

## TP2 - Parte B - PenTest Scanning

A82200 - Henrique Faria and A81139 - Paulo Bento

Universidade do Minho, Mestrado Integrado em Engenharia Informática

**Resumo** Na primeira parte do trabalho explora-se os vários tipos de scan possíveis com o nmap, passando por detetar os hosts, portas, sistema operativo e serviços. Na segunda parte explora-se a capacidade do OpenVAS para detetar vulnerabilidade, como a diferença entre os resultados detetados pelo mesmo e não pelo Snort. Finalmente tenta-se solucionar alguns problemas detetados com o OpenVas/Snort.

**Palavras-chave:** Nmap · Snort · OpenVas · PenTest · Scanning · SYN Scan · TCP Scan · Vulnerabilidades · CVE

## 1 Parte I

### 1.1 Q1 - Quatro Scans Diferentes

Os seguintes comandos serão executados com target o host Metaexploitable 2 que está localizado no IP 172.16.1.130 e a maquina que os executa em 172.16.1.129.

Os comandos executados correspondem a um Host Discovery, a um UDP scan, a um TCP Connect Scan e um SYN Scan. Sendo explicados nas próximas secções.

#### Host Discovery

O seguinte comando está associado com a descoberta de hosts, também conhecido, como "ping scan". É usado para, de uma forma menos intrusiva e sem fazer scans, detetar os hosts que estão ligados a rede. Em principio, pode ser detetado por IDS, no entanto como pode ser usado também por os administradores de rede seria pouco conveniente bloquear este tipo de tráfego.

```
nmap -sn target
```

O resultado do scan ao metasplitable resulta no XML em anexo 3.1. Pelo mesmo podemos ver que o comando detetou que o host está ligado e a responder, devolvendo também o MAC.

Na figura 1 podemos notar que este tipo de "scan" causa pouco tráfego e passa bastante despercebido para que possa ser detetado visto que faz só um pedido ARP como qualquer outro host na rede. Segundo o manual do nmap devia ter feito um ICMP echo request, um TCP SYN à porta 443 e um TCP ACK à porta 80, mas não foi capturado pelo Wireshark. Em todo o caso as mesmas conclusões mantem-se.

1	0.000000000	Vmware_39:46:88	Broadcast	ARP	42 Who has 172.16.1.130? Tell 172.16.1.129
2	0.000325783	Vmware_7d:0c:d6	Vmware_39:46:88	ARP	60 172.16.1.130 is at 00:0c:29:7d:0c:d6
3	0.031892609	172.16.1.129	172.16.1.1	DNS	85 Standard query 0x8a7a PTR 130.1.16.172.in-addr.arpa
4	0.032000385	172.16.1.1	172.16.1.129	ICMP	113 Destination unreachable (Port unreachable)
5	1.939379583	fe80::250:56ff:fec0::	ff02::2	ICMPv6	70 Router Solicitation from 00:50:56:c0:00:02
6	4.033324193	172.16.1.129	172.16.1.1	DNS	85 Standard query 0x8a7b PTR 130.1.16.172.in-addr.arpa
7	4.034604645	172.16.1.1	172.16.1.129	ICMP	113 Destination unreachable (Port unreachable)
8	5.223599508	Vmware_39:46:88	Vmware_c0:00:02	ARP	42 Who has 172.16.1.1? Tell 172.16.1.129
9	5.223940102	Vmware_c0:00:02	Vmware_39:46:88	ARP	60 172.16.1.1 is at 00:50:56:c0:00:02
10	5.267484782	Vmware_c0:00:02	Vmware_39:46:88	ARP	60 Who has 172.16.1.129? Tell 172.16.1.1
11	5.267527968	Vmware_39:46:88	Vmware_c0:00:02	ARP	42 172.16.1.129 is at 00:0c:29:39:46:88
12	8.034848364	172.16.1.129	172.16.1.1	DNS	85 Standard query 0x8a7c PTR 130.1.16.172.in-addr.arpa
13	8.035174138	172.16.1.1	172.16.1.129	ICMP	113 Destination unreachable (Port unreachable)
14	16.834796217	Vmware_7d:0c:d6	Broadcast	ARP	60 Who has 172.16.1.254? Tell 172.16.1.130

Figura 1. Captura do Wireshark ao nmap -sn

#### UDP Scan

O seguinte comando é utilizado para fazer scan as portas que respondem a pacotes UDP. Este envia a maioria de pacotes UDP "vazios" excepto o que seja de protocolos especifico para as portas que queramos ou para todas.

As portas podem ser detetadas como quatro estados diferentes open, open filtered, closed, filtered. Caso a "porta" responda, encontra-se no primeiro estado, caso não responda com nada, open filtered. Os outros dois estados depende do ICMP com tipo unreachable error. Caso seja código 3 está closed com outros códigos está filtered.

```
nmap -sU target
```

A deteção de portas aberta pode ter vários problemas um deles é que certas portas abertas não respondem a payloads vazios e, as Firewalls que podem ter filtrado os pacotes também não. Por conseguinte, existe a possibilidade de que a porta seja marcada como open filtered. Algumas portas podem ser detetadas com o comando usado para detetar versões já que as respostas que não responderam a pacotes vazios podem responder ao protocolo específico. Esse comando é usado na secção Q4.

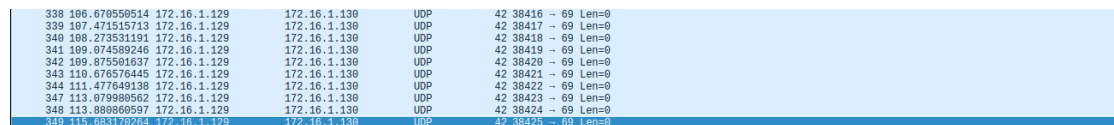
O resultado do scan encontra-se no XML em Anexo 3.2. Existem quatro portas open correspondendo ao serviço domain, rpcbind, netbios-ns, nfs. E três open filtered correspondendo aos serviços dhcpc, tftp, netbios-dgm.

Este filtro o que provoca uma grande quantidade de pacotes serem enviados e recebidos como podemos ver na captura de Wireshark na figura 2. São enviados e recebidos em conjunto 2689 pacotes.



**Figura 2.** Último pacote gerado por nmap -sU

Seguidamente, na figura 3 e na figura 4 podemos ver um exemplo de tráfego para um caso de open filtered e para uma porta open. E, finalmente um caso em que a porta foi determinada como Closed na figura 5.



**Figura 3.** Pacotes gerados por um caso de Open Filtered no nmap -sU



**Figura 4.** Pacotes gerados por um caso de Open no nmap -sU

## TCP Connect Scan

O seguinte comando é executado quando o SYN scan não é possível. Por exemplo, no caso de redes que sejam IPv6. No entanto, o controlo sobre este tipo de scan é menor gerando um número maior de pacotes para gerar a mesma informação que o SYN scan (Número de pacotes na figura 8). No entanto, a diferença de pacotes pode não ser muita caso a maioria das portas estejam fechadas.

```
nmap -sT target
```

1322	525.8780954150	172.16.1.129	172.16.1.130	UDP	42	38416 - 1234	Len=0
1323	526.679492697	172.16.1.129	172.16.1.130	UDP	42	38417 - 1234	Len=0
1324	526.65060502	172.16.1.129	172.16.1.130	ICMP	78	Destination unreachable (Port unreachable)	

▶ Frame 1324: 78 bytes on wire (560 bits), 78 bytes captured (560 bits) on interface 0							
▶ Ethernet II, Src: VMware_7d:0c:06 (00:0c:29:7d:0c:06), Dst: VMware_39:46:88 (00:0c:29:39:46:88)							
▶ Internet Protocol Version 4, Src: 172.16.1.129, Dst: 172.16.1.129							
▶ Internet Control Message Protocol							
Type: 3 (Destination unreachable)							
Code: 3 (Port unreachable)							
Checksum: 9e582a [correct]							
[Checksum Status: Good]							
Unused: 00000000							
▶ Internet Protocol Version 4, Src: 172.16.1.129, Dst: 172.16.1.130							
▶ User Datagram Protocol, Src Port: 38417, Dst Port: 1234							

**Figura 5.** Pacotes gerados por um caso de Closed no nmap -sU

Este modo do nmap realiza o seguinte. Primeiro tenta estabelecer ligação com o host destino através do three-way handshake, seguidamente fecha a conexão usando um pacote RST como pode-se ver na figura 6. A título de exemplo um exemplo de conexão falhada na figura 7.

62	13.048869661	172.16.1.129	172.16.1.130	TCP	74	38818 - 23 [SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3509656377 TSecr=0 WS=128
90	13.053328203	172.16.1.129	172.16.1.130	TCP	74	23 - 38818 [SYN, ACK]	Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=137212 TSecr=35096563
161	13.053581780	172.16.1.129	172.16.1.130	TCP	66	38818 - 23 [ACK]	Seq=1 Ack=1 Win=64256 Len=0 TSval=3509656382 TSecr=137212
169	13.054093049	172.16.1.129	172.16.1.130	TCP	60	38818 - 23 [RST, ACK]	Seq=1 Ack=1 Win=64256 Len=0 TSval=3509656386 TSecr=137212

**Figura 6.** Pacotes gerados por o nmap -sT para uma conexão

867	13.169481558	172.16.1.129	172.16.1.130	TCP	74	58552 - 24 [SYN]	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3509656438 TSecr=0 WS=128
877	13.169698451	172.16.1.130	172.16.1.129	TCP	60	24 - 58552 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0

**Figura 7.** Pacotes gerados por o nmap -sT aquando de uma falha na conexão

O comando gera o XML seguinte que se encontra em Anexo 3.3. Analisando o XML pode-se ver que foram detetados 23 portas Open para conexões TCP desde o serviço FTP ate o ajp13. O resto das portas foram todas marcadas como Closed.

Um IDS devia detetar este tipo de scan como detetaria o SYN scan que seria mais "leve". No entanto, a maioria não contem este tipo de mecanismo para filtrar os scans. No entanto pode adicionar algum tipo de aviso a um log visto que um host abriu uma conexão e , seguidamente, fechou, sem enviar nenhum tipo de pacotes "úteis". Considerando esse tipo de tráfego como anómalo.

2858	13.140940182	172.16.1.130	172.16.1.129	TCP	60	8701 - 44682 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
------	--------------	--------------	--------------	-----	----	-------------------------	-------------------------

**Figura 8.** Número de Pacotes gerado por nmap -sT

## SYN Scan

O SYN Scan é executado com o seguinte comando do nmap. Ao contrário do TCP Connect scan este só envia o packet SYN para "começar" a conexão, no entanto, após receber o SYN ACK do host objetivo lista como Open e deixa o OS enviar um pacote RST para "cortar" o three-way handshake (Figura 9). Caso o próprio servidor retorne um pacote RST então é classificada

como Closed(Figura 10).Caso receba nenhuma resposta mesmo de várias tentativas ou receba um ICMP unreachable error então marca como filtered.

`nmap -sS`

O resultado do XML também encontra-se em Anexo 3.4.Os resultados retirados do mesmo são que existem , como detetado anteriormente, 23 portas Open e 977 portas Closed. Correspondendo aos mesmos serviços encontrados por o TCP Connection Scan.

70	13.682114287	172.16.1.129	172.16.1.130	TCP	50 46123 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
74	13.682253951	172.16.1.130	172.16.1.129	TCP	60 80 → 46123 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
75	13.682261343	172.16.1.129	172.16.1.130	TCP	54 46123 → 80 [RST] Seq=1 Win=0 Len=0

**Figura 9.** Pacotes gerados com `nmap -sS` resultado em port Open

713	13.195403685	172.16.1.129	172.16.1.130	TCP	50 46123 → 79 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
719	13.195533411	172.16.1.130	172.16.1.129	TCP	60 79 → 46123 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

**Figura 10.** Pacotes gerados com `nmap -sS` resultado em port Closed

A seguir podemos ver o numero de pacotes gerados tanto recebidos como enviados na figura 11. O SYN Scan é menos intrusivo que o TCP Connect Scan já que só executa a primeira parte do three-away handshake e o número de pacotes é menor como referido anteriormente.No entanto necessita privilegios para raw-packets. Apesar destas propriedades ainda pode ser detetado e filtrado por Firewall pessoais e IDS bem configurados.

2835	13.143102231	172.16.1.130	172.16.1.129	TCP	60 3737 → 46123 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
------	--------------	--------------	--------------	-----	--

**Figura 11.** Número de Pacotes gerado por `nmap -sS`

## 1.2 Q2 - Mais Quatro Scans

Os seguintes nmaps executados verificam que o host scanme (45.33.32.156) está ativo.Os comandos que irão ser executados para cada host , isto é, para o scanme e Metaexploitable 2 serão apresentados, explicados e analisados nas seções seguintes.Estes comandos são especificamente um ACK scan, TCP FIN scan, TCP NULL scan e um TCP Xmas scan.

