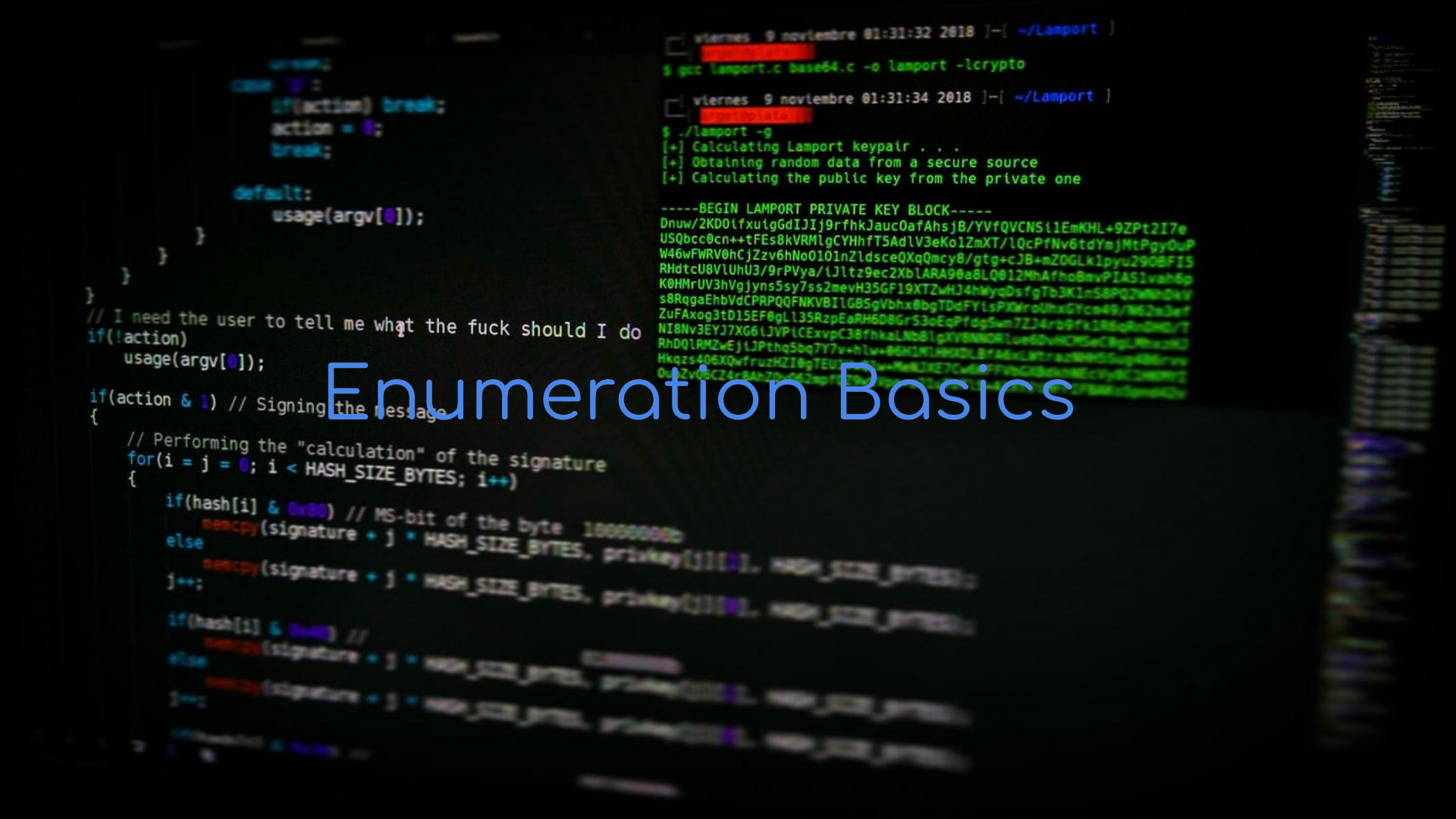
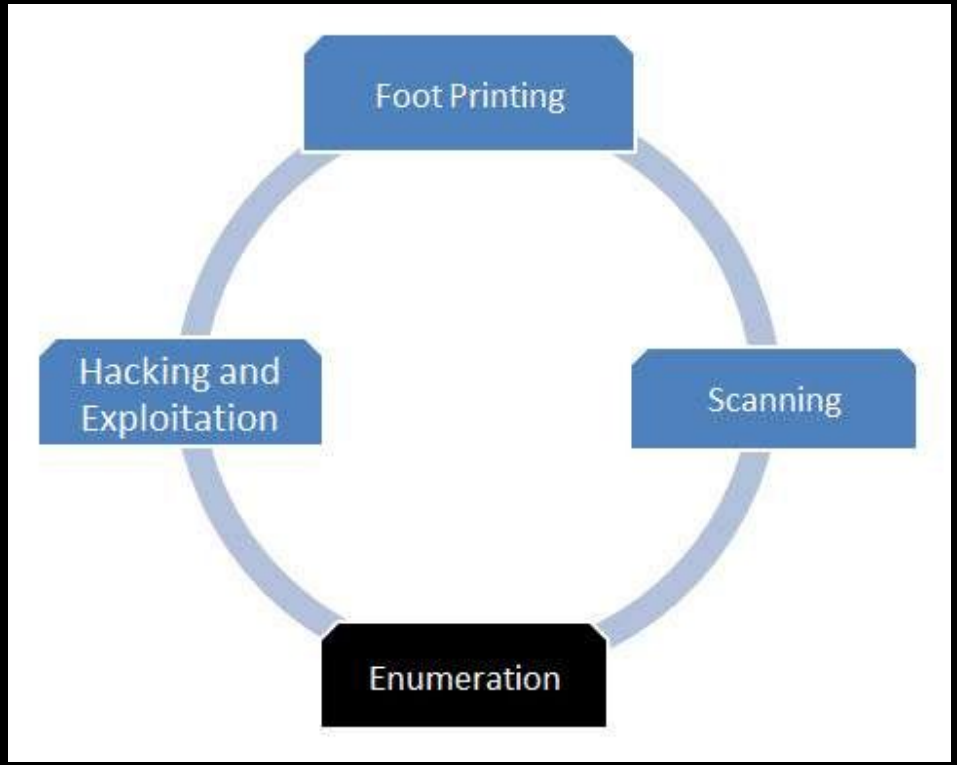


