Deploy security measures

Learning Activities

The following are the performance criteria:

- Physical control measures are implemented according to the ICT security policy
- Logical security control measures are implemented according to the ICT security policy
- ICT Security policy is implemented according to the Kenya security Act 2018

Trainees to demonstrate knowledge in relation to:

- Implement security measures contained in the ICT security policy
- Apply physical and logical risk mitigation measures
- Take corrective action
- Security audit to identify security gaps
- Generate system audit report

Information Sheet

Implement security measures contained in the ICT security policy:

- Identify your risks
- Learn from others
- Make sure the policy conforms to legal requirements
- Level of security equals to the level of risk
- Include staff in policy development
- Train your employees
- Get it in writing
- Set clear penalties and enforce them
- Update your staff
- Install the tools you need

Read: Successful ICT policy: https://www.computerworld.com/article/2572970/10-steps-to-a-successful-security-policy.html

Read: Kenya's ICT policy: http://icta.go.ke/national-ict-policy/

A **logical mitigation** strategy ties assets to threats to vulnerabilities to identify risks. Solutions for the identified risks typically enhance three facets of security: Policies, Procedures and Training; Physical/Electronic Security Systems; and Security Personnel.

Corrective action is a process of communicating with the employee to improve attendance, unacceptable behavior or performance. You may take corrective action when other methods such as coaching and performance management have not been successful.

The **network security audit** is a process that many managed security service providers (MSSPs) offer to their customers. In this process, the MSSP investigates the customer's cyber security policies and the assets on the network to identify any deficiencies that put the customer at risk of a security breach.

Self-Assessment

i. What is corrective action?

ii. Define network security audit?

iii. Review the computer lab and prepare a report if it conforms to the ICT Security Act 2018.

iv. Security levels should be _________ to risks involved.

A. Equal

B. Great

C. Appoximate

v. National security of Kenya is govern by ___________ .

A. ICT Authority

B. Police

C. Network of ICT

Tools, Equipment, Supplies and Materials

Firewall, Malware Protection, Software Updates, Audit and Accountability

References

- https://www.computerworld.com/article/2572970/10-steps-to-a-successful-security-policy.html
- https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/data-and-system-security-measures.html
- Cyber Security, authored by John G. Voeller published by Wiley 2014

Test system vulnerability

Learning Activities

The following are the performance criteria:

- Schedule system testing plan is developed
- Vulnerable levels of the system are identified
- Security ethical penetration is done as per the ICT security policy
- Report on system vulnerability is generated
- Corrective action is taken based on the System Vulnerability report

Trainees to demonstrate knowledge in relation to:

- Definition of vulnerability
- System testing schedule
- Levels of system vulnerability
- Ethical penetration
- System vulnerability test report

Information Sheet

Computer vulnerability is a cyber-security term that refers to a defect in a system that can leave it open to attack. This vulnerability could also refer to any type of weakness present in a computer itself, in a set of procedures, or in anything that allows information security to be exposed to a threat.

Level of system vulnerability Critical, High, Medium, and Low

Read: types of vulnerability: https://www.atlassian.com/trust/security/security-severity-levels

Severity Levels for Security Issues

Severity Framework and Rating

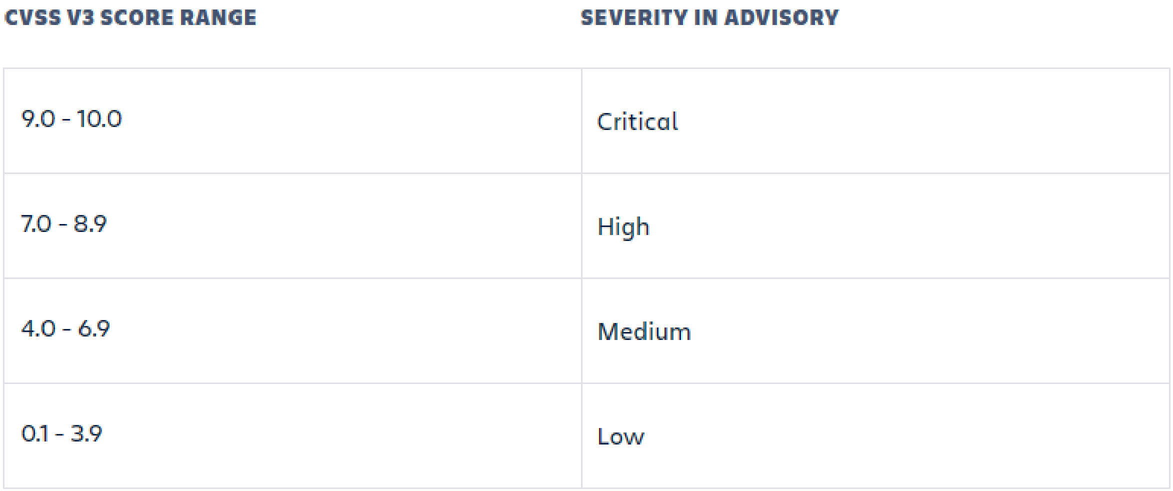
Common Vulnerability Scoring System (CVSS) is a method of assessing security risk and prioritization for each discovered vulnerability. CVSS is an industry standard vulnerability metric. You can learn more about CVSS at FIRST.org.

