

# Relatório Final

## Cibersegurança Ofensiva e Defensiva I

Mestrado em Cibersegurança e Informática Forense

Rui Pedro Lopes Silva, nº 2230055

Leiria, janeiro de 2024

# Lista de Figuras

Figura 1 - Domínio no SpiderFoot .....	6
Figura 2 - Domain / IP Whois do ViewDNS.info .....	7
Figura 3 - Reverse IP Lookup no ViewDNS.info .....	7
Figura 4 - IP History no ViewDNS.info .....	8
Figura 5 - DNS Record Lookup no ViewDNS.info .....	8
Figura 6 - DNSSEC Test no ViewDNS.info .....	8
Figura 7 - Reverse DNS no CentralOps.net .....	9
Figura 8 - IP range no Netcraft.com .....	10
Figura 9 - Traceroute no Traceroute-online.com .....	10
Figura 10 - Emails no hunter.io .....	11
Figura 11 - Email de funcionário no hunter.io .....	11
Figura 12 - Teste com insucesso no theHarvester .....	12
Figura 13 - Hosts Ligados .....	13
Figura 14 - Hosts Ligados no NetDiscover .....	13
Figura 15 - Portos TCP dos Hosts Ativos .....	14
Figura 16 - Scan atrás de IDS e Firewall .....	14
Figura 17 - Banners .....	15
Figura 18 - SO .....	15
Figura 19 - NetBIOS Name .....	16
Figura 20 - Tabela de nomes com nbstat .....	16
Figura 21 - Tabela de nomes com nbtstat .....	17
Figura 22 - Protocolo SNMP com o snmpwalk .....	17
Figura 23 - Protocolo SNMP com nmap .....	18
Figura 24 - Protocolo LDAP com rpcclient .....	18
Figura 25 - Protocolo SMB com nmap .....	19
Figura 26 - IPsec com nmap .....	19
Figura 27 - Nikto .....	20

# Índice

1. Introdução.....	5
1.1. Objetivos.....	5
2. Rastreamento e Reconhecimento .....	6
2.1. Análise ao DNS .....	6
2.1.1. <i>SpiderFoot</i> .....	6
2.1.2. <i>ViewDNS.info</i> .....	7
2.1.3. <i>Central Ops.net</i> .....	9
2.2. Análise à Rede .....	9
2.2.1. <i>Netcraft.com</i> .....	9
2.2.2. <i>Traceroute-online.com</i> .....	10
2.3. Análise da Engenharia Social .....	11
2.3.1. <i>Hunter.io</i> .....	11
2.4. Ferramentas sem sucesso .....	11
3. Sistema Virtualizado .....	13
3.1. <i>Scanning</i> .....	13
3.1.1. <i>Host</i> ligados .....	13
3.1.2. Portos abertos dos <i>hosts</i> ligados .....	14
3.1.3. <i>Scan</i> através de <i>IDS</i> e <i>Firewall</i> .....	14
3.1.4. <i>Banners</i> e <i>SO</i> .....	14
3.2. Enumeração .....	16
3.2.1. <i>NetBIOS</i> .....	16
3.2.2. <i>SNMP</i> .....	17
3.2.3. <i>LDAP</i> e <i>SMB</i> .....	18
3.2.4. <i>IPsec</i> .....	19
3.3. Identificação e Análise das Vulnerabilidades .....	20
3.3.1. <i>Nikto</i> .....	20

3.3.2.	<i>Nessus</i> .....	20
3.4.	Soluções Para Mitigar as Vulnerabilidades.....	21
3.4.1.	<i>SSL Version 2 and 3 Protocol Detection</i> .....	21
3.4.2.	<i>Samba 'AndX' Request Heap-Based Buffer Overflow</i> .....	21
3.4.3.	<i>OpenSSL Heartbeat Information Disclosure (Heartbleed)</i> .....	21
3.4.4.	<i>SNMP Agent Default Community Name (public)</i> .....	21
4.	Anexo A.....	22

# 1. Introdução

O presente relatório retrata os resultados e documentos elaborados nas diferentes etapas do trabalho proposto no âmbito da unidade curricular de Cibersegurança Ofensiva e Defensiva do Mestrado em Cibersegurança e Informática Forense do Instituto Politécnico de Leiria.

A fase de rastreamento e reconhecimento ou *footprinting* é a primeira fase no processo da metodologia usada em testes de penetração. Esta fase consiste na identificação do alvo e na recolha de informação sobre este e de outros associados ao mesmo. A informação recolhida sobre o alvo abrange informações sobre o tipo de rede e equipamento, o tipo de tecnologia, as filiais, utilizadores e cargos, endereços de rede/*email*/utilizadores, *softwares* e *hardware* utilizados e os sistemas operativos.

## 1.1. Objetivos

O objetivo deste relatório é apresentar os resultados das diferentes etapas propostas do projeto. Este relatório contém o pedido de autorização de avaliação dos sistemas devidamente assinado (*PenTest Request*), bem como as técnicas e ferramentas utilizadas para o rastreamento e reconhecimento do domínio da organização selecionada, neste caso a “x”. Por fim, contém também as atividades de *footprinting*, *scanning*, enumeração e identificação e análise das vulnerabilidades de um sistema virtualizado.

