

Forum: [Hack Forums](#)

Thread: [Enumeration](#)

Venusaur - January 5, 2020, 11:13 am

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.

```
Code 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.

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.