Severity Levels

Severity levels are based on a self-calculated CVSS score for each specific vulnerability.

- Critical
- High
- Medium
- Low

CVSS v3, uses the following severity rating system:

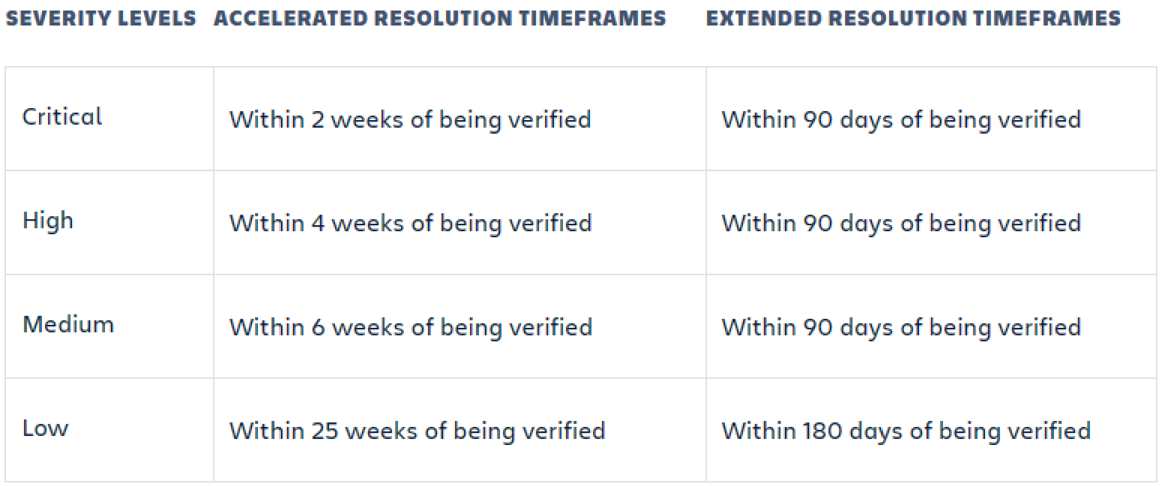


CVSS V3 SCORE RANGE	SEVERITY IN ADVISORY
9.0 - 10.0	Critical
7.0 - 8.9	High
4.0 - 6.9	Medium
0.1 - 3.9	Low

Remediation Timeline

Service level objectives for fixing security vulnerabilities are set based on the security severity level and the affected product.

CVSS Resolution Timeframe:



SEVERITY LEVELS	ACCELERATED RESOLUTION TIMEFRAMES	EXTENDED RESOLUTION TIMEFRAMES
Critical	Within 2 weeks of being verified	Within 90 days of being verified
High	Within 4 weeks of being verified	Within 90 days of being verified
Medium	Within 6 weeks of being verified	Within 90 days of being verified
Low	Within 25 weeks of being verified	Within 180 days of being verified

A **System test schedule** includes the testing steps or tasks, the target start and end dates, and responsibilities. It should also describe how the test will be reviewed, tracked, and approved.

Ethical penetration is a broader term that includes all hacking methods, and other related cyber-attack methods. The goal of ethical hacking is still to identify vulnerabilities and fix them before criminals can exploit them, but the approach is much wider in scope than simple testing. In other words, ethical hacking is more of an umbrella term, while penetration testing represents one subset of all ethical hacking techniques.

Watch: Ethical penetration: https://youtu.be/BEdaiUzUsgM

Ethical Hacker or Penetration Tester: What is the difference?