### ACK Scan

O comando seguinte executa um ACK scan para a maquina objetivo.O scan envia pacotes ACK para o host ,não para determinar se as portas estão Open ou Open Filtered, mas ,sim, para determinar se a porta está Filtered ou Unfiltered,ou seja, para determinar o ruleset da Firewall (conjunto de regras que usa para filtrar) e se esta mantém o registo das conexões ativas presentes no sistema.Caso assim seja, irá filtrar os ACK visto que o nmap não esta conectado ao serviço/porta á qual está direcionada o scan.

`nmap -sA target`

O scan interpreta um pacote RST de resposta como Unfiltered(Figura 12), caso não haja resposta como Filtered e um ICMP unreachable erro também como filtered.

33	13.085357646	172.16.1.129	172.16.1.130	TCP	54 56155 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
38	13.086019448	172.16.1.130	172.16.1.129	TCP	60 80 → 56155 [RST] Seq=1 Win=0 Len=0

**Figura 12.** Pacotes gerados por uma porta Unfiltered com `nmap -sA`

Ambos os resultados XML para as duas maquinas encontram-se em Anexo 3.5 e Anexo 3.6. Ambos apresentam os mesmos resultados. Para as portas analisadas foram detetadas todas como unfiltered. Os pacotes gerados pelo `nmap` são por volta dos 2000 para as duas maquinas no total (enviados mais recebidos) como pode-se ver nas seguintes figuras.

2012	13.191149241	172.16.1.130	172.16.1.129	TCP	60 5950 → 56155 [RST] Seq=1 Win=0 Len=0
------	--------------	--------------	--------------	-----	---

**Figura 13.** Número total de pacotes gerados pelo scan `-sA` para a Metaexploitable 2

2000	9.204980380	45.33.32.150	192.168.171.129	TCP	60 443 → 56652 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
------	-------------	--------------	-----------------	-----	---

**Figura 14.** Número total de pacotes gerados pelo scan `-sA` para o Scanme

### TCP FIN, NULL, Xmas Scan

Os três comandos seguintes executam, respetivamente, um TCP FIN scan, TCP NULL Scan e um TCP Xmas Scan. Todos eles exploram uma "vulnerabilidade" presente no RFC do TCP que diz "if the [destination] port state is CLOSED .... an incoming segment not containing a RST causes a RST to be sent in response." também não responde com RST caso seja um SYN ou um ACK. O objetivo dos comandos descobrir quais as portas que estão Closed e quais estão Open.

O TCP FIN scan marca a flag que representa que o pacote é um FIN.

`nmap -sF`

O TCP NULL scan deixa as flags do header a 0, isto é, deixa o pacote sem tipo.

`nmap -sN`

O TCP Xmas scan marca todas as Flags que pode, ou seja, FIN, PSH e URG.

`nmap -sX`

A interpretação pode ser Open Filtered caso não haja resposta. Caso seja um pacote RST está Closed. E, caso, seja um ICMP unreachable error então a porta está Filtered.

Estes tipos de scan pode passar mais despercebidos que um ACK scan ou que até um SYN scan através de Firewall que não mantenham registo das ligações. No entanto, existem três problemas com este tipo de scan.

Primeiro, os IDS modernos já podem ser configurados para detetar este tipo de scan. Segundo, nem todos os sistemas seguem o RFC do TCP implementando todos os aspetos. E, por último, pode não ser possível distinguir entre uma porta aberta e uma filtrada já que a Firewall pode simplesmente não responder e filtrar o pacote.

Idealmente, complementar-se-ia este scan com um SYN scan ou outro parecido que possa detetar se as portas estão abertas. Desta forma, os consequentes scans irão "correr" menos portas passando mais despercebidos.

Analisando os resultados dos nmap's executados direcionados ao Metaexploitable 2. Os três comandos retornam que existem 23 portas Open Filtered, as mesmas descobertas nos scans anteriores. Podemos ver nas figuras 16, 18, 20 exemplos de portas assinaladas como closed e nas figuras 15, 17, 19 de portas sinalizadas como Open Filtered pelos diferentes comandos. Os resultados do nmap estão no Anexo 3.7, Anexo 3.8 e Anexo 3.9.

44	13.093793111	172.16.1.129	172.16.1.130	TCP	54 35280 → 80 [FIN] Seq=1 Win=1024 Len=0
787	14.191977333	172.16.1.129	172.16.1.130	TCP	54 35281 → 80 [FIN] Seq=1 Win=1024 Len=0

**Figura 15.** Pacotes gerados por o nmap -sF com uma porta Open Filtered para o Metaexploitable 2

211	13.122398726	172.16.1.129	172.16.1.130	TCP	54 35280 → 79 [FIN] Seq=1 Win=1024 Len=0
261	13.126214277	172.16.1.130	172.16.1.129	TCP	60 79 → 35280 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

**Figura 16.** Pacotes gerados por o nmap -sF com uma porta Closed para o Metaexploitable 2

20	13.076507830	172.16.1.129	172.16.1.130	TCP	54 45234 → 80 [<None>] Seq=1 Win=1024 Len=0
855	14.183900814	172.16.1.129	172.16.1.130	TCP	54 45235 → 80 [<None>] Seq=1 Win=1024 Len=0

**Figura 17.** Pacotes gerados por o nmap -sN com uma porta Open Filtered para o Metaexploitable 2

1314	14.208006695	172.16.1.129	172.16.1.130	TCP	54 45234 → 79 [<None>] Seq=1 Win=1024 Len=0
1320	14.208124160	172.16.1.130	172.16.1.129	TCP	60 79 → 45234 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

**Figura 18.** Pacotes gerados por o nmap -sN com uma porta Closed para o Metaexploitable 2

49	13.111635767	172.16.1.129	172.16.1.130	TCP	54 56962 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
688	14.207107495	172.16.1.129	172.16.1.130	TCP	54 56963 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

**Figura 19.** Pacotes gerados por o nmap -sX com uma porta Open Filtered para o Metaexploitable 2

Seguidamente, proceder-se-á a analisar os resultados feitos ao host Scanme. Os XML resultantes dos comandos executados estão nos Anexos 3.10, 3.11, 3.12. Os resultados são todos iguais

619	13.192338887	172.16.1.129	172.16.1.130	TCP	54 56962 → 79 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
633	13.193230020	172.16.1.130	172.16.1.129	TCP	60 79 → 56962 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

**Figura 20.** Pacotes gerados por o nmap -sX com uma porta Closed para o Metaexploitable 2

para as 1000 portas analisadas , isto é, Open Filtered. Combinando com o resultado do ACK scan o mais provável é que as portas estejam todas Open.

Finalmente, do mesmo modo que para a Metaexploitable apresenta-se alguns exemplos de Open Filtered capturados pelo Wireshark aquando do scan feito ao Scanme. Nas figuras 21,22,23 são exemplos dos pacotes trocados no caso supra referido pelo TCP FIN scan, TCP NULL scan e o TCP Xmas scan.

O volume de dados encontra-se em volta dos 2000 pacotes também sendo muito parecido entre eles e com ACK scan.

399	1.818290572	192.168.171.129	45.33.32.156	TCP	54 64672 → 79 [FIN] Seq=1 Win=1024 Len=0
487	1.923351184	192.168.171.129	45.33.32.156	TCP	54 64673 → 79 [FIN] Seq=1 Win=1024 Len=0

**Figura 21.** Pacotes gerados por o nmap -sF com uma porta Closed para o Scanme

921	2.509880587	192.168.171.129	45.33.32.156	TCP	54 40006 → 79 [<None>] Seq=1 Win=1024 Len=0
996	2.610458032	192.168.171.129	45.33.32.156	TCP	54 40007 → 79 [<None>] Seq=1 Win=1024 Len=0

**Figura 22.** Pacotes gerados por o nmap -sN com uma porta Closed para o Scanme

1075	2.758751979	192.168.171.129	45.33.32.156	TCP	54 53748 → 81 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
1146	2.859147267	192.168.171.129	45.33.32.156	TCP	54 53749 → 81 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

**Figura 23.** Pacotes gerados por o nmap -sX com uma porta Closed para o Scanme

### 1.3 Q3 - Sistema Operativo da VM Metasploitable 2

Nesta secção ir-se-á descrever como foi detetado o Sistema Operativo da Metasploitable 2 através do NMap. Explicando sucintamente como o próprio Nmap o faz. Analisando também os resultados obtidos.

O comando utilizado para reconhecer o sistema operativo usado pela VM Metasploitable 2 foi:

```
nmap -O 172.16.130
```

O comando faz a deteção do sistema operativo através de TCP/IP fingerprinting, isto é, envia pacotes TCP e UDP para examinar os bits que se encontram nas respostas. Alguns dos testes realizados são o tamanho inicial da janela, o suporte a certas opções do TCP entre outros. Seguidamente, compara com a base de dados de fingerprint para tentar reconhecer o sistema operativo que daria essas respostas.

Através das funcionalidades do Zenmap foi extraído o resultado do scan para um xml que se encontra em Anexo 3.13. Na resposta podemos ver também os serviços ativos nas várias portas



como o MAC. Ao continuar a ler a resposta podemos ver que a máquina analisada corre um sistema operativo Linux entre as versões 2.6.9 e 2.6.33 com o kernel linux.kernel: 2.6. Na tag do XML <os> podemos quais as portas usadas e sobre que protocolo tal como a accuracy do resultado que, neste caso, é de 100%.

#### 1.4 Q4 - Serviços Ativos na VM Metasploitable 2

Nesta questão ir-se-á descrever como foram detetados os serviços ativos na máquina Metasploitable 2 utilizando o Nmap e, como este o faz. Seguidamente dos serviços detetados analisar-se-á o CVE mais recente para três desses serviços, ou seja, o CVE mais recente para cada um dos serviços escolhidos.

Os serviços ativos do sistema VM Metasploitable 2 foram detetados utilizando o comando :

```
nmap -sV --version-all
```

O comando foi utilizado com a flag --version-all de forma a receber o maior detalhe sobre os serviços e as suas versões. Contudo esta metodologia pode ser mais facilmente detetada.

O Nmap utiliza probes especializadas para detetar as versões dos serviços através das respostas que estes devolvem. Este tenta descobrir desde o protocolo usado, o serviço localizado na porta como a versão do mesmo, caso possível.

O resultado gerado por o nmap e extraído para um XML encontra-se no Anexo 3.14. Através do resultado podemos concluir que existem 23 portas abertas. Nestas encontram-se vários serviços ativos entre eles um servidor Apache na versão 2.2.8, um implementação do SSH (OpenSSH 4.7p1) e também uma base de dados PostgreSQL DB que se encontra entre as versões 8.3.0 e 8.3.7. Realça-se a porta 6000 que apesar da porta estar aberta foi impossível para o nmap descobrir a versão do serviço X11. Esta informação encontra-se disponível no texto do XML também como nas tags finais <port> onde se refere todos os campos que se refere no texto.

Os serviços especificados anteriormente para as versões que se encontram instaladas sofrem das seguintes vulnerabilidades descritas nas seguintes seções.

#### Apache 2.2.8

A vulnerabilidade mais recente encontrada afeta os servidores Apache 2.2.0 até 2.4.29.

Identificada por o CVE-2018-1312. A vulnerabilidade tem CVSS de 6.8 e um vetor de ataque descrito na figura seguinte.

CVSS Score	<b>6.8</b>
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None

**Figura 24.** Vetor de Ataque da CVE-2018-1312

A vulnerabilidade torna o sistema a ataques por repetição visto que ao gerar o HTTP Digest authentication challenge o nonce utilizado para prever este tipo de ataques não é devidamente

gerado utilizando uma pseudo-random seed. Caso um Cluster de servers utilize a mesma configuração para o Digest, o atacante poderia repetir as HTTP requests para os vários servidores sem ser detetado.

## OpenSSH 4.7p1

A vulnerabilidade afeta todas as versões do OpenSSH antes da versao 7.5\_p1-r3 não inclusive. Identificada pelo CVE-2017-15906 tem CVSS de 5.0 e o seguinte vetor de ataque.

CVSS Score	<b>5.0</b>
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. )
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	269

**Figura 25.** Vetor de Ataque do CVE-2017-15906

A vulnerabilidade permite criar ficheiros com lenght zero por um atacante. Isto é possível visto que não é propriamente impedido ao atacante de utilizar operações de escrita no modo de readonly. Exatamente na função process\_open no ficheiro de código sftp-server.c.

