

Universidade do Minho
Mestrado em Engenharia Informática
Tecnologia de Segurança
Trabalho Prático 2
Vulnerabilidades e Exposições Comuns (CVE)

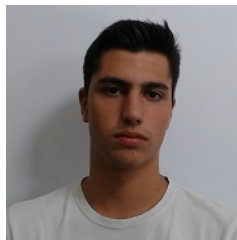
Grupo 5

PG47124

Daniel Filipe Santos Sousa,

PG47317

João Manuel Silva Amorim



Parte A



Para esta parte do trabalho prático foi nos pedido que puséssemos em prática os nossos conhecimentos sobre footprinting e escolhêssemos duas empresas, uma corporação grande e um negócio local, para analisar e identificar que tipo de sistemas e infraestruturas é que usam, utilizando técnicas de busca de informação passiva. Como tal, o nosso grupo escolheu a empresa de telecomunicações NOS como a nossa grande corporação e a empresa de venda de material informático PCDIGA como negócio local.

PCDIGA

A PCDIGA consiste numa empresa de venda de produtos informáticos e comparada com a NOS é uma empresa mais pequena. Como o site desta empresa permite fazer encomendas, recolhe informações sobre dados bancários e moradas, por isso achamos que seria interessante descobrir se o site deles tem algum tipo desta informação pública. Começamos por utilizar a ferramenta Whois Lookup do site Domain Tools para pesquisar sobre o domain “pcdiga.com” percebemos que o servidor onde o site está alojado pertencem à empresa Cloudflare e a informação sobre o mesmo encontra-se oculta(Ver Figura 1 e 2).

Whois Record for PcDiga.com

— Domain Profile

Registrant	GDPR Masked
Registrant Org	GDPR Masked
Registrant Country	pt
Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com IANA ID: 303 URL: www.publicdomainregistry.com,http://www.publicdomainregistry.com Whois Server: whois.publicdomainregistry.com abuse-contact@publicdomainregistry.com (p) 12013775952
Registrar Status	clientTransferProhibited
Dates	6,789 days old Created on 2003-08-25 Expires on 2024-08-25 Updated on 2019-08-09
Name Servers	AIDA.NS.CLOUDFLARE.COM (has 23,415,522 domains) CARTER.NS.CLOUDFLARE.COM (has 23,415,522 domains)
Tech Contact	GDPR Masked GDPR Masked, GDPR Masked, GDPR Masked, GDPR Masked, GDPR Masked gdpr-masking@gdpr-masked.com
IP Address	104.22.76.251 - 2 other sites hosted on this server
IP Location	 - New Jersey - Newark - Cloudflare Inc.
ASN	 AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)
Domain Status	Registered And Active Website
IP History	24 changes on 24 unique IP addresses over 18 years
Registrar History	3 registrars
Hosting History	19 changes on 12 unique name servers over 18 years

— Website

Figura 1 - Resultado do Whois Lookup ao domain “pcdiga.com”.

```
Domain Name: PCDIGA.COM
Registry Domain ID: 102583196_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2019-08-09T22:14:31Z
Creation Date: 2003-08-25T16:29:21Z
Registrar Registration Expiration Date: 2024-08-25T16:29:21Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/
/epp#clientTransferProhibited
Registry Registrant ID: GDPR Masked
Registrant Name: GDPR Masked
Registrant Organization: GDPR Masked
Registrant Street: GDPR Masked
Registrant City: GDPR Masked
Registrant State/Province: Leiria
Registrant Postal Code: GDPR Masked
Registrant Country: PT
Registrant Phone: GDPR Masked
Registrant Phone Ext:
Registrant Fax: GDPR Masked
Registrant Fax Ext:
Registrant Email: gdpr-masking@gdpr-masked.com
Registry Admin ID: GDPR Masked
Admin Name: GDPR Masked
Admin Organization: GDPR Masked
Admin Street: GDPR Masked
Admin City: GDPR Masked
Admin State/Province: GDPR Masked
Admin Postal Code: GDPR Masked
Admin Country: GDPR Masked
Admin Phone: GDPR Masked
Admin Phone Ext:
Admin Fax: GDPR Masked
Admin Fax Ext:
Admin Email: gdpr-masking@gdpr-masked.com
Registry Tech ID: GDPR Masked
Tech Name: GDPR Masked
Tech Organization: GDPR Masked
Tech Street: GDPR Masked
Tech City: GDPR Masked
Tech State/Province: GDPR Masked
Tech Postal Code: GDPR Masked
Tech Country: GDPR Masked
Tech Phone: GDPR Masked
Tech Phone Ext:
Tech Fax: GDPR Masked
Tech Fax Ext:
Tech Email: gdpr-masking@gdpr-masked.com
Name Server: aida.ns.cloudflare.com
Name Server: carter.ns.cloudflare.com
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
```

Figura 2 - Resultado do Whois Lookup ao domain “pcdiga.com” (continuação).

Como grupo ficamos surpresos com a PCDIGA, pois não estávamos à espera que recorressem a uma empresa externa, para além disso contrataram uma empresa de renome o que nos leva a querer que o seu site esteja bem protegido.

NOS

Primeiramente, o nosso grupo começou por procurar informação pública acerca de funcionários com cargos importantes dentro da empresa, para isso utilizamos o site Around Deal e o LinkedIn. O primeiro site é uma plataforma que contém informação sobre empresas e os seus funcionários e através da pesquisa do nome da empresa “NOS SGPS” conseguimos obter uma lista de funcionários e dependendo do funcionário há informação disponível ou não como podemos ver na Figura 3.