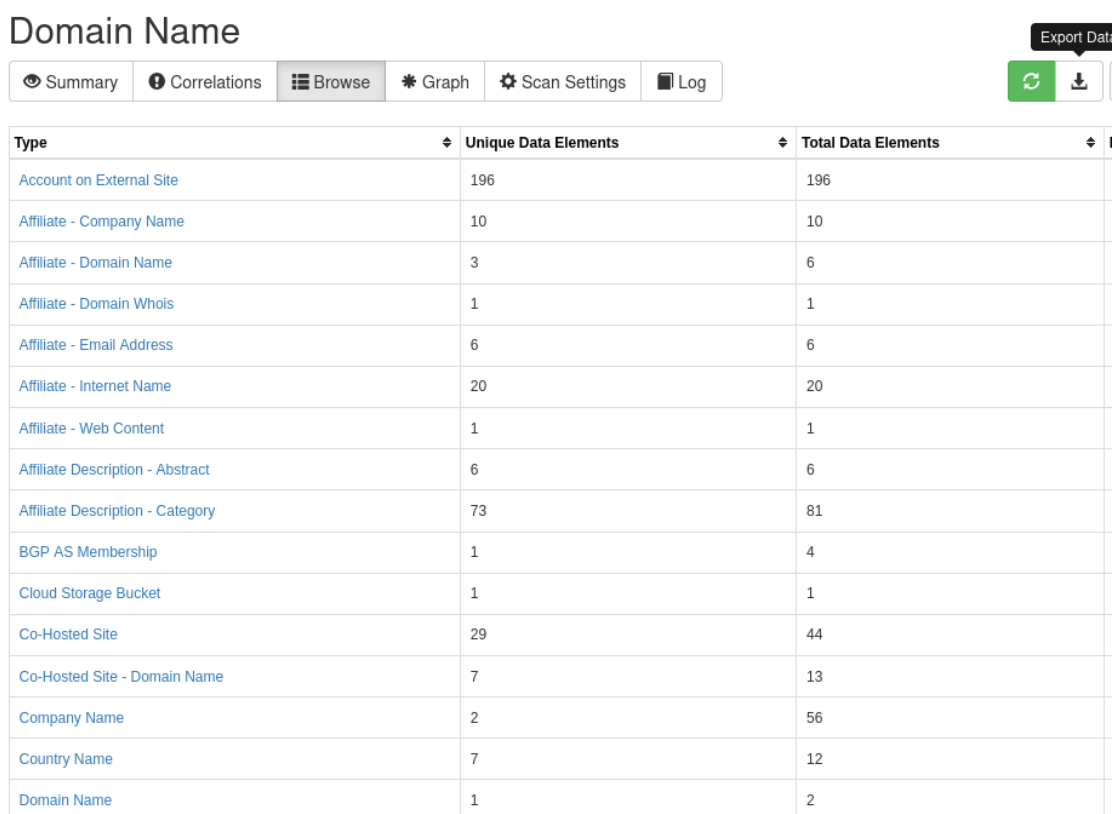
## 2. Rastreamento e Reconhecimento

A organização escolhida para a realização desta etapa do projeto, fazendo o rastreamento e reconhecimento do domínio foi a “x”. Nesta etapa vamos apresentar os resultados encontrados, bem como as ferramentas utilizadas para obtenção das informações à cerca do domínio desta organização.

### 2.1. Análise ao DNS

#### 2.1.1. *SpiderFoot*

O *Spiderfoot* representa uma *framework* de inteligência de ameaças *open-source*, com a capacidade de coletar, analisar e visualizar dados provenientes de fontes abertas. O *Spiderfoot* destina-se à obtenção de diversos tipos de dados de fontes abertas, como por exemplo os registos DNS, fornecendo informações detalhadas sobre endereços IP, nomes de domínio e servidores de nomes, como observado na figura seguinte.



Type	Unique Data Elements	Total Data Elements
Account on External Site	196	196
Affiliate - Company Name	10	10
Affiliate - Domain Name	3	6
Affiliate - Domain Whois	1	1
Affiliate - Email Address	6	6
Affiliate - Internet Name	20	20
Affiliate - Web Content	1	1
Affiliate Description - Abstract	6	6
Affiliate Description - Category	73	81
BGP AS Membership	1	4
Cloud Storage Bucket	1	1
Co-Hosted Site	29	44
Co-Hosted Site - Domain Name	7	13
Company Name	2	56
Country Name	7	12
Domain Name	1	2

Figura 1 - Domínio no *SpiderFoot*

Depois de visualizar as opções mais importantes, concluímos que as ferramentas que iremos abordar a seguir, são mais fáceis em termos de visualização.

### 2.1.2. *ViewDNS.info*

O *ViewDNS.info* é um serviço online que fornece uma variedade de ferramentas e informações relacionadas a domínios e serviços DNS usando como *input* um domínio, email, ou endereço IP. Para a análise recorrendo a esta ferramenta escolhemos executar as seguintes funcionalidades:

#### ***Domain / IP Whois***

Nesta funcionalidade é usado um domínio ou IP para procurar informação sobre estes, na imagem que se segue podemos observar que não é revelado muita informação, apenas os NServers, o estado e a data da última modificação.

```
Domain: [REDACTED]
Nserver: a.ns14.net
Nserver: b.ns14.net
Nserver: c.ns14.net
Nserver: d.ns14.net
Status: connect
Changed: 2017-02-10T12:35:48+01:00
```

Figura 2 - *Domain / IP Whois* do *ViewDNS.info*

#### ***Reverse IP Lookup***

Com esta funcionalidade é possível encontrar outros domínios hospedados no mesmo servidor, este apenas precisa como *input* o IP ou domínio do *website*, neste caso “x”. Com isto obteve-se uma lista de domínios hospedados no mesmo servidor como demonstra a próxima figura.