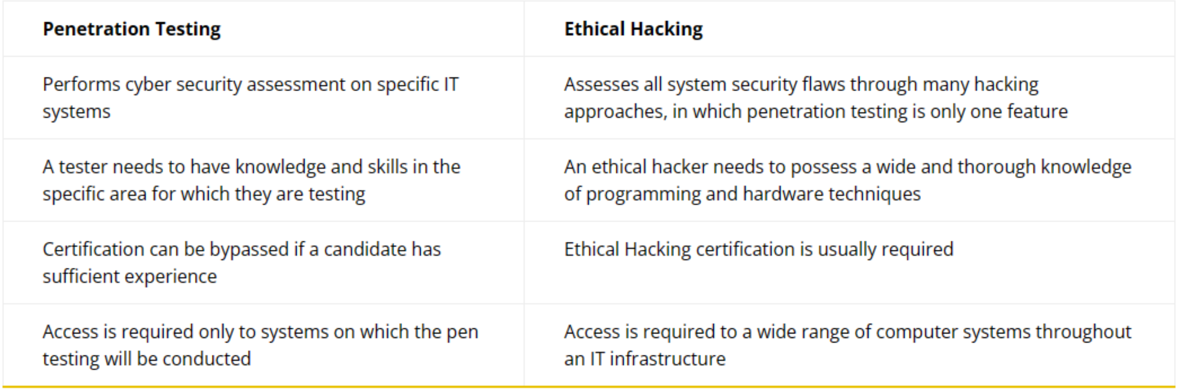
Penetration testing is a process, which identifies security vulnerabilities, flaws risks, and unreliable environments. It can be seen as a way to successfully penetrate a specific information system without causing any damage. It essentially mimics what cyber criminals would attempt, and anticipates how the system could be compromised.

Organizations conduct pen tests to strengthen their corporate defence systems. This includes all computer systems and associated infrastructure. While penetration testing can help organizations improve their cybersecurity, it is best to be proactive before trouble arises. Pen testing should be performed on a regular basis, since cyber criminals are constantly finding new weak points in emerging systems, programs, and applications. A pen test may not provide comprehensive security answers for your corporation; it will significantly minimize the possibility of a successful attack.

Ethical hacking is a broader term that includes all hacking methods, and other related cyber-attack methods. The goal of ethical hacking is still to identify vulnerabilities and fix them before criminals can exploit them, but the approach is much wider in scope than pen testing. In other words, ethical hacking is more of an umbrella term, while penetration testing represents one subset of all ethical hacking techniques.

Some people disagree with hacking being considered "ethical," even if the approach is used to proactively identify and fix corporate security flaws. Still, the term "ethical hacker" is growing in popularity, as cybersecurity is becoming more and more crucial for organizations. In addition, the demand for job candidates with cyber security certifications is growing significantly.

Here is a quick summary of the difference between Penetration Testing and Ethical Hacking:



Penetration Testing	Ethical Hacking
Performs cyber security assessment on specific IT systems	Assesses all system security flaws through many hacking approaches, in which penetration testing is only one feature
A tester needs to have knowledge and skills in the specific area for which they are testing	An ethical hacker needs to possess a wide and thorough knowledge of programming and hardware techniques
Certification can be bypassed if a candidate has sufficient experience	Ethical Hacking certification is usually required
Access is required only to systems on which the pen testing will be conducted	Access is required to a wide range of computer systems throughout an IT infrastructure

A **vulnerability report** is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

Self-Assessment

i. What is ethical penetration?

ii. Define computer vulnerability.

iii. Explain level system vulnerability.

iv. Identify the vulnerability levels of a system. Prepare a case study using an example.

v. Prepare report at a worksite on the security system on their computers and network.

vi. ________ is a broader term that includes all hacking methods, and other related cyber attack methods.

A. Vulnerability

B. Ethical penetration

C. A System test schedule

vii. When is it better to perform a vulnerability assessment versus a penetration test?

A. It is necessary to perform them together

B. When you seek a larger overview of the environment, versus a smaller view

C. Penetration tests are full of false positives and should not be used

D. Penetration tests are potentially damaging to devices and should not be used

viii. ____________ is a weakness that can be exploited by attackers.

A. System with virus

B. System without firewall

C. System with vulnerabilities

D. System with strong password

Tools, Equipment, Supplies and Materials

Wireshark, Nmap, Metasploit, sqlmap

References

- https://www.hudsoncourses.com/ethical-hacker-vs-penetration-tester/
- https://www.atlassian.com/trust/security/security-severity-levels
- Cyber Security, authored by John G. Voeller published by Wiley 2014