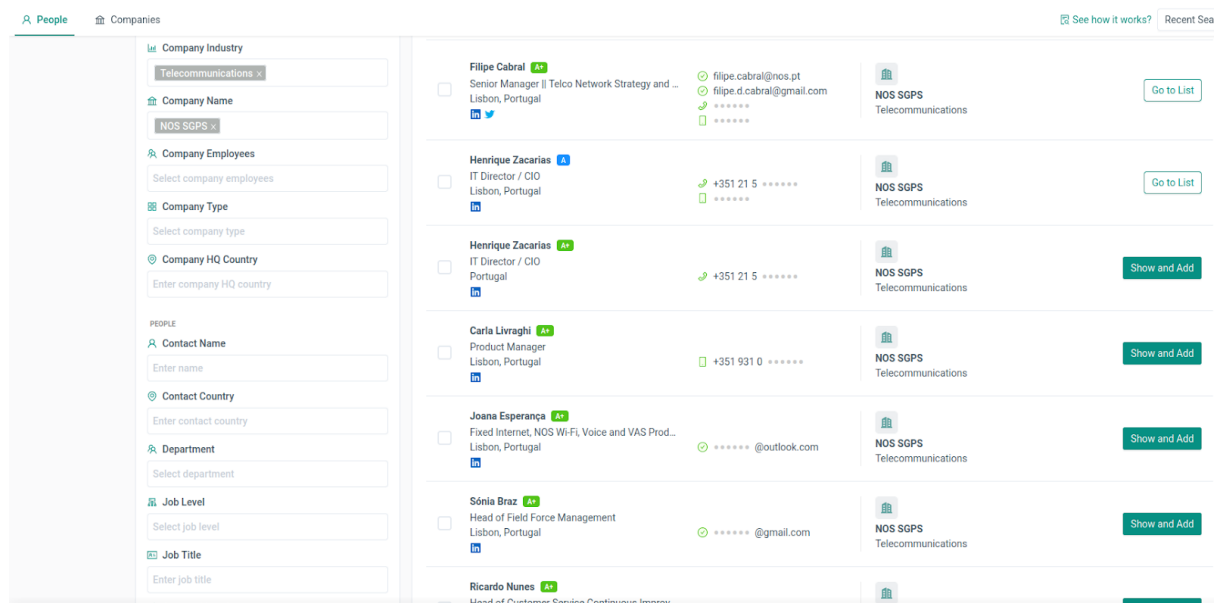


Figura 3 - Lista de funcionários encontrada.

Como é visível a informação encontra-se oculta pois para a revelar é preciso pagar. Com a utilização deste site destacamos as seguintes pessoas: Henrique Zacarias, Jorge Seabra e Filipe Cabral, CIO, Network Infrastructure Manager e Senior Manager, respetivamente. Decidimos que estes 3 funcionários seriam de interesse para o trabalho, pois os dois primeiros têm cargos importantes na empresa pelo que poderíamos procurar pelos mesmos noutras redes sociais com a vista a fazer o profiling e através de técnicas de social engineering ter acesso a algum tipo de informação que só eles teriam. Decidimos destacar o terceiro funcionário uma vez que este também deve ter permissões que outros funcionários não têm no sistema, e para além disso é o funcionário que tinha mais informação pública disponível o que tornaria mais fácil um tracing do mesmo. Como prova disso temos as seguintes figuras, obtidas através da ferramenta Spokeo People Search, onde podemos ver que seria possível obter mais informação sobre o mesmo.

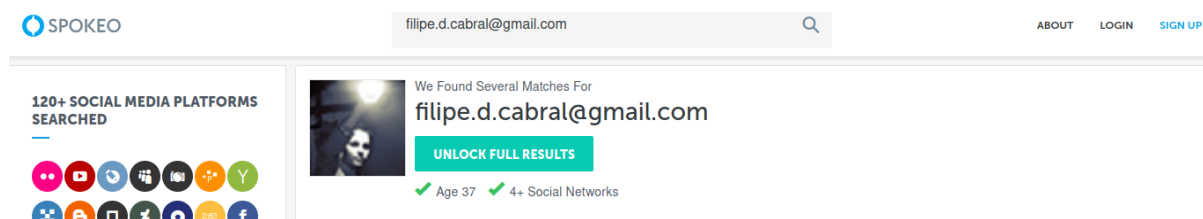


Figura 4 - Resultado da pesquisa no Spokeo.

RESULTS ARE READY!

Filipe Cabral
Latest report as of 03/26/2022

Report Includes Available Information On:

- OWNER'S NAME: ✓ Filipe Cabral
- SOCIAL PROFILES: ✓ 4 Social Profiles Found
- PROFILE PHOTOS: ✓ See Available Results
- DATING PROFILES: ✓ See Available Results
- CONTACT DETAILS: ✓ See Available Results
- ADDRESS HISTORY: ✓ See Available Results

PICK YOUR OPTION

FULL SOCIAL REPORT

\$0.95 51% OFF
SPECIAL PRICE

CONTINUE >

437 people have purchased this recently

Special Offer with FREE Trial Membership gives you:

- ✓ Full Access to Social Search
Find people in the U.S. by social to quickly see their full name, social profiles, photos, and more.
- ✓ Instant Access to Name, Phone & Address Search

Social Report Only
\$1.95 regular price

CONTINUE >

Figura 5 - Resultado da pesquisa no Spokeo (continuação).

De seguida, através do LinkedIn procuramos vagas de emprego na empresa com vista a obter informações sobre tecnologias que a mesma usa para depois pesquisarmos se há vulnerabilidades associadas às mesmas, e na vagas de emprego para engenheiro DevOps vimos que pediam experiência com Apache Kafka, RabbitMQ, Docker e Kubernetes, para além destas tecnologias também pedem conhecimentos sobre serviços RESTfull. Com isto podemos assumir que a empresa utiliza estas tecnologias nos seus serviços, pelo que podemos procurar vulnerabilidades nestas tecnologias pois podem se refletir nos serviços da empresa. Por fim, utilizamos outras ferramentas de scanning passivo para tentar descobrir informação sobre os servidores da empresa. Para tal, começamos por utilizar o comando “whois nos.pt” e utilizamos a ferramenta Whois Lookup do site Domain Tools para pesquisar pelo DNS nos.pt, os resultados são visíveis nas figuras abaixo.

```

jsoao@kali:~$ whois nos.pt
Domain: nos.pt
Domain Status: Registered
Creation Date: 12/03/2009 12:01:26
Expiration Date: 01/07/2025 23:59:00
Owner Name: NOS COMUNICAÇÕES, S.A.
Owner Address: APARTADO 8134
Owner Locality: LISBOA
Owner ZipCode: 1802-001
Owner Locality ZipCode: EC CABO RUIVO
Owner Country Code: PT
Owner Email: act.internet@nos.pt,psm.dns@isp.novis.pt,act.internet@zonoptimus.pt,regi
strar@KPNQwest.pt
Admin Name: NOS, SGPS, S.A.
Admin Address: Apartado 8134
Admin Locality: Lisboa
Admin ZipCode: 1802-001
Admin Locality ZipCode: EC Cabo Ruivo
Admin Country Code: PT
Admin Email: dns-admin@nos.pt,marie.c.abreu@nos.pt
Name Server: ns2.novis.pt | IPv4: and IPv6:
Name Server: ns1.novis.pt | IPv4: and IPv6:
Name Server: ns2.nos.pt | IPv4: 194.79.69.131 and IPv6: 2001:1588:4001:9::1
Name Server: ns1.nos.pt | IPv4: 194.79.69.129 and IPv6: 2001:1588:4001:8::1
Name Server: ns0006.secondary.cloudflare.com | IPv4: and IPv6:
Name Server: ns0204.secondary.cloudflare.com | IPv4: and IPv6:

```

Figura 6 - Resultado do comando “whois nos.pt”.