Domain	Last Resolved Date
[REDACTED]	2023-12-25
	2023-12-25
	2023-12-27
	2023-12-26
	2023-12-23
	2023-12-22
	2023-12-21
	2023-12-20

Figura 3 - *Reverse IP Lookup* no *ViewDNS.info*

Aqui podemos entender melhor a infraestrutura do servidor e observar a presença de diversos domínios no mesmo endereço IP.

## ***IP History***

Esta funcionalidade mostra uma lista de endereços IP que o domínio teve como hospedeiro, a sua localização e o dono desse IP.

IP Address	Location	IP Address Owner	Last seen on this IP
			2023-12-27
			2021-09-09
			2018-08-09
			2015-11-19
			2015-10-29
			2012-03-22

Figura 4 - *IP History* no *ViewDNS.info*

## ***DNS Record Lookup***

Nesta funcionalidade é apresentada informação relativa ao DNS do domínio, onde podemos ver informações específicas associadas ao DNS, como mostra a figura seguinte.

Name	TTL	Class	Type	Priority	Data
	21600	IN	SOA		
	21600	IN	NS		
	21600	IN	NS		
	21600	IN	NS		
	21600	IN	NS		
	60	IN	A		
	60	IN	TXT		
	60	IN	TXT		
	60	IN	TXT		
	60	IN	TXT		
	60	IN	TXT		
	60	IN	TXT		
	60	IN	TXT		
	60	IN	TXT		
	60	IN	MX	0	

Figura 5 - *DNS Record Lookup* no *ViewDNS.info*

## ***DNSSEC Test***

Esta funcionalidade permite saber se o *Domain Name System Security Extensions* (DNSSEC) está configurado no domínio especificado. Como se pode ver na próxima figura, o “x” não tem o DNSSEC ativo.



Figura 6 - *DNSSEC Test* no *ViewDNS.info*

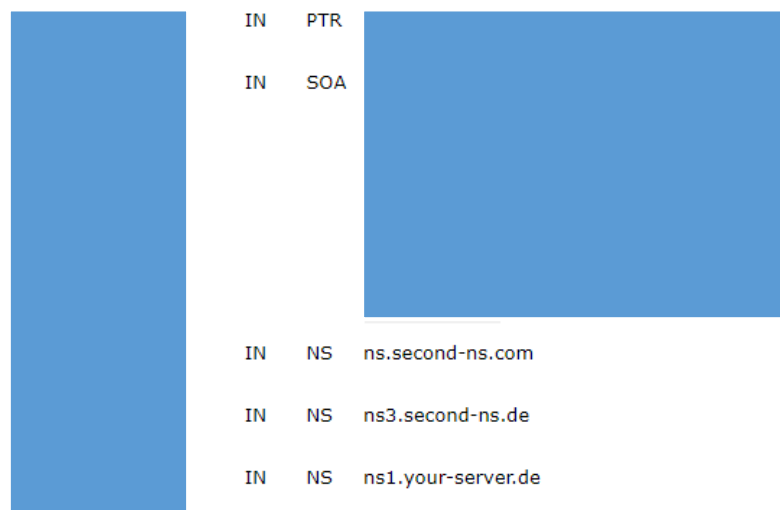


O DNSSEC é importante pois adiciona camadas de autenticação e verificação de integridade aos registos do DNS, garantindo que as respostas do DNS não são modificadas no caminho entre o servidor e o cliente.

### 2.1.3. *Central Ops.net*

O *CentralOps.net* é um serviço *online* que fornece diversas ferramentas úteis para análise de informações relacionadas a domínios e servidores na *Internet*.

Podemos concluir que esta ferramenta apresenta resultados idênticos à ferramenta apresentada anteriormente *ViewDNS.info*. Uma informação que esta ferramenta obteve, que em comparação com as outras não tivemos, é os registos relativos ao PTR, que identifica o IP inverso usado para o mapeamento inverso de números para *hosts*.



IN	PTR	
IN	SOA	
IN	NS	ns.second-ns.com
IN	NS	ns3.second-ns.de
IN	NS	ns1.your-server.de

Figura 7 - Reverse DNS no *CentralOps.net*

## 2.2. Análise à Rede

### 2.2.1. *Netcraft.com*

O *Netcraft.com* é um serviço *online* onde podemos ver informações sobre a infraestrutura da *Internet*, incluindo dados sobre servidores, sistemas operacionais, *software* de servidor, *hosts*, entre outros. Utilizamos este serviço para visualizar o range de IP utilizado pelo domínio “x”, como podemos observar na seguinte figura.

IP delegation			
IPv4 address <span></span>			
IP range	Country	Name	Description
<span></span>		IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
		78-RIPE	RIPE Network Coordination Centre
		<span></span>	

Figura 8 - IP range no Netcraft.com

### 2.2.2. Traceroute-online.com

O *Traceroute-online* é um serviço online dedicado a realizar *traceroutes* e mapear o caminho dos pacotes na rede. Na figura abaixo podemos ver os *IP/Host Names*, bem como o país desses, o ISP para ver onde estão hospedados os diversos serviços e tempo de resposta dos pedidos.

Hop	IP / Host Name	ISP	Netblock	Country	Loss	Response
1					0.0%	0.11ms
2					0.0%	0.35ms
3					0.0%	0.50ms
4					0.0%	1.10ms
5					0.0%	9.97ms
6					0.0%	1.34ms
7					50.0%	1.31ms
8					0.0%	2.33ms
9						
10					0.0%	83.25ms
11					0.0%	100.29ms
12					0.0%	96.33ms
13					0.0%	96.47ms
14					0.0%	96.63ms
15					0.0%	99.02ms

Figura 9 - Traceroute no Traceroute-online.com

## 2.3. Análise da Engenharia Social

### 2.3.1. Hunter.io

O Hunter.io é um serviço online que fornece ferramentas relacionadas à busca e verificação de endereços de *email*. Ao usar esta ferramenta conseguimos obter alguns endereços de *email*, como mostra a figura seguinte.

