IT 413 MIDTERM REVIEWER

NETWORKING TECHNOLOGY

CSMA/CD

(Carrier Sense Multiple Access with Collisio

Penetration Testing

Exercise Types

Some organizations create competing teams to conduct penetration exercises that are longer than a penetration test.

For instance, in such a scenario, there can be three or four teams:
• The red team is the adversary, trying to attack the system while remaining unnoticed. • The
re the defenders, and they try to thwart the efforts of the red team. •
team that defines the goals and rules and oversees the exercise.
are less technical but possess knowledge about governance and
is the referee of this exercise.
purple team, where members of the red and blue team work together
d explore ways to improve controls.

Penetration Testing

Packet Analyzer

Packet analyzers, or packet sniffers, intercept, and log n

Packet analyzers, or packet sniffers, intercept, and log network traffic. They perform the below functions — either for legitimate purposes like troubleshooting or illegitimate purposes such as compromising data:

- Network problem analysis.
- Detection of network intrusion attempts.
- Isolation of exploited systems.
- Traffic logging.
- Detection of network misuse.

Network and Server Profiling

Network Anomaly Detection (Cont.)

- The figure illustrates a simplified version of an algorithm designed to detect an unusual condition at the border routers of an enterprise.

- For example, the cybersecurity analyst provided the following values: X = 5, Y = 100, Z = 30, N = 500
- Now, the algorithm can be interpreted as: every fifth minute, get a sampling of 1/100th of the flows during second thirty.
- If the number of flows is > 500, generate an alarm.
- If the number of flows is < 500, do nothing.

- This is a simple example of using a traffic profile to identify the potential for data loss.

- **Rule-based detection** analyzes decoded packets for attacks based on pre-defined patterns.

Common Vulnerability Scoring System (CVSS)

CVSS Base Metric Group

The figure highlights the Base Metric Group.

Common Vulnerability Scoring System (CVSS)

The CVSS Process (Cont.)

- After the Base Metric group is completed, the numeric severity rating is displayed, as shown in the figure.

- A vector string is also created that summarizes the choices made.
- If other metric groups are completed, those values are appended to the vector string.
- The string consists of the initial(s) for the metric, and an abbreviated value for the selected metric value separated by a colon.
- The metric-value pairs are separated by slashes.
- The vector strings allow the results of the assessment to be easily shared and compared.

Common Vulnerability Scoring System (CVSS) The CVSS Process (Cont.)

The key for the Base Metric group is:

Attack Vector AV [N, A, L, P] N = Network, A = Adjacent, L = Local, P = Physical Attack Complexity

AC [L, H] L = Low, H = High

Privileges Required High
PR [N, L, H] N = None, L = Low, H =

User Interaction UI [N, R] N = None, R = Required Scope S [U, C] U =

Unchanged, C = Changed

Confidentiality Impact None
C [H, L, N] H = High, L = Low, N =

Integrity Impact I [H, L, N] H = High, L = Low, N = None

Availability Impact A [H, L, N] H = High, L = Low, N = None

Common Vulnerability Scoring System (CVSS)

The CVSS Process (Cont.)

The values for the numeric severity rating string **CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N** are listed in the table:

Attack Vector, AV Network

Attack Complexity, AC Low

Privileges Required, PR High

User Interaction, UI None

Scope, S Unchanged

Confidentiality Impact, C Low

Integrity Impact, I Low

Availability Impact, A None

Common Vulnerability Scoring System (CVSS)

CVSS Reports

- The table shows the ranges of scores and the corresponding qualitative meaning.
- Frequently, the Base and Temporal metric group scores will be supplied to customers by the application or security vendor in whose product the vulnerability has been discovered.
- The affected organization completes the environmental metric group to tailor the vendor-supplied scoring to the local context.
- The resulting score serves to guide the affected organization in the allocation of resources to

address the vulnerability.

- The higher the severity rating, the greater the potential impact of an exploit and the greater the urgency in addressing the vulnerability. • While not as precise as the numeric CVSS scores, the qualitative labels are especially useful for communicating with stakeholders who are unable to relate to the numeric scores.
- In general, any vulnerability that exceeds 3.9 should be addressed.

None 0

Low 0.1 – 3.9 Medium 4.0 – 6.9 High 7.0 – 8.9 Critical 9.0 – 10.0

Secure Device Management

Asset Management

- It involves the implementation of systems that track the location and configuration of networked devices and software across an enterprise.
- As part of any security management plan, organizations must know what equipment accesses the network, where that equipment is within the enterprise and logically on the network, and what software and data those systems store or can access.
- Asset management not only tracks corporate assets and other authorized devices, but also can be used to identify devices that are not authorized on the network.
- NIST describes potential techniques and tools for operationalizing an asset management process: • Automated discovery and inventory of the actual state of devices
- Articulation of the desired state for those devices using policies, plans, and procedures in the organization's information security plan
- Identification of non-compliant authorized assets
- Remediation or acceptance of device state, iteration of desired state definition
- Repeat the process at regular intervals, or ongoing

Secure Device Management

Asset Management (Cont.)

- The figure provides an overview of this process.