[PROFILE](#)
[CONNECT](#)
[MONITOR](#)
[SUPPORT](#)

Whois Lookup

[Home](#) > [Whois Lookup](#) > [Nos.pt](#)

Whois Record for Nos.pt

Domain Profile

Registrar Status	taken
Name Servers	NS0006.SECONDARY.CLOUDFLARE.COM (has 23,415,522 domains) NS0204.SECONDARY.CLOUDFLARE.COM (has 23,415,522 domains) NS1.NOS.PT (has 16 domains) NS1.NOVIS.PT (has 1,111 domains) NS2.NOS.PT (has 16 domains) NS2.NOVIS.PT (has 1,111 domains)
Tech Contact	—
IP Address	212.113.183.252 - 4 other sites hosted on this server
IP Location	Lisboa - Lisboa - Nos Comunicacoes S.a.
ASN	AS2860 NOS_COMUNICACOES, PT (registered Jan 18, 1994)
Hosting History	5 changes on 5 unique name servers over 8 years

Website

Website Title	500 SSL negotiation failed:
Response Code	500

Whois Record (last updated on 2022-03-27)

```

% NOTE: The registry for this domain name does not publish ownership
% records (whois records) in the standard format. This data
% represents the most likely status of the domain based on
% information provided by the Internet's domain name servers (DNS).

domain: nos.pt
status: taken
nameserver: ns0006.secondary.cloudflare.com
nameserver: ns0204.secondary.cloudflare.com
nameserver: ns1.nos.pt
nameserver: ns1.novis.pt
nameserver: ns2.nos.pt
nameserver: ns2.novis.pt

% For more information, please visit http://www.dns.pt/

```

Figura 7 - Resultado do Whois Lookup ao domínio “nos.pt”.

Pelos resultados conseguimos perceber que têm seis servidores, dois deles sabemos os endereços IPv4 e IPv6. Dos outros quatro, dois deles pertencem à Cloudflare e pelos nomes parecem ser servidores secundários. Como grupo pensamos que a NOS tem estes servidores da Cloudflare para caso os servidores deles fiquem de alguma forma inativos, os servidores secundários como são geridos por uma empresa externa não são afetados e o seu serviço continua ativo.

Sendo que se trata de uma grande empresa, o nosso grupo não estava à espera de encontrar tanta informação, sobretudo comparado com a empresa local que escolhemos.

Com estes dados tentamos investigar um pouco mais, e através da ferramenta de reverse IP ainda do mesmo site conseguimos encontrar 3 domains associados ao IP 212.113.183.252 (ver Figura 8) e utilizamos o comando “whois” para os dois domains que ainda não tínhamos visto e obtivemos os seguintes resultados (Figura 9, 10 e 11).

DOMAINTOOLS PROFILE CONNECT MONITOR

Home > Reverse IP Lookup > 212.113.183.252

212.113.183.252 Reverse IP Lookup

Enter an IP address and our patented Reverse IP Lookup tool will include all gTLD domains and any known ccTLD domains.

Lookup Connected Domains

Example: 65.55.53.233 or 64.233.161.%

Reverse IP Lookup Results – more than 3 domains hosted on

Domain
1. nos.pt
2. nosdiscos.pt
3. optimusdiscos.com

Figura 8 - Resultado do Reverse IP Lookup ao IP “212.113.183.252”.

joao@kali: ~ - Related Tools

<https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en>

```
(joao@kali)~$ whois nosdiscos.pt
Domain: nosdiscos.pt
Domain Status: Registered
Creation Date: 10/04/2014 17:55:59
Expiration Date: 09/04/2022 23:59:59
Owner Name:
Owner Address:
Owner Locality:
Owner ZipCode:
Owner Locality ZipCode:
Owner Country Code:
Owner Email:
Admin Name: NOS, SGPS, S.A.
Admin Address: Apartado 8134
Admin Locality: Lisboa
Admin ZipCode: 1802-001
Admin Locality ZipCode: EC Cabo Ruivo
Admin Country Code: PT
Admin Email: dns-admin@nos.pt,marie.c.abreu@nos.pt
Name Server: ns1.novis.pt | IPv4: and IPv6:
Name Server: ns2.novis.pt | IPv4: and IPv6:
```

Name Server Monitor
Monitor the daily activity of any name server and receive notification of all new and/or deleted domains.

Hosting History
View historical IP addresses, name servers, and registrars for any given domain name.

IP Explorer
Explore the range of all IP addresses and discover how any particular IP block is being utilized.

IP Monitor
Passively monitor additions and changes to registered domain names associated with an IP Address.

Bulk Parse Whois
Upload a list of domain names, and receive a csv file with parsed Whois records for the domains.

Figura 9 - Resultado do Whois Lookup ao domain “nosdiscos.pt”.

```
joao@kali:~$ whois optimusdiscos.com
Domain Name: OPTIMUSDISCOS.COM
Registry Domain ID: 1549020255_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2022-03-09T15:50:07Z
Creation Date: 2009-03-24T13:05:50Z
Registry Expiry Date: 2023-03-24T13:05:50Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.NOVIS.PT
Name Server: NS2.NOVIS.PT
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-03-26T12:00:31Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
```

Figura 10 - Resultado do Whois Lookup ao domain “optimusdiscos.com”.

```
joao@kali:~$ whois optimusdiscos.com
Tech Street: Statutory Masking Enabled
Tech City: Statutory Masking Enabled
Tech State/Province: Statutory Masking Enabled
Tech Postal Code: Statutory Masking Enabled
Tech Country: Statutory Masking Enabled
Tech Phone: Statutory Masking Enabled
Tech Phone Ext: Statutory Masking Enabled
Tech Fax: Statutory Masking Enabled
Tech Fax Ext: Statutory Masking Enabled
Tech Email: abuse@web.com
Registry Billing ID: Statutory Masking Enabled
Billing Name: Statutory Masking Enabled
Billing Organization: Statutory Masking Enabled
Billing Street: Statutory Masking Enabled
Billing City: Statutory Masking Enabled
Billing State/Province: Statutory Masking Enabled
Billing Postal Code: Statutory Masking Enabled
Billing Country: Statutory Masking Enabled
Billing Phone: Statutory Masking Enabled
Billing Phone Ext: Statutory Masking Enabled
Billing Fax: Statutory Masking Enabled
Billing Fax Ext: Statutory Masking Enabled
Billing Email: abuse@web.com
Name Server: NS1.NOVIS.PT
Name Server: NS2.NOVIS.PT
DNSSEC: unsigned
Registrar Abuse Contact Email: domain.operations@web.com
```

Figura 11 - Resultado do Whois Lookup ao domain “optimusdiscos.com” (continuação).

