Penetration Testing, CVSS & EPSS

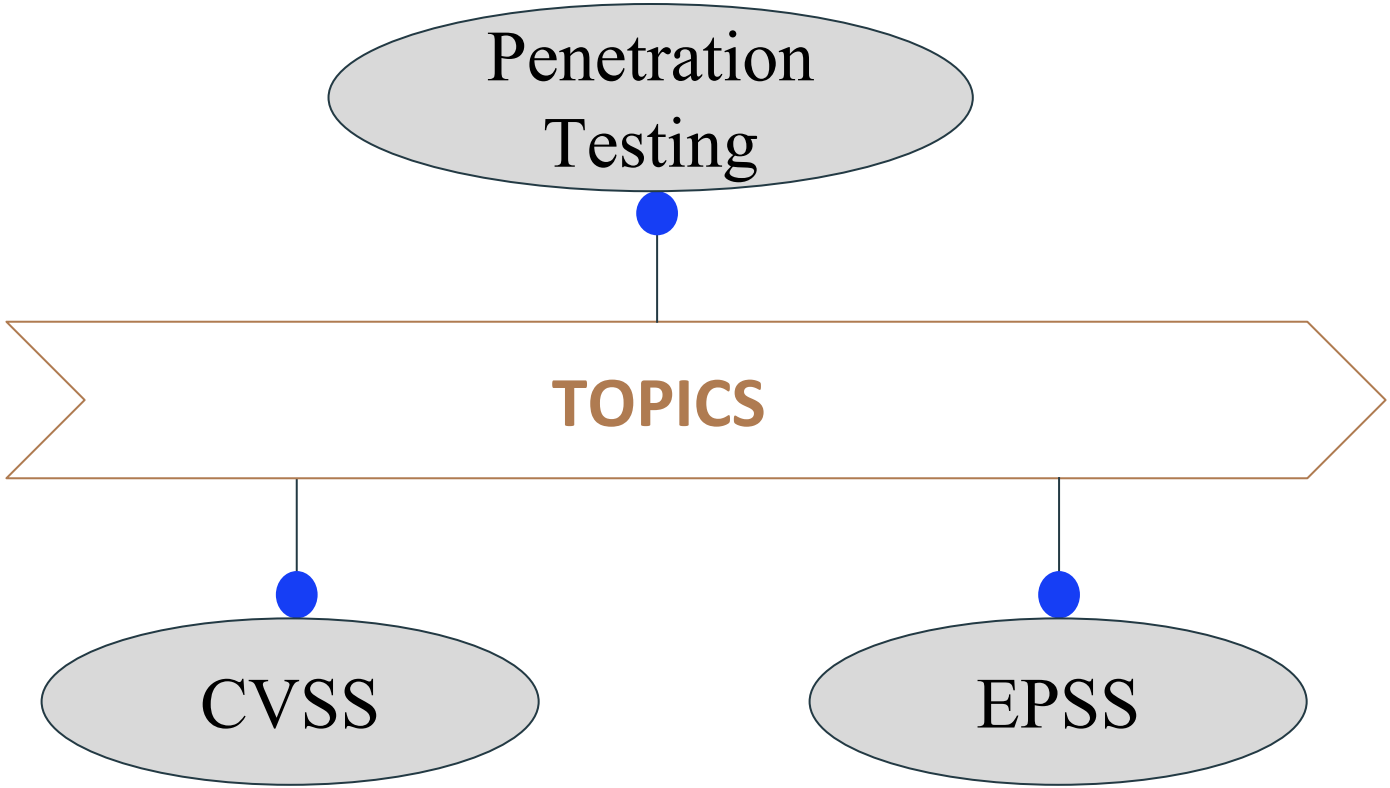
Submitted to

Dr. Mohammed Shafiul Alam Khan
Professor,Institute of Information Technology
University of Dhaka

Presented by

Arnab Das (BSSE-1308)
Abir Ashab Niloy (BSSE-1315)
Mahir Faisal (BSSE-1316)
Sabbir Hossen (BSSE-1333)

November 18, 2024


Penetration Testing
TOPICS
CVSS
EPSS

What is Penetration Testing?

