Vulnerability Assessment & Penetration Testing

~Jithin Netticadan

CEH v12 | CAP | Qualys

Vulnerability Assessment & Penetration Testing (VAPT)

Vulnerability refers to a weakness in the design or implementation of a system that can be exploited to compromise the security of the system. (S/W or H/W misconfiguration & poor programming.

Vulnerability management involves identifying, assessing, prioritizing, and mitigating vulnerabilities in an organization's IT infrastructure.

Penetration testing also known as ethical hacking, is the practice of simulating cyber attacks against an organization's IT infrastructure, applications, and systems to identify security vulnerabilities.

Types of Hackers

White Hat

Grey Hat

Black Hat

Cyber Terrorists

Industrial Spies

Insiders

Script Kiddies

Hacktivists

State-Sponsored

Testing Methodologies

SAST

White-box testing for application source code, binary code, or byte code to detect vulnerabilities without the program being executed.

IAST

Highlights and analyzes vulnerabilities live during application runtime.

DAST

Black-box testing for running applications to highlight external vulnerabilities.

RASP

Security solution integrated into an application or runtime environment to highlight and thwart security attacks live.

Phases of Testing

Reconnaissance

Retrieve information from resources that are already publicly available.

Involves directly interacting with the target system to gain information.

Scanning

Port Scan

Discover the network's live hosts, IP addresses, and open ports of the live hosts.

OS & Version Discovery

Discover the OS and system architecture.
Discover the services running/listening.

Enumeration

Create active connections & perform directed queries to gain more information about the target.
Extract usernames, machine names, network resources, shares, and services from a system or network.

Vulnerability Assessment

In-depth examination of the ability of a system or application, including current security procedures and controls, to withstand exploitation.

Used to:

- Identify weaknesses that could be exploited
- Predict the effectiveness of additional security measures in protecting information resources from attack

Two approaches:

- Active Scanning
- Passive Scanning

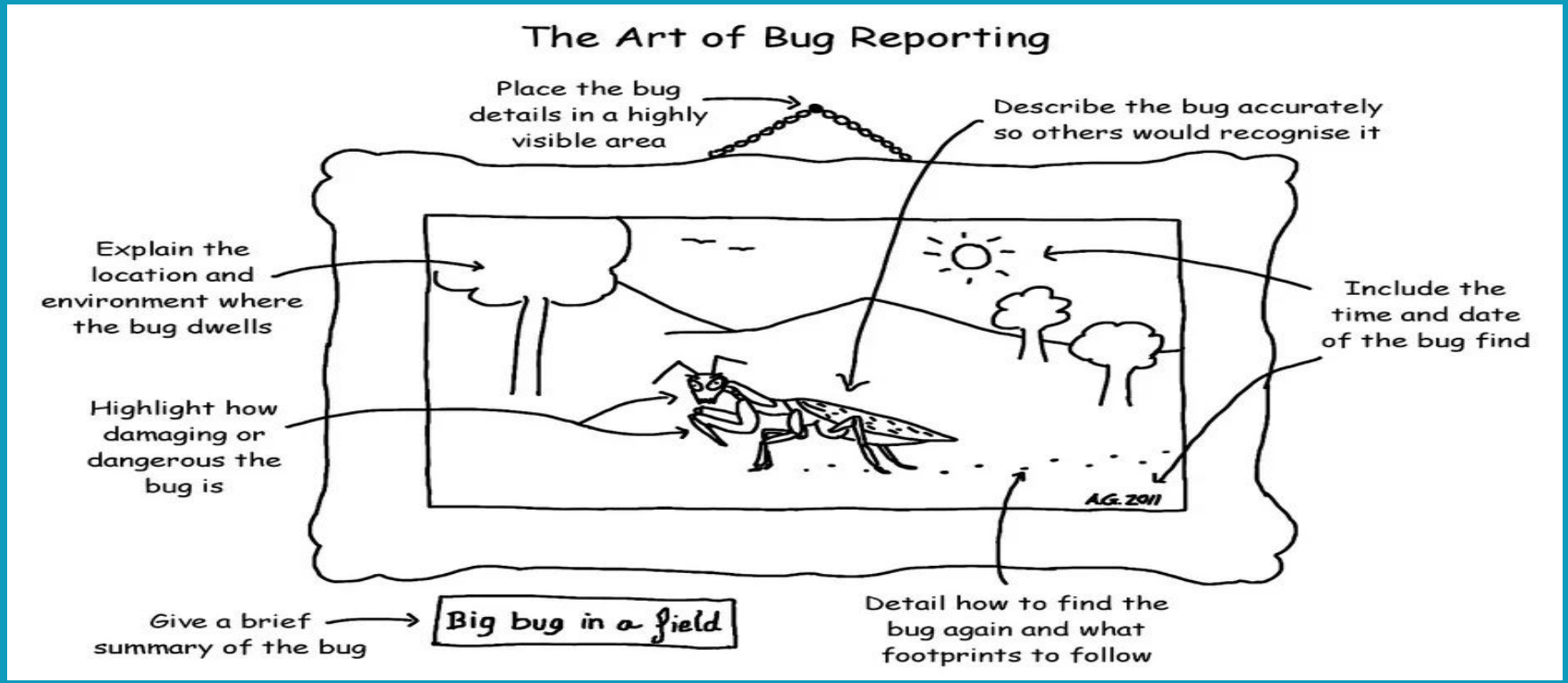
Exploitation

An attempt to use the identified vulnerabilities to gain unauthorised access to the target system.

Types of exploitation techniques:

- Remote
- Local
- Client-Side
- Social Engineering

Reporting


The Art of Bug Reporting
Place the bug details in a highly visible area
Describe the bug accurately so others would recognise it
Explain the location and environment where the bug dwells
Include the time and date of the bug find
Highlight how damaging or dangerous the bug is
A.G. 2011
Give a brief summary of the bug
Big bug in a field
Detail how to find the bug again and what footprints to follow

Thank you