Podemos ver que o domínio “optimusdiscos.com” tem quase toda a informação escondida o que nos leva a querer que este deve ser o servidor principal da empresa. Por fim, conseguimos também obter a localização dos servidores aos quais sabemos o endereço IP através da feature GeoIP do site MAXMIND (Ver Figura 12).

GeoIP2 City Plus Web Service Results

IP Address	Country Code	Location	Network	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
194.79.69.131	PT	Loures, Lisbon, Portugal, Europe	194.79.69.0/24	2670-015	38.8333, -9.1653	1000	Nos Comunicacoes, S.A.	Nos Comunicacoes, S.A.	novis.pt	
194.79.69.129	PT	Loures, Lisbon, Portugal, Europe	194.79.69.0/24	2670-015	38.8333, -9.1653	1000	Nos Comunicacoes, S.A.	Nos Comunicacoes, S.A.	novis.pt	
212.113.183.252	PT	Portugal, Europe	212.113.176.0/21		38.7057, -9.1359	200	Nos Comunicacoes, S.A.	Nos Comunicacoes, S.A.	netcabo.pt	

Figura 12 - Resultado do GeoIP.

Parte B

Q1: Selecione um conjunto de ferramentas e técnicas de varredura ativa para identificar e detalhar vulnerabilidades e fraquezas para as quais o Sistema Metasploitable 3 está exposto. A sua resposta deverá listar os serviços a correr neste sistema e as vulnerabilidades e/ou fraquezas relacionados a cada um. Para os serviços com diferentes vulnerabilidades, escolha a mais recente ou a mais grave.

Inicialmente usamos a ferramenta nmap com a flag -sV para identificar as versões dos respetivos serviços na máquina virtual que hospeda o metasploitable 3.

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.1 (protocol 2.0)
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012
3000/tcp	open	http	WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016-11-21))
3306/tcp	open	mysql	MySQL 5.5.20-log
3389/tcp	open	tcpwrapped	
4848/tcp	open	ssl/http	Oracle Glassfish Application Server
7676/tcp	open	java-message-service	Java Message Service 301
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8022/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
8031/tcp	open	ssl/unknown	
8080/tcp	open	http	Sun GlassFish Open Source Edition 4.0
8181/tcp	open	ssl/intermapper?	
8383/tcp	open	http	Apache httpd
8443/tcp	open	ssl/https-alt?	
9200/tcp	open	wap-wsp?	
49152/tcp	open	msrpc	Microsoft Windows RPC
49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC
49155/tcp	open	msrpc	Microsoft Windows RPC

Figura 13 - Uso de nmap para identificar versões.

Para a versão do openssh a correr no sistema a última vulnerabilidade identificada foi a **CVE-2021-36368** que diz respeito a se um cliente estiver a fazer uma autenticação através de uma chave pública com "agent forwarding" mas sem a flag "oLogLevel=verbose", e um atacante modificou ,sem se notar, o servidor para suportar um método sem autenticação um cliente não consegue determinar se a autenticação FIDO vai confirmar que o cliente se deseja ligar a esse servidor, ou que o utilizador deseja permitir que esse servidor se ligue a um servidor diferente por conta do utilizador.

CVSS v3.1 Severity and Metrics:
Base Score: 3.7 LOW
Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
Impact Score: 1.4
Exploitability Score: 2.2

Attack Vector (AV): Network
Attack Complexity (AC): High
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): Low
Integrity (I): None
Availability (A): None

Figura 14 - cvss da última vulnerabilidade identificada para a versão em causa de openssl

Posteriormente encontramos a porta 8585 onde temos informações sobre a versão do apache utilizado, que neste caso é a 2.2.12, informações sobre o php e ainda informações sobre a versão do mysql que é a 5.5.20, mas que já sabíamos do scan de portas. As extensões utilizadas também são identificadas.

Server Configuration
Apache Version : 2.2.21
PHP Version : 5.3.10
Loaded Extensions :

- Core
- date
- iconv
- pcre
- tokenizer
- PDO
- xmlreader
- mysql
- xdebug
- bcmath
- ereg
- json
- Reflection
- zip
- Phar
- xmlwriter
- mysqli
- calendar
- filter
- mcrypt
- session
- zlib
- SimpleXML
- apache2handler
- pdo_mysql
- com_dotnet
- ftp
- SPL
- standard
- libxml
- wddx
- mbstring
- pdo_sqlite
- ctype
- hash
- odbc
- mysqlnd
- dom
- xml
- gd
- mhash

MySQL Version : 5.5.20

Figura 15 - Configuração do servidor do metasploitable 3

Para a versão do apache do sistema identifica-se a vulnerabilidade **CVE-2022-22721** que se refere a que se um “LimitXMLRequestBody” está alterado para permitir request bodies maiores que 350 MB nos sistemas um overflow de inteiros acontecia e mais tarde provocaria uma escrita “out of bounds”.

CVSS v3.1 Severity and Metrics:
Base Score: 9.8 CRITICAL
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Impact Score: 5.9
Exploitability Score: 3.9

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

Figura 16 - cvss da última vulnerabilidade referente a versão do apache

Relativamente à base de dados encontramos a seguinte vulnerabilidade, que foi a última a ser publicada em julho de 2021 a **CVE-2021-2356**.

A vulnerabilidade difícil de explorar permite que um atacante com acesso privilegiado à rede através de múltiplos protocolos possa comprometer o MySQL Server. Ataques bem sucedidos desta vulnerabilidade podem resultar na capacidade não autorizada de causar uma falha não autorizada ou repetida (DOS completo) do MySQL Server, bem como a atualização, inserção ou eliminação não autorizada do acesso a alguns dados do MySQL Server.

