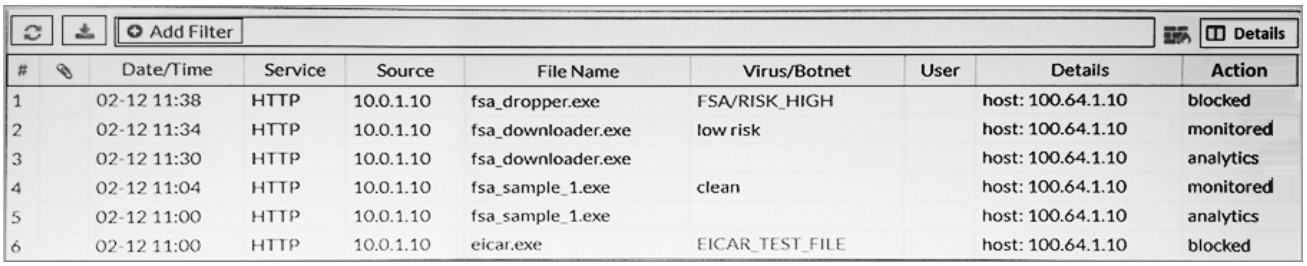
D. Files from removable storage

Answer: AD

Explanation:

FortiClient supports integration with FortiSandbox, including on-premise FortiSandbox appliances and FortiSandbox Cloud. When configured, FortiSandbox automatically scans files downloaded on the endpoint or from removable media attached to the endpoint or mapped network drives. FortiClient also automatically scans files downloaded with an email client on the endpoint or from the Internet. In each case, if the file is not detected locally, and FortiSandbox integration is configured, FortiClient sends the file to the FortiSandbox for further analysis. Endpoint users can also manually submit files to FortiSandbox for scanning. Reference:
https://docs.fortinet.com/document/forticlient/6.2.2/administration-guide/554226/sandboxdetection

3.Examine the FortiGate antivirus logs shown in the exhibit, than answer the following question:



Add Filter | Details

#	Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action
1	02-12 11:38	HTTP	10.0.1.10	fsa_dropper.exe	FSA/RISK_HIGH		host: 100.64.1.10	blocked
2	02-12 11:34	HTTP	10.0.1.10	fsa_downloader.exe	low risk		host: 100.64.1.10	monitored
3	02-12 11:30	HTTP	10.0.1.10	fsa_downloader.exe			host: 100.64.1.10	analytics
4	02-12 11:04	HTTP	10.0.1.10	fsa_sample_1.exe	clean		host: 100.64.1.10	monitored
5	02-12 11:00	HTTP	10.0.1.10	fsa_sample_1.exe			host: 100.64.1.10	analytics
6	02-12 11:00	HTTP	10.0.1.10	eicar.exe	EICAR_TEST_FILE		host: 100.64.1.10	blocked

Based on the logs shown, which of the following statements is correct? (Choose two.)
A. The fsa_dropper.exe file was blocked using a local black list entry.
B. The fsa_sample_1.exe file was not sent to FortiSandbox.
C. The eicar.exe file was blocked using a FortiGiard generated signature.
D. The fsa_downloader.exe file was not blocked by FortiGate.
Answer: CD

4.At which stage of the kill chain will an attacker use tools, such as nmap, ARIN, and banner grabbing, on the targeted organization's network?
A. Exploitation
B. Reconnaissance
C. Lateral movement
D. Weaponization
Answer: B

5.FortiGate root VDOM is authorized and configured to send suspicious files to FortiSandbox for inspection. The administrator creates a new VDOM, and then generates some traffic so that the new VDOM sends a file to FortiSandbox for the first time.
Which of the following is true regarding this scenario?
A. FortiSandbox will accept the file, but not inspect it until the administrator manually configures the new VDOM on FortiSandbox.
B. FortiSandbox will inspect all files based on the root VDOM authorization state and configuration.
C. FortiSandbox will accept the file, but not inspect it until the administrator manually authorizes the new VDOM on FortiSandbox.
D. By default, FortiSandbox will autoauthorize the new VDOM, and inspect files as they are received.
Answer: B