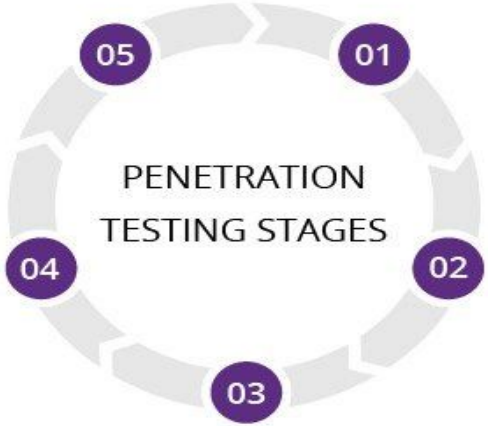
- A method of assessing the security of a system by simulating an attack.
- Identifies vulnerabilities before they can be exploited.

Purpose: To strengthen security measures and safeguard data.

Types of Penetration Testing

- **Black Box Testing**:
  - Tester has no prior knowledge of the system.
  - Mimics an external attack.
- **White Box Testing**:
  - Tester has full knowledge of the system (e.g., source code, architecture).
  - Mimics an internal attack.
- **Grey Box Testing**:
  - Partial knowledge of the system.
  - Simulates an insider threat with limited access.

Phases of Penetration Testing



Planning and reconnaissance
Test goals are defined and intelligence is gathered.

Scanning
Scanning tools are used to understand how a target responds to intrusions.

Gaining access
Web application attacks are staged to uncover a target's vulnerabilities.

Maintaining access
APTs are imitated to see if a vulnerability can be used to maintain access.

Analysis and WAF configuration
Results are used to configure WAF settings before testing is run again.

Common Pentesting Terms

- **Vulnerability**: A weakness in a system that attackers can exploit to compromise security.
- **Exploit**: A method or code used to take advantage of a vulnerability in a system.
- **Payload**: The part of an exploit that performs the malicious action once the system is compromised.
- **Privilege Escalation**: Gaining unauthorized higher-level access to a system.
- **Attack Vector**: The path or method used to exploit a vulnerability (e.g., phishing).
- **Zero-Day**: A newly discovered vulnerability without a vendor patch available.
- **Post-Exploitation**: Actions taken after exploiting a system, like data extraction or maintaining access.
- **OWASP Top 10**: A list of the most critical security risks for web applications.

Common Cyber Attacks

- **Phishing**: Deceptive emails or messages designed to trick individuals into revealing sensitive information like passwords or credit card numbers.
- **SQL Injection**: Exploiting a web application's database query vulnerabilities to gain unauthorized access or manipulate data.
- **Denial of Service (DoS)**: Overloading a system, network, or website with traffic to make it unavailable to users.
- **Man-in-the-Middle (MITM)**: Intercepting and altering communications between two parties without their knowledge.
- **Ransomware**: Malware that encrypts a victim’s data and demands payment for its release.

Common Web Vulnerabilities

- **SQL Injection**: Exploiting input fields to inject malicious SQL queries, enabling unauthorized database access or manipulation.
- **XSS (Cross-Site Scripting)**: Injecting malicious scripts into web pages viewed by users, leading to data theft or session hijacking.
- **Broken Authentication**: Flaws in authentication processes that allow attackers to compromise user credentials or sessions.
- **Security Misconfiguration**: Improperly configured security settings that expose systems to potential attacks.
- **Insecure Direct Object References (IDOR)**: Exposing internal objects (e.g., files, database records) directly, allowing unauthorized access.
- **Server-Side Request Forgery (SSRF)**: Exploiting a server to make malicious requests to internal or external resources.

Common Network Attacks

- **Port Scanning**: Probing a network to discover open ports and identify running services for potential exploitation.
- **Eavesdropping**: Intercepting network communications to capture sensitive data like passwords or messages.
- **Packet Sniffing**: Capturing and analyzing network traffic to gather information or exploit vulnerabilities.
- **Replay Attacks**: Capturing and reusing legitimate network data (e.g., authentication tokens) to gain unauthorized access.
- **IP Spoofing**: Faking an IP address to impersonate a trusted system and bypass security measures.
- **DNS Poisoning**: Manipulating DNS records to redirect users to malicious websites or intercept traffic.

Common Penetration Testing Tools

- **Reconnaissance Tools**: Nmap, Shodan
- **Exploitation Frameworks**: Metasploit, Burp Suite
- **Password Attack Tools**: John the Ripper, Hydra
- **Web Vulnerability Scanners**: OWASP ZAP, Nikto
- **Network Tools**: Wireshark, Aircrack-ng
- **Mobile Testing Tools**: MobSF, Drozer

Penetration Testing Certifications

- **Beginner-Level**
  - CompTIA PenTest+
  - CEH (Certified Ethical Hacker)
- **Intermediate-Level**
  - OSCP (Offensive Security Certified Professional)
  - GIAC GPEN (Certified Penetration Tester)
- **Advanced-Level**
  - OSWE (Offensive Security Web Expert)
  - GXPN (GIAC Exploit Researcher and Advanced Penetration Tester)

➢ CVSS helps evaluate the severity of security vulnerabilities in software, networks, and systems.

