

Universidade do Minho

UNIVERSIDADE DO MINHO
MESTRADO INTEGRADO EM ENGENHARIA
INFORMÁTICA

SEGURANÇA DE SISTEMAS INFORMÁTICOS

Trabalho Prático Nº2

Autores:

Filipa Silva, A81015
Pedro Queirós, A84220

Grupo:2

27 de dezembro de 2020

Conteúdo

1	Introdução	4
2	Coleta Passiva vs Coleta Ativa de Informações	4
3	Parte A	5
3.1	Câmara Municipal de Braga	5
3.1.1	Análise de Informações de Registo de Domínio	5
3.1.2	Análise da Página WEB	6
3.1.3	Estratégias de Segurança	6
3.2	EDP - Energias de Portugal	7
3.2.1	Análise de Informações de Registo de Domínio	8
3.2.2	Análise da Página WEB	9
3.2.3	Estratégias de Segurança	10
3.3	Diferenças entre as duas empresas	10
4	Parte B	11
4.1	Questão 1	11
4.2	Questão 2	17
4.3	Questão 3	19
4.3.1	Heartbleed exploit	19
4.3.2	GhostCat LFI Attempt Inbound	21
4.4	Questão 4	23
4.5	Questão 5	24
4.5.1	ManageEngine Desktop Central 10 < Build 100479 Remote Code Execution (direct check)	24
4.5.2	SMB Signing not required	25
4.5.3	Terminal Services Doesn't Use Network Level Authentication (NLA) Only	26
5	Conclusão	28

Lista de Figuras

1	Informações relativas ao domínio <code>cm-braga.pt</code>	5
2	<i>Website</i> da Câmara Municipal de Braga.	6
3	<i>Website</i> da <i>Alfamind - Tecnologias</i>	7
4	Informações relativas ao domínio <code>edp.pt</code>	8
5	Informações relativas ao endereço IP 51.124.82.43.	9
6	<i>Website</i> da EDP.	10
7	Execução e resultados do comando <code>nmap -sV 172.20.2.2</code>	11
8	Continuação dos resultados do comando <code>nmap -sV 172.20.2.2</code>	12
9	Vulnerabilidade referente ao <i>OpenSSH</i>	12
10	Vulnerabilidade referente ao <i>Microsoft Windows RPC</i>	13
11	Vulnerabilidade referente ao <i>WEBrick httpd</i>	14
12	Vulnerabilidade referente ao <i>MySQL</i>	14
13	Vulnerabilidade referente ao <i>Apache JServ</i>	15
14	Vulnerabilidade referente ao <i>Sun GlassFish</i>	16
15	Vulnerabilidade referente ao <i>Apache HTTP</i>	16
16	Contagem das vulnerabilidades do Sistema <i>Metasploitable 3</i>	17
17	Listagem de algumas vulnerabilidades do Sistema <i>Metasploitable 3</i>	17
18	Remediações do Sistema <i>Metasploitable 3</i>	18
19	Anomalia <i>Heartbleed</i>	19
20	Continuação da anomalia <i>Heartbleed</i>	20
21	<i>Wireshark</i> da anomalia <i>Heartbleed</i>	20
22	Anomalia <i>GhostCat LFI</i>	21
23	Continuação da anomalia <i>GhostCat LFI</i>	21
24	<i>Wireshark</i> anomalia <i>GhostCat LFI</i>	22
25	Vulnerabilidade 1 - <i>High/Critical</i>	24
26	Confirmação da resolução de uma vulnerabilidade 1 (<i>High/Critical</i>).	25
27	Vulnerabilidade 2 - <i>Medium</i>	25
28	Resolução de uma vulnerabilidade 2 (<i>Medium</i>).	26
29	Vulnerabilidade 3 - <i>Medium</i>	26
30	Resolução de uma vulnerabilidade 3 (<i>Medium</i>).	27

1 Introdução

Este trabalho prático divide-se em duas partes independentes: a primeira consiste no uso de técnicas de coleta passiva de informação em sistemas e infraestruturas reais; a segunda passa por identificar vulnerabilidades e fraquezas de um sistema através de um ambiente de testes que usa técnicas de busca ativa.

Na **parte A** escolhem-se duas empresas, uma de dimensão local e outra de dimensão mundial, ambas com serviços *on-line* e utilizam-se técnicas de busca passiva para identificar detalhes nos seus sistemas. Posto isto, fez-se uma descrição das técnicas utilizadas e dos resultados obtidos pela utilização das mesmas, bem como a recomendação de algumas estratégias de segurança que podem ser adotadas. Por fim, compara-se as diferentes posturas implementadas pelos administradores de ambos os domínios.

Na **parte B** deu-se resposta a cinco questões colocadas no enunciado, fundamentando-as devidamente e comprovando as respostas através de imagens. Tal como foi mencionado, anteriormente recorreu-se a um ambiente de testes que usa ferramentas de varredura ativa instaladas no *Sistema Auditor*.

