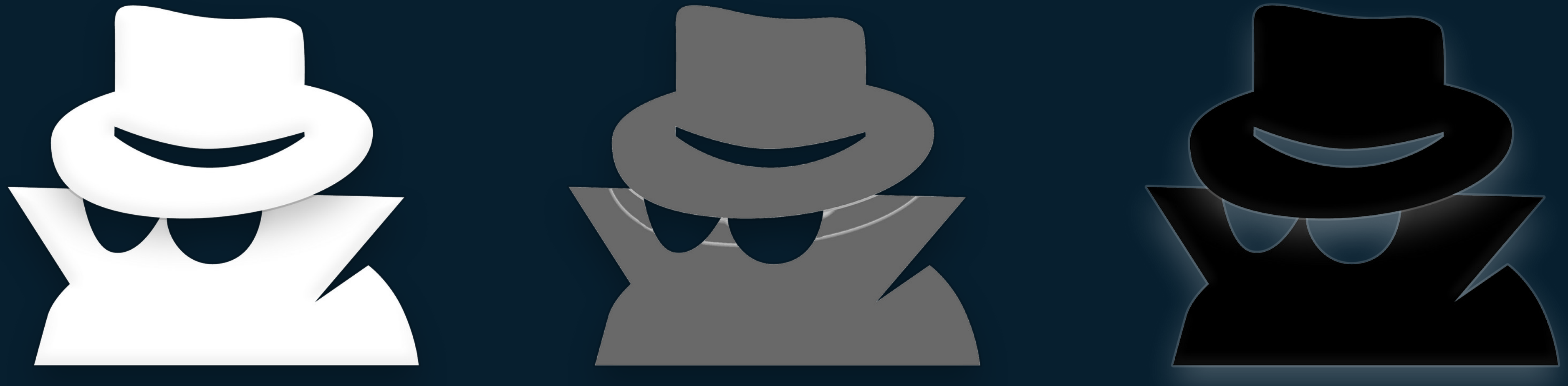
Cyber Security SG

What is penetration testing

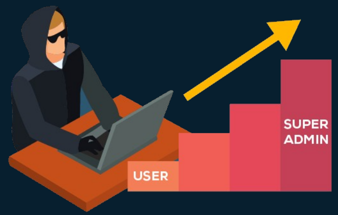
- Testing and analyzing the security of defenses to protect assets and pieces of information
- It is an **authorized audit** of a computer system’s security as agreed by the owners of the systems

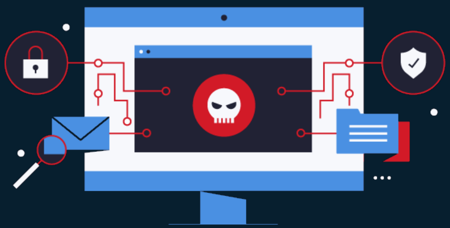
Hacker Hats

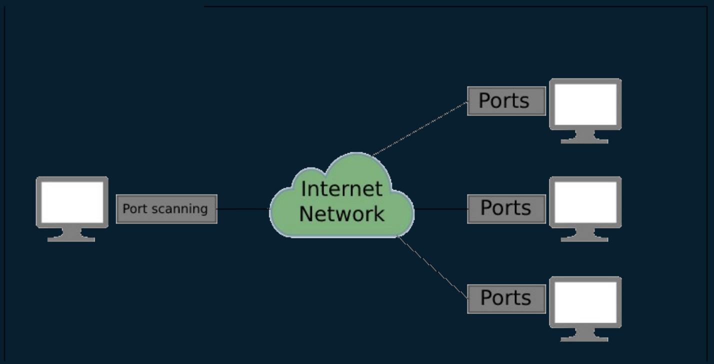


Stages of testing

→ Information Gathering
→ Enumeration/Scanning
→ Exploitation
→ Privilege Escalation
→ Post-exploitation