## PostgreSQL 8.3.7

A versão do serviço não foi precisamente identificada. Por consequência, pesquisar-se-á por vulnerabilidades para a versão mais recente possível.

A vulnerabilidade afeta todas as versoes anteriores a 9 e quase todas antes da 10.5. Identificada pelo CVE-2018-1115 tem CVSS de 6.4 e o seu vetor de ataque esta descrito na figura seguinte.

CVSS Score	<b>6.4</b>
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. )
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	CWE id is not defined for this vulnerability

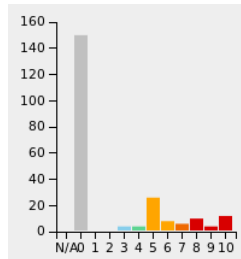
**Figura 26.** Vetor de Ataque do CVE-2018-1115

A vulnerabilidade permite ,aos atacante que possam conetar-se a base de dados, em certos cenários, "crashar"o servidor ou distribuir as mensagens de log por ficheiros de log não desejados. É possível visto que o modulo "adminpack" instala uma função nova pg\_logfile\_rotate() que é um alias para uma função do próprio postgresQL. Essa função built-in só deveria ser executada por superuser ,no entanto o alias pode ser executado por qualquer utilizador.

## 2 Parte II

### 2.1 Q5 - Resultados Globais

Após o scan feito pelo OpenVass obtivemos os seguintes dados.



**Figura 27.** Gravidade das vulnerabilidades encontradas

Nesta figura podemos observar o número de vulnerabilidades conhecidas e atualmente na base de dados do OpenVass encontradas no Metasploite2. Em seguida apresentam-se as vulnerabilidades encontradas no Sistema visado.

#### Apache HTTP Server

O servidor avaliado corre com um servidor Apache HTTP e está vulnerável a permitir acesso a informação sensível através das cookies. O error ocorre devido á resposta de erro por defeito com código de estado 400, quando não é configurado um documento personalizado de erro.

Isto pode levar a que um atacante consiga obter informação sensível que possa auxiliar num ataque futuro.

Pode ser facilmente corrigido atualizando para uma versão 2.2.22 ou posterior.

#### phpMyAdmin

O servidor está a correr phpMyAdmin e é vulnerável a cross-site scripting. Isto permite que atacantes conduzam ataques com injeção de código HTML arbitrário para gerar ataques de phishing.

Ainda não foi criada uma solução e provavelmente nenhuma será criada. Deve-se mudar o serviço ou desabilitar a resposta.

#### Samba MS-RPC

Esta vulnerabilidade permite que atacantes executem comandos arbitrários na shell. Com isto o atacante pode correr comandos na shell com as permissões da aplicação.

Para corrigir isto basta fazer uma atualização do software usado.

#### PostgreSQL

Podia-se aceder a uma base de dados PostgreSQL ao usar credenciais fracas, nomeadamente com a password "postgres".

Para evitar acessos indevidos deve-se redefinir a palavra pass o mais cedo possível.

### **VNC Brute Force Login**

Este método passa por tentar aceder como uma password dada via protocolo VNC, a password usada é password.

Basta substituir a password por uma mais difícil.

### **DistCC**

Esta vulnerabilidade passa por aproveitar a falta de restrições nos acessos às portas do servidor, dado que o DistCC confia cegamente nos clientes. Um atacante pode simplesmente correr comandos arbitrários no servidor.

Este problema resolve-se fazendo uma atualização do software.

### **Distributed Ruby**

Esta falha permite que sistemas não autorizados executem comandos distribuídos, isto pois o Distributed Ruby não previne atividades de acesso privilegiado, caso este corra com acesso privilegiado um atacante pode executar comandos ou scripts ruby.

Para colmatar a falha basta restringir as permissões do serviço caso se permita o acesso a utilizadores não confiáveis ou então definir ACLs apropriadas no sistema.

### **Ingreslock**

Uma backdoor é instalado no servidor remoto. O serviço responde a um id: uid=0, gid=0. Com isto um atacante pode executar código arbitrário com privilégios "root".

Não há correção disponível para esta vulnerabilidade.

## **2.2 Q6 - Tráfego Anómalo**

Nesta secção serão analisados dois exemplos de tráfego anómalo reportados pelo Snort.

### **PROTOCOL - SNMP AgentX/tcp request**

O 5º pacote identificado pelo Snort corresponde ao pacote número 233 do WireShark.

Este pacote corre sobre TCP e tem origem no endereço: 172.16.1.128, porta: 46754 destinando-se ao endereço: 172.16.1.129, porta: 80.

### **CVE-2002-0012**

- CVSS Scores & Vulnerability Types	
CVSS Score	<b>10.0</b>
Confidentiality Impact	<b>Complete</b> (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	<b>Complete</b> (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	<b>Complete</b> (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	<b>Low</b> (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. )
Authentication	<b>Not required</b> (Authentication is not required to exploit the vulnerability.)
Gained Access	<b>Admin</b>
Vulnerability Type(s)	Denial Of Service Gain privileges
CWE ID	<a href="#">264</a>

**Figura 28.** CVE-2002-0012

Definição: Há vulnerabilidades num grande número de implementações do SNMP que permitem que atacantes possam efetuar ataques de denial of Service ou ganhar privilégios via uma armadilha SNMPv1.

Modo de proceder: O atacante provoca um erro cujo estado seja 400. Devido a um erro na criação de um documento personalizado este pode ser explorado para expor "httpOnly"cookies.

### FTP Command Overflow Attempt

O 13º pacote identificado pelo Snort corresponde ao pacote número 9484 do WireShark.

Este pacote corre sobre TCP fazendo uso de FTP e tem origem no endereço: 172.16.1.128, porta: 56385 destinando-se ao endereço: 172.16.1.129, porta: 21.

De seguida apresenta-se o CVE mais recente relacionado com este problema.

### CVE-2007-0019

- CVSS Scores & Vulnerability Types	
CVSS Score	<b>6.5</b>
Confidentiality Impact	<b>Partial</b> (There is considerable informational disclosure.)
Integrity Impact	<b>Partial</b> (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	<b>Partial</b> (There is reduced performance or interruptions in resource availability.)
Access Complexity	<b>Low</b> (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. )
Authentication	<b>Single system</b> (The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).)
Gained Access	<b>User</b>
Vulnerability Type(s)	Execute Code Overflow
CWE ID	CWE id is not defined for this vulnerability

**Figura 29.** CVE-2002-0012

Definição: O atacante executa código arbitrário fazendo uso de um comando LIST longo e outros pedidos ao serviço FTP permitindo que estes executem código arbitrário com pedidos não especificados ao serviço HTTP.

### 2.3 Q7 - Vulnerabilidades Snort vs OpenVass




- A principal razão para o Snort apresentar vulnerabilidades que o OpenVas não reporta deve-se aos falsos positivos.  
Há comportamentos reconhecidos como tráfego anómalo, por exemplo um "port scan" feito por um administrador da rede. O Snort vai detetar este tráfego e sinaliza-lo como tal, no entanto não se trata de uma tentativa de intrusão. Já o OpenVass não reporta este scan visto que apenas reporta falhas anómalas como por exemplo a utilização do serviço regexd sem ser sobre ssh que permite o envio de passwords em texto limpo.
- Uma razão pela qual o Snort pode apresentar mais falhas do que o OpenVas trata-se de o OpenVas trabalhar sobre aplicações e o Snort sobre a camada de rede. Assim o Snort pode reportar vários pacotes com comportamento anómalo como um "port scan", no entanto estes pacotes não representam necessariamente a tentativa de exploração de uma falha pois por exemplo este scan pode ter sido feito pelo administrador da rede. Já o OpenVass deteta e reporta uma falha numa aplicação ou serviço no qual este fornece de alguma forma manipulação ou obtenção de informação sensível.

### 2.4 Q8 - Correção de vulnerabilidades

Para visualização da correção das falhas alvo, note-se que o OpenVass faz um scan seguindo sempre a mesma ordem de teste portanto após a indicação de como foi corrigida cada falha aparecerá uma imagem com o antes e o depois das correções e vendo a falha anterior á falha alvo e a posterior constatar-se-á que a falha a ser corrigida foi de facto colmatada.

#### HTTP Debugging Methods (Trace/Track) Enabled

- Descrição da Vulnerabilidade: O servidor Web permite metodos de rastreamento HTTP que são usados para corrigir conexões ao servidor web. Neste caso o método ativo é o TRACE. Com esta vulnerabilidade o atacante pode enganar o sistema fazendo com que este lhe envie as suas credencias.
- Método de resolução: Basta desabilitar o uso do Trace para corrigir esta vulnerabilidade. Para proceder á correção do problema primeiro foi preciso encontrar o ficheiro do apache2 responsável por desabilitar o trace, este ficheiro chama-se *httpd.conf* e está localizado em */etc/apache2/*.  
Em seguida abriu-se este ficheiro recorrendo ao comando nano como superuser: *sudo nano httpd.conf* e escreveu-se o seguinte no ficheiro: *TraceEnable Off*.

HTTP Security Headers Detection		80%	172.16.1.129	80/tcp	Mon Nov 25 19:31:53 2019
HTTP Debugging Methods (TRACE/TRACK) Enabled		99%	172.16.1.129	80/tcp	Mon Nov 25 19:34:08 2019
phpinfo() output Reporting		80%	172.16.1.129	80/tcp	Mon Nov 25 19:33:52 2019

**Figura 30.** HTTP Debugging Methods (Trace/Track) Enabled

HTTP Security Headers Detection		80%	172.16.1.129	80/tcp	Tue Nov 26 04:02:48 2019
phpinfo() output Reporting		80%	172.16.1.129	80/tcp	Tue Nov 26 04:05:29 2019

Figura 31. HTTP Debugging Methods (Trace/Track) Disabled

- Vulnerabilidades extra corrigidas: Nenhuma.

### Rexecd Service Detection

- Descrição da Vulnerabilidade: Este serviço permite a execução de comandos na shell de um computador remoto. No entanto o rexec permite a autenticação lendo o username e password descriptados da socket.
- Método de resolução: Desabilitar o uso do serviço rexec e usar alternativas como o SSH. Para realizar isto temos de ir até á pasta /etc, nesta abrimos com o comando `sudo nano inetd.conf` o ficheiro inetd.conf e alteramos a linha: `exec stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rexecd` para `exec stream tcp nowait root /usr/sbin/sshd /usr/sbin/in.rexecd`. Isto fará com que este serviço inicie o servidor rexecd usando ssh.

Telnet Service Detection		80%	172.16.1.129	23/tcp	Mon Nov 25 19:21:43 2019
rexec Passwordless / Unencrypted Cleartext Login		80%	172.16.1.129	512/tcp	Mon Nov 25 19:32:32 2019
PostgreSQL Detection		80%	172.16.1.129	5432/tcp	Mon Nov 25 19:19:04 2019

Figura 32. Rexecd Service over tcpd

Telnet Service Detection		80%	172.16.1.129	23/tcp	Tue Nov 26 03:54:25 2019
PostgreSQL Detection		80%	172.16.1.129	5432/tcp	Tue Nov 26 03:52:16 2019

Figura 33. Rexecd Service over sshd



- Vulnerabilidades extra corrigidas: Nenhuma.

### Bind Shell Backdoor Detection



- Descrição da Vulnerabilidade: Há uma possível backdoor instalada no servidor remoto. O comando está a responder a um `id=0(root)` e `gid=0(root)`. Um atacante pode executar um comando no contexto da aplicação e comprometer o sistema.

- Método de resolução: Existem 3 métodos de corrigir esta vulnerabilidade.
- Verificar se o servidor foi comprometido e reinstalar o sistema se necessário.
- Desativar o ingreslock.

O método aplicado é o bloqueio do início do serviço simplesmente comentando a linha *ingeslock stream tcp nowait root /bin/bash bash -i*.

PHP-CGI-based setups vulnerability when parsing query string parameters from php files.		7.5 (High)	95%	172.16.1.129	80/tcp	Mon Nov 25 19:36:51 2019
Possible Backdoor: Ingreslock		10.0 (High)	99%	172.16.1.129	1524/tcp	Mon Nov 25 19:38:19 2019
PostgreSQL weak password		9.0 (High)	99%	172.16.1.129	5432/tcp	Mon Nov 25 19:39:53 2019

**Figura 34.** Ingreslock backdoor enabled

PHP-CGI-based setups vulnerability when parsing query string parameters from php files.		7.5 (High)	95%	172.16.1.129	80/tcp	Tue Nov 26 04:08:40 2019
PostgreSQL weak password		9.0 (High)	99%	172.16.1.129	5432/tcp	Tue Nov 26 04:11:45 2019

**Figura 35.** Ingreslock Service not started

- Vulnerabilidades extra corrigidas: Nenhuma.

