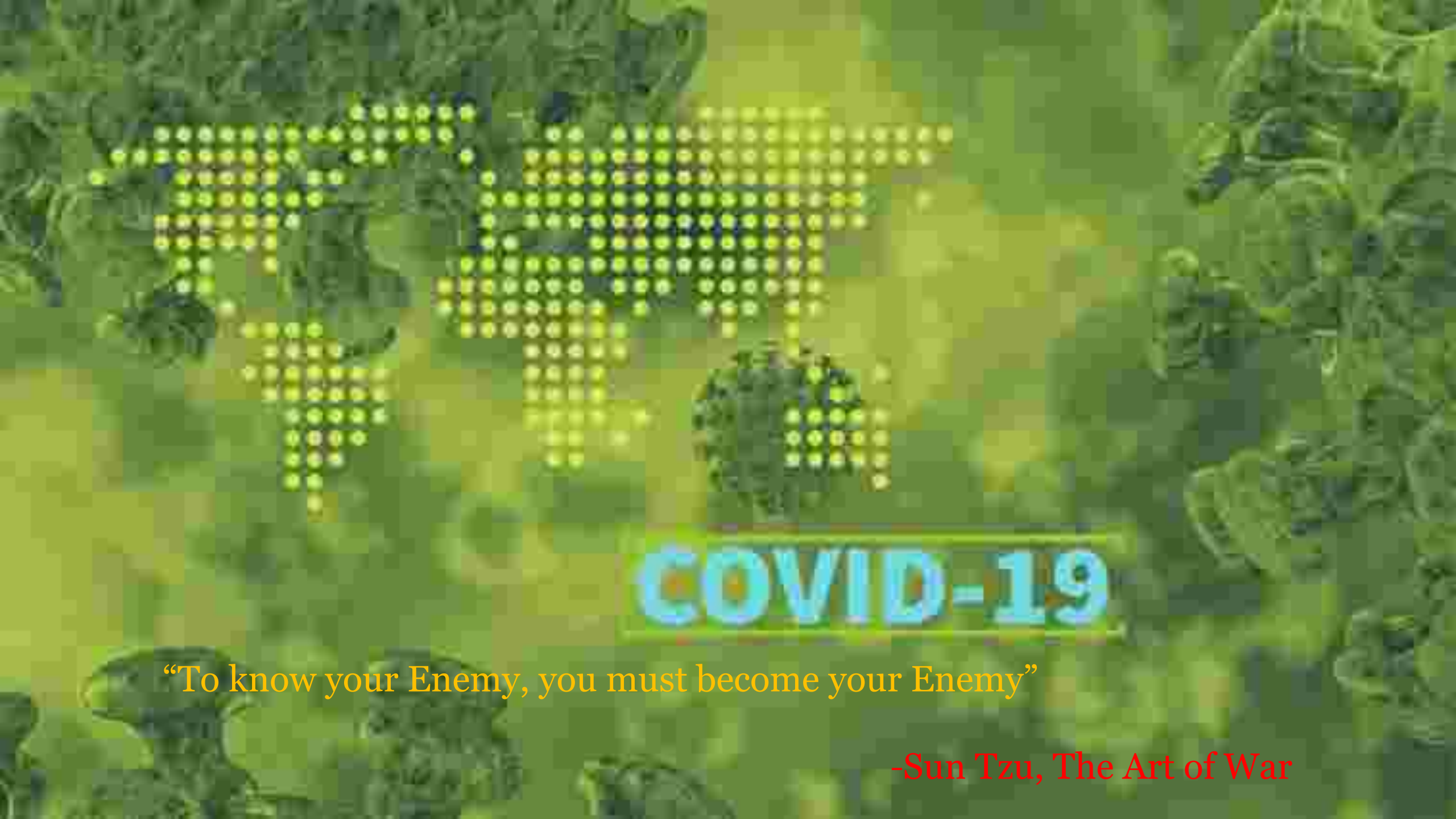
VULNERABILITY ASSESSMENT & PENETRATION TESTING (VAPT)



“To know your Enemy, you must become your Enemy”

