**Network**

**Security**

**Class 10**

**Lab 27**

|  |
| --- |
| Lab Objectives:  * Exploitation * Enumeration |

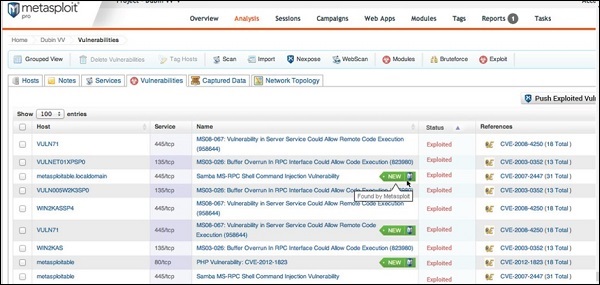
# Exploitation

## IMG_256Exploitation is a piece of programmed software or script which can allow hackers to take control over a system.

## Hackers normally use vulnerability scanners like Nessus, Nexpose, OpenVAS, etc to find these vulnerabilities.

# Metasploit

## A powerful tool to locate vulnerabilities in a system.

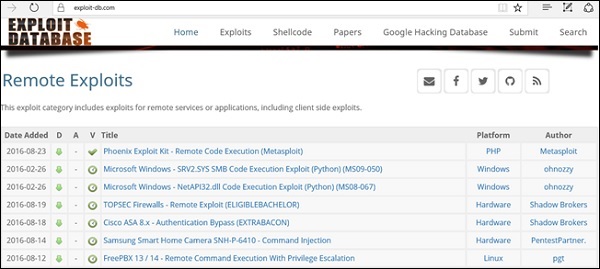


## Based on the vulnerabilities, we find exploits. Here, we will discuss some of the best vulnerability search engines that you can use.

# Exploit Database

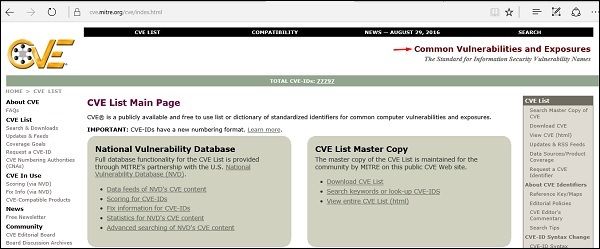
## <https://www.exploit-db.com/> is the place where you can find all the exploits related to a vulnerability.





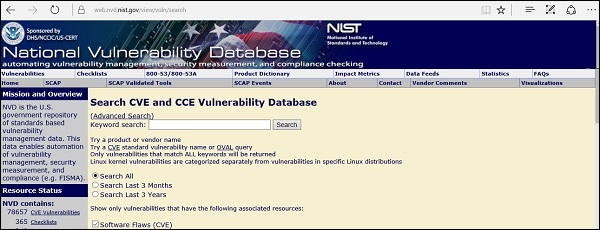
# Common Vulnerabilities and Exposures

## Common Vulnerabilities and Exposures (CVE) is the standard for information security vulnerability names. CVE is a dictionary of publicly known information security vulnerabilities and exposures. It’s free for public use. <https://cve.mitre.org/>



# National Vulnerability Database

## National Vulnerability Database (NVD) is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance. You can locate this database at − <https://nvd.nist.gov/> NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.

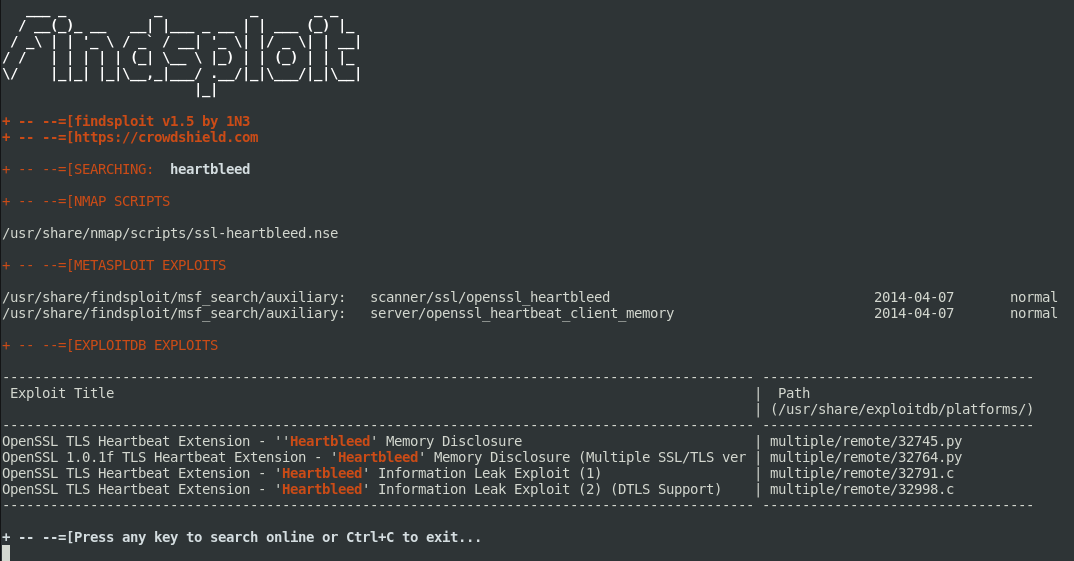


## In general, you will see that there are two types of exploits −

## Remote Exploits − These are the type of exploits where you don’t have access to a remote system or network. Hackers use remote exploits to gain access to systems that are located at remote places.

## IMG_256

## Local Exploits − Local exploits are generally used by a system user having access to a local system.

* 

# Quick Fix

## Vulnerabilities generally arise due to missing updates, so it is recommended that you update your system on a regular basis, for example, once a week.

## In Windows environment, you can activate automatic updates by using the options available in the Control Panel → System and Security → Windows Updates.

## In Linux , you can use the following command to install automatic update package.

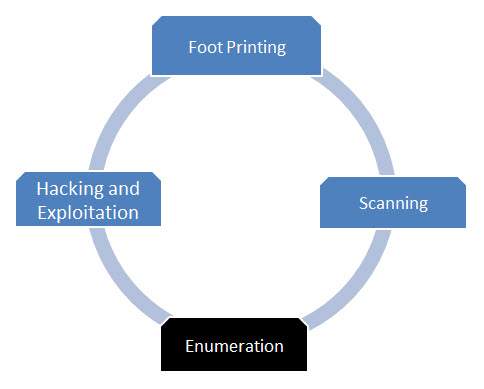
yum -y install yum-cron

## IMG_260

## 

Enumeration

## Enumeration belongs to the first phase of Ethical Hacking, i.e., “Information Gathering”. This is a process where the attacker establishes an active connection with the victim and try to discover as much attack vectors as possible, which can be used to exploit the systems further.



## Enumeration can be used to gain information on −

## Network shares

## SNMP data, if they are not secured properly

## IP tables

## Username of different systems

## Passwords policies lists

## Enumerations depend on the services that the systems offer. They can be −

## DNS enumeration

## NTP enumeration

## SNMP enumeration

## Linux/Windows enumeration

## SMB enumeration

## Let us now discuss some of the tools that are widely used for Enumeration.

# NTP Suite

## NTP Suite is used for NTP enumeration. This is important because in a network environment, you can find other primary servers that help the hosts to update their times and you can do it without authenticating the system.

## Take a look at the following example.

ntpdate 192.168.1.100 01 Sept 12:50:49 ntpdate[627]:

adjust time server 192.168.1.100 offset 0.005030 sec

or

ntpdc [-ilnps] [-c command] [hostname/IP\_address]

root@test]# ntpdc -c sysinfo 192.168.1.100

\*\*\*Warning changing to older implementation

\*\*\*Warning changing the request packet size from 160 to 48

system peer: 192.168.1.101

system peer mode: client

leap indicator: 00

stratum: 5

precision: -15

root distance: 0.00107 s

root dispersion: 0.02306 s

reference ID: [192.168.1.101]

reference time: f66s4f45.f633e130, Sept 01 2016 22:06:23.458

system flags: monitor ntp stats calibrate

jitter: 0.000000 s

stability: 4.256 ppm

broadcastdelay: 0.003875 s

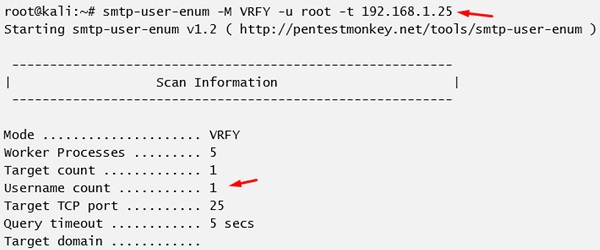
authdelay: 0.000107 s

# enum4linux

## IMG_256enum4linux is used to enumerate Linux systems. Take a look at the following screenshot and observe how we have found the usernames present in a target host.

# smtp-user-enum

## smtp-user-enum tries to guess usernames by using SMTP service. Take a look at the following screenshot to understand how it does so.



# Quick Fix

## It is recommended to disable all services that you don’t use. It reduces the possibilities of OS enumeration of the services that your systems are running.