### VNC Server 'password' Password

- Descrição da Vulnerabilidade: O servidor VNC a correr no computador remoto utiliza uma password fraca, por defeito esta password é 'password'. Um atacante pode tirar partido disto para obter controlo sobre o sistema.

Note-se que antes de podermos corrigir o a falha do VNC tivemos de o inicializar com o comando: *sudo vncserver*. Isto pois o VCN estava mal inicializado, posteriormente foi criado um ficheiro *passwd* em */home/msfadmin/.vnc/* onde foi colocada a nova password do vnc.

- Método de resolução: Alterar a palavra pass para uma forte.

Para proceder á geração de uma password forte utilizamos um gerador online com 16 caracteres. A password obtida foi: *5?V=X#ℰkAdB'H6+y*, infelizmente o vnc tem as password truncadas para 8 caracteres automaticamente, assim a password usada foi: *5?V=X#ℰk*.

*Nota:* Como as passwords do VNC são truncadas para 8 caracteres, este é extremamente inseguro. Como o objetivo do trabalho é corrigir o mesmo apenas mudamos a password, no entanto achamos melhor que seja usado outro serviço e que este seja descontinuado.



OS Detection Consolidation and Reporting		80%	172.16.1.129	general/tcp	Mon Nov 25 19:32:38 2019
VNC Brute Force Login		95%	172.16.1.129	5900/tcp	Mon Nov 25 19:38:34 2019

Figura 36. VNC Server com a password 'password'

Vulnerability		Severity	QoD	Host	Location	Created
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm		4.0 (Medium)	80%	172.16.1.129	5432/tcp	Tue Nov 26 08:51:52 2019
OS Detection Consolidation and Reporting		0.0 (Log)	80%	172.16.1.129	general/tcp	Tue Nov 26 08:57:12 2019
VNC Brute Force Login		0.0 (Log)	95%	172.16.1.129	5902/tcp	Tue Nov 26 09:01:32 2019

Figura 37. VNC Server com a password '5?V=X#&amp;k'

Vulnerability		Severity	QoD	Host	Location	Actions
VNC Brute Force Login		0.0 (Log)	95%	172.16.1.129	5902/tcp	
<b>Summary</b> Try to log in with given passwords via VNC protocol.						
<b>Vulnerability Detection Result</b> Too many unsuccessful connection attempts are made which means the scanner IP got blocked. Therefore the brute force check was aborted.						

Figura 38. Resultado do acesso ao VNC Server com a password '5?V=X#&amp;k'

- Vulnerabilidades extra corrigidas: Nenhuma
- Vulnerabilidades criadas: A correção da vulnerabilidade proposta levou ao aparecimento de outra vulnerabilidade: *Denial of Service (DoS)*, como se vê na figura acima.

### 3 Anexos

#### 3.1 Nmap para Host Discovery

Listing 1.1. Nmap OS

```

1 <?xml version="1.0" encoding="iso-8859-1"?>
2 <?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="
  text/xsl"?><nmaprun start="1574544133" profile_name=""
  xmloutputversion="1.04" scanner="nmap" version="7.80" startstr="Sat
  Nov 23 16:22:13 2019" args="nmap -sn 172.16.1.130"><verbose level="0
  "></verbose><debugging level="0"></debugging><output type="
  interactive">Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-23
  16:22 EST
3 Nmap scan report for 172.16.1.130
4 Host is up (0.00034s latency).
5 MAC Address: 00:0C:29:7D:0C:D6 (VMware)
6 Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
7 </output><host comment=""><status state="up"></status><address addrtype=
  "ipv4" vendor="" addr="172.16.1.130"></address><address addrtype="
  mac" vendor="VMware" addr="00:0C:29:7D:0C:D6"></address><hostnames>
  /hostnames><ports></ports><os></os><uptime lastboot="" seconds="">
  /uptime><tcpsequence index="" values="" difficulty=""></tcpsequence>
  <ipidsequence values="" class=""></ipidsequence><tcptssequence values
  ="" class=""></tcptssequence></host><runstats><finished timestr="Sat
  Nov 23 16:22:26 2019" time="1574544146"></finished><hosts down="0"
  total="1" up="1"></hosts></runstats></nmaprun>

```

#### 3.2 Nmap para UDP Scan

Listing 1.2. Nmap OS

```

1 <?xml version="1.0" encoding="iso-8859-1"?>
2 <?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="
  text/xsl"?><nmaprun start="1574545125" profile_name=""
  xmloutputversion="1.04" scanner="nmap" version="7.80" startstr="Sat
  Nov 23 16:38:45 2019" args="nmap -sU 172.16.1.130"><scaninfo
  services=""
  " protocol="udp" numservices="1000" type="udp"></scaninfo><verbose
  level="0"></verbose><debugging level="0"></debugging><output type="
  interactive">Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-23
  16:38 EST
3 Nmap scan report for 172.16.1.130
4 Host is up (0.00048s latency).
5 Not shown: 993 closed ports
6 PORT      STATE      SERVICE
7 53/udp    open       domain
8 68/udp    open|filtered dhcpc
9 69/udp    open|filtered tftp
10 111/udp   open       rpcbind
11 137/udp   open       netbios-ns
12 138/udp   open|filtered netbios-dgm
13 2049/udp  open       nfs
14 MAC Address: 00:0C:29:7D:0C:D6 (VMware)
15
16 Nmap done: 1 IP address (1 host up) scanned in 1102.82 seconds

```

```

17 </output><host comment=""><status state="up"></status><address addrtype=
="ipv4" vendor="" addr="172.16.1.130"></address><address addrtype="
mac" vendor="VMware" addr="00:0C:29:7D:0C:D6"></address><hostnames>
/hostnames><ports><extraports count="993" state="closed"></
extraports><port protocol="udp" portid="53"><state reason="udp-
response" state="open" reason_ttl="64"></state><service method="
table" conf="3" name="domain"></service></port><port protocol="udp"
portid="68"><state reason="no-response" state="open|filtered"
reason_ttl="0"></state><service method="table" conf="3" name="dhcpc"
></service></port><port protocol="udp" portid="69"><state reason="no-
response" state="open|filtered" reason_ttl="0"></state><service
method="table" conf="3" name="tftp"></service></port><port protocol=
"udp" portid="111"><state reason="udp-response" state="open"
reason_ttl="64"></state><service method="table" conf="3" name="
rpcbind"></service></port><port protocol="udp" portid="137"><state
reason="udp-response" state="open" reason_ttl="64"></state><service
method="table" conf="3" name="netbios-ns"></service></port><port
protocol="udp" portid="138"><state reason="no-response" state="open|
filtered" reason_ttl="0"></state><service method="table" conf="3"
name="netbios-dgm"></service></port><port protocol="udp" portid="
2049"><state reason="udp-response" state="open" reason_ttl="64"></
state><service method="table" conf="3" name="nfs"></service></port>
</ports><os></os><uptime lastboot="" seconds=""></uptime><tcpsequence
index="" values="" difficulty=""></tcpsequence><ipidsequence values
="" class=""></ipidsequence><tcptssequence values="" class=""></
tcptssequence><host><runstats><finished timestr="Sat Nov 23 16
:57:08 2019" time="1574546228"></finished><hosts down="0" total="1"
up="1"></hosts></runstats></nmaprun>

```

### 3.3 Nmap para TCP Connect scan

Listing 1.3. Nmap OS

```

1 <?xml version="1.0" encoding="iso-8859-1"?>
2 <?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="
text/xsl"?><nmaprun start="1574544947" profile_name=""
xmloutputversion="1.04" scanner="nmap" version="7.80" startstr="Sat
Nov 23 16:35:47 2019" args="nmap -sT 172.16.1.130"><scaninfo
services="
1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,
" protocol="tcp" numservices="1000" type="connect"></scaninfo>
verbose level="0"></verbose><debugging level="0"></debugging><output
type="interactive">Starting Nmap 7.80 ( https://nmap.org ) at
2019-11-23 16:35 EST
3 Nmap scan report for 172.16.1.130
4 Host is up (0.00067s latency).
5 Not shown: 977 closed ports
6 PORT      STATE SERVICE
7 21/tcp    open  ftp
8 22/tcp    open  ssh
9 23/tcp    open  telnet
10 25/tcp    open  smtp
11 53/tcp    open  domain
12 80/tcp    open  http
13 111/tcp   open  rpcbind
14 139/tcp   open  netbios-ssn
15 445/tcp   open  microsoft-ds
16 512/tcp   open  exec
17 513/tcp   open  login

```

```

18 514/tcp open shell
19 1099/tcp open rmiregistry
20 1524/tcp open ingreslock
21 2049/tcp open nfs
22 2121/tcp open ccproxy-ftp
23 3306/tcp open mysql
24 5432/tcp open postgresql
25 5900/tcp open vnc
26 6000/tcp open X11
27 6667/tcp open irc
28 8009/tcp open ajp13
29 8180/tcp open unknown
30 MAC Address: 00:0C:29:7D:0C:D6 (VMware)
31
32 Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
33 </output><host comment=""><status state="up"></status><address addrtype=
  ="ipv4" vendor="" addr="172.16.1.130"></address><address addrtype="
  mac" vendor="VMware" addr="00:0C:29:7D:0C:D6"></address><hostnames>
  /hostnames><ports><extraports count="977" state="closed"></
  extraports><port protocol="tcp" portid="21"><state reason="syn-ack"
  state="open" reason_ttl="0"></state><service method="table" conf="3"
  name="ftp"></service></port><port protocol="tcp" portid="22"><state
  reason="syn-ack" state="open" reason_ttl="0"></state><service
  method="table" conf="3" name="ssh"></service></port><port protocol="
  tcp" portid="23"><state reason="syn-ack" state="open" reason_ttl="0">
  </state><service method="table" conf="3" name="telnet"></service></
  port><port protocol="tcp" portid="25"><state reason="syn-ack" state=
  "open" reason_ttl="0"></state><service method="table" conf="3" name=
  "smtp"></service></port><port protocol="tcp" portid="53"><state
  reason="syn-ack" state="open" reason_ttl="0"></state><service method
  ="table" conf="3" name="domain"></service></port><port protocol="tcp
  " portid="80"><state reason="syn-ack" state="open" reason_ttl="0">
  </state><service method="table" conf="3" name="http"></service></port>
  <port protocol="tcp" portid="111"><state reason="syn-ack" state="
  open" reason_ttl="0"></state><service method="table" conf="3" name="
  rpcbind"></service></port><port protocol="tcp" portid="139"><state
  reason="syn-ack" state="open" reason_ttl="0"></state><service method
  ="table" conf="3" name="netbios-ssn"></service></port><port protocol
  ="tcp" portid="445"><state reason="syn-ack" state="open" reason_ttl=
  "0"></state><service method="table" conf="3" name="microsoft-ds">
  </service></port><port protocol="tcp" portid="512"><state reason="syn-
  ack" state="open" reason_ttl="0"></state><service method="table"
  conf="3" name="exec"></service></port><port protocol="tcp" portid="
  513"><state reason="syn-ack" state="open" reason_ttl="0"></state>
  <service method="table" conf="3" name="login"></service></port><port
  protocol="tcp" portid="514"><state reason="syn-ack" state="open"
  reason_ttl="0"></state><service method="table" conf="3" name="shell"
  ></service></port><port protocol="tcp" portid="1099"><state reason="
  syn-ack" state="open" reason_ttl="0"></state><service method="table"
  conf="3" name="rmiregistry"></service></port><port protocol="tcp"
  portid="1524"><state reason="syn-ack" state="open" reason_ttl="0">
  </state><service method="table" conf="3" name="ingreslock"></service>
  </port><port protocol="tcp" portid="2049"><state reason="syn-ack"
  state="open" reason_ttl="0"></state><service method="table" conf="3"
  name="nfs"></service></port><port protocol="tcp" portid="2121">
  <state reason="syn-ack" state="open" reason_ttl="0"></state><service
  method="table" conf="3" name="ccproxy-ftp"></service></port><port
  protocol="tcp" portid="3306"><state reason="syn-ack" state="open"
  reason_ttl="0"></state><service method="table" conf="3" name="mysql"
  ></service></port><port protocol="tcp" portid="5432"><state reason="
  syn-ack" state="open" reason_ttl="0"></state><service method="table"