-Sun Tzu, The Art of War

WHAT IS HACKING

- “the activity of illegally using a computer to access information stored on another computer system or to spread a computer virus”
  - Cambridge dictionary

- “The gaining of unauthorized access to data in a system or computer”
  - Oxford Dictionary

TYPES OF HACKING

TYPES OF HACKER

CATEGORIES OF HACKERS

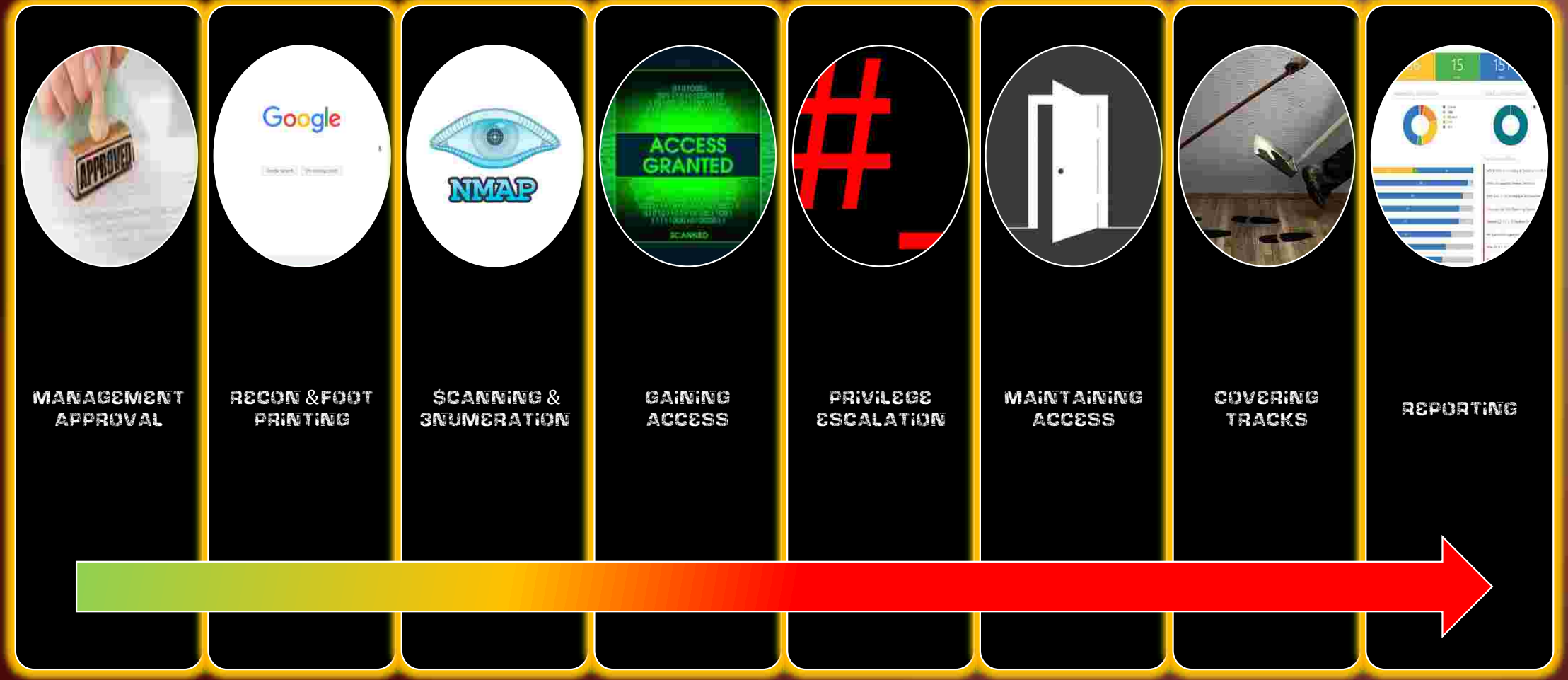
- Script kiddie
- Elite hacker (leet or 1337)
- Hacktivist
- Ethical hacker
- Neophyte
- Nation state
- Organized criminal gangs

IS IT ETHICAL ?