CVSS v3.1 Severity and Metrics:
Base Score: 5.9 MEDIUM
Vector: AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H
Impact Score: 4.2
Exploitability Score: 1.6

Attack Vector (AV): Network
Attack Complexity (AC): High
Privileges Required (PR): Low
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): None
Integrity (I): Low
Availability (A): High

Figura 17 - cvss da vulnerabilidade **CVE-2021-2356**

Para a versão do php identificamos a vulnerabilidade que identifica que um número de instâncias de buffers “over-reading” heap-based estão presentes em funções da expressão regular mbstring quando fornecidos com dados multibyte inválidos. Estes

ocorrem quando um padrão de expressão regular de multibyte contém sequências de multibyte inválidas.

CVSS v3.0 Severity and Metrics:
Base Score: 9.8 CRITICAL
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Impact Score: 5.9
Exploitability Score: 3.9

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

Figura 18 - CVSS da vulnerabilidade **CVE-2019-9023**

Acerca do sistema operativo corremos o nmap com a flag para o sistema operativo e ele forneceu-nos a versão do windows que corre na máquina sendo o Windows Server 2008 R2.

```
Device type: general purpose
Running: Microsoft Windows 7
OS CPE: cpe:/o:microsoft:windows_7::sp1
OS details: Microsoft Windows 7 SP1
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Figura 19 - resultado do nmap com as flags -sV e -O

Existe uma vulnerabilidade de execução de código remoto quando o Windows Search lida com objetos na memória, chamados de "Windows Search Remote Code Execution Vulnerability". Isto afeta a versão do sistema.

CVSS v3.0 Severity and Metrics:
Base Score: 8.8 HIGH
Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Impact Score: 5.9
Exploitability Score: 2.8

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): Low
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

Figura 20 - CVSS da vulnerabilidade CVE-2018-8450

Q2: Discuta os resultados globais do processo de varredura activa ao Sistema Mestasploitable 3. Avalie também as diferenças entre o resultado do sistema automático de identificação de vulnerabilidades e o resultado que obteve no item Q1 da Parte B deste enunciado.

Através da varredura executada com o scanner de vulnerabilidades Nessus obtivemos os seguintes resultados.



Figura 21- Gráfico das vulnerabilidades identificadas

No total foram identificadas 49 vulnerabilidades sendo oito delas consideradas críticas, 11 consideradas de alto risco, 28 de médio risco e 4 de baixo risco. Ainda foram identificadas outras informações contando com 154.

Também foi identificado o OS do sistema da máquina, bem como o endereço mac.

Host Details	
IP:	172.20.5.2
MAC:	08:00:27:21:94:D2
OS:	Microsoft Windows Server 2008 R2 Standard Service Pack 1
Start:	Today at 2:25 PM
End:	Today at 2:51 PM
Elapsed:	27 minutes
KB:	Download

Figura 22 - Detalhes do Host do metasploitable 3

Comparativamente às vulnerabilidades identificadas no exercício um estas foram bastante diferentes. Houve serviços que foram identificados no exercício um que coincidem com os da varredura do Nessus, porém as vulnerabilidades apresentadas foram diferentes. No Nessus, foram identificadas vulnerabilidades que o grupo não identificou.

Sev	Score	Name	Family	Count	
CRITICAL	9.8	Elasticsearch Transport Protocol Unspecified Remote Code Execution	Databases	1	
MIXED	...	Microsoft Windows (Multiple Issues)	Windows	8	
MIXED	...	Zohocorp Manageengine Desktop Central (Multiple Issues)	CGI abuses	6	
MIXED	...	Elasticsearch (Multiple Issues)	CGI abuses	4	
MIXED	...	Apache Tomcat (Multiple Issues)	Web Servers	2	
MIXED	...	SSL (Multiple Issues)	General	41	
MIXED	...	IETF Md5 (Multiple Issues)	General	3	
HIGH	...	Oracle Glassfish Server (Multiple Issues)	CGI abuses	2	
MEDIUM	5.1 *	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Windows	1	
MIXED	...	TLS (Multiple Issues)	Service detection	11	
MIXED	...	Microsoft Windows (Multiple Issues)	Misc.	4	
MIXED	...	SSL (Multiple Issues)	Service detection	2	
LOW	3.7	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	3	

Figura 23 - Vulnerabilidades identificadas no Nessus

Como mostra a figura 9 foram identificadas muito mais vulnerabilidades em muitos mais serviços do que o grupo identificou manualmente.

No nessus também foram identificadas cinco correções para cinco vulnerabilidades identificadas.

Action	Vulns	Hosts
ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities: Upgrade to ManageEngine Desktop Central version 9 build 92027 or later.	3	1
Apache Tomcat AJP Connector Request Injection (Ghostcat): Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.	2	1
Elasticsearch ESA-2015-06: Users should upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted applications have access to the transport protocol port.	2	1
Elasticsearch Transport Protocol Unspecified Remote Code Execution: Users should upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted applications have access to the transport protocol port	2	1
Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check): Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.	2	1

Figura 24 - Correções para vulnerabilidades

Q3: Examine o output do IDS e escolha dois eventos identificados como tráfego anômalo. Para cada evento escolhido, identifique o respectivo tráfego capturado via Analisador de tráfego e o descreva. Se possível, inclua o CVE da vulnerabilidade e o método de identificação usado pelo scanner.

1. SNMP AgentX/tcp request

