You suspect that someone has been trying to log into your server without permission. Which log file should you check to see if any recent login failures have been occurring on the server?

Application log

Security log

DNS log

System log

Answer: B

Explanation: The Security log will maintain a list of all the security-related events, such as successful and unsuccessful login attempts to the server. You can view this by opening the Security Log in the Event Manager.

-=-=-=-

You are using SNORT as an intrusion detection system for your network and have configured it to identify and alert on any packets that matches this specific pattern:

alert tcp $EXTERNAL\_NET any -> $HOME\_NET 139

flow:to\_server,established

content:"|eb2f 5feb 4a5e 89fb 893e 89f2|"

msg:"EXPLOIT x86 linux samba overflow"

reference:bugtraq,1816

reference:cve,CVE-1999-0811

classtype:attempted-admin

Which type of monitoring method are you relying upon?

Behavioral-based

Anomaly-based

Signature-based

Statistically-based

Answer: C

Explanation: SNORT is an open-source intrusion detection system. What is being shown in the question is an example of a SNORT signature that is used to detect any packets that are attempting to connect to the internal network from the external network over port 139 (NetBIOS). Now, none of that matters for this question though. What you should have been focused on was the fact that the question stated it would alert on any packet that “matches this specific pattern”, which classifies this as a signature-based detection method.

-=-=-=-

You have been hired to conduct an audit of a computer system. The organization is required to categorize your audit under a specific type of security control in order to issue the funding for your contract. What type of control should this audit be classified as?

Protective

Administrative

Detective

Corrective

Answer: C

Explanation: A computer security audit is considered a detective control since you are trying to uncover any misconfigurations, vulnerabilities, or issues in the network by conducting an audit of the existing policies, vulnerability scans, and have not hired on to conduct an incident response (which would be considered a corrective control).