- yes
  - If performed by a **white hat** hacker
  - Obtains permission to access the network
  - Respects the company’s privacy
  - Observes good security best practices
  - Notifies the software and hardware developers of any found vulnerability

THE HACKER MINDSET

ETHICAL HACKING METHODOLOGY



ASSET

- any data, device, or other component of the computing environment
- activities that should be protected from anyone besides the people that are allowed to view or manipulate the information

VULNERABILITY

- A flaw or a weakness inside the asset that could be used to gain unauthorized access to it
- The successful compromise of a vulnerability may result in data manipulation, or privilege elevation, etc.,

THREAT

- a possible danger to the computer system
- A successful exploitation of vulnerability is threat
- A threat may be a malicious hacker who is trying to gain unauthorized access

EXPLOIT

- An exploit is something that takes advantage of vulnerability in an asset
- causes unintended or unanticipated behavior in a target system
- allows an attacker to gain access to data or information.

RISK

- the impact (or damage) resulting from the successful compromise of an asset

Risk = Threat * vulnerabilities * impact

VULNERABILITY ASSESSMENT

- the process of identifying, quantifying, and prioritizing the vulnerabilities in a system
- use of automated testing tools to identify threats and the risks
- Operating systems,, Application Software and Network are scanned in order to identify the occurrence of vulnerabilities

INFORMATION GATHERING

- Information gathering is the first phase of hacking
- gather as much information as possible regarding the target's online presence
- information gathering techniques can be classified into two main categories
  - Active information gathering
  - Passive information gathering

ACTIVE INFORMATION GATHERING

- directly engage with the target
- Gather information about open ports, services and OS etc.,
- easily detected by IDS, IPS, and firewalls
- generate a log of their presence

PASSIVE INFORMATION GATHERING

- do not directly engage with the target
- use search engines, social media, and other websites to gather information about the target
- does not generate any log of presence on the target system
- useful when we perform phishing, keylogging, browser exploitation, and other client side attacks

SOURCES FOR INFORMATION GATHERING

- Social media website
- Search engines
- Forums
- Press releases
- People search
- Job sites

GOOGLE HACKING

- A type of recon method using google
- Hackers use the advanced search parameters provided by google for improved targeted search
- These search parameters are termed as Google dorks
- An attacker may be able to gather very interesting information on the target

GOOGLE HACKING DATABASE

- Created by offensive security
- Has a list of Google dorks that can be used to obtain a variety of information
- Now available as part of the exploit database

https://www.exploit-db.com/google-hacking-database

ENUMERATION

- process of extracting user names, machine names, network resources, shares and services from a system
- the attacker creates an active connection to the system
- performs directed queries to gain more information about the target
- gathered information is used to identify the vulnerabilities or weak points in system security

