

# Levantamento de Informações

+ O objetivo aqui é fazer uma varredura com o nmap do metasploit nos hosts com a porta 139 e 445 de toda a rede que estão abertas e, em seguida, identificar o sistema operacional que está funcionando neles

+ Para pesquisar módulos auxiliares que ajudem na detecção do smb, podemos:

```
search type:auxiliary smb
```

+ Vamos escolher o módulo que nos permite ver o serviço e a versão que estão rodando na máquina:

```
use auxiliary/scanner/smb/smb_version
```

+ Como temos muitos hosts scaneados, pra não passar cada um dos endereços de ip à mão, podemos

```
services -p 445 --rhosts
```

→ Isso irá armazenar todos os endereços desse ip em um arquivo que automaticamente será setado no nosso RHOSTS. Então, basta que apliquemos o **run**

+ Quando dermos o comando **hosts** (ou o **services**), veremos as versões dos serviços rodando por trás das portas

```
msf6 auxiliary(scanner/smb/smb_version) > services
```

host	port	proto	name	state	info
172.16.1.4	139	tcp	netbios-ssn	open	
172.16.1.4	445	tcp	smb	open	
172.16.1.60	139	tcp	netbios-ssn	open	
172.16.1.60	445	tcp	smb	open	SMB Detected (versions:1) (preferred dialect:)(signatures:optional)Windows XP (name:WKS01) (domain:GBUSINESS)
172.16.1.107	139	tcp	netbios-ssn	open	
172.16.1.107	445	tcp	smb	open	SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:required) (uptime:349w 4d 2h 6m 20s) (guid:{3e406130-d9ac-4493-ad02-fd92ad446ad9}) (authentication domain:GBUSINESS)Windows 2008 R2 Enterprise (build:7600) (name:SRVINT) (domain:GBUSINESS)
172.16.1.108	139	tcp	smb	open	Windows 6.1 (Samba 4.2.14-Debian)
172.16.1.165	139	tcp	smb	open	SMB Detected (versions:)(preferred dialect:)(signatures:optional)
172.16.1.233	139	tcp	netbios-ssn	open	
172.16.1.233	445	tcp	smb	open	SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.0.2) (signatures:required) (uptime:288w 1d 1h 51m 22s) (guid:{170091b1-6cb8-467d-85f4-3f8a44b60c77}) (authentication domain:DHCE)Windows 2012 R2 Datacenter (build:9600) (name:SRVSPIDER) (domain:DHCE)
172.16.1.243	139	tcp	netbios-ssn	open	
172.16.1.243	445	tcp	smb	open	SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:)(encryption capabilities:AES-128-GCM) (signatures:required) (guid:{bcb2481-878c-4f78-8d14-9d35411685dd}) (authentication domain:ORIONSCORP2)
172.16.1.245	139	tcp	netbios-ssn	open	
172.16.1.245	445	tcp	smb	open	SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-GCM) (signatures:optional) (guid:{1a9d8401-eece-4818-94e2-befd79380185}) (authentication domain:ORIONSCORP2)
172.16.1.253	139	tcp	netbios-ssn	open	
172.16.1.253	445	tcp	smb	open	SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-GCM) (signatures:optional) (guid:{9bb89b8d-9bd6-4cfb-9f8d-40c251a958e5}) (authentication domain:ORIONSCORP2)