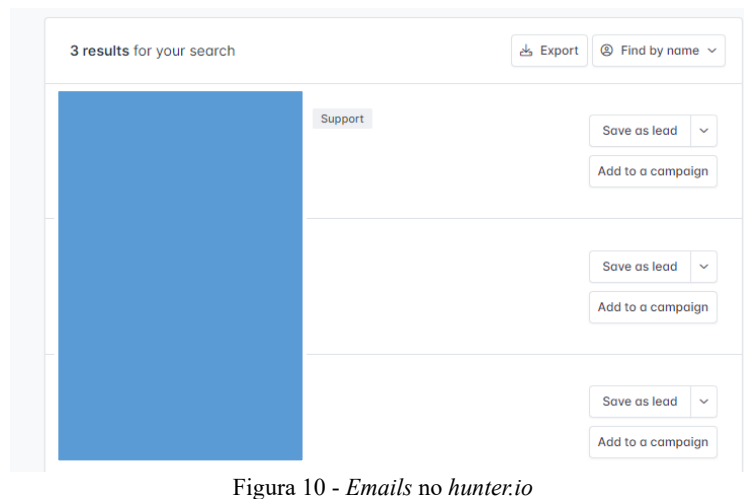


Figura 10 - Emails no hunter.io

Ainda nesta mesma ferramenta e aprofundando um pouco mais a mesma, ainda conseguimos obter um endereço de *email* de uma funcionária dos recursos humanos bem como o contato telefônico, representado na próxima figura.

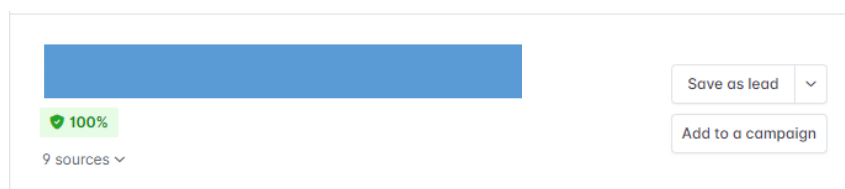


Figura 11 - Email de funcionário no hunter.io

## 2.4. Ferramentas sem sucesso

Ainda foram usadas outras ferramentas para obtenção de resultados, mas não foi realizado com sucesso. Como por exemplo, na figura em baixo encontra-se a ferramenta *theHarvester*, uma ferramenta de linha de comandos, que recolhe informações como *emails*, nomes, subdomínios, entre outras.

[illegible]

Figura 12 - Teste com insucesso no *theHarvester*

## 3. Sistema Virtualizado

O sistema virtualizado utilizado foi o *Bee-Box* que é uma Máquina Virtual Linux personalizada pré-instalada com o *bWAPP*. A *bee-box*, tem a oportunidade de explorar todas as vulnerabilidades do *bWAPP* e oferece várias maneiras de fazer testes de penetração.

### 3.1. Scanning

Para a realização do *scanning* no sistema virtualizado foram executados 4 passos essenciais para a descoberta de *hosts*, portos e serviços na rede. Maioritariamente estes passos foram realizados com a ferramenta *nmap*.

#### 3.1.1. Host ligados

Para determinar os *hosts* ligados na *range* do endereço IP, utilizamos a ferramenta *nmap* com o comando que se pode observar na figura seguinte.

```
(kali@kali)-[~]
└─$ sudo nmap -sn 192.168.205.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 10:02 EST
Nmap scan report for 192.168.205.1
Host is up (0.00017s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.205.2
Host is up (0.00020s latency).
MAC Address: 00:50:56:E8:A6:35 (VMware)
Nmap scan report for 192.168.205.128
Host is up (0.00092s latency).
MAC Address: 00:0C:29:CF:03:9C (VMware)
Nmap scan report for 192.168.205.254
Host is up (0.00025s latency).
MAC Address: 00:50:56:F8:DC:BC (VMware)
Nmap scan report for 192.168.205.129
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.96 seconds
```

Figura 13 - Hosts Ligados

Também recorremos a outra ferramenta chamada *NetDiscover*, embora este não detetou o último endereço IP, como no *nmap*, como comprova a figura seguinte.

Currently scanning: Finished!		Screen View: Unique Hosts	
8 Captured ARP Req/Rep packets, from 4 hosts.		Total size: 480	
IP	At MAC Address	Count	Len MAC Vendor / Hostname
192.168.205.1	00:50:56:c0:00:08	1	60 VMware, Inc.
192.168.205.2	00:50:56:e8:a6:35	3	180 VMware, Inc.
192.168.205.128	00:0c:29:cf:03:9c	2	120 VMware, Inc.
192.168.205.254	00:50:56:fd:aa:55	2	120 VMware, Inc.