```
[**] [1:1421:11] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/26-14:25:32.659794 172.20.5.1:62034 → 172.20.5.2:705
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
*****S* Seq: 0x330AEE7B Ack: 0x0 Win: 0x1000 TcpLen: 28
TCP Options (4) ⇒ MSS: 1460 NOP NOP SackOK
[Xref ⇒ http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0013][Xref ⇒
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0012][Xref ⇒ http://
www.securityfocus.com/bid/4132][Xref ⇒ http://www.securityfocus.com/bid/
4089][Xref ⇒ http://www.securityfocus.com/bid/4088]
```

Figura 11-Tráfego capturado pelo Snort

Analisando o IDS snort, escolhemos este evento como tráfego anômalo. Este diz respeito ao protocolo SNMP e verificamos que não se encontra explícita no nessus.

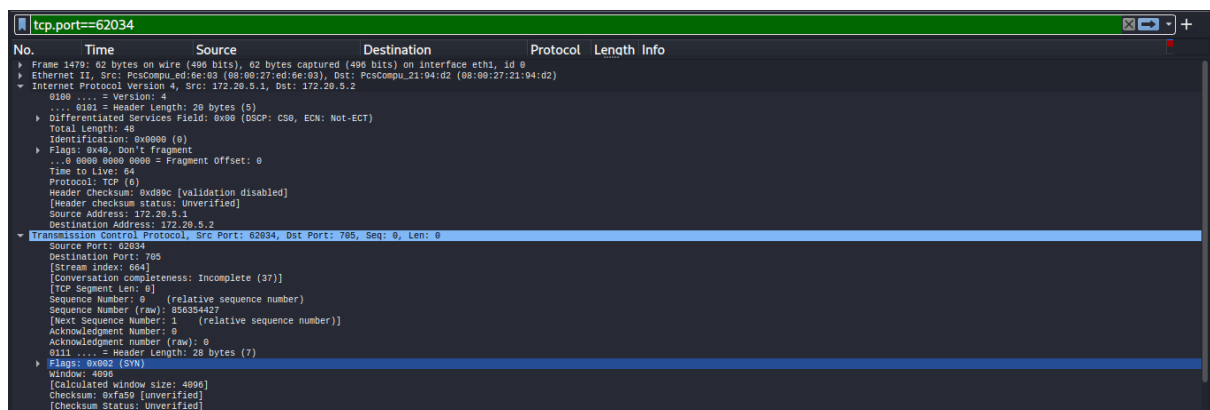


Figura 25 - Captura wireshark do tráfego anômalo

A representação da transmissão deste pacote está presente no wireshark, visualizado na figura 25 onde se vê a descrição do protocolo de transmissão do protocolo de internet, as flags do pacote entre outras coisas.

Apesar de não estar presente no Nessus realizou-se uma breve pesquisa sobre a vulnerabilidade que pode ser consultada em [3].

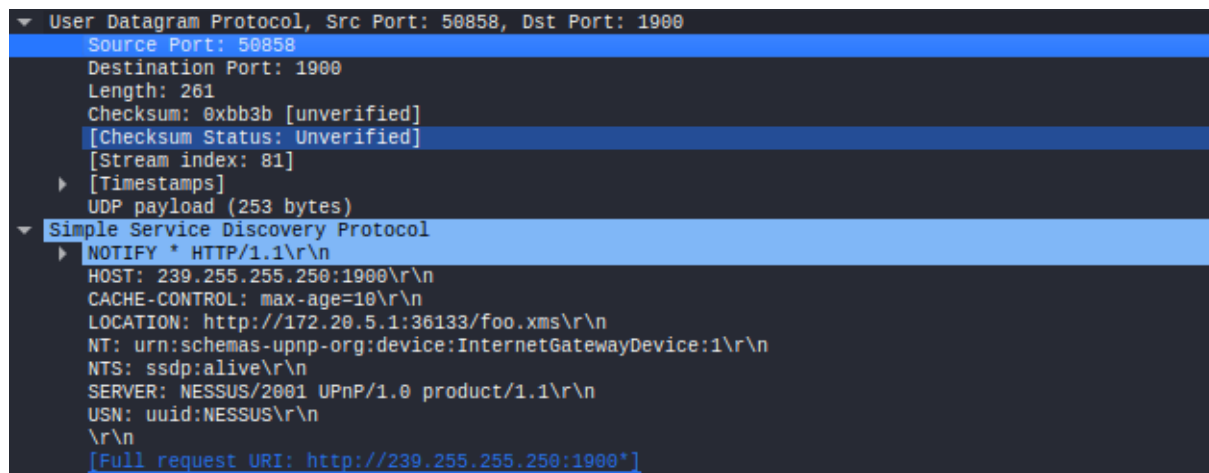
A outra anomalia escolhida foi referente a “UPnP malformed advertisement” que também estava presente no snort mas não estava presente no Nessus.

2. MISC UPnP malformed advertisement

```
[**] [1:1384:8] MISC UPnP malformed advertisement [**]  
[Classification: Misc Attack] [Priority: 2]  
03/26-14:27:54.251712 172.20.5.1:50858 → 172.20.5.2:1900  
UDP TTL:64 TOS:0x0 ID:31337 IpLen:20 DgmLen:281  
Len: 253  
[Xref ⇒ http://www.microsoft.com/technet/security/bulletin/MS01-059.msp]  
[Xref ⇒ http://cve.mitre.org/cgi-bin/cvename.cgi?name=2001-0877][Xref ⇒  
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2001-0876][Xref ⇒ http://www.securityfocus.com/bid/3723]
```

Figura 26 - Tráfego capturado pelo Snort

O pacote está representado no wireshark, visível na figura 14, onde podemos retirar informações sobre o SSDP, com o Host, o Server a localização entre outros.



The image shows a Wireshark packet capture of a User Datagram Protocol (UDP) packet. The packet is from source port 50858 to destination port 1900. The payload is a Simple Service Discovery Protocol (SSDP) message. The message is a NOTIFY packet for HTTP/1.1. The message body contains the following fields: HOST: 239.255.255.250:1900, CACHE-CONTROL: max-age=10, LOCATION: http://172.20.5.1:36133/foo.xms, NT: urn:schemas-upnp-org:device:InternetGatewayDevice:1, NTS: ssdp:alive, SERVER: NESSUS/2001 UPnP/1.0 product/1.1, and USN: uuid:NESSUS. The packet is marked as a full request URI: http://239.255.255.250:1900*.

Figura 27 - Captura de wireshark de tráfego anômalo

Como também não havia informação no Nessus fez-se uma breve pesquisa e a informação sobre a vulnerabilidade encontra-se em [4].

Q4: Observe que algumas notificações do IDS não possuem vulnerabilidade correspondente no relatório do Scanner de vulnerabilidades. Apresente e discuta as possíveis razões para estas diferenças.

O ids como tem um método diferente de análise do scanner de vulnerabilidades, ou seja capta todo o tráfego na interface escolhida.

Deste modo, pode ser capturado tráfego considerado anômalo sem que tenha uma vulnerabilidade correspondente no Scanner.