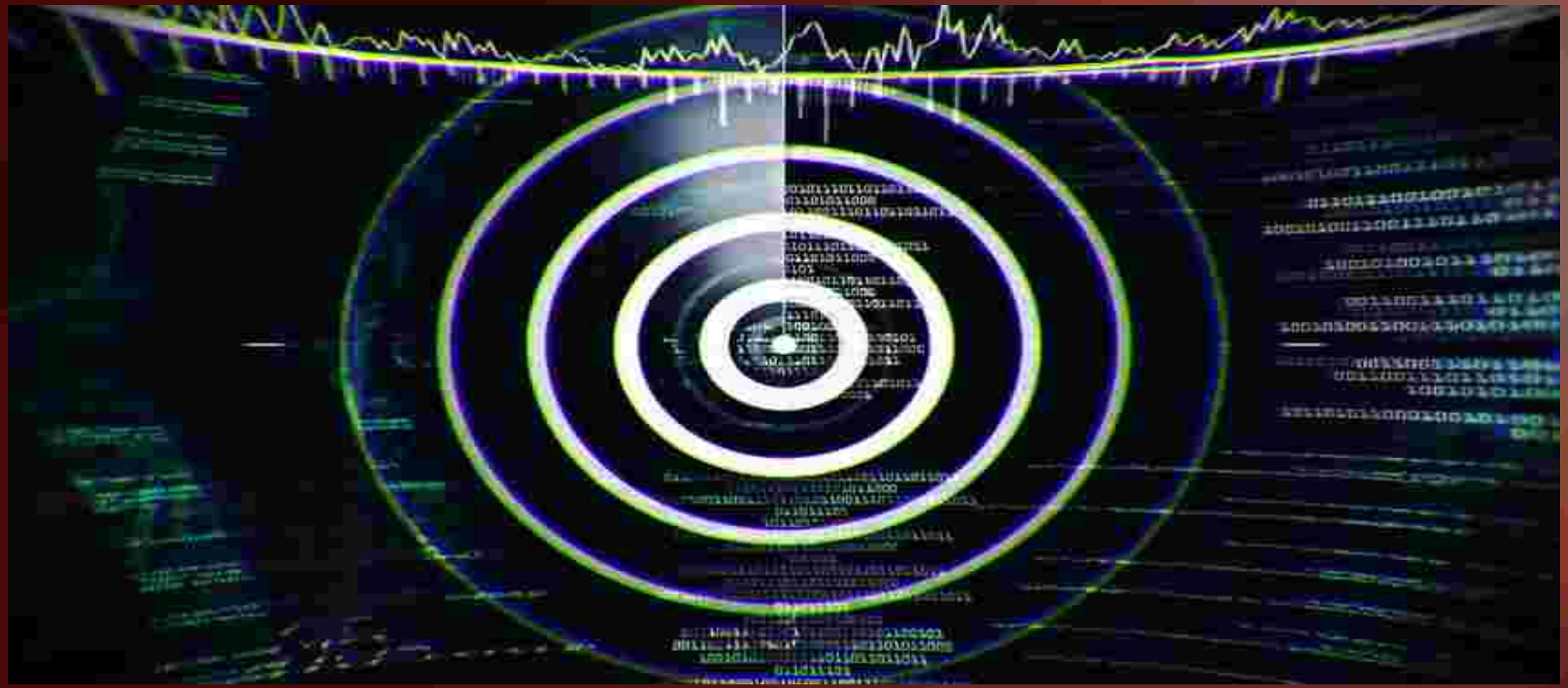
WHAT TO ENUMERATE ?

- Network Resource and shares
- Users and Groups
- Routing tables
- Auditing and Service settings
- Machine names
- Applications and banners
- SNMP and DNS details