➢ It provides a numerical score (ranging from 0 to 10) based on factors like the complexity of exploiting the vulnerability, potential impact on confidentiality, integrity, and availability.

➢ This scoring system enables organizations to prioritize which vulnerabilities need immediate attention and which can be addressed later

CVSS(continued):

Key Terms & Activities

The CVSS score is calculated based on multiple factors, divided into three primary groups:

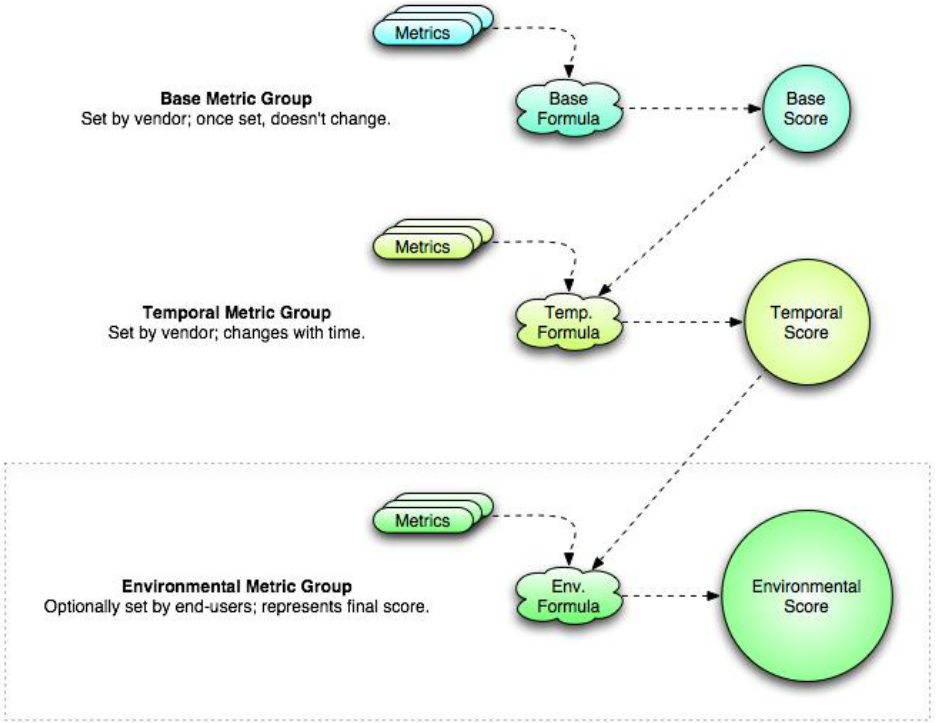
Base Score – Measures how dangerous a vulnerability is, based on how hard it is to exploit and the level of access needed. Easier access means a higher score.

Temporal Score – Update the base score depending on the exploit's current status, like whether a fix is available or if the vulnerability is currently being used by attackers.

Environmental Score – Update the score depending on how critical the affected system is to the specific organization.

CVSS(continued):

Key Terms & Activities



CVSS(continued):

CVSS Scoring System

CVSS(continued):

Example in Action

Imagine a software vulnerability that allows unauthorized access to sensitive data. If the exploit is simple to execute and affects highly confidential data, this vulnerability might score around **9.8**. This high score would alert security teams to address this issue promptly, as the risk it poses is substantial.

Challenge Addressed

Before CVSS, there was no consistent way to communicate or prioritize vulnerabilities, leading to inefficient allocation of resources and missed security threats. CVSS standardizes the scoring, helping teams focus on the most urgent vulnerabilities first and ensuring that high-risk issues are prioritized across the industry.

CVSS(continued):

Impact on Security

Improves Security: CVSS helps organizations focus on fixing the most critical vulnerabilities first, reducing the chances of cyberattacks.

Data-Driven Planning: Provides clear, measurable scores that help teams prioritize resources effectively

Prevents Breaches: By addressing high-risk vulnerabilities, it minimizes the likelihood of data theft or system damage

Supports Compliance: Demonstrates a standardized and effective approach to risk management, helping organizations meet security regulations

Builds Resilience: Strengthens overall cybersecurity infrastructure by addressing vulnerabilities in a strategic manner

EPSS (Exploit Prediction Scoring System)

- A framework to estimate the likelihood of a vulnerability being exploited.
- Complements CVSS.
- Dynamic and data-driven.