```

[**] [1:524:8] BAD-TRAFFIC tcp port 0 traffic [**]
[Classification: Misc activity] [Priority: 3]
03/26-14:27:50.943878 172.20.5.1:45437 → 172.20.5.2:0
TCP TTL:64 TOS:0x0 ID:51904 IpLen:20 DgmLen:40
*****S* Seq: 0x35968D70 Ack: 0x0 Win: 0x200 TcpLen: 20

```

Figura 28 - Exemplo de captura do snort

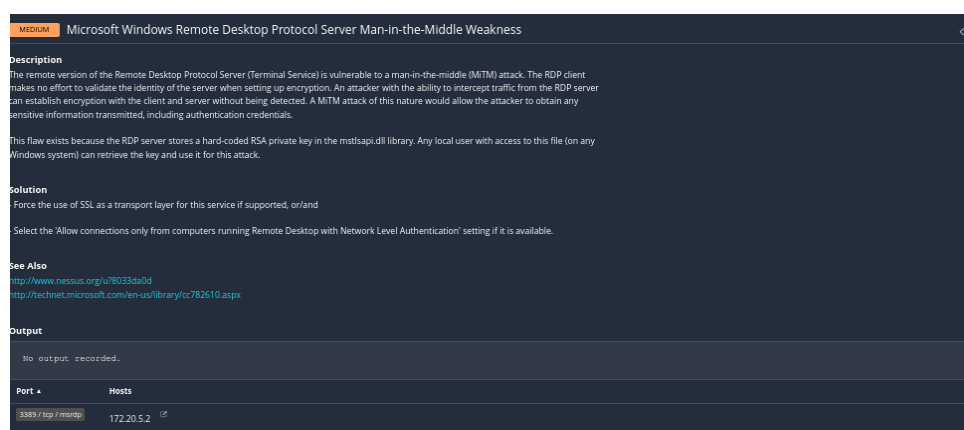
Nesta captura de tráfego verificamos que não possui uma vulnerabilidade visto que só foi notificado uma vez que estávamos a passar o scanner de vulnerabilidades no metasploitable 3.

Outra possibilidade seria de o resultado do IDS tivesse sido mais preciso do que o scanner de vulnerabilidades e identificar vulnerabilidades diferentes das identificadas pelo scanner.

Q5: Escolha três vulnerabilidades identificadas pelo Scanner de vulnerabilidades, sendo, pelo menos, uma classificada como High/Critical e uma classificada como Medium. Pesquise a documentação referente às formas de corrigir a fonte do problema e efetue os procedimentos necessários para tal. Ao final dos procedimentos escolhidos para cada vulnerabilidade, execute uma nova varredura para garantir que estas já não são identificadas. Discuta a solução dada e inclua os ficheiros resultantes da varredura antes e depois das respectivas correções.

Fizemos uma análise geral sobre as vulnerabilidades identificadas e sobre o método de como corrigi-las.

1. Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness



The screenshot shows a Nessus vulnerability report for the 'Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness'. The report is categorized as 'MEDIUM'. The description states that the remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MITM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MITM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials. The flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack. The solution is to force the use of SSL as a transport layer for this service if supported, or/and select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available. The 'See Also' section includes links to a Nessus.org advisory and a Microsoft library article. The 'Output' section shows 'No output recorded.' and a table with 'Port' 3389/tcp and 'Hosts' 172.20.5.2.

Figura 29 - Descrição do Nessus da vulnerabilidade

A sua descrição encontra-se em [7].

Corrigimos a vulnerabilidade de acordo como foi sugerido no nessus onde ativamos autenticação a nível de rede.

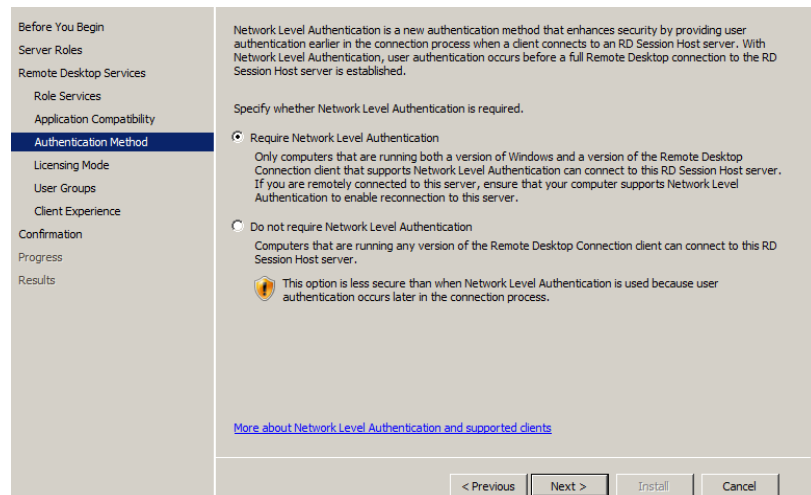


Figura 30 - Demonstração da correção da vulnerabilidade identificada na figura 29

2. Terminal Services Encryption Level is not FIPS-140 Compliant

Escolhemos também uma vulnerabilidade low onde tivemos apenas de mudar o método de encriptação. Esta vulnerabilidade é descrita como a definição de codificar usada pelo serviço de “remote Terminal Services” não é compatível com FIPS-140.