```

```

    conf="3" name="postgresql"</service></port></port protocol="tcp"
    portid="5900">state reason="syn-ack" state="open" reason_ttl="0"</
    state><service method="table" conf="3" name="vnc"></service></port><
    port protocol="tcp" portid="6000">state reason="syn-ack" state="
    open" reason_ttl="0"</state><service method="table" conf="3" name="
    X11"></service></port></port protocol="tcp" portid="6667">state
    reason="syn-ack" state="open" reason_ttl="0"</state><service method
    ="table" conf="3" name="irc"></service></port></port protocol="tcp"
    portid="8009">state reason="syn-ack" state="open" reason_ttl="0"</
    state><service method="table" conf="3" name="ajp13"></service></port
    ></port protocol="tcp" portid="8180">state reason="syn-ack" state="
    open" reason_ttl="0"</state><service method="table" conf="3" name="
    unknown"></service></port></ports><os></os><uptime lastboot="
    seconds=" "></uptime><tcpsequence index=" " values=" " difficulty=" ">
    tcpsequence<ipidsequence values=" " class=" "></ipidsequence>
    tcptssequence values=" " class=" "></tcptssequence></host><runstats>
    finished timestr="Sat Nov 23 16:36:00 2019" time="1574544960"></
    finished><hosts down="0" total="1" up="1"></hosts></runstats></
    nmaprun>

```

### 3.4 Nmap para SYN Scan

Listing 1.4. Nmap OS

```

1 <?xml version="1.0" encoding="iso-8859-1"?>
2 <?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="
  text/xsl"?><nmaprun start="1574545054" profile_name="
  xmloutputversion="1.04" scanner="nmap" version="7.80" startstr="Sat
  Nov 23 16:37:34 2019" args="nmap -sS 172.16.1.130"><scaninfo
  services="
  1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,
  " protocol="tcp" numservices="1000" type="syn"></scaninfo><verbose
  level="0"></verbose><debugging level="0"></debugging><output type="
  interactive">Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-23
  16:37 EST
3 Nmap scan report for 172.16.1.130
4 Host is up (0.00016s latency).
5 Not shown: 977 closed ports
6 PORT      STATE SERVICE
7 21/tcp    open  ftp
8 22/tcp    open  ssh
9 23/tcp    open  telnet
10 25/tcp    open  smtp
11 53/tcp    open  domain
12 80/tcp    open  http
13 111/tcp   open  rpcbind
14 139/tcp   open  netbios-ssn
15 445/tcp   open  microsoft-ds
16 512/tcp   open  exec
17 513/tcp   open  login
18 514/tcp   open  shell
19 1099/tcp  open  rmiregistry
20 1524/tcp  open  ingreslock
21 2049/tcp  open  nfs
22 2121/tcp  open  ccproxy-ftp
23 3306/tcp  open  mysql
24 5432/tcp  open  postgresql
25 5900/tcp  open  vnc
26 6000/tcp  open  X11

```

```

27 6667/tcp open  irc
28 8009/tcp open  ajp13
29 8180/tcp open  unknown
30 MAC Address: 00:0C:29:7D:0C:D6 (VMware)
31
32 Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
33 </output><host comment=""><status state="up"></status><address addrtype=
  ="ipv4" vendor="" addr="172.16.1.130"></address><address addrtype="
  mac" vendor="VMware" addr="00:0C:29:7D:0C:D6"></address><hostnames>
  /hostnames><ports><extraports count="977" state="closed"></
  extraports><port protocol="tcp" portid="21"><state reason="syn-ack"
  state="open" reason_ttl="64"></state><service method="table" conf="3
  " name="ftp"></service></port><port protocol="tcp" portid="22">
  <state reason="syn-ack" state="open" reason_ttl="64"></state><service
  method="table" conf="3" name="ssh"></service></port><port protocol=
  "tcp" portid="23"><state reason="syn-ack" state="open" reason_ttl="
  64"></state><service method="table" conf="3" name="telnet"></service
  ></port><port protocol="tcp" portid="25"><state reason="syn-ack"
  state="open" reason_ttl="64"></state><service method="table" conf="3
  " name="smtp"></service></port><port protocol="tcp" portid="53">
  <state reason="syn-ack" state="open" reason_ttl="64"></state><service
  method="table" conf="3" name="domain"></service></port><port
  protocol="tcp" portid="80"><state reason="syn-ack" state="open"
  reason_ttl="64"></state><service method="table" conf="3" name="http"
  ></service></port><port protocol="tcp" portid="111"><state reason="
  syn-ack" state="open" reason_ttl="64"></state><service method="table
  " conf="3" name="rpcbind"></service></port><port protocol="tcp"
  portid="139"><state reason="syn-ack" state="open" reason_ttl="64"></
  state><service method="table" conf="3" name="netbios-ssn"></service>
  </port><port protocol="tcp" portid="445"><state reason="syn-ack"
  state="open" reason_ttl="64"></state><service method="table" conf="3
  " name="microsoft-ds"></service></port><port protocol="tcp" portid="
  512"><state reason="syn-ack" state="open" reason_ttl="64"></state><
  service method="table" conf="3" name="exec"></service></port><port
  protocol="tcp" portid="513"><state reason="syn-ack" state="open"
  reason_ttl="64"></state><service method="table" conf="3" name="login
  "></service></port><port protocol="tcp" portid="514"><state reason="
  syn-ack" state="open" reason_ttl="64"></state><service method="table
  " conf="3" name="shell"></service></port><port protocol="tcp" portid
  ="1099"><state reason="syn-ack" state="open" reason_ttl="64"></state
  ><service method="table" conf="3" name="rmiregistry"></service></
  port><port protocol="tcp" portid="1524"><state reason="syn-ack"
  state="open" reason_ttl="64"></state><service method="table" conf="3
  " name="ingreslock"></service></port><port protocol="tcp" portid="
  2049"><state reason="syn-ack" state="open" reason_ttl="64"></state>
  <service method="table" conf="3" name="nfs"></service></port><port
  protocol="tcp" portid="2121"><state reason="syn-ack" state="open"
  reason_ttl="64"></state><service method="table" conf="3" name="
  ccproxy-ftp"></service></port><port protocol="tcp" portid="3306">
  <state reason="syn-ack" state="open" reason_ttl="64"></state><service
  method="table" conf="3" name="mysql"></service></port><port
  protocol="tcp" portid="5432"><state reason="syn-ack" state="open"
  reason_ttl="64"></state><service method="table" conf="3" name="
  postgresql"></service></port><port protocol="tcp" portid="5900">
  <state reason="syn-ack" state="open" reason_ttl="64"></state><service
  method="table" conf="3" name="vnc"></service></port><port protocol=
  "tcp" portid="6000"><state reason="syn-ack" state="open" reason_ttl=
  "64"></state><service method="table" conf="3" name="X11"></service>
  </port><port protocol="tcp" portid="6667"><state reason="syn-ack"
  state="open" reason_ttl="64"></state><service method="table" conf="3
  " name="irc"></service></port><port protocol="tcp" portid="8009">

```

```

state reason="syn-ack" state="open" reason_ttl="64">/state</service>
method="table" conf="3" name="ajp13">/service</port></port>
protocol="tcp" portid="8180">state reason="syn-ack" state="open"
reason_ttl="64">/state</service> method="table" conf="3" name="
unknown">/service</port></ports></os></os> uptime lastboot=""
seconds="">/uptime</tcpsequence index="" values="" difficulty="">/
tcpsequence</ipidsequence values="" class="">/ipidsequence</
tcptssequence values="" class="">/tcptssequence</host></runstats>
finished timestr="Sat Nov 23 16:37:47 2019" time="1574545067">/
finished</hosts down="0" total="1" up="1">/hosts</runstats>/
nmaprun>

```

### 3.5 Nmap para o Metaexploitable 2 - Ack Scan

Listing 1.5. Nmap OS

```

1 <?xml version="1.0" encoding="iso-8859-1"?>
2 <?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="
text/xsl"?>nmaprun start="1574546506" profile_name=""
xmloutputversion="1.04" scanner="nmap" version="7.80" startstr="Sat
Nov 23 17:01:46 2019" args="nmap -sA 172.16.1.130">scaninfo
services="
1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119 125,135,139,143-144,146,
" protocol="tcp" numservices="1000" type="ack">/scaninfo</verbose
level="0">/verbose</debugging level="0">/debugging</output type="
interactive">Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-23
17:01 EST
3 Nmap scan report for 172.16.1.130
4 Host is up (0.00053s latency).
5 All 1000 scanned ports on 172.16.1.130 are unfiltered
6 MAC Address: 00:0C:29:7D:0C:D6 (VMware)
7
8 Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds
9 </output></host comment="">status state="up">/status</address addrtypes="
ip v4" vendor="" addr="172.16.1.130">/address</address addrtypes="
mac" vendor="VMware" addr="00:0C:29:7D:0C:D6">/address</hostnames>
/hostnames</ports></extraports count="1000" state="unfiltered">/
extraports</ports></os></os> uptime lastboot="" seconds="">/uptime>
<tcpsequence index="" values="" difficulty="">/tcpsequence</
ipidsequence values="" class="">/ipidsequence</tcptssequence values
="" class="">/tcptssequence</host></runstats>finished timestr="Sat
Nov 23 17:01:59 2019" time="1574546519">/finished</hosts down="0"
total="1" up="1">/hosts</runstats>/nmaprun>

```

### 3.6 Nmap para o Scanme - Ack Scan

Listing 1.6. Nmap OS

```

1 <?xml version="1.0" encoding="iso-8859-1"?>
2 <?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="
text/xsl"?>nmaprun start="1574547327" profile_name=""
xmloutputversion="1.04" scanner="nmap" version="7.80" startstr="Sat
Nov 23 17:15:27 2019" args="nmap -sA 45.33.32.156">scaninfo
services="
1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119 125,135,139,143-144,146,
" protocol="tcp" numservices="1000" type="ack">/scaninfo</verbose
level="0">/verbose</debugging level="0">/debugging</output type="
interactive">Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-23
17:15 EST

```

```

3 Nmap scan report for scanme.nmap.org (45.33.32.156)
4 Host is up (0.00013s latency).
5 All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are unfiltered
6
7 Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
8 </output><host comment=""><status state="up">/status<address addrtype=
  ="ipv4" vendor="" addr="45.33.32.156">/address<hostnames<hostname
  type="PTR" name="scanme.nmap.org">/hostname>/hostnames<ports<
  extraports count="1000" state="unfiltered">/extraports>/ports<os>
  </os><uptime lastboot="" seconds="">/uptime<tcpsequence index=""
  values="" difficulty="">/tcpsequence<ipidsequence values="" class=
  "">/ipidsequence<tcptssequence values="" class="">/tcptssequence>
  </host><runstats<finished timestr="Sat Nov 23 17:15:27 2019" time="
  1574547327">/finished><hosts down="0" total="1" up="1">/hosts>/
  runstats</nmaprun>

```

### 3.7 Nmap para o Metaexploitable 2 - TCP FIN Scan

Listing 1.7. Nmap OS

```

1 <?xml version="1.0" encoding="iso-8859-1"?>
2 <?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="
  text/xsl"?><nmaprun start="1574546553" profile_name=""
  xmloutputversion="1.04" scanner="nmap" version="7.80" startstr="Sat
  Nov 23 17:02:33 2019" args="nmap -sF 172.16.1.130"><scaninfo
  services="
  1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-
  " protocol="tcp" numservices="1000" type="fin">/scaninfo><verbose
  level="0">/verbose><debugging level="0">/debugging><output type="
  interactive">Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-23
  17:02 EST
3 Nmap scan report for 172.16.1.130
4 Host is up (0.0020s latency).
5 Not shown: 977 closed ports
6 PORT      STATE SERVICE
7 21/tcp    open  filtered ftp
8 22/tcp    open  filtered ssh
9 23/tcp    open  filtered telnet
10 25/tcp    open  filtered smtp
11 53/tcp    open  filtered domain
12 80/tcp    open  filtered http
13 111/tcp   open  filtered rpcbind
14 139/tcp   open  filtered netbios-ssn
15 445/tcp   open  filtered microsoft-ds
16 512/tcp   open  filtered exec
17 513/tcp   open  filtered login
18 514/tcp   open  filtered shell
19 1099/tcp  open  filtered rmiregistry
20 1524/tcp  open  filtered ingreslock
21 2049/tcp  open  filtered nfs
22 2121/tcp  open  filtered ccproxy-ftp
23 3306/tcp  open  filtered mysql
24 5432/tcp  open  filtered postgresql
25 5900/tcp  open  filtered vnc
26 6000/tcp  open  filtered X11
27 6667/tcp  open  filtered irc
28 8009/tcp  open  filtered ajp13
29 8180/tcp  open  filtered unknown
30 MAC Address: 00:0C:29:7D:0C:D6 (VMware)