Figura 14 - Hosts Ligados no *NetDiscover*

### 3.1.2. Portos abertos dos *hosts* ligados

Para ver os portos TCP abertos, fizemos uso de um comando *nmap* que verifica todas as portas TCP disponíveis no intervalo de 1-65535. Optámos por fazer para o IP demonstrado em baixo, pois é o da máquina onde estamos a realizar as atividades de *scanning*.

```
(kali@kali)-[~]
$ nmap -p- 192.168.205.128
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 09:33 EST
Nmap scan report for 192.168.205.128
Host is up (0.0049s latency).
Not shown: 65516 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
666/tcp   open  doom
3306/tcp  open  mysql
3632/tcp  open  distccd
5901/tcp  open  vnc-1
6001/tcp  open  X11:1
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
9080/tcp  open  glrpc
9443/tcp  open  tungsten-https
```

Figura 15 - Portos TCP dos *Hosts* Ativos

### 3.1.3. *Scan* através de *IDS* e *Firewall*

A execução do comando demonstrado na figura abaixo, realiza um *scan SYN* de portas usando fragmentação de pacotes (opção *-f*), este deteta o sistema operacional, serviços e versões, e ainda mostra informações detalhadas sobre o processo. O uso de fragmentação de pacotes evita que as *firewall* e *IDS* percebam o objetivo.

```
(kali@kali)-[~]
$ sudo nmap -sS -T4 -A -f -v 192.168.205.128
```

Figura 16 - *Scan* atrás de *IDS* e *Firewall*

### 3.1.4. *Banners* e SO

A obtenção dos *banners* é o método utilizado para descobrir as versões do sistema operativo ou dos serviços que estão em execução no sistema virtualizado. Executámos um script específico (*--script=banner*), para obter informações de *banner* dos serviços que estão com as portas abertas.







```
VMware Network Adapter VMnet8:
Node IpAddress: [192.168.205.1] Scope Id: []
```

NetBIOS Remote Machine Name Table			
Name	Type		Status
BEE-BOX	<00>	UNIQUE	Registered
BEE-BOX	<03>	UNIQUE	Registered
BEE-BOX	<20>	UNIQUE	Registered
@@_MSBROWSE_@	<01>	GROUP	Registered
ITSECGAMES	<1D>	UNIQUE	Registered
ITSECGAMES	<1E>	GROUP	Registered
ITSECGAMES	<00>	GROUP	Registered

Figura 21 - Tabela de nomes com *nbtstat*

### 3.2.2. SNMP

Com o protocolo SNMP podemos obter contas de utilizadores e informações acerca de dispositivos. Utilizamos a ferramenta *snmpwalk* para visualizar os OID, que são sequências numéricas usadas para identificar objetos gerenciados pelo protocolo SNMP, que deu uma grande lista de dados, na figura seguinte mostra alguns desses dados, como os processos de sistema, portas locais TCP entre muito outros.

```
(kali@kali)-[~]
$ snmpwalk -c public -v1 -t 10 192.168.205.128
iso.3.6.1.2.1.1.1.0 = STRING: "Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (309801) 0:51:38.01
iso.3.6.1.2.1.1.4.0 = STRING: "Your master bee"
iso.3.6.1.2.1.1.5.0 = STRING: "bee-box"
iso.3.6.1.2.1.1.6.0 = STRING: "Every bee needs a home!"
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the SNMP User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (0) 0:00:00.00
```

Figura 22 - Protocolo SNMP com o *snmpwalk*

Também utilizamos mais uma vez a ferramenta *nmap*, como mostra a figura seguinte, com um *script* específico (`--script="snmp*"`), para obter estas mesmas informações, mas de forma mais simples.

```

snmp-netstat:
TCP 0.0.0.0:21      0.0.0.0:0
TCP 0.0.0.0:25      0.0.0.0:0
TCP 0.0.0.0:139     0.0.0.0:0
TCP 0.0.0.0:445     0.0.0.0:0
TCP 0.0.0.0:512     0.0.0.0:0
TCP 0.0.0.0:513     0.0.0.0:0
TCP 0.0.0.0:514     0.0.0.0:0
TCP 0.0.0.0:666     0.0.0.0:0
TCP 0.0.0.0:3306    0.0.0.0:0
TCP 0.0.0.0:3632    0.0.0.0:0
TCP 0.0.0.0:5901    0.0.0.0:0
TCP 0.0.0.0:6001    0.0.0.0:0
TCP 0.0.0.0:8080    0.0.0.0:0
TCP 0.0.0.0:8443    0.0.0.0:0
TCP 0.0.0.0:9080    0.0.0.0:0
TCP 0.0.0.0:9443    0.0.0.0:0
TCP 127.0.0.1:631   0.0.0.0:0
UDP 0.0.0.0:68      *:
UDP 0.0.0.0:123     *:
UDP 0.0.0.0:137     *:
UDP 0.0.0.0:138     *:
UDP 0.0.0.0:161     *:
UDP 0.0.0.0:5353    *:
UDP 0.0.0.0:34821   *:
UDP 127.0.0.1:123   *:
UDP 192.168.205.128 *:
UDP 192.168.205.128 *:
UDP 192.168.205.128 *:
snmp-brute:
public - Valid credentials
private - Valid credentials
snmp-sysdescr: Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686
System uptime: 2h10m32.49s (783249 timeticks)
snmp-interfaces:
lo
IP address: 127.0.0.1 Netmask: 255.0.0.0
Type: softwareLoopback Speed: 10 Mbps
Status: up
Traffic stats: 349.01 Kb sent, 349.01 Kb received
eth0
IP address: 192.168.205.128 Netmask: 255.255.255.0
MAC address: 00:0c:29:cf:03:9c (VMware)
Type: ethernetCsmacd Speed: 10 Mbps
Status: up
Traffic stats: 6.29 Mb sent, 7.48 Mb received
MAC Address: 00:0c:29:cf:03:9c [VMware]