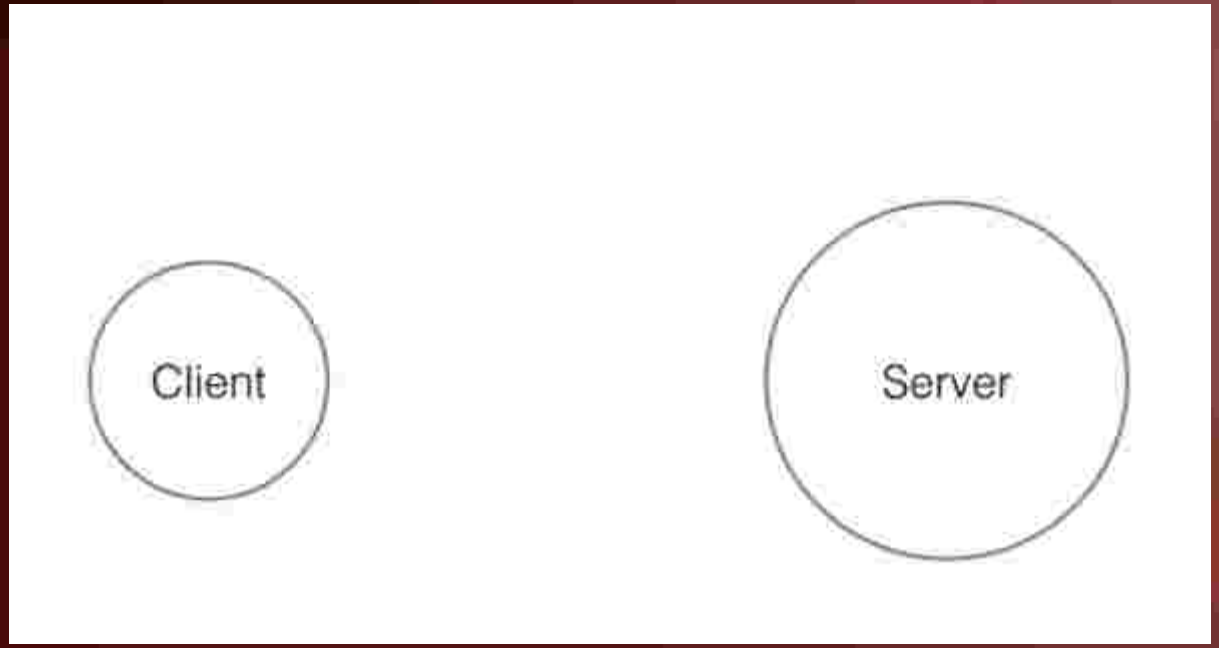
ENUMERATION TECHNIQUES

- Extracting user names using email ID's
- Extract information using the default password
- Brute Force Active Directory
- Extract user names using SNMP
- Extract user groups from Windows
- Extract information using DNS Zone transfer

SCANNING



THREE WAY HANDSHAKE



OS FINGERPRINTING


```
# nmap -O 10.0.2.4
# nmap -A 10.0.2.4
```

ZENMAP

- GUI for nmap utility
- Cross platform software
- Frequently used commands can be saved as profiles
- Scan results can be compared
- Recent scans are stored in a searchable database

VULNERABILITY SCANNING

IDENTIFYING VULNERABILITIES

- Scan network-accessible systems by pinging them or sending them TCP/UDP packets
- Identify open ports and services running on scanned systems
- If possible, remotely log in to systems to gather detailed system information
- Correlate system information with known vulnerabilities

EVALUATING VULNERABILITIES

- Is this vulnerability a true or false positive?
- Could someone directly exploit this vulnerability from the Internet?
- How difficult is it to exploit this vulnerability?
- Is there known, published exploit code for this vulnerability?
- What would be the impact to the business if this vulnerability were exploited?
- Are there any other security controls in place that reduce the likelihood and/or impact of this vulnerability being exploited?
- How old is the vulnerability/how long has it been on the network?

VULNERABILITY DATABASES

- Nvd
- Mitre
- Cve details
- Security focus
- Microsoft security bulletins
- Redhat Security advisories
- CERT recommendations

CVE

- Common vulnerabilities and exposure
- CVE is a list of vulnerabilities and exposures that aims to provide common names for publicly known problems.
- The goal of CVE is to make it easier to share data across tools, repositories, and services
- CVE Identifiers are unique, common identifiers for publicly known information security vulnerabilities.
- Governed by mitre corporation

CVE

- Each CVE Identifier includes the following:
  - CVE identifier number (i.e., "CVE-1999-0067").
  - indication of "entry" or "candidate" status.
  - Brief description of the security vulnerability or exposure.
  - Any pertinent references like vulnerability reports and advisories or OVAL-ID
  - CVE Identifiers are used by product/service vendors and researchers as a standard method for identifying vulnerabilities

CWE

- Common weakness enumeration
- a community-developed list of common software security weaknesses.
- serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.
- Listed by research, development and architectural concepts
- Maintained by the Mitre corporation

CVSS

- Common vulnerability scoring system
- CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity.
- The numerical score can then be translated into a qualitative representation to help organizations properly assess and prioritize their vulnerability management processes.

cvss 1.0 cvss 2.0 cvss 3.0

CVSS

0.1 – 3.9

4.0 – 6.9

7.0 – 8.9

9.0 – 10.0

CPE

- Common platform enumeration
- a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets
- The current version of CPE is 2.3

OVAL

- Open vulnerability and assessment language
- an international,infosec community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services
- includes a language used to encode system details, and an assortment of content repositories held throughout the community
- Used by security content automation protocol

SCAP

- Security content automation protocol
- a method for using specific standards to enable the automated vulnerability management, measurement, and policy compliance evaluation of systems deployed in an organization
- National Vulnerability Database (NVD) is the U.S. government content repository for SCAP
- OpenSCAP tool implements scap protocol using OVAL