```



```

31
32 Nmap done: 1 IP address (1 host up) scanned in 14.73 seconds
33 </output><host comment=""><status state="up"></status><address addrtype=
="ipv4" vendor="" addr="172.16.1.130"></address><address addrtype="
mac" vendor="VMware" addr="00:0C:29:7D:0C:D6"></address><hostnames>
</hostnames><ports><extraports count="977" state="closed"></
extraports><port protocol="tcp" portid="21"><state reason="no-
response" state="open|filtered" reason_ttl="0"></state><service
method="table" conf="3" name="ftp"></service></port><port protocol="
tcp" portid="22"><state reason="no-response" state="open|filtered"
reason_ttl="0"></state><service method="table" conf="3" name="ssh">
</service></port><port protocol="tcp" portid="23"><state reason="no-
response" state="open|filtered" reason_ttl="0"></state><service
method="table" conf="3" name="telnet"></service></port><port
protocol="tcp" portid="25"><state reason="no-response" state="open|
filtered" reason_ttl="0"></state><service method="table" conf="3"
name="smtp"></service></port><port protocol="tcp" portid="53"><state
reason="no-response" state="open|filtered" reason_ttl="0"></state>
<service method="table" conf="3" name="domain"></service></port><port
protocol="tcp" portid="80"><state reason="no-response" state="open|
filtered" reason_ttl="0"></state><service method="table" conf="3"
name="http"></service></port><port protocol="tcp" portid="111">
<state reason="no-response" state="open|filtered" reason_ttl="0">
</state><service method="table" conf="3" name="rpcbind"></service>
</port><port protocol="tcp" portid="139"><state reason="no-response"
state="open|filtered" reason_ttl="0"></state><service method="table"
conf="3" name="netbios-ssn"></service></port><port protocol="tcp"
portid="445"><state reason="no-response" state="open|filtered"
reason_ttl="0"></state><service method="table" conf="3" name="
microsoft-ds"></service></port><port protocol="tcp" portid="512">
<state reason="no-response" state="open|filtered" reason_ttl="0">
</state><service method="table" conf="3" name="exec"></service>
</port><port protocol="tcp" portid="513"><state reason="no-response" state=
"open|filtered" reason_ttl="0"></state><service method="table" conf=
"3" name="login"></service></port><port protocol="tcp" portid="514">
<state reason="no-response" state="open|filtered" reason_ttl="0">
</state><service method="table" conf="3" name="shell"></service>
</port><port protocol="tcp" portid="1099"><state reason="no-response"
state="open|filtered" reason_ttl="0"></state><service method="table"
conf="3" name="rmiregistry"></service></port><port protocol="tcp"
portid="1524"><state reason="no-response" state="open|filtered"
reason_ttl="0"></state><service method="table" conf="3" name="
ingreslock"></service></port><port protocol="tcp" portid="2049">
<state reason="no-response" state="open|filtered" reason_ttl="0">
</state><service method="table" conf="3" name="nfs"></service>
</port><port protocol="tcp" portid="2121"><state reason="no-response" state=
"open|filtered" reason_ttl="0"></state><service method="table" conf=
"3" name="ccproxy-ftp"></service></port><port protocol="tcp" portid=
"3306"><state reason="no-response" state="open|filtered" reason_ttl=
"0"></state><service method="table" conf="3" name="mysql"></service>
</port><port protocol="tcp" portid="5432"><state reason="no-response"
state="open|filtered" reason_ttl="0"></state><service method="
table" conf="3" name="postgresql"></service></port><port protocol="
tcp" portid="5900"><state reason="no-response" state="open|filtered"
reason_ttl="0"></state><service method="table" conf="3" name="vnc">
</service></port><port protocol="tcp" portid="6000"><state reason="
no-response" state="open|filtered" reason_ttl="0"></state><service
method="table" conf="3" name="X11"></service></port><port protocol="
tcp" portid="6667"><state reason="no-response" state="open|filtered"
reason_ttl="0"></state><service method="table" conf="3" name="irc">
</service></port><port protocol="tcp" portid="8009"><state reason="

```

```

no-response" state="open|filtered" reason_ttl="0"</state><service
method="table" conf="3" name="ajp13"</service></port></port protocol
="tcp" portid="8180"><state reason="no-response" state="open|
filtered" reason_ttl="0"></state><service method="table" conf="3"
name="unknown"</service></port></ports><os></os><uptime lastboot=""
seconds=""></uptime><tcpsequence index="" values="" difficulty=""><
/tcpsequence><ipidsequence values="" class=""></ipidsequence><
tcptssequence values="" class=""></tcptssequence></host><runstats>
finished timestr="Sat Nov 23 17:02:48 2019" time="1574546568"></
finished><hosts down="0" total="1" up="1"></hosts></runstats></
nmaprun>

```

### 3.8 Nmap para o Metaexploitable 2 - TCP NULL Scan

Listing 1.8. Nmap OS

```

1 <?xml version="1.0" encoding="iso-8859-1"?>
2 <?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="
  text/xsl"?><nmaprun start="1574546598" profile_name=""
  xmloutputversion="1.04" scanner="nmap" version="7.80" startstr="Sat
  Nov 23 17:03:18 2019" args="nmap -sN 172.16.1.130"><scaninfo
  services="
  1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-
  " protocol="tcp" numservices="1000" type="null"></scaninfo><verbose
  level="0"></verbose><debugging level="0"></debugging><output type="
  interactive">Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-23
  17:03 EST
3 Nmap scan report for 172.16.1.130
4 Host is up (0.00047s latency).
5 Not shown: 977 closed ports
6 PORT      STATE      SERVICE
7 21/tcp    open|filtered  ftp
8 22/tcp    open|filtered  ssh
9 23/tcp    open|filtered  telnet
10 25/tcp    open|filtered  smtp
11 53/tcp    open|filtered  domain
12 80/tcp    open|filtered  http
13 111/tcp   open|filtered  rpcbind
14 139/tcp   open|filtered  netbios-ssn
15 445/tcp   open|filtered  microsoft-ds
16 512/tcp   open|filtered  exec
17 513/tcp   open|filtered  login
18 514/tcp   open|filtered  shell
19 1099/tcp  open|filtered  rmiregistry
20 1524/tcp  open|filtered  ingreslock
21 2049/tcp  open|filtered  nfs
22 2121/tcp  open|filtered  ccproxy-ftp
23 3306/tcp  open|filtered  mysql
24 5432/tcp  open|filtered  postgresql
25 5900/tcp  open|filtered  vnc
26 6000/tcp  open|filtered  X11
27 6667/tcp  open|filtered  irc
28 8009/tcp  open|filtered  ajp13
29 8180/tcp  open|filtered  unknown
30 MAC Address: 00:0C:29:7D:0C:D6 (VMware)
31
32 Nmap done: 1 IP address (1 host up) scanned in 14.57 seconds
33 </output><host comment=""><status state="up"></status><address addrtype=
  ="ipv4" vendor="" addr="172.16.1.130"></address><address addrtype="

```

```

mac" vendor="VMware" addr="00:0C:29:7D:0C:D6">/address</hostnames>
/hostnames</ports><extraports count="977" state="closed">
</extraports><port protocol="tcp" portid="21"><state reason="no-
response" state="open|filtered" reason_ttl="0">/state><service
method="table" conf="3" name="ftp">/service></port><port protocol="
tcp" portid="22"><state reason="no-response" state="open|filtered"
reason_ttl="0">/state><service method="table" conf="3" name="ssh">
</service></port><port protocol="tcp" portid="23"><state reason="no-
response" state="open|filtered" reason_ttl="0">/state><service
method="table" conf="3" name="telnet">/service></port><port
protocol="tcp" portid="25"><state reason="no-response" state="open|
filtered" reason_ttl="0">/state><service method="table" conf="3"
name="smtp">/service></port><port protocol="tcp" portid="53"><state
reason="no-response" state="open|filtered" reason_ttl="0">/state>
<service method="table" conf="3" name="domain">/service></port><port
protocol="tcp" portid="80"><state reason="no-response" state="open|
filtered" reason_ttl="0">/state><service method="table" conf="3"
name="http">/service></port><port protocol="tcp" portid="111">
<state reason="no-response" state="open|filtered" reason_ttl="0">
</state><service method="table" conf="3" name="rpcbind">/service>
</port><port protocol="tcp" portid="139"><state reason="no-response"
state="open|filtered" reason_ttl="0">/state><service method="table"
conf="3" name="netbios-ssn">/service></port><port protocol="tcp"
portid="445"><state reason="no-response" state="open|filtered"
reason_ttl="0">/state><service method="table" conf="3" name="
microsoft-ds">/service></port><port protocol="tcp" portid="512">
<state reason="no-response" state="open|filtered" reason_ttl="0">
</state><service method="table" conf="3" name="exec">/service>
</port><port protocol="tcp" portid="513"><state reason="no-response"
state="open|filtered" reason_ttl="0">/state><service method="table"
conf="3" name="login">/service></port><port protocol="tcp" portid="514">
<state reason="no-response" state="open|filtered" reason_ttl="0">
</state><service method="table" conf="3" name="shell">/service>
</port><port protocol="tcp" portid="1099"><state reason="no-response"
state="open|filtered" reason_ttl="0">/state><service method="table"
conf="3" name="rmiregistry">/service></port><port protocol="tcp"
portid="1524"><state reason="no-response" state="open|filtered"
reason_ttl="0">/state><service method="table" conf="3" name="
ingreslock">/service></port><port protocol="tcp" portid="2049">
<state reason="no-response" state="open|filtered" reason_ttl="0">
</state><service method="table" conf="3" name="nfs">/service>
</port><port protocol="tcp" portid="2121"><state reason="no-response"
state="open|filtered" reason_ttl="0">/state><service method="table"
conf="3" name="ccproxy-ftp">/service></port><port protocol="tcp"
portid="3306"><state reason="no-response" state="open|filtered"
reason_ttl="0">/state><service method="table" conf="3" name="mysql">
</service></port><port protocol="tcp" portid="5432"><state reason="no-response"
state="open|filtered" reason_ttl="0">/state><service method="
table" conf="3" name="postgresql">/service></port><port protocol="
tcp" portid="5900"><state reason="no-response" state="open|filtered"
reason_ttl="0">/state><service method="table" conf="3" name="vnc">
</service></port><port protocol="tcp" portid="6000"><state reason="
no-response" state="open|filtered" reason_ttl="0">/state><service
method="table" conf="3" name="X11">/service></port><port protocol="
tcp" portid="6667"><state reason="no-response" state="open|filtered"
reason_ttl="0">/state><service method="table" conf="3" name="irc">
</service></port><port protocol="tcp" portid="8009"><state reason="
no-response" state="open|filtered" reason_ttl="0">/state><service
method="table" conf="3" name="ajp13">/service></port><port protocol
="tcp" portid="8180"><state reason="no-response" state="open|
filtered" reason_ttl="0">/state><service method="table" conf="3"

```

```

name="unknown"</service></port></ports><os></os><uptime lastboot=""
seconds=""></uptime><tcpsequence index="" values="" difficulty=""></
tcpsequence><ipidsequence values="" class=""></ipidsequence><
tcptssequence values="" class=""></tcptssequence></host><runstats>
finished timestr="Sat Nov 23 17:03:33 2019" time="1574546613"></
finished><hosts down="0" total="1" up="1"></hosts></runstats></
nmaprun>

```

### 3.9 Nmap para o Metaexploitable 2 - TCP Xmas Scan

Listing 1.9. Nmap OS

```

1 <?xml version="1.0" encoding="iso-8859-1"?>
2 <?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="
  text/xsl"?><nmaprun start="1574546652" profile_name=""
  xmloutputversion="1.04" scanner="nmap" version="7.80" startstr="Sat
  Nov 23 17:04:12 2019" args="nmap -sX 172.16.1.130"><scaninfo
  services="
  1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-
  " protocol="tcp" numservices="1000" type="xmas"></scaninfo><verbose
  level="0"></verbose><debugging level="0"></debugging><output type="
  interactive">Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-23
  17:04 EST
3 Nmap scan report for 172.16.1.130
4 Host is up (0.00055s latency).
5 Not shown: 977 closed ports
6 PORT      STATE SERVICE
7 21/tcp    open|filtered ftp
8 22/tcp    open|filtered ssh
9 23/tcp    open|filtered telnet
10 25/tcp    open|filtered smtp
11 53/tcp    open|filtered domain
12 80/tcp    open|filtered http
13 111/tcp   open|filtered rpcbind
14 139/tcp   open|filtered netbios-ssn
15 445/tcp   open|filtered microsoft-ds
16 512/tcp   open|filtered exec
17 513/tcp   open|filtered login
18 514/tcp   open|filtered shell
19 1099/tcp  open|filtered rmiregistry
20 1524/tcp  open|filtered ingreslock
21 2049/tcp  open|filtered nfs
22 2121/tcp  open|filtered ccproxy-ftp
23 3306/tcp  open|filtered mysql
24 5432/tcp  open|filtered postgresql
25 5900/tcp  open|filtered vnc
26 6000/tcp  open|filtered X11
27 6667/tcp  open|filtered irc
28 8009/tcp  open|filtered ajp13
29 8180/tcp  open|filtered unknown
30 MAC Address: 00:0C:29:7D:0C:D6 (VMware)
31
32 Nmap done: 1 IP address (1 host up) scanned in 14.70 seconds
33 </output><host comment=""><status state="up"></status><address addrtype=
  ="ipv4" vendor="" addr="172.16.1.130"></address><address addrtype="
  mac" vendor="VMware" addr="00:0C:29:7D:0C:D6"></address><hostnames>
  /hostnames><ports><extraports count="977" state="closed"></
  extraports><port protocol="tcp" portid="21"><state reason="no-
  response" state="open|filtered" reason_ttl="0"></state><service