```

Figura 23 - Protocolo SNMP com *nmap*

### 3.2.3. LDAP e SMB

Com o protocolo LDAP e SMB, podemos ter acesso a serviços de diretoria, que podem fornecer conjuntos de registos de forma organizada através de uma estrutura lógica e hierárquica. Como mostra a próxima figura, fizemos uso da ferramenta *rpcclient* para obter alguma dessas informações, como o *querydomaininfo*, o *enumdomusers* e o *srvinfo*.

```

(kali@kali)~$ sudo rpcclient -U "" 192.168.205.128
Password for [WORKGROUP\]:
rpcclient $> querydomaininfo
Domain: ITSECGAMES
Server: BEE-BOX
Comment: bee-box server (Samba 3.0.28a)
Total Users: 2
Total Groups: 0
Total Aliases: 0
Sequence No: 1703606681
Force Logoff: -1
Domain Server State: 0x1
Server Role: ROLE_DOMAIN_PDC
Unknown 3: 0x1
rpcclient $> enumdomusers
user:[nobody] rid:[0x1f5]
user:[bee] rid:[0xbb8]
rpcclient $> queryuser nobody
User Name : nobody
Full Name : nobody
Home Drive :
Dir Drive : (null)
Profile Path:
Logon Script:
Description :
Workstations:
Comment : (null)

```

Figura 24 - Protocolo LDAP com *rpcclient*

Outra forma de obter estes resultados é correr alguns *scripts* incorporados na ferramenta *nmap*, como mostra as próximas figuras. Neste caso, em vez da obtenção de uma lista com as informações todas dos *users*, grupos, entre outros, é necessário correr um *script* para cada um desses.

```
(kali@kali)-[~]
└─$ sudo nmap -sS -p 445 192.168.205.128 --script smb-enum-users
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 11:01 EST
Nmap scan report for 192.168.205.128
Host is up (0.00024s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:CF:03:9C (VMware)

Host script results:
| smb-enum-users:
|   BEE-BOX\bee (RID: 3000)
|   Full name: bee,,,
|   Flags: Normal user account
|   BEE-BOX\nobody (RID: 501)
|   Full name: nobody
|   Flags: Normal user account
|_
Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

(kali@kali)-[~]
└─$ sudo nmap -sS -p 445 192.168.205.128 --script smb-enum-groups
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 11:02 EST
Nmap scan report for 192.168.205.128
Host is up (0.00017s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:CF:03:9C (VMware)

Host script results:
| smb-enum-groups:
|   BEE-BOX
|   Groups: n/a
|   Users: nobody\x00, bee\x00
|   Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|   Account lockout disabled
|_
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

```
(kali@kali)-[~]
└─$ sudo nmap -sS -p 445 192.168.205.128 --script smb-enum-domains
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 11:02 EST
Nmap scan report for 192.168.205.128
Host is up (0.00020s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:CF:03:9C (VMware)

Host script results:
| smb-enum-domains:
|   Builtin
|   Groups: n/a
|   Users: n/a
|   Creation time: unknown
|   Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|   Account lockout disabled
|   BEE-BOX
|   Groups: n/a
|   Users: nobody\x00, bee\x00
|   Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|   Account lockout disabled
|_
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

Figura 25 - Protocolo *SMB* com *nmap*

### 3.2.4. *IPsec*

Realizamos um simples *scan* ao *ISAKMP*, no porto 500, para saber de existia um servidor *VPN IPsec*, como mostra a figura abaixo.

```
(kali@kali)-[~]
└─$ sudo nmap -sU -p 500 192.168.205.128
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-26 11:32 EST
Nmap scan report for 192.168.205.128
Host is up (0.00028s latency).

PORT      STATE SERVICE
500/udp   closed isakmp
MAC Address: 00:0C:29:CF:03:9C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Figura 26 - *IPsec* com *nmap*

### 3.3. Identificação e Análise das Vulnerabilidades

Nesta última fase, trata-se da pesquisa de vulnerabilidades e falhas de desenvolvimento e implementação, que permitem a exploração de falhas em SO e aplicações. Vai ser apresentado uma classificação das vulnerabilidades em anexo, gerada por uma ferramenta que vamos falar mais à frente, onde estas podem ser baseadas em níveis de severidade baixo, médio, alto ou crítico.

#### 3.3.1. Nikto

O *Nikto* é uma ferramenta de código aberto utilizada para análise de vulnerabilidades em servidores *web*. Serve para identificar possíveis problemas de segurança, configurações incorretas e outros riscos. Na figura seguinte podemos observar a ferramenta *nikto* a analisar o nosso *host* na porta 80.

```
(kali@kali)~$ nikto -p 80 -h 192.168.205.128
- Nikto v2.5.0

+ Target IP: 192.168.205.128
+ Target Hostname: 192.168.205.128
+ Target Port: 80
+ Start Time: 2023-12-29 06:48:39 (GMT-5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
+ /: Server may leak inodes via ETags, header found with file /, inode: 838422, size: 588, mtime: Sun Nov 2 13:20:24 2014. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site-attacks
+ OpenSSL/0.9.8g appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
+ mod_ssl/2.2.8 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ PHP/5.2.4-2ubuntu5 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.bak, index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracking
+ mod_ssl/2.2.8 OpenSSL/0.9.8g - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell.
+ PHP/5.2 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561
+ /phpmyadmin/changelog.php: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.
+ /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /icons/: Directory indexing found.
+ /README: README file found.
+ /INSTALL.txt: Default file found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8101 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time: 2023-12-29 06:48:53 (GMT-5) (14 seconds)