Enumeration Basics

What is enumeration in Hacking?

Enumeration is defined as the process of extracting user names, machine names, network resources, shares and services from a system. In this phase, the attacker creates an active connection to the system and performs directed queries to gain more information about the target. The gathered information is used to identify the vulnerabilities or weak points in system security and tries to exploit in the System gaining phase.

Why enumerate?



Main Objectives of Enumeration

Enumeration is used to gather the below

- Usernames, Group names
- Hostnames
- Network shares and services
- IP tables and routing tables
- Service settings and Audit configurations
- Application and banners
- SNMP and DNS Details

Find the network range:

If you want to break into an organization's network, you should know the network range first. This is because if you know the network range, then you can mask yourself as a user falling within the range and then try to access the network. So the first step in enumeration is to obtain information about network range. You can find the network range of target organization with the help of tools such as Whois Lookup.

Determine Subnet Mask :

Once you find the network range of the target network, then calculate the subnet mask required for the IP range using tools such as Subnet Mask Calculator. You can use the calculated subnet mask as an input to many of the ping sweep and port scanning tools for further enumeration, which includes discovering hosts and open ports

Port scanning:

It is very important to discover the open ports and close them if they are not required. This is because open ports are the doorways for an attacker to break into a target's security perimeter. Therefore, perform port scanning to check for the open ports on the nodes. This can be accomplished with the help of tools such as Nmap.

Host Discovery:

We should determine the Operating System that is installed on our target which can be achieved using nmap while scanning for open ports and services.

MAIN THINGS to enumerate:

SMB enumeration:

SMB stands for Server Message Block. It is mainly used for providing shared access to files, printers and miscellaneous communications between nodes on a network. It also provides an authenticated inter-process communication mechanism.

DNS Enumeration:

DNS enumeration retrieves information regarding all the DNS servers and their corresponding records related to an organization. DNS enumeration will yield usernames, computer names, and IP addresses of potential target systems.

NTP Enumeration:

NTP (Network Time Protocol) utilizes UDP port 123. Through NTP enumeration you can gather information such as a list of hosts connected to NTP server, IP addresses, system names, and operating systems running on the client system in a network. All this information can be enumerated by querying the server.

SNMP Enumeration:

Simple Network Management Protocol is an application layer protocol which uses UDP protocol to maintain and manage routers, hubs, switches and other network devices. SNMP is a popular protocol found enabled on a variety of operating systems like Windows Server, Linux & UNIX servers as well as network devices.

SMTP Enumeration:

SMTP stands for Simple Mail Transfer Protocol and it is designed for electronic mail (E-Mail) transmissions. SMTP is based on client-server architecture and works on Transmission Control Protocol (TCP) on well-known port number 25. SMTP uses Mail Exchange (MX) servers to send the mail to via the Domain Name Service, however, should an MX server not detected; SMTP will revert and try an A or alternatively SRV records.

LDAP Enumeration:

LDAP stands for Lightweight Directory Access Protocol. By querying the LDAP service you can enumerate valid user names, departmental details, and address details. You can use this information to perform social engineering and other kinds of attacks. You can perform LDAP enumeration using tools such as Softerra LDAP Administrator.

Why enumeration is a part of Hacking?

As a pen tester, conduct enumeration penetration tests to check whether the target network is revealing any sensitive information that may help an attacker to perform a well-planned attack. Apply all types of enumeration techniques to gather sensitive information such as user accounts, IP address, email contacts, DNS, network resources and shares, application information, and much more. Try to discover as much information as possible regarding the target. This helps you determine the vulnerabilities/weaknesses in the target organization's security.