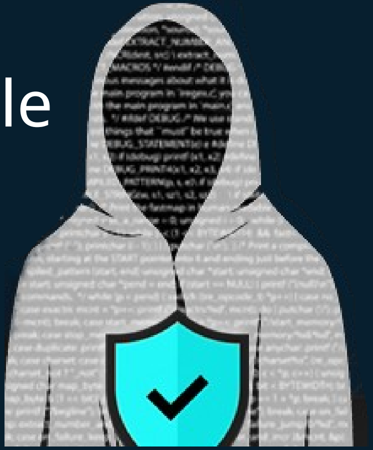




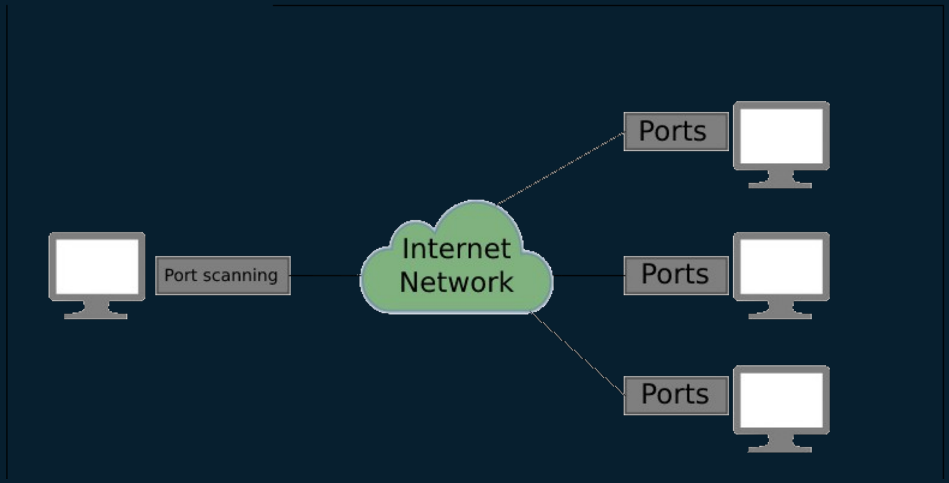


Information Gathering

- Collecting as much publicly accessible information about a target, OSINT and research



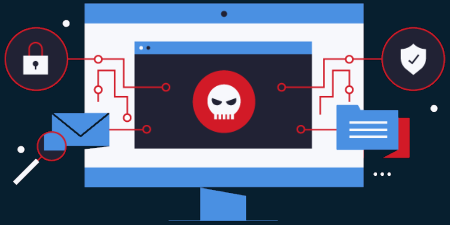
Enumeration/Scanning



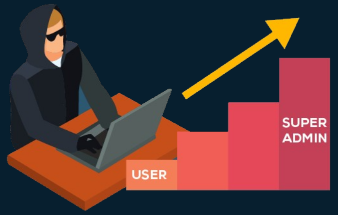
- Discovering applications and services running on the systems. finding a web server that may be potentially vulnerable.

Exploitation

- This stage involves leveraging vulnerabilities discovered on a system or application.
- This stage can involve the use of public exploits or exploiting application logic.



Privilege Escalation



- Once you have successfully exploited a system or application (known as a foothold), this stage is the attempt to expand your access to a system. You can escalate horizontally and vertically, where horizontally is accessing another account of the same permission group (i.e. another user), whereas vertically is that of another permission group (i.e. an administrator).

Post-Exploitation

- What other hosts can be targeted (pivoting)
- What additional information can we gather from the host now that we are a privileged user
- Covering your tracks
- Reporting

nmap

- Used for enumeration and scanning
- List of hosts :
  - Nmap -iL list_of_hosts.txt
  - Nmap -iL 10.10.12.13/29
  - Nmap -iL 10.10.0-255.101-125
  - -sC
    - Scripts from nmap for better enumeration
  - -sV
    - Probe open ports to determine service/version info
  - -T4
    - Prohibits the dynamic scan delay from exceeding 10ms
  - -Pn
    - Skips host discovery (that determines active machines)
  - -oN
    - Output to file

gobuster

- Directory/file & DNS scanning tool written in Go
- Given a url and a wordlist it will search for any directories of a url site

gftobins

- https://gtfobins.github.io
- List of Unix binaries that can be used to bypass local security restrictions (used in privilege escalation)

Μηχανηματα :

- Κάθε 2η Πέμπτη του Μήνα 15:00-17:00