```

```

method="table" conf="3" name="ftp">/service>/port>port protocol="
tcp" portid="22">state reason="no-response" state="open|filtered"
reason_ttl="0">/state>service method="table" conf="3" name="ssh">
/service>/port>port protocol="tcp" portid="23">state reason="no-
response" state="open|filtered" reason_ttl="0">/state>service
method="table" conf="3" name="telnet">/service>/port>port
protocol="tcp" portid="25">state reason="no-response" state="open|
filtered" reason_ttl="0">/state>service method="table" conf="3"
name="smtp">/service>/port>port protocol="tcp" portid="53">state
reason="no-response" state="open|filtered" reason_ttl="0">/state>
service method="table" conf="3" name="domain">/service>/port>port
protocol="tcp" portid="80">state reason="no-response" state="open|
filtered" reason_ttl="0">/state>service method="table" conf="3"
name="http">/service>/port>port protocol="tcp" portid="111">
state reason="no-response" state="open|filtered" reason_ttl="0">
state>service method="table" conf="3" name="rpcbind">/service>
/port>port protocol="tcp" portid="139">state reason="no-response"
state="open|filtered" reason_ttl="0">/state>service method="table"
conf="3" name="netbios-ssn">/service>/port>port protocol="tcp"
portid="445">state reason="no-response" state="open|filtered"
reason_ttl="0">/state>service method="table" conf="3" name="
microsoft-ds">/service>/port>port protocol="tcp" portid="512">
state reason="no-response" state="open|filtered" reason_ttl="0">
state>service method="table" conf="3" name="exec">/service>/port>
<port protocol="tcp" portid="513">state reason="no-response" state=
"open|filtered" reason_ttl="0">/state>service method="table" conf=
"3" name="login">/service>/port>port protocol="tcp" portid="514">
<state reason="no-response" state="open|filtered" reason_ttl="0">
state>service method="table" conf="3" name="shell">/service>/port
>port protocol="tcp" portid="1099">state reason="no-response"
state="open|filtered" reason_ttl="0">/state>service method="table"
conf="3" name="rmiregistry">/service>/port>port protocol="tcp"
portid="1524">state reason="no-response" state="open|filtered"
reason_ttl="0">/state>service method="table" conf="3" name="
ingreslock">/service>/port>port protocol="tcp" portid="2049">
state reason="no-response" state="open|filtered" reason_ttl="0">
state>service method="table" conf="3" name="nfs">/service>/port>
port protocol="tcp" portid="2121">state reason="no-response" state=
"open|filtered" reason_ttl="0">/state>service method="table" conf=
"3" name="ccproxy-ftp">/service>/port>port protocol="tcp" portid=
"3306">state reason="no-response" state="open|filtered" reason_ttl=
"0">/state>service method="table" conf="3" name="mysql">/service>
</port>port protocol="tcp" portid="5432">state reason="no-response"
state="open|filtered" reason_ttl="0">/state>service method="
table" conf="3" name="postgresql">/service>/port>port protocol="
tcp" portid="5900">state reason="no-response" state="open|filtered"
reason_ttl="0">/state>service method="table" conf="3" name="vnc">
</service>/port>port protocol="tcp" portid="6000">state reason="
no-response" state="open|filtered" reason_ttl="0">/state>service
method="table" conf="3" name="X11">/service>/port>port protocol="
tcp" portid="6667">state reason="no-response" state="open|filtered"
reason_ttl="0">/state>service method="table" conf="3" name="irc">
</service>/port>port protocol="tcp" portid="8009">state reason="
no-response" state="open|filtered" reason_ttl="0">/state>service
method="table" conf="3" name="ajp13">/service>/port>port protocol
="tcp" portid="8180">state reason="no-response" state="open|
filtered" reason_ttl="0">/state>service method="table" conf="3"
name="unknown">/service>/port>/ports>os>/os>uptime lastboot="
seconds=">/uptime>tcpsequence index=" values=" difficulty=">
/tcpsequence>ipidsequence values=" class=">/ipidsequence>
tcptssequence values=" class=">/tcptssequence>/host>runstats>

```

```

finished timestr="Sat Nov 23 17:04:26 2019" time="1574546666">/
finished</hosts down="0" total="1" up="1">/hosts</runstats</
nmaprun>

```

### 3.10 Nmap para o Scanme - TCP FIN Scan

Listing 1.10. Nmap OS

```

1 <?xml version="1.0" encoding="iso-8859-1"?>
2 <?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="
  text/xsl"?>nmaprun start="1574547352" profile_name="
  xmloutputversion="1.04" scanner="nmap" version="7.80" startstr="Sat
  Nov 23 17:15:52 2019" args="nmap -sF 45.33.32.156">scaninfo
  services="
  1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-
  " protocol="tcp" numservices="1000" type="fin">/scaninfo</verbose
  level="0">/verbose</debugging level="0">/debugging</output type="
  interactive">Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-23
  17:15 EST
3 Nmap scan report for scanme.nmap.org (45.33.32.156)
4 Host is up (0.00038s latency).
5 All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are open|
  filtered
6
7 Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds
8 </output>host comment="">status state="up">/status</address addrtype
  ="ipv4" vendor="" addr="45.33.32.156">/address</hostnames</hostname
  type="PTR" name="scanme.nmap.org">/hostname</hostnames</ports</
  extraports count="1000" state="open|filtered">/extraports</ports</
  os</os>uptime lastboot="" seconds="">/uptime</tcpsequence index="
  " values="" difficulty="">/tcpsequence</ipidsequence values=""
  class="">/ipidsequence</tcptssequence values="" class="">/
  tcptssequence</host>runstats</finished timestr="Sat Nov 23 17
  :15:56 2019" time="1574547356">/finished</hosts down="0" total="1"
  up="1">/hosts</runstats</nmaprun>

```

### 3.11 Nmap para o Scanme - TCP NULL Scan

Listing 1.11. Nmap OS

```

1 <?xml version="1.0" encoding="iso-8859-1"?>
2 <?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="
  text/xsl"?>nmaprun start="1574547387" profile_name="
  xmloutputversion="1.04" scanner="nmap" version="7.80" startstr="Sat
  Nov 23 17:16:27 2019" args="nmap -sN 45.33.32.156">scaninfo
  services="
  1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-
  " protocol="tcp" numservices="1000" type="null">/scaninfo</verbose
  level="0">/verbose</debugging level="0">/debugging</output type="
  interactive">Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-23
  17:16 EST
3 Nmap scan report for scanme.nmap.org (45.33.32.156)
4 Host is up (0.00026s latency).
5 All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are open|
  filtered
6
7 Nmap done: 1 IP address (1 host up) scanned in 4.25 seconds

```

```

8 </output><host comment=""><status state="up"></status><address addrtype=
  ="ipv4" vendor="" addr="45.33.32.156"></address><hostnames><hostname
    type="PTR" name="scanme.nmap.org"></hostname></hostnames><ports><
  extraports count="1000" state="open|filtered"></extraports></ports><
  os></os><uptime lastboot="" seconds=""></uptime><tcpsequence index=""
    values="" difficulty=""></tcpsequence><ipidsequence values=""
    class=""></ipidsequence><tcptssequence values="" class=""></
  tcptssequence></host><runstats><finished timestr="Sat Nov 23 17
    :16:31 2019" time="1574547391"></finished><hosts down="0" total="1"
    up="1"></hosts></runstats></nmaprun>

```

### 3.12 Nmap para o Scanme - TCP Xmas Scan

Listing 1.12. Nmap OS

```

1 <?xml version="1.0" encoding="iso-8859-1"?>
2 <?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="
  text/xsl"?><nmaprun start="1574547428" profile_name=""
  xmloutputversion="1.04" scanner="nmap" version="7.80" startstr="Sat
  Nov 23 17:17:08 2019" args="nmap -sX 45.33.32.156"><scaninfo
    services="
      1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119 125,135,139,143-144,146,
      " protocol="tcp" numservices="1000" type="xmas"></scaninfo><verbose
    level="0"></verbose><debugging level="0"></debugging><output type="
      interactive">Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-23
      17:17 EST
3 Nmap scan report for scanme.nmap.org (45.33.32.156)
4 Host is up (0.00054s latency).
5 All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are open|
  filtered
6
7 Nmap done: 1 IP address (1 host up) scanned in 4.25 seconds
8 </output><host comment=""><status state="up"></status><address addrtype=
  ="ipv4" vendor="" addr="45.33.32.156"></address><hostnames><hostname
    type="PTR" name="scanme.nmap.org"></hostname></hostnames><ports><
  extraports count="1000" state="open|filtered"></extraports></ports><
  os></os><uptime lastboot="" seconds=""></uptime><tcpsequence index=""
    values="" difficulty=""></tcpsequence><ipidsequence values=""
    class=""></ipidsequence><tcptssequence values="" class=""></
  tcptssequence></host><runstats><finished timestr="Sat Nov 23 17
    :17:12 2019" time="1574547432"></finished><hosts down="0" total="1"
    up="1"></hosts></runstats></nmaprun>

```

### 3.13 Nmap Para reconhecer Sistema Operativo

Listing 1.13. Nmap OS

```

1 <?xml version="1.0" encoding="iso-8859-1"?>
2 <?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="
  text/xsl"?><nmaprun start="1574547657" profile_name=""
  xmloutputversion="1.04" scanner="nmap" version="7.80" startstr="Sat
  Nov 23 17:20:57 2019" args="nmap -O 172.16.1.130"><scaninfo services=
    ="
      1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119 125,135,139,143-144,146,
      " protocol="tcp" numservices="1000" type="syn"></scaninfo><verbose
    level="0"></verbose><debugging level="0"></debugging><output type="
      interactive">Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-23
      17:20 EST

```

```

3 Nmap scan report for 172.16.1.130
4 Host is up (0.00078s latency).
5 Not shown: 977 closed ports
6 PORT      STATE SERVICE
7 21/tcp    open  ftp
8 22/tcp    open  ssh
9 23/tcp    open  telnet
10 25/tcp    open  smtp
11 53/tcp    open  domain
12 80/tcp    open  http
13 111/tcp   open  rpcbind
14 139/tcp   open  netbios-ssn
15 445/tcp   open  microsoft-ds
16 512/tcp   open  exec
17 513/tcp   open  login
18 514/tcp   open  shell
19 1099/tcp  open  rmiregistry
20 1524/tcp  open  ingreslock
21 2049/tcp  open  nfs
22 2121/tcp  open  ccproxy-ftp
23 3306/tcp  open  mysql
24 5432/tcp  open  postgresql
25 5900/tcp  open  vnc
26 6000/tcp  open  X11
27 6667/tcp  open  irc
28 8009/tcp  open  ajp13
29 8180/tcp  open  unknown
30 MAC Address: 00:0C:29:7D:0C:D6 (VMware)
31 Device type: general purpose
32 Running: Linux 2.6.X
33 OS CPE: cpe:/o:linux:linux_kernel:2.6
34 OS details: Linux 2.6.9 - 2.6.33
35 Network Distance: 1 hop
36
37 OS detection performed. Please report any incorrect results at https://
  nmap.org/submit/ .
38 Nmap done: 1 IP address (1 host up) scanned in 15.57 seconds
39 </output><host comment=""><status state="up">/status><address addrtype=
  ="ipv4" vendor="" addr="172.16.1.130">/address><address addrtype="
  mac" vendor="VMware" addr="00:0C:29:7D:0C:D6">/address><hostnames>
  /hostnames><ports><extraports count="977" state="closed">/
  extraports><port protocol="tcp" portid="21"><state reason="syn-ack"
  state="open" reason_ttl="64">/state><service method="table" conf="3
  " name="ftp">/service></port><port protocol="tcp" portid="22">
  state reason="syn-ack" state="open" reason_ttl="64">/state><service
  method="table" conf="3" name="ssh">/service></port><port protocol=
  "tcp" portid="23"><state reason="syn-ack" state="open" reason_ttl="
  64">/state><service method="table" conf="3" name="telnet">/service
  ></port><port protocol="tcp" portid="25"><state reason="syn-ack"
  state="open" reason_ttl="64">/state><service method="table" conf="3
  " name="smtp">/service></port><port protocol="tcp" portid="53">
  state reason="syn-ack" state="open" reason_ttl="64">/state><service
  method="table" conf="3" name="domain">/service></port><port
  protocol="tcp" portid="80"><state reason="syn-ack" state="open"
  reason_ttl="64">/state><service method="table" conf="3" name="http"
  ></service></port><port protocol="tcp" portid="111"><state reason="
  syn-ack" state="open" reason_ttl="64">/state><service method="table
  " conf="3" name="rpcbind">/service></port><port protocol="tcp"
  portid="139"><state reason="syn-ack" state="open" reason_ttl="64">
  /state><service method="table" conf="3" name="netbios-ssn">/service>
  </port><port protocol="tcp" portid="445"><state reason="syn-ack"