2 Coleta Passiva vs Coleta Ativa de Informações

Em Tecnologia de Segurança, a **coleta passiva** trata-se de um processo que visa a adquirir o máximo de conhecimentos de um sistema, sem que haja contacto entre o mesmo e o atacante. Através de um conjunto de técnicas e ferramentas, o atacante consegue obter variadas informações sobre o sistema, sem que este se aperceba disso, uma vez que esta recolha é realizada através de uma navegação normal ao *website*.

Quanto à **coleta ativa** diz-se ser a forma mais crua e agressiva de estudar uma invasão. As informações anteriormente recolhidas na fase de coleta passiva, serão agora usadas para moldar sondagens e comunicar diretamente com os alvos, com a intenção de identificar potenciais ameaças e vulnerabilidades. Para isto, é imprescindível conhecer as especificações do Sistema Operativo, quais os serviços disponíveis no servidor e as informações da versão da aplicação.

3 Parte A

3.1 Câmara Municipal de Braga

Quanto à empresa local, o grupo optou por escolher a Câmara Municipal de Braga, visto que é uma entidade que fornece serviços *on-line* não só aos habitantes da cidade, como também aos seus visitantes/turistas. Deste modo, podem obter mais informações acerca da cidade bem como das atividades realizadas e/ou os locais de interesse turístico e gastronómico, entre outras coisas.

3.1.1 Análise de Informações de Registo de Domínio

De acordo com as ferramentas de busca passiva apresentadas nos slides da aula prática, o grupo optou por efetuar a pesquisa do registo de domínio com recurso ao utilitário WHOIS. Posto isto, acedeu-se ao link <https://whois.domaintools.com/cm-braga.pt> para obter as informações apresentadas de seguida.

Whois Record for Cm-Braga.pt	
Domain Profile	
Registrar Status	taken
Name Servers	NS1.PTEMPRESAS.PT (has 8,838 domains) NS10.PTEMPRESAS.PT (has 8,838 domains) NS2.PTEMPRESAS.PT (has 8,838 domains)
Tech Contact	—
IP Address	62.28.4.75 - 1 other site is hosted on this server
IP Location	PT - Braga - Braga - Municipio De Braga
ASN	AS15525 MEO-EMPRESAS, PT (registered Jul 27, 2000)
Hosting History	1 change on 2 unique name servers over 4 years
Website	
Website Title	Braga City Council
Server Type	Apache
Response Code	200
Terms	360 (Unique: 219, Linked: 235)
Images	30 (Alt tags missing: 0)
Links	135 (Internal: 100, Outbound: 7)
Whois Record (last updated on 2020-12-14)	
<pre>% 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: cm-braga.pt status: taken nameserver: ns1.ptempresas.pt nameserver: ns10.ptempresas.pt nameserver: ns2.ptempresas.pt</pre>	

Figura 1: Informações relativas ao domínio cm-braga.pt.

A partir da recolha desta informação, considerou-se importante destacar os nomes dos servidores deste domínio, o endereço IP e a sua localização, bem como a organização que suporta este website, neste caso a empresa MEO.

3.1.2 Análise da Página WEB

Através da análise da página WEB tenta-se encontrar informações que completem as já anteriormente recolhidas. Tal como é possível observar na imagem seguinte, este *site* tem uma apresentação não muito complexa o que facilita o encontro de informações relevantes para os atacantes.

Assim sendo, para além da localização da empresa e dos contactos gerais da mesma, do rodapé retira-se uma informação bastante pertinente e que está assinalada a vermelho. Isto é, o nome da empresa que desenvolveu o *website* - Alfamind (*Innovation Systems*). Importa também referir que a página é desenvolvida utilizando linguagens de programação como CSS e XHTML.



Figura 2: Website da Câmara Municipal de Braga.

Uma vez recolhida a informação na página WEB, opta-se por dar continuidade à busca passiva e proceder à descoberta do responsável da página, para isto, analisou-se com detalhe a página da empresa. Através da página pode confirmar-se que a Câmara Municipal de Braga é um dos seus clientes/parceiros, porém não há informação relativa aos seus funcionários.

O próximo passo será procurar funcionários com recurso a redes sociais, neste caso o LinkedIn. Aqui, encontram-se informações acerca de 3 funcionários da empresa, sendo que um deles é o diretor executivo portanto este poderia ser uma hipótese de contacto para se descobrir o responsável do *site* da Câmara Municipal. Sendo esta uma abordagem passiva, não se deve realizar esse contacto e, por isso, nada se pode concluir nesse aspecto.

3.1.3 Estratégias de Segurança

A partir de todo o "percurso" de obtenção de informações, podem ser identificadas várias das tecnologias usadas pela empresa responsável pela criação e manutenção do site. Algumas delas são inclusive apresentadas *on-line* tal como se pode constatar na

figura 3. Um atacante que vise a aprontar um ataque, pode facilmente reconhecer as tecnologias, efetuar uma pesquisa sobre as suas vulnerabilidades e pôr em risco a confidencialidade e integridade dos dados presentes nesta página WEB.

