Security Assessments

Network

The network is the element that connects all the computing systems together, carrying data between the systems and users.

Application

Applications are the software programs that perform data processing on the information in a system.

Being the operational element with respect to the data, as well as the typical means of interfacing between users and the data, applications are common targets of attackers.

Web Applications

Web applications are just applications that are accessible across the web.

All the details of standard applications still apply, but the placing of the system on the web adds additional burdens on the system to prevent unauthorized access and keep web-based risks under control.

Maneuver

Maneuver refers to the ability to move within a network.

Countering Maneuvers Mechanisms

Watch for traffic at chokepoints (that is, points where the unauthorized entity must pass)

Analyze the company's own network infrastructure, through the eyes of an attacker, and provide insight into how the network can be connected to provide better defenses against lateral movement, both in terms of connections and logging.

Advisories and Bulletins

They are published sets of information from partners, such as security vendors, industry groups, the government, information sharing groups, and other sources of "trusted" information.

These are external sources of threat feeds and need to be processed by security personnel to determine their applicability and how to use them to improve defenses for the enterprise.

Reviewing Configurations

System configurations play a significant role in system security.

Misconfigurations leave a system in a more vulnerable state, sometimes even causing security controls to be bypassed completely.

There are protocols and standards for measuring and validating configurations.

The Common Configuration Enumeration (CCE)

Common Platform Enumeration (CPE) guides

Part of the National Vulnerability Database (NVD) maintained by NIST

Common Vulnerabilities and Exposures (CVE)/ Common Vulnerability Scoring System (CVSS)

CVE

The Common Vulnerabilities and Exposures (CVE) enumeration is a list of known vulnerabilities in software systems.

Each vulnerability in the list has an identification number, description, and reference.

CVSS

The Common Vulnerability Scoring System (CVSS) is a scoring system to determine how risky a vulnerability can be to a system.

Ranges from 0 to 10. As the CVSS score increases, so does the severity of risk from the vulnerability.

Risk Rating	CVSS Score
Low	0.1–3.9
Medium	4.0–6.9
High	7.0–8.9
Critical	9.0–10

Exam Tips

Credentialed scans are more involved, requiring credentials and extra steps to log in to a system, whereas non-credentialed scans can be done more quickly across multiple machines using automation.

Credentialed scans can reveal additional information over non-credentialed scans.

When an intrusion detection system (IDS) does not generate an alert from a malware attack, this is a false negative.

Intelligence fusion is a process involving collecting and analyzing threat feeds from both internal and external sources on a large scale.

Maneuvering is also a defensive tactic used by security professionals to disrupt or prevent an attacker from moving laterally as part of the attack chain.

This is a highly tested item. A false positive occurs when expected or normal behavior is wrongly identified as malicious. The detection of a failed login followed by a successful login being labeled as malicious, when the activity was caused by a user making a mistake after recently changing their password, is an example of a false positive.

Threat Hunting

Threat hunting is the practice of proactively searching for cyber threats that are inside a network, yet remain undetected.

Cyber threat hunting uses tools, techniques, and procedures (TTPs) to uncover unauthorized actors in your network that have not been detected by your defenses.

If the attacker can get past that line of defense, they can hide in a network for months, if not years.

Attackers can use system resources to continue their presence, a technique known as "living off the land."

Indicators of attack (IOA) comprise a series of actions an attacker must accomplish to perform an attack. (i.e. creating an account, moving data off a network, etc..)

Indicators of compromise (IOCs) are artifacts left behind by the activities of an attacker. (i.e. IP address, files, etc..)

Threat hunters use these clues to focus on where an attacker has been, what they have done, and where they are likely to go next.

Threat Feeds

Sources of information concerning adversaries.

Can come from internal and external sources.

External sources of threat information come from various outside entities, and as a result they may or may not align with your particular environment.

Intelligence Fusion

Threat intelligence is the knowledge behind a threat's capabilities, infrastructure, motives, goals, and resources.

Threat intelligence fusion enables a defender to identify and contextualize the threats they face in the environment, using the information from threat intelligence allowing them to take better decisive actions to better protect the organization.

Vulnerability Scans

Vulnerability scanning is the process of examining services on computer systems for known vulnerabilities in software.

This is basically a simple process of determining the specific version of a software program and then looking up the known vulnerabilities.

Positives and Negatives

The choice of the terms positive and negative relate to the result of the test.

False Positive is when a normal action is marked as malicious.

False Negative is when a malicious action is marked as normal.

Log Reviews

A properly configured log system can provide tremendous insight into what has happened on a computer system.

The key is in proper configuration so that you capture the events you want without adding extraneous data.

Log reviews can provide information as to security incidents, policy violations (or attempted policy violations), and other abnormal conditions that require further analysis.

Credentialed vs. Non-Credentialed

Vulnerability scans can be perform

and without credentials

Non-Credentialed is the view of a

outsider on the network.

Credentialed vulnerability scans c

deeper into a host and return mor

accurate and critical risk informati

Frequently these scans are used t

First, a non-credentialed scan is p

across large network segments us

automated tools. Then, based on t

preliminary results, more detailed

credentialed scans are run on mac

with the most promise for vulnera

Intrusive vs. Non-Intrusive

Vulnerability scans can be intrusive or non-intrusive to the system being scanned.

A non-intrusive scan is typically a simple scan of open ports and services.

An intrusive scan attempts to leverage potential vulnerabilities through an explo

to demonstrate the vulnerabilities.