```



```

state="open" reason_ttl="64">/state<service method="table" conf="3"
" name="microsoft-ds">/service</port><port protocol="tcp" portid="
512">state reason="syn-ack" state="open" reason_ttl="64">/state<
service method="table" conf="3" name="exec">/service</port><port
protocol="tcp" portid="513">state reason="syn-ack" state="open"
reason_ttl="64">/state<service method="table" conf="3" name="login
">/service</port><port protocol="tcp" portid="514">state reason="
syn-ack" state="open" reason_ttl="64">/state<service method="table
" conf="3" name="shell">/service</port><port protocol="tcp" portid
="1099">state reason="syn-ack" state="open" reason_ttl="64">/state
<service method="table" conf="3" name="rmiregistry">/service</
port><port protocol="tcp" portid="1524">state reason="syn-ack"
state="open" reason_ttl="64">/state<service method="table" conf="3"
" name="ingreslock">/service</port><port protocol="tcp" portid="
2049">state reason="syn-ack" state="open" reason_ttl="64">/state<
service method="table" conf="3" name="nfs">/service</port><port
protocol="tcp" portid="2121">state reason="syn-ack" state="open"
reason_ttl="64">/state<service method="table" conf="3" name="
ccproxy-ftp">/service</port><port protocol="tcp" portid="3306">
state reason="syn-ack" state="open" reason_ttl="64">/state<service
method="table" conf="3" name="mysql">/service</port><port
protocol="tcp" portid="5432">state reason="syn-ack" state="open"
reason_ttl="64">/state<service method="table" conf="3" name="
postgresql">/service</port><port protocol="tcp" portid="5900">
state reason="syn-ack" state="open" reason_ttl="64">/state<service
method="table" conf="3" name="vnc">/service</port><port protocol=
"tcp" portid="6000">state reason="syn-ack" state="open" reason_ttl=
"64">/state<service method="table" conf="3" name="X11">/service<
/port><port protocol="tcp" portid="6667">state reason="syn-ack"
state="open" reason_ttl="64">/state<service method="table" conf="3"
" name="irc">/service</port><port protocol="tcp" portid="8009">
state reason="syn-ack" state="open" reason_ttl="64">/state<service
method="table" conf="3" name="ajp13">/service</port><port
protocol="tcp" portid="8180">state reason="syn-ack" state="open"
reason_ttl="64">/state<service method="table" conf="3" name="
unknown">/service</port></ports><os><portused state="open" portid=
"21" proto="tcp">/portused<portused state="closed" portid="1"
proto="tcp">/portused<portused state="closed" portid="43821" proto
="udp">/portused<osmatch line="59153" name="Linux 2.6.9 - 2.6.33"
accuracy="100">osclass type="general purpose" osfamily="Linux"
vendor="Linux" osgen="2.6.X" accuracy="100">/osclass</osmatch</os
<uptime lastboot="Sat Nov 23 16:13:34 2019" seconds="4058">/uptime
<tcpsequence index="188" values="F52E9630,F4FB8363,F514E106,
F55AFD3F,F5789A3F,F5A003FE" difficulty="Good luck!">/tcpsequence<
ipidsequence values="0,0,0,0,0,0" class="All zeros">/ipidsequence<
tcptssequence values="6306B,63075,6307F,63088,63092,6309C" class="
100HZ">/tcptssequence</host><runstats<finished timestr="Sat Nov
23 17:21:12 2019" time="1574547672">/finished<hosts down="0" total
="1" up="1">/hosts</runstats</nmaprun>

```

### 3.14 Nmap para detetar os Serviços

Listing 1.14. Nmap OS

```

1 <?xml version="1.0" encoding="iso-8859-1"?>
2 <?xml-stylesheet href="file:///usr/bin/./share/nmap/nmap.xsl" type="
text/xsl"?><nmaprun start="1574548040" profile_name="
xmloutputversion="1.04" scanner="nmap" version="7.80" startstr="Sat
Nov 23 17:27:20 2019" args="nmap -sV --version-all 172.16.1.130">

```

```

scaninfo services="
1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-
" protocol="tcp" numservices="1000" type="syn"</scaninfo><verbose
level="0"></verbose><debugging level="0"></debugging><output type="
interactive">Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-23
17:27 EST
3 Nmap scan report for 172.16.1.130
4 Host is up (0.0013s latency).
5 Not shown: 977 closed ports
6 PORT      STATE SERVICE      VERSION
7 21/tcp    open  ftp          vsftpd 2.3.4
8 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
9 23/tcp    open  telnet       Linux telnetd
10 25/tcp    open  smtp         Postfix smtpd
11 53/tcp    open  domain       ISC BIND 9.4.2
12 80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
13 111/tcp   open  rpcbind      2 (RPC #100000)
14 139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
15 445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
16 512/tcp   open  exec         netkit-rsh rexecd
17 513/tcp   open  login        OpenBSD or Solaris rlogind
18 514/tcp   open  shell        Netkit rshd
19 1099/tcp  open  java-rmi     GNU Classpath grmiregistry
20 1524/tcp  open  bindshell    Metasploitable root shell
21 2049/tcp  open  nfs          2-4 (RPC #100003)
22 2121/tcp  open  ftp          ProFTPD 1.3.1
23 3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
24 5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
25 5900/tcp  open  vnc          VNC (protocol 3.3)
26 6000/tcp  open  X11          (access denied)
27 6667/tcp  open  irc          UnrealIRCd
28 8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
29 8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
30 MAC Address: 00:0C:29:7D:0C:D6 (VMware)
31 Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.
    LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
32
33 Service detection performed. Please report any incorrect results at
    https://nmap.org/submit/ .
34 Nmap done: 1 IP address (1 host up) scanned in 40.56 seconds
35 </output><host comment=""><status state="up"></status><address addrtypes="
    "ip v4" vendor="" addr="172.16.1.130"></address><address addrtypes="
    mac" vendor="VMware" addr="00:0C:29:7D:0C:D6"></address><hostnames><
    /hostnames><ports><extraports count="977" state="closed"></
    extraports><port protocol="tcp" portid="21"><state reason="syn-ack"
    state="open" reason_ttl="64"></state><service product="vsftpd"
    version="2.3.4" method="probed" conf="10" name="ftp"></service></
    port><port protocol="tcp" portid="22"><state reason="syn-ack" state=
    "open" reason_ttl="64"></state><service product="OpenSSH" name="ssh"
    extrainfo="protocol 2.0" version="4.7p1 Debian 8ubuntu1" conf="10"
    method="probed"></service></port><port protocol="tcp" portid="23"><
    state reason="syn-ack" state="open" reason_ttl="64"></state><service
    product="Linux telnetd" method="probed" conf="10" name="telnet"></
    service></port><port protocol="tcp" portid="25"><state reason="syn-
    ack" state="open" reason_ttl="64"></state><service product="Postfix
    smtpd" method="probed" conf="10" name="smtp"></service></port><port
    protocol="tcp" portid="53"><state reason="syn-ack" state="open"
    reason_ttl="64"></state><service product="ISC BIND" version="9.4.2"
    method="probed" conf="10" name="domain"></service></port><port
    protocol="tcp" portid="80"><state reason="syn-ack" state="open"
    reason_ttl="64"></state><service product="Apache httpd" name="http"

```

```

extrainfo="(Ubuntu) DAV/2" version="2.2.8" conf="10" method="probed"
</service></port><port protocol="tcp" portid="111"><state reason="
syn-ack" state="open" reason_ttl="64"></state><service version="2"
extrainfo="RPC #100000" method="probed" conf="10" name="rpcbind"></
service></port><port protocol="tcp" portid="139"><state reason="syn-
ack" state="open" reason_ttl="64"></state><service product="Samba
smbd" name="netbios-ssn" extrainfo="workgroup: WORKGROUP" version="
3.X - 4.X" conf="10" method="probed"></service></port><port protocol
="tcp" portid="445"><state reason="syn-ack" state="open" reason_ttl=
"64"></state><service product="Samba smbd" name="netbios-ssn"
extrainfo="workgroup: WORKGROUP" version="3.X - 4.X" conf="10"
method="probed"></service></port><port protocol="tcp" portid="512">
<state reason="syn-ack" state="open" reason_ttl="64"></state><service
product="netkit-rsh rexecd" method="probed" conf="10" name="exec">
</service></port><port protocol="tcp" portid="513"><state reason="syn-
ack" state="open" reason_ttl="64"></state><service product="OpenBSD
or Solaris rlogind" method="probed" conf="10" name="login"></
service></port><port protocol="tcp" portid="514"><state reason="syn-
ack" state="open" reason_ttl="64"></state><service product="Netkit
rshd" method="probed" conf="10" name="shell"></service></port><port
protocol="tcp" portid="1099"><state reason="syn-ack" state="open"
reason_ttl="64"></state><service product="GNU Classpath grmiregistry"
method="probed" conf="10" name="java-rmi"></service></port><port
protocol="tcp" portid="1524"><state reason="syn-ack" state="open"
reason_ttl="64"></state><service product="Metasploitable root shell"
method="probed" conf="10" name="bindshell"></service></port><port
protocol="tcp" portid="2049"><state reason="syn-ack" state="open"
reason_ttl="64"></state><service version="2-4" extrainfo="RPC
#100003" method="probed" conf="10" name="nfs"></service></port><port
protocol="tcp" portid="2121"><state reason="syn-ack" state="open"
reason_ttl="64"></state><service product="ProFTPD" version="1.3.1"
method="probed" conf="10" name="ftp"></service></port><port protocol
="tcp" portid="3306"><state reason="syn-ack" state="open" reason_ttl
="64"></state><service product="MySQL" version="5.0.51a-3ubuntu5"
method="probed" conf="10" name="mysql"></service></port><port
protocol="tcp" portid="5432"><state reason="syn-ack" state="open"
reason_ttl="64"></state><service product="PostgreSQL DB" version="
8.3.0 - 8.3.7" method="probed" conf="10" name="postgresql"></service
></port><port protocol="tcp" portid="5900"><state reason="syn-ack"
state="open" reason_ttl="64"></state><service product="VNC"
extrainfo="protocol 3.3" method="probed" conf="10" name="vnc"></
service></port><port protocol="tcp" portid="6000"><state reason="syn-
ack" state="open" reason_ttl="64"></state><service extrainfo="
access denied" method="probed" conf="10" name="X11"></service></port
><port protocol="tcp" portid="6667"><state reason="syn-ack" state="
open" reason_ttl="64"></state><service product="UnrealIRCd" method="
probed" conf="10" name="irc"></service></port><port protocol="tcp"
portid="8009"><state reason="syn-ack" state="open" reason_ttl="64">
</state><service product="Apache Jserv" extrainfo="Protocol v1.3"
method="probed" conf="10" name="ajp13"></service></port><port
protocol="tcp" portid="8180"><state reason="syn-ack" state="open"
reason_ttl="64"></state><service product="Apache Tomcat/Coyote JSP
engine" version="1.1" method="probed" conf="10" name="http"></
service></port></ports><os></os><uptime lastboot="" seconds=""></
uptime><tcpsequence index="" values="" difficulty=""></tcpsequence>
<ipidsequence values="" class=""></ipidsequence><tcptssequence values
="" class=""></tcptssequence></host><runstats><finished timestr="Sat
Nov 23 17:28:01 2019" time="1574548081"></finished><hosts down="0"
total="1" up="1"></hosts></runstats></nmaprun>

```