+ 1 host(s) tested
```

Figura 27 - Nikto

#### 3.3.2. Nessus

O *Nessus* é uma ferramenta conhecida pela capacidade de identificar e avaliar vulnerabilidades em sistemas, redes e aplicações. No anexo A segue o relatório que esta

ferramenta gerou, onde iremos falar a seguir destas vulnerabilidades e apresentar algumas soluções para mitigar estas.

### **3.4. Soluções Para Mitigar as Vulnerabilidades**

Neste tópico vamos abordar algumas soluções para combater ou mitigar as vulnerabilidades encontradas. Iremos falar das que, ao fim da conclusão do relatório da ferramenta *Nessus* se encontram no nível de severidade crítico e alguns no nível elevado.

#### **3.4.1. *SSL Version 2 and 3 Protocol Detection***

As versões SSL 2 e 3 contêm vulnerabilidades conhecidas e expostas na *internet*, para isso o melhor é desativar o suporte ao SSLv2 e SSLv3 no servidor e configurar o uso de TLS (*Transport Layer Security*) em vez de SSL.

#### **3.4.2. *Samba 'AndX' Request Heap-Based Buffer Overflow***

Esta é uma vulnerabilidade crítica que pode permitir que os atacantes executem código sem restrições ou verificações adequadas. Para isso é aconselhável manter o *samba* atualizado ou mesmo configurar a *firewall* para bloquear o acesso ao protocolo SMB.

#### **3.4.3. *OpenSSL Heartbeat Information Disclosure (Heartbleed)***

Esta vulnerabilidade permite que os atacantes roubem informações confidenciais de sistemas executando o *OpenSSL*. Para ajudar aconselha-se a atualizar regularmente a versão do *software OpenSSL*, atualizar para uma versão que não seja afetada pelo *Heartbleed* e emitir novamente certificados TLS e chaves privadas após a aplicação das correções.

#### **3.4.4. *SNMP Agent Default Community Name (public)***

Este SNMP está configurado com a comunidade SNMP padrão "*public*". O SNMP usa comunidades para autenticação e controle de acesso a informações gerenciadas por SNMP. Para mitigar esta vulnerabilidade, pode-se alterar a comunidade padrão e implementar mais segurança, como criptografia e autenticação, para proteger a comunicação SNMP.

## 4. Anexo A



### Bee-Box

---

Report generated by Nessus™  
Dec 2023 14:07:04 EST

Tue, 26

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

- 192.168.205.128.....4

Nessus  
Essentials

## **Vulnerabilities by Host**



192.168.205.128



## Vulnerabilities

Total: 118

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0*	5.9	58327	Samba 'AndX' Request Heap-Based Buffer Overflow
HIGH	7.5	5.1	71783	Network Time Protocol Daemon (ntpd) monlist Command Enabled DoS
HIGH	7.5	6.1	73412	OpenSSL Heartbeat Information Disclosure (Heartbleed)
HIGH	7.5	4.9	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	7.4	78515	Drupal Database Abstraction API SQLi
HIGH	7.5*	5.2	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	4.4	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.8	-	97861	Network Time Protocol (NTP) Mode 6 Scanner
MEDIUM	5.6	7.7	77200	OpenSSL 'ChangeCipherSpec' MiTM Vulnerability

MEDIUM	5.3	1.4	<a href="#">88098</a>	Apache Server ETag Header Information Disclosure
MEDIUM	5.3	-	<a href="#">10677</a>	Apache mod_status /server-status Information Disclosure
MEDIUM	5.3	4.0	<a href="#">11213</a>	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	<a href="#">57608</a>	SMB Signing not required
MEDIUM	5.3	-	<a href="#">15901</a>	SSL Certificate Expiry
MEDIUM	5.3	-	<a href="#">45411</a>	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	<a href="#">26928</a>	SSL Weak Cipher Suites Supported
MEDIUM	5.3	2.2	<a href="#">134220</a>	nginx < 1.17.7 Information Disclosure
MEDIUM	6.4*	5.2	<a href="#">43156</a>	NTP ntpd Mode 7 Error Response Packet Loop Remote DoS
MEDIUM	4.0*	6.3	<a href="#">52611</a>	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	5.0*	3.6	<a href="#">76474</a>	SNMP 'GETBULK' Reflection DDoS
MEDIUM	4.3*	-	<a href="#">90317</a>	SSH Weak Algorithms Supported
MEDIUM	4.3*	4.5	<a href="#">81606</a>	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	3.6	<a href="#">70658</a>	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	<a href="#">153953</a>	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	4.5	<a href="#">83875</a>	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	4.5	<a href="#">83738</a>	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.1	<a href="#">78479</a>	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.6*	-	<a href="#">71049</a>	SSH Weak MAC Algorithms Enabled
LOW	N/A	-	<a href="#">69551</a>	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
LOW	2.6*	-	<a href="#">10407</a>	X Server Detection
INFO	N/A	-	<a href="#">10114</a>	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	<a href="#">46180</a>	Additional DNS Hostnames
INFO	N/A	-	<a href="#">18261</a>	Apache Banner Linux Distribution Disclosure

INFO	N/A	-	<a href="#">48204</a>	Apache HTTP Server Version
INFO	N/A	-	<a href="#">84574</a>	Backported Security Patch Detection (PHP)
INFO	N/A	-	<a href="#">39520</a>	Backported Security Patch Detection (SSH)