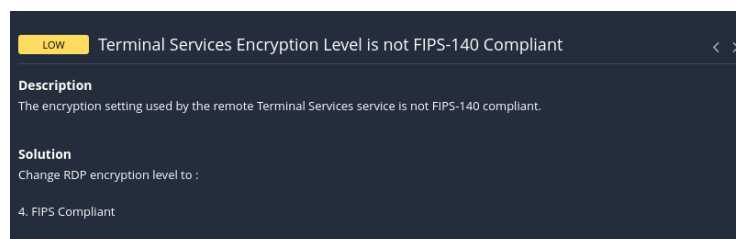


Figura 31 - Descrição do Nessus da vulnerabilidade

Apenas foi preciso ir ao RDP-Tcp properties e mudar o nível de encriptação.

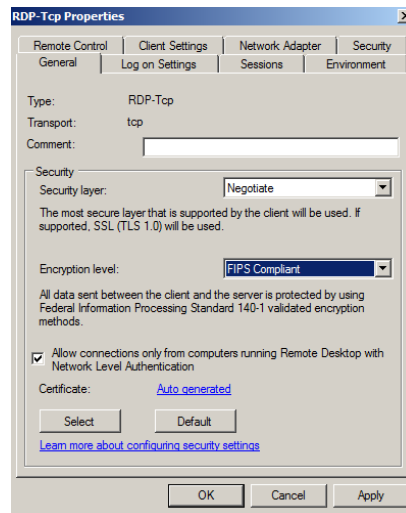


Figura 32 - Forma como corrigir a vulnerabilidade apresentada na figura 31

3. Elasticsearch Transport Protocol Unspecified Remote Code Execution

A vulnerabilidade crítica identificada e corrigida foi sobre o ElasticSearch Protocol. A sua descrição encontra-se em [8].

CRITICAL

Elasticsearch Transport Protocol Unspecified Remote Code Execution

< >

Description

Elasticsearch could allow a remote attacker to execute arbitrary code on the system, caused by an error in the transport protocol. An attacker could exploit this vulnerability to execute arbitrary code on the system.

Solution

Users should upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted applications have access to the transport protocol port

See Also

<http://www.nessus.org/u?c6b6cf1a>

Figura 33 - Descrição do Nessus da vulnerabilidade

Para a resolução desta alterou-se o método de ligação à porta que deixou de ser uma conexão aberta e passou a ser uma conexão segura e encriptada.

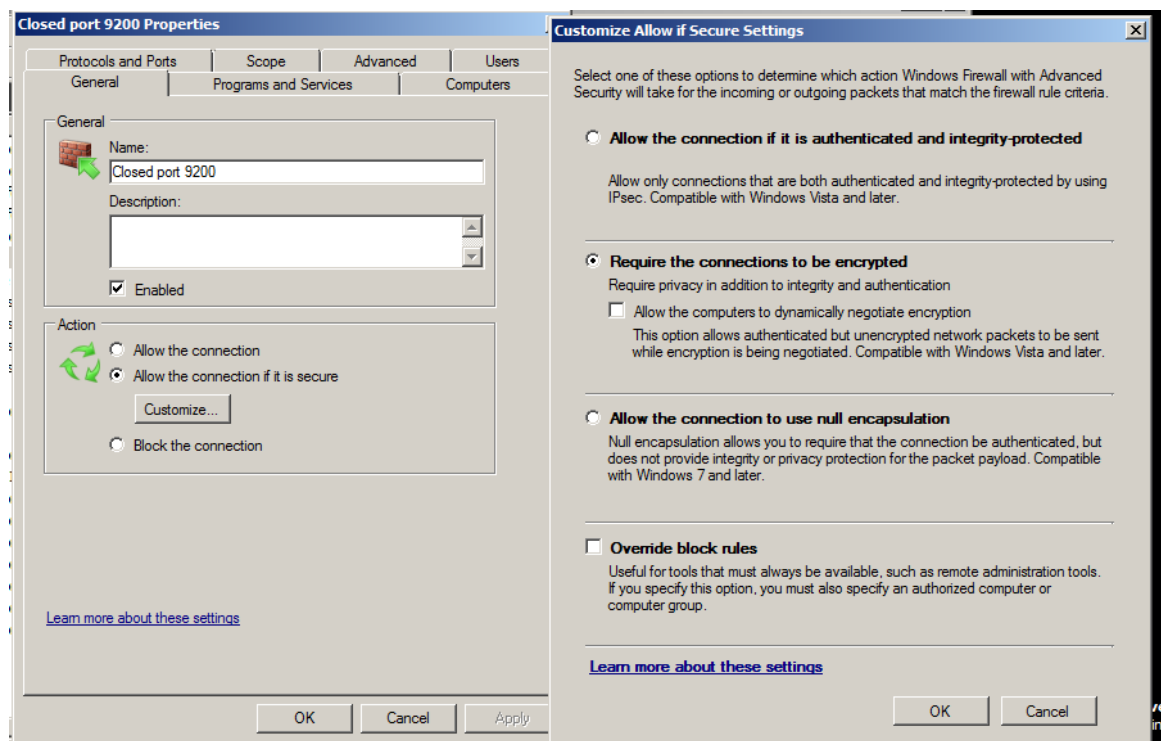


Figura 34 - Correção da vulnerabilidade da figura 33

Foi criada uma nova regra para esta porta definindo-se os novos parâmetros.

4. SMB signing not required

Adicionalmente corrigimos também outra vulnerabilidade média que apenas foi necessário ativar um política de segurança na máquina de Metaspitable 3. A sua descrição encontra-se em [9].

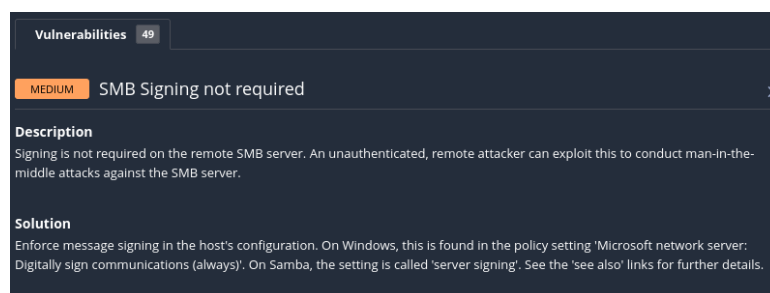


Figura 35 - Descrição do Nessus da vulnerabilidade

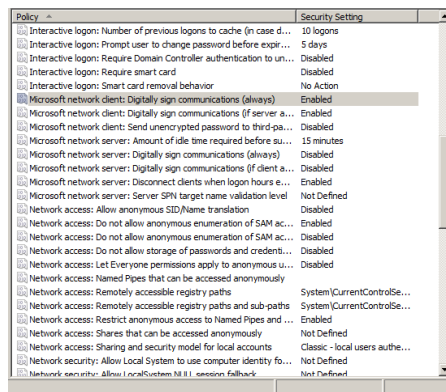


Figura 36 - Correção da vulnerabilidade da figura 35

Verificou-se que ao corrigir as vulnerabilidades identificadas para correção, muitas outras também foram corrigidas passando de 49 vulnerabilidades identificadas para apenas 25.

Para informações adicionais sobre a varredura, vão ser anexados os resultados das varreduras antes de serem aplicadas as correções e depois de serem aplicadas.

Referências:

1. <https://whois.domaintools.com/nos.pt> , acedido dia 22/3/2022
2. <https://reverseip.domaintools.com/search/?q=nos.pt> , acedido dia 22/3/2022
3. <https://research.domaintools.com/> , acedido dia 22/3/2022
4. https://www.snort.org/rule_docs/1-1421 acedido dia 26/03/2022
5. https://www.snort.org/rule_docs/1-1384 acedido dia 26/03/2022
6. <https://www.maxmind.com/en/home>, acedido dia 26/3/2022
7. <http://www.nessus.org/u?c6b6cf1a> , acedido dia 27/3/2022
8. <http://www.nessus.org/u?8033da0d>, acedido dia 27/3/2022
9. <https://www.nessus.org/u?df39b8b3> , acedido dia 27/3/2022