# Executive Vulnerability Management Glossary

Created By: Apurv Tiwari, Teaching Assistant

Instructor: Dr. Nikki Robinson

1. **0-day Vulnerability :** A zero-day vulnerability is a software security flaw that is known to the software vendor but doesn't have a patch in place to fix the flaw. It has the potential to be exploited by cybercriminals.
2. **API:** An application program interface is a set of routines, protocols, and tools for building software applications**.**
3. **APT :** An Advanced Persistent Threat (APT) is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data.
4. **Attack Vector :** A path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome.
5. **Authenticated Security Scan :** An essential tool to obtain accurate vulnerability information on covered devices by authenticating to scanned devices to obtain detailed and accurate information about the operating system and installed software, including configuration issues and missing security patches.
6. **BlueKeep :** Refer CVE-2019-0708 for details; Exploits a vulnerability that exists within Remote Desktop Protocol(RDP) to perform remote code execution on an unprotected system.
7. **Code Review :** Code review is a phase in the software development process in which the authors of code, peer reviewers, and perhaps quality assurance (QA) testers get together to review code.
8. **Configuration Management :** A systems engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.

9. **Critical Assets/Low Hanging Fruit :** Any device that uses a routable protocol to communicate outside the electronic security perimeter (ESP), uses a routable protocol within a control center, or is dial-up accessible.
10. **CVSS :** Common Vulnerability Scoring System, open source industry standard for assessing severity of vulnerabilities.
11. **Effective Workflow :** A Workflow is a sequence of tasks that processes a set of data. Workflows are the paths that describe how something goes from being undone to done, or raw to processed.
12. **End of life Software :** "End-of-life" is a term used with respect to a product supplied to customers, indicating that the product is in the end of its useful life, and a vendor stops marketing, selling, or rework sustaining it.
13. **False Positives :** A test result which wrongly indicates that a particular condition or attribute is present.
14. **FIPS :** Federal Information Processing Standards are a set of standards that describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.
15. **Gate Review :** Gate reviews give management visibility into the project's progress to-date, changes since the last Gate, and the project manager's plan for the near term. At this point management may let the project proceed, delay, alter, or cancel the project before further work is performed.
16. **Hotfix :** A small piece of code developed to correct a major software bug or fault and released as quickly as possible.
17. **Impact of a Vulnerability :** The damage caused to a business unit if a vulnerability is exploited.
18. **Likelihood :** The state of being probable or chance of a threat occurring.
19. **NIST RMF :** The Risk Management Framework is a set of information security policies and standards for federal government developed by The National Institute of Standards and Technology (NIST).
20. **NIST SP :** National Institute of Standards and Technology Special Publication provides a catalog of security and privacy controls for all U.S. federal information systems except those related to national security.
21. **NVD(National Vulnerability Database) :** The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content

Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance.

22. **OWASP :** The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software.
23. **Patch Management :** The process of managing a network of computers by regularly deploying all missing patches to keep computers up to date.
24. **Patch Management Lifecycle :** Patch management is a strategy for systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system.
25. **Risk Assessment :** Risk assessment is a term used to describe the overall process or method where you: Identify hazards and risk factors that have the potential to cause harm (hazard identification). Analyze and evaluate the risk associated with that hazard (risk analysis, and risk evaluation).
26. **Risk Committee :** The Risk Committee is an independent committee of the Board of Directors that has, as its sole and exclusive function, responsibility for the oversight of the risk management policies and practices of the corporation's global operations and oversight of the operation of the corporation's global risk management framework.
27. **Risk Exposure :** The measure of potential future loss resulting from a specific activity or event.
28. **Risk Identification :** The process of determining risks that could potentially prevent the program, enterprise, or investment from achieving its objectives. It includes documenting and communicating the concern.
29. **Risk Profile:** A quantitative analysis of the types of threats an organization, asset, project or individual faces. The goal of a risk profile is to provide a non-subjective understanding of risk by assigning numerical values to variables representing different types of threats and the danger they pose.
30. **Risk Response :** A planning and decision making process whereby stakeholders decide how to deal with each risk.
31. **Security Liaison :** The Security Liaison is the Security Team's point of contact at each agency for security related requests, issues, and communication.
32. **Segmentation :** Segmentation divides a computer network into smaller parts. The purpose is to improve network performance and security.
33. **SIEM :** Security Information and Event Management, SIEM software collects and aggregates log data generated throughout the organization's technology infrastructure,

from host systems and applications to network and security devices such as firewalls and antivirus filters.

34. **SOC :** A security operations center is a centralized unit that deals with security issues on an organizational and technical level.
35. **Spectre/Meltdown :** Critical vulnerabilities in processors which allow programs to steal data currently being processed.
36. **SQL Injection :** The placement of malicious code in SQL statements, via web page input. SQL in Web Pages.
37. **SSL :** Secure Sockets Layer; a protocol for establishing authenticated and encrypted links between networked computers.
38. **Technical Refresh :** Tech refresh is the cycle of regularly updating key elements of your IT infrastructure to maximise system performance.
39. **Tenable VPR(Vulnerability Priority Rating) :** The VPR is a dynamic companion to the static data provided by the vulnerability's CVSS score and severity, since Tenable updates the VPR to reflect the current threat landscape. VPR values range from 0.1-10.0, with a higher value representing a higher likelihood of exploitation.
40. **Test Environment :** A testing environment is a setup of software and hardware for the testing teams to execute test cases. In other words, it supports test execution with hardware, software and network configured.
41. **Threat Agent :** Also known as a threat actor; any person or thing that acts (or has the power to act) to cause, carry, transmit, or support a threat.
42. **Threat Detection :** The process by which you find threats on your network, your systems or your applications.
43. **Threat Intelligence :** Evidence-based knowledge, including context, mechanisms, indicators, implications, and action-oriented advice about an existing or emerging menace or hazard to assets.
44. **Threat Modelling :** A process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified, enumerated, and mitigations can be prioritized.
45. **Virtualization :** Virtualization is the process of running a virtual instance of a computer system in a layer abstracted from the actual hardware. Most commonly, it refers to running multiple operating systems on a computer system simultaneously.
46. **Vulnerability Management :** The process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them.

47. **XSS :** Cross-site Scripting is a type of security vulnerability, in which malicious scripts are injected into otherwise benign and trusted websites.
48. **Zero Client :** Also known as ultra thin client, is a server-based computing model in which the end user's computing device has no local storage.

**References**


1. https://www.us-cert.gov/ncas/alerts/AA19-168A
2. https://www.rapid7.com/fundamentals/vulnerability-management-and-scanning/
3. https://meltdownattack.com/
4. https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-identification