INFO	N/A	-	<a href="#">39521</a>	Backported Security Patch Detection (WWW)
INFO	N/A	-	<a href="#">45590</a>	Common Platform Enumeration (CPE)
INFO	N/A	-	<a href="#">54615</a>	Device Type
INFO	N/A	-	<a href="#">18638</a>	Drupal Software Detection
INFO	N/A	-	<a href="#">35716</a>	Ethernet Card Manufacturer Detection
INFO	N/A	-	<a href="#">86420</a>	Ethernet MAC Addresses
INFO	N/A	-	<a href="#">10092</a>	FTP Server Detection
INFO	N/A	-	<a href="#">84502</a>	HSTS Missing From HTTPS Server
INFO	N/A	-	<a href="#">43111</a>	HTTP Methods Allowed (per directory)
INFO	N/A	-	<a href="#">10107</a>	HTTP Server Type and Version
INFO	N/A	-	<a href="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	<a href="#">10397</a>	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	-	<a href="#">10785</a>	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	<a href="#">11011</a>	Microsoft Windows SMB Service Detection
INFO	N/A	-	<a href="#">100871</a>	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	<a href="#">106716</a>	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	<a href="#">14274</a>	Nessus SNMP Scanner
INFO	N/A	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	<a href="#">10884</a>	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	<a href="#">117886</a>	OS Security Patch Assessment Not Available

INFO	N/A	-	<a href="#">181418</a>	OpenSSH Detection
INFO	N/A	-	<a href="#">50845</a>	OpenSSL Detection
INFO	N/A	-	<a href="#">57323</a>	OpenSSL Version Detection
INFO	N/A	-	<a href="#">48243</a>	PHP Version Detection
INFO	N/A	-	<a href="#">66334</a>	Patch Report
INFO	N/A	-	<a href="#">10263</a>	SMTP Server Detection
INFO	N/A	-	<a href="#">42088</a>	SMTP Service STARTTLS Command Support
INFO	N/A	-	<a href="#">35296</a>	SNMP Protocol Version Detection
INFO	N/A	-	<a href="#">34022</a>	SNMP Query Routing Information Disclosure
INFO	N/A	-	<a href="#">10550</a>	SNMP Query Running Process List Disclosure
INFO	N/A	-	<a href="#">10800</a>	SNMP Query System Information Disclosure
INFO	N/A	-	<a href="#">10551</a>	SNMP Request Network Interfaces Enumeration
INFO	N/A	-	<a href="#">185519</a>	SNMP Server Detection
INFO	N/A	-	<a href="#">40448</a>	SNMP Supported Protocols Detection
INFO	N/A	-	<a href="#">70657</a>	SSH Algorithms and Languages Supported
INFO	N/A	-	<a href="#">149334</a>	SSH Password Authentication Accepted
INFO	N/A	-	<a href="#">10881</a>	SSH Protocol Versions Supported
INFO	N/A	-	<a href="#">153588</a>	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	<a href="#">10267</a>	SSH Server Type and Version Information
INFO	N/A	-	<a href="#">56984</a>	SSL / TLS Versions Supported
INFO	N/A	-	<a href="#">45410</a>	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	<a href="#">10863</a>	SSL Certificate Information
INFO	N/A	-	<a href="#">70544</a>	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	<a href="#">21643</a>	SSL Cipher Suites Supported
INFO	N/A	-	<a href="#">62563</a>	SSL Compression Methods Supported

INFO	N/A	-	<a href="#">57041</a>	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	<a href="#">51891</a>	SSL Session Resume Supported
INFO	N/A	-	<a href="#">156899</a>	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	<a href="#">25240</a>	Samba Server Detection
INFO	N/A	-	<a href="#">104887</a>	Samba Version
INFO	N/A	-	<a href="#">96982</a>	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)
INFO	N/A	-	<a href="#">22964</a>	Service Detection
INFO	N/A	-	<a href="#">11153</a>	Service Detection (HELP Request)
INFO	N/A	-	<a href="#">25220</a>	TCP/IP Timestamps Supported
INFO	N/A	-	<a href="#">87242</a>	TLS NPN Supported Protocol Enumeration
INFO	N/A	-	<a href="#">62564</a>	TLS Next Protocols Supported
INFO	N/A	-	<a href="#">121010</a>	TLS Version 1.1 Protocol Detection
INFO	N/A	-	<a href="#">136318</a>	TLS Version 1.2 Protocol Detection
INFO	N/A	-	<a href="#">110723</a>	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	<a href="#">10287</a>	Traceroute Information
INFO	N/A	-	<a href="#">11154</a>	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	<a href="#">20094</a>	VMware Virtual Machine Detection
INFO	N/A	-	<a href="#">19288</a>	VNC Server Security Type Detection
INFO	N/A	-	<a href="#">65792</a>	VNC Server Unencrypted Communication Detection
INFO	N/A	-	<a href="#">10342</a>	VNC Software Detection
INFO	N/A	-	<a href="#">135860</a>	WMI Not Available
INFO	N/A	-	<a href="#">32318</a>	Web Site Cross-Domain Policy File Detection
INFO	N/A	-	<a href="#">11424</a>	WebDAV Detection
INFO	N/A	-	<a href="#">10150</a>	Windows NetBIOS / SMB Remote Host Information Disclosure

INFO	N/A	-	<a href="#">106628</a> lighttpd HTTP Server Detection
------	-----	---	---

---

INFO	N/A	-	<a href="#">66717</a> mDNS Detection (Local Network)
------	-----	---	--

---

INFO	N/A	-	<a href="#">106375</a> nginx HTTP Server Detection
------	-----	---	--

---

\*  
indicate  
s the  
v3.0  
score  
was not  
availabl  
e; the  
v2.0  
score  
is  
shown