NESSUS

- Nessus is one of the most popular vulnerability scanner
- It was initially free and open source, but they closed the source code in 2005 and removed the free "Registered Feed" version in 2008.
- Nessus is constantly updated, with more than 70,000 plugins.
- includes remote and local (authenticated) security checks,
- a client/server architecture with a web-based interface
- an embedded scripting language for writing your own plugins

EXPLOITATION

PENETRATION TESTING

- penetration test is a subclass of ethical hacking
- a set of methods and procedures that aim at testing/protecting an organization’s security
- helpful in finding vulnerabilities in an organization
- check whether an attacker will be able to exploit them to gain unauthorized access

TYPES OF PENETRATION TESTING

- Network penetration testing
- Web application penetration testing
- Mobile application penetration testing
- Social engineering penetration testing
- Physical penetration testing

TYPES OF PENETRATION TESTS

PENETRATION TESTING STANDARDS

- Pentest execution standard (ptes)
- Opensource security testing methodology manual (osstmm)
- National institute of standards and technology (nist 800-115) standard
- Open web application security project (owasp) standards

PENTEST EXECUTION STANDARD (PTES)

- The PTES consists of seven main sections.
  - Pre-engagement Interactions
  - Intelligence Gathering
  - Threat Modelling
  - Vulnerability Analysis
  - Exploitation
  - Post Exploitation
  - Reporting

OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL

- OSSTMM consists of
  - Operational Security Metrics
  - Trust Analysis
  - Work Flow.
  - Human Security Testing
  - Physical Security Testing
  - Wireless Security Testing
  - Telecommunications Security Testing
  - Data Networks Security Testing
  - Compliance Regulations
  - Reporting with the STAR

NIST 800-115

- Information Systems Security Assessment Framework ((ISSAF))
- Covers a vast area of assessments
- Currently not active
- One of the earlier standard of assessments

OPEN WEB APPLICATION SECURITY PROJECT

- OWASP foundation established in 2001
- Free and open to all
- OWASP top 10 web application security threats
- OWASP ASVS
- OWASP Testing Guide

OTHER STANDARDS

- PCI Penetration testing guide
- Penetration Testing Framework UK
- CREST Penetration Testing Guide
- FedRAMP Penetration Test Guidance

METASPLOIT

- one of the most powerful tools used for penetration testing
- comes in two versions:
  - Commercial: Metasploit Pro
  - Community: Metasploit Framework
- Metasploit can be used either with command prompt or UI
- Armitage is the GUI complementing the Metasploit framework

REPORTING

REPORT TEMPLATE

- Executive Summary
  - Brief high-level summary of pentest scope
  - major findings
- Statement of Scope
  - A detailed definition of the scope of the network & systems tested
  - Identification of critical systems
  - explanation of why they are included in the test as targets

REPORT TEMPLATE

- Statement of Methodology
  - Details on the methodologies used
- Statement of Limitations
  - Document any restrictions imposed on testing
    - designated testing hours,
    - bandwidth restrictions,
    - special testing requirements for legacy systems, etc.

REPORT TEMPLATE

- Testing Narrative
  - Provide details on to how the testing was performed
  - testing progress
  - Document any issues encountered during testing
- Segmentation of Test Results
  - Summarize the testing performed to validate and segment it based on issues

REPORT TEMPLATE

- Findings
  - how the target may be or have been exploited using the vulnerability.
  - Risk ranking/severity of each vulnerability
  - Targets affected
  - References (if available)
    - CVE, CWE, BID, OSBDB, etc
    - Vendor and/or researcher
  - Description of finding

REPORT TEMPLATE

- Tools Used
- Cleaning up the Environment Post-Penetration Test
  - removal of test accounts
  - Removal of database entries added or modified
  - uninstall of test tools
  - restoring active protection-
  - system settings,.).
  - Provide directions how security controls have been restored.

"Attack is the secret of defense; defense is the planning of an attack"

-Sun Tzu, The Art of War


Thank You!