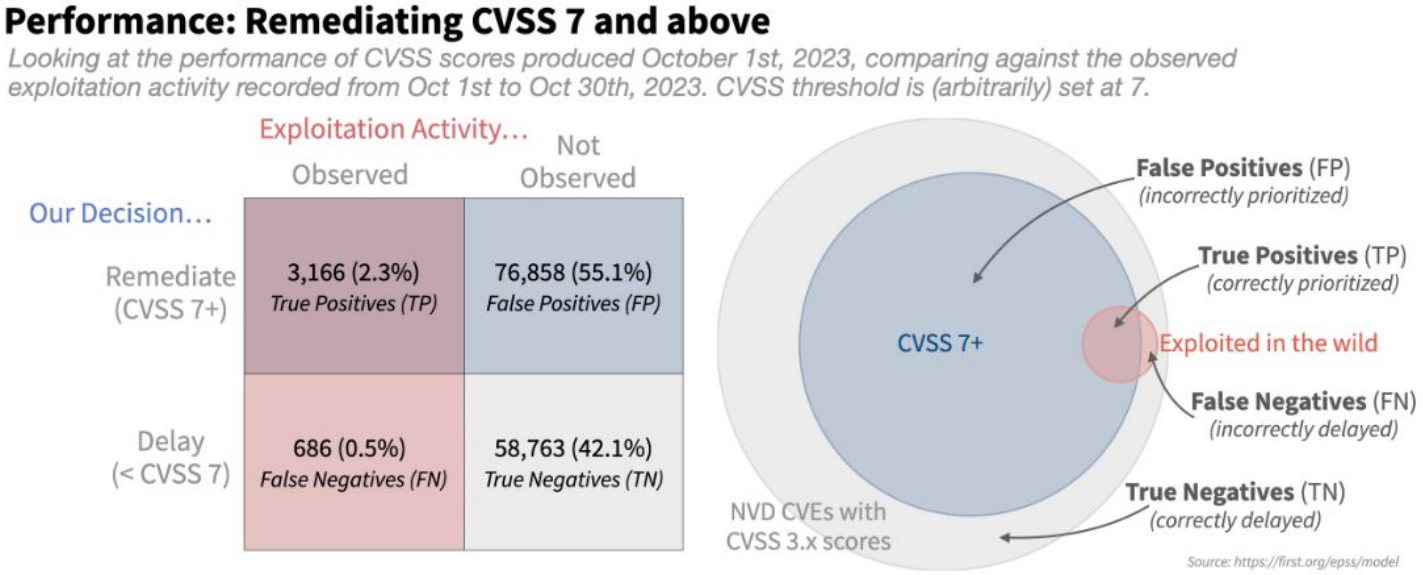
Key Factors that EPSS Considers

- ➢ Complexity of the attack.
- ➢ Likelihood of discovery of the vulnerability.
- ➢ Potential impact of a successful attack.
- ➢ Current threat landscape.

Why EPSS?

- ➢ Vulnerabilities are constantly discovered.
- ➢ Not all vulnerabilities are exploited.
- ➢ Focuses efforts on the highest risk.

Why EPSS? (contd.)



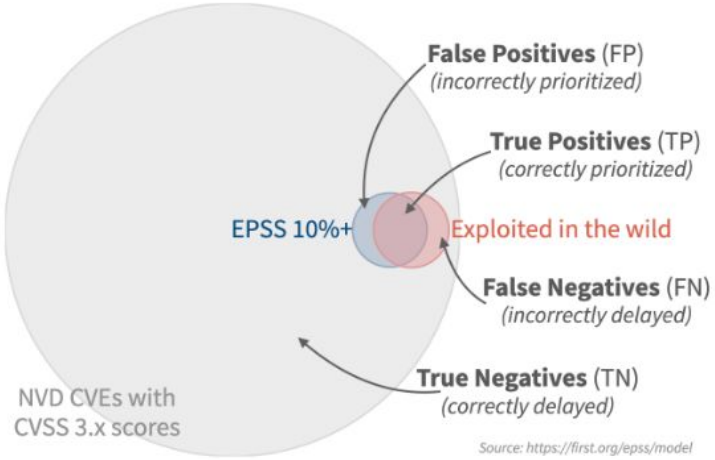
Collected from https://orca.security/resources/blog/epss-scoring-system-explained/

Why EPSS? (contd.)