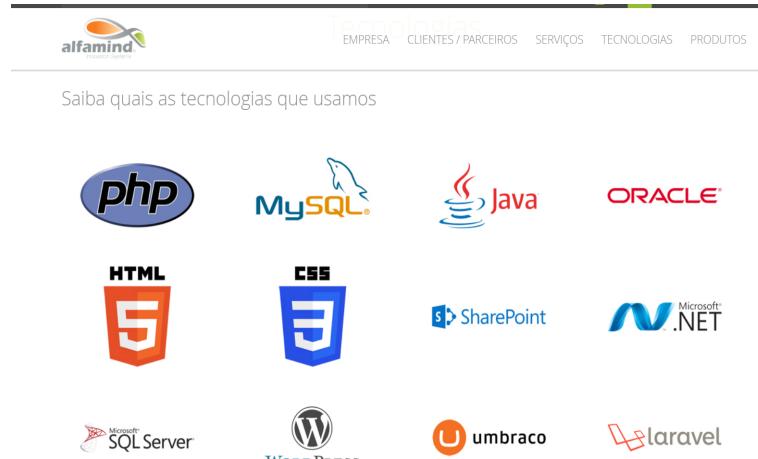


Figura 3: Website da Alfamind - Tecnologias.

Claramente que, um ato feito como possível publicidade a uma empresa, pode tornar um enorme risco para a empresa. Deste modo, e com este estudo concreto, o grupo deixa algumas recomendações de estratégias importantes no que concerne à segurança:

- Não disponibilizar as tecnologias utilizadas na construção de páginas WEB, nem na página da empresa responsável, nem na página do cliente.
- Não associar a empresa a que se trabalha ao perfil pessoal, num contexto de rede social.
- Não utilizar o mesmo nome em redes sociais pessoais e profissionais, uma vez que se torna simples encontram informações pessoais.

3.2 EDP - Energias de Portugal

Para a grande corporação, o grupo optou por incidir a sua pesquisa sob a EDP, uma vez que é uma empresa com dimensão mundial, que tem presença em mais de 15 países de continentes distintos. A sua organização centra-se na área da eletricidade e comercialização de gás e conta com mais de 12 mil funcionários.

3.2.1 Análise de Informações de Registo de Domínio

Assim como na secção anterior, para uma primeira análise, recorreu-se à ferramenta WHOIS que permite estudar os domínios e endereços de IP de um *website*.

Whois Record for Edp.pt	
— Domain Profile	
Registrar Status	taken
Name Servers	NS.EDP.COM.PT (has 9 domains) NS.EDP.PT (has 1 domains)
Tech Contact	—
IP Address	51.124.82.43 is hosted on a dedicated server
IP Location	🇳🇱 - Noord-holland - Amsterdam - Microsoft Limited
ASN	AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
Hosting History	1 change on 2 unique name servers over 5 years
— Website	
Website Title	⚠ 500 SSL negotiation failed.
Response Code	500
Whois Record (last updated on 2020-12-14)	
<pre>% 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: edp.pt status: taken nameserver: ns.edp.com.pt nameserver: ns.edp.pt % For more information, please visit http://www.dns.pt/</pre>	

Figura 4: Informações relativas ao domínio `edp.pt`.

Os resultados obtidos permitem-nos inferir que há dois servidores distintos, sendo que um deles, NS.EDP.COM.PT tem 9 domínios e o outro tem apenas um. O endereço de IP encontra-se localizado em Amesterdão, Holanda e a empresa que o suporta é a Microsoft.

Continuando a utilizar a ferramenta WHOIS, inspecionou-se agora o endereço IP do domínio (figura 5), sendo estes dados mais internos e em maior quantidade, pois muita da informação apresentada relaciona-se com o registo e administração do endereço em questão.

Observa-se que o intervalo de endereços IP se encontra entre 51.124.0.0 e 51.124.255. 255, endereços geridos pela Microsoft (referência na parte final correspondente à *route*). Verifica-se a divulgação de informação de uma pessoa real, Divya Quamara, o seu contacto e morada.

A pesquisa poderia continuar, recolhendo-se informações da mesma forma, através da identificação do MNTNER - neste caso MICROSOFT-MAINT - que é responsável pelos registos de bloqueio de rede em si.

IP Information for 51.124.82.43	
Quick Stats	
IP Location	Netherlands Amsterdam Microsoft Limited
ASN	AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
Whois Server	whois.ripe.net
IP Address	51.124.82.43
Reverse IP	1 website uses this address.
<pre>% Abuse contact for '51.124.0.0 - 51.124.255.255' is ' abuse@microsoft.com . inetnum: 51.124.0.0 - 51.124.255.255 org: ORG-MA42-RIPE netname: MICROSOFT descr: Microsoft Limited UK country: GB admin-c: DHS439-RIPE tech-c: MRP43-RIPE status: LEGACY mnt-by: RIPE-NCC-LEGACY-MNT mnt-by: MICROSOFT-MAINT created: 2015-05-21T17:07:47Z last-modified: 2016-07-25T09:38:58Z source: RIPE organisation: ORG-MA42-RIPE org-name: Microsoft Limited org-type: LIR descr: Microsoft Corporation AS8075 descr: To report suspected security issues spec ifíc to descr: traffic emanating from Microsoft online services, descr: including the distribution of malicious content descr: or other illicit or illegal material thr ough a descr: Microsoft online service, please submit reports descr: to: descