







# Metasploit

A powerful tool to locate vulnerabilities in a system.

Host	Service	Name	Status	References
VULN71	445/tcp	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (18 Total)
VULNET01XPSPO	135/tcp	MS03-026: Buffer Overrun in RPC Interface Could Allow Code Execution (823960)	Exploited	CVE-2003-0352 (13 Total)
metasploitable.localdomain	445/tcp	Samba MS-RPC Shell Command Injection Vulnerability	Exploited	CVE-2007-2447 (31 Total)
VULN009W2K3SP0	135/tcp	MS03-026: Buffer Overrun in RPC Interface Could Allow Code Execution (823960)	Exploited	CVE-2003-0352 (13 Total)
WIN2KASPF4	445/tcp	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (18 Total)
VULN71	445/tcp	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (18 Total)
WIN2KAS	135/tcp	MS03-026: Buffer Overrun in RPC Interface Could Allow Code Execution (823960)	Exploited	CVE-2003-0352 (13 Total)
metasploitable	80/tcp	PHP Vulnerability: CVE-2012-1823	Exploited	CVE-2012-1823 (18 Total)
metasploitable	445/tcp	Samba MS-RPC Shell Command Injection Vulnerability	Exploited	CVE-2007-2447 (31 Total)

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.

**The Exploit Database**

The Exploit Database (EDB) is a CVE compliant archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our goal is to collect exploits from various sources and concentrate them in one, easy to navigate database

[Download the Exploit Database Archive](#)

**EXPLOIT DATABASE**

**CVE Compliant**

**CVE** cve.mitre.org



exploit-db.com

**EXPLOIT DATABASE**

Home Exploits Shellcode Papers Google Hacking Database Submit Search

## Remote Exploits

This exploit category includes exploits for remote services or applications, including client side exploits.

Date Added	D	A	V	Title	Platform	Author
2016-08-23			✓	Phoenix Exploit Kit - Remote Code Execution (Metasploit)	PHP	Metasploit
2016-02-26			✓	Microsoft Windows - SRV2.SYS SMB Code Execution Exploit (Python) (MS09-050)	Windows	ohnozy
2016-02-26			✓	Microsoft Windows - NetAPI32.dll Code Execution Exploit (Python) (MS08-067)	Windows	ohnozy
2016-08-19			✓	TOPSEC Firewalls - Remote Exploit (ELIGIBLEBACHELOR)	Hardware	Shadow Brokers
2016-08-18			✓	Cisco ASA 8.x - Authentication Bypass (EXTRABACON)	Hardware	Shadow Brokers
2016-08-14			✓	Samsung Smart Home Camera SNH-P-6410 - Command Injection	Hardware	PentestPartner.
2016-08-12			✓	FreePBX 13 / 14 - Remote Command Execution With Privilege Escalation	Linux	pgt

## 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/>

← → ↻ cve.mitre.org/cve/index.html

**CVE LIST** **COMPATIBILITY** **NEWS — AUGUST 20, 2016** **SEARCH**

**Common Vulnerabilities and Exposures**  
The Standard for Information Security Vulnerability Names

TOTAL CVE-IDs: 22292

HOME > CVE LIST

**About CVE**  
FAQs  
**CVE List**  
Search & Downloads  
Updates & Feeds  
Coverage Goals  
Request a CVE-ID  
CVE Numbering Authorities (CNAs)  
**CVE In Use**  
Scoring (via NVD)  
Fix Info (via NVD)  
CVE-Compatible Products  
**News**  
Free Newsletter  
**Community**  
CVE Editorial Board  
Board Discussion Archives

**CVE List Main Page**  
CVE® is a publicly available and free to use list or dictionary of standardized identifiers for common computer vulnerabilities and exposures.  
**IMPORTANT:** CVE-IDs have a new numbering format. [Learn more.](#)

**National Vulnerability Database**  
Full database functionality for the CVE List is provided through MITRE's partnership with the U.S. National Vulnerability Database (NVD).  

- Data feeds of NVD's CVE content
- Scoring for CVE-IDs
- Fix information for CVE-IDs
- Statistics for NVD's CVE content
- Advanced searching of NVD's CVE content

**CVE List Master Copy**  
The master copy of the CVE List is maintained for the community by MITRE on this public CVE Web site.  

- Download CVE List
- Search keywords or look-up CVE-IDs
- View entire CVE List (html)

**CVE List**  
Search Master Copy of CVE  
Download CVE  
View CVE (html)  
Updates & RSS Feeds  
Data Sources/Product Coverage  
Request a CVE Identifier  
**About CVE Identifiers**  
Reference Key/Maps  
Editorial Policies  
CVE Editor's Commentary  
Search Tips  
CVE-ID Syntax Change  
CVE-ID Syntax



Sponsored by DHS/NICUS/CERT

# National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | 800-53/800-33A | Product Dictionary | Impact Metrics | Data Feeds | Statistics | FAQs

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments | Visualizations

## Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

## Resource Status

NVD contains:  
78657 CVE vulnerabilities  
365 Checklists

Search CVE and CCE Vulnerability Database

(Advanced Search)  
Keyword search:  Search

Try a product or vendor name  
Try a CVE standard vulnerability name or OVAL query  
Only vulnerabilities that match ALL keywords will be returned  
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

☒ Search All  
☐ Search Last 3 Months  
☐ Search Last 3 Years

Show only vulnerabilities that have the following associated resources:

☒ Software Flaws (CVE)

***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.





**Local Exploits** – Local exploits are generally used by a system user having access to a local system.

```

Findsploit

+ -- ==[findsploit v1.5 by INS
+ -- ==[https://crowdshield.com
+ -- ==[SEARCHING: heartbleed
+ -- ==[NMAP SCRIPTS
/usr/share/nmap/scripts/ssl-heartbleed.nse
+ -- ==[METASPLOIT EXPLOITS
/usr/share/findsploit/msf_search/auxiliary: scanner/ssl/openssl heartbleed 2014-04-07 normal
/usr/share/findsploit/msf_search/auxiliary: server/openssl_heartbeat_client_memory 2014-04-07 normal
+ -- ==[EXPLOITDB EXPLOITS

-----
Exploit Title | Path
              | (/usr/share/exploitdb/platforms/)
-----
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure | multiple/remote/32745.py
OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure (Multiple SSL/TLS ver | multiple/remote/32764.py
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak Exploit (1) | multiple/remote/32791.c
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak Exploit (2) (DTLS Support) | multiple/remote/32998.c
-----
+ -- ==[Press any key to search online or Ctrl+C to exit...