Performance: Remediating EPSS 10% and above

Looking at the performance of EPSS scores produced October 1st, 2023, comparing against the observed exploitation activity recorded from Oct 1st to Oct 30th, 2023. EPSS threshold is (arbitrarily) set at 10%.

Our Decision… \ Exploitation Activity…	Observed	Not Observed
Remediate (EPSS 10%+)	2,435 (1.8%) *True Positives (TP)*	1,300 (0.9%) *False Positives (FP)*
Delay (< EPSS 10%)	1,417 (1%) *False Negatives (FN)*	134,321 (96.3%) *True Negatives (TN)*



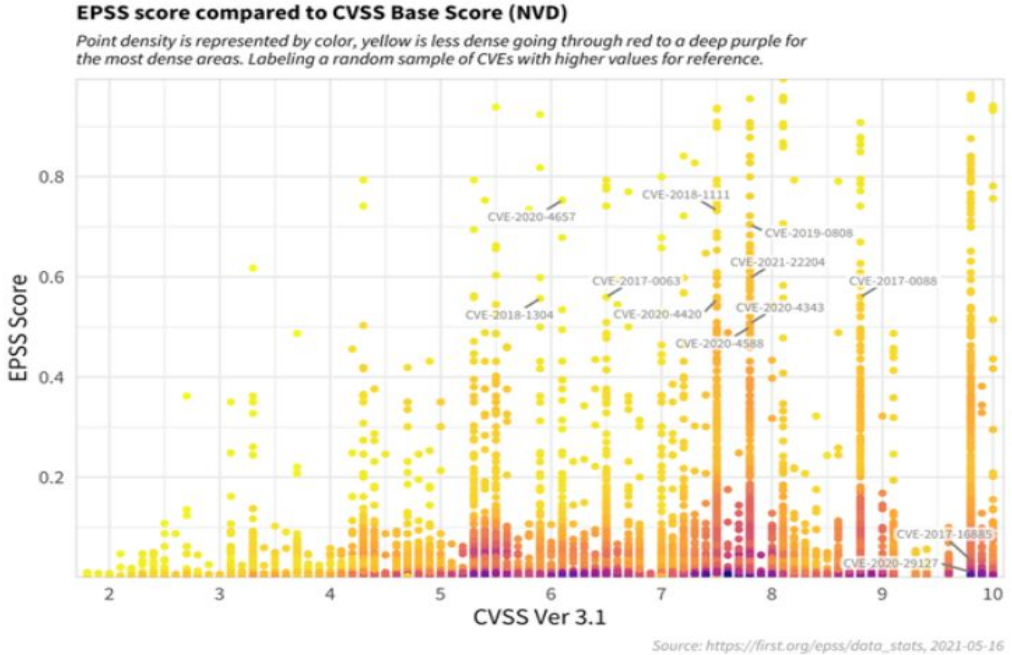
Collected from https://orca.security/resources/blog/epss-scoring-system-explained/

Why EPSS? (contd.)

96% of the vulnerabilities, scored with EPSS score of less than 10%, were neither exploited or prioritized for remediation (True Negative (TN)). 1.8% were both exploited and prioritized for remediation (TP).

Collected from https://orca.security/resources/blog/epss-scoring-system-explained/

Why EPSS? (contd.)



Collected from https://orca.security/resources/blog/epss-scoring-system-explained/

How to use EPSS?

- **Access EPSS scores through the FIRST website.** https://www.first.org/epss/
- **Integrate EPSS into vulnerability management workflow.**
- **Use EPSS to complement CVSS and other security tools.**

How EPSS works?

➢ **Uses information from various data sources like vulnerability database, exploit repositories, real-world attack data.**

➢ **Scores probability of exploitation from 0 to 1 using ML and statistical models.**

➢ **Changes assigned scores as new data becomes available.**

EPSS in Action:

1. A vulnerability with CVSS 9 but EPSS 0.05
Action: **lower priority**

2. A vulnerability with CVSS 7 but EPSS 0.9
Action: **higher priority**

Benefits of EPSS

- **Prioritization:** Focus on high-risk vulnerabilities.
- **Efficiency:** Avoid wasting resources on lower-risk vulnerabilities.
- **Proactivity:** Stay prepared for any potential attacks.
- **Complementary:** Works alongside existing security tools, measures and strategies.

Thank You!