```



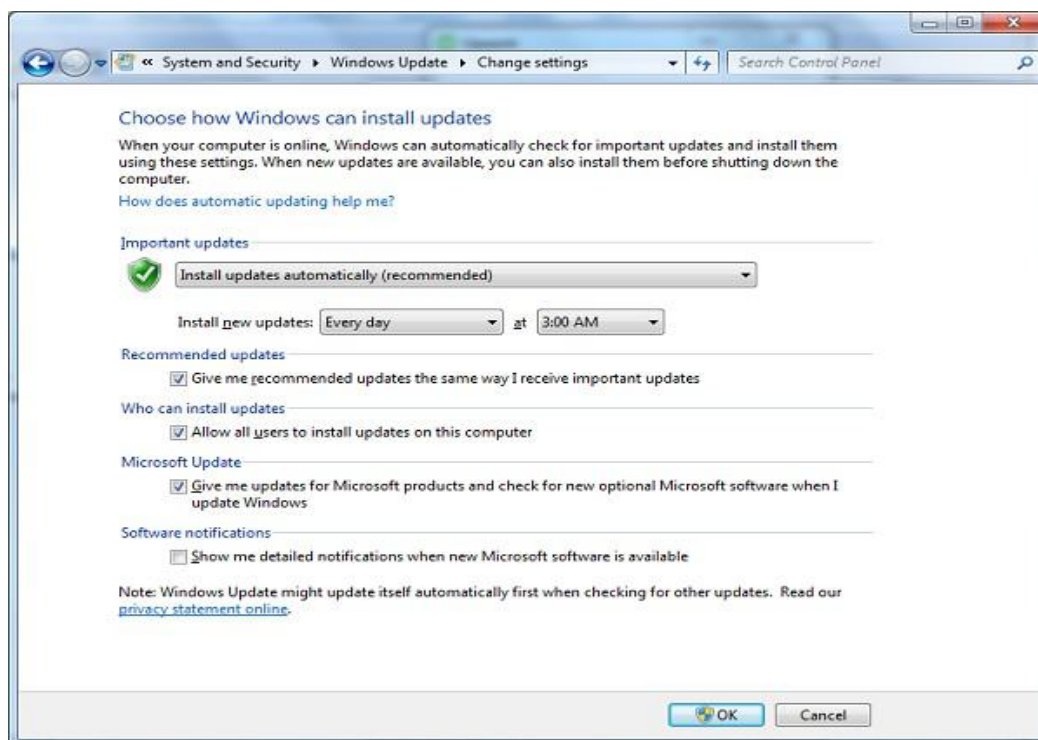
## Quick Fix

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.

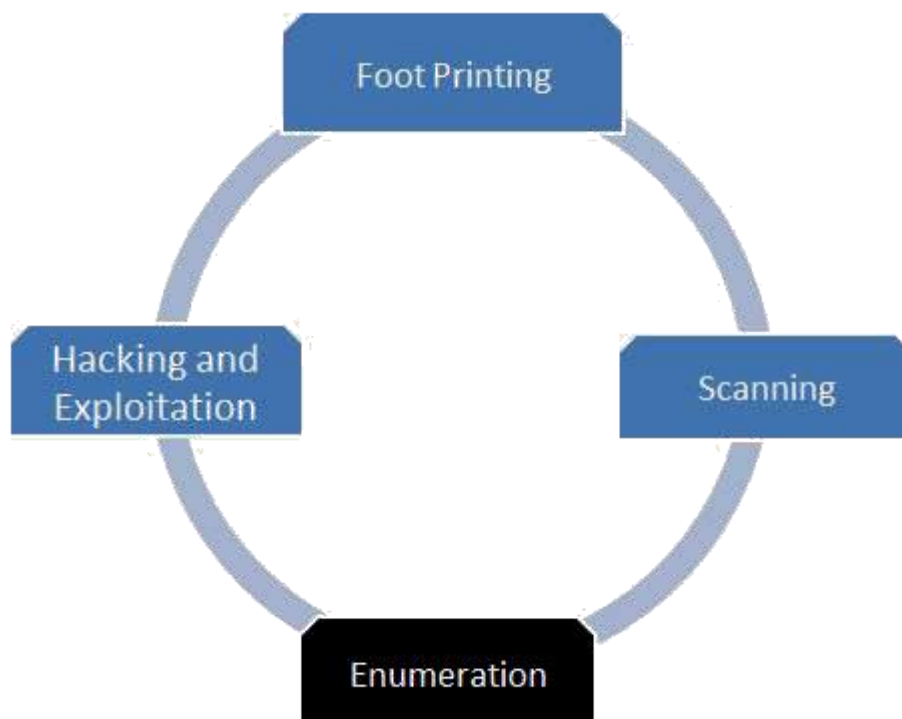
```
yum -y install yum-cron
```



# 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.









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  
ntpd [-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

enum4linux 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.

```
root@kali:~# enum4linux -U -o 192.168.1.200  
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ )  
  
=====
```

Target Information
Target ..... 192.168.1.200
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. <u>administrator, guest, krbtgt, domain admins, root, bin, none</u>

```
=====
```

Enumerating Workgroup/Domain on 192.168.1.200
---

```
=====
```



## 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.

```
root@kali:~# smtp-user-enum -M VRFY -u root -t 192.168.1.25
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

-----
|                               Scan Information                               |
-----

Mode ..... VRFY
Worker Processes ..... 5
Target count ..... 1
Username count ..... 1
Target TCP port ..... 25
Query timeout ..... 5 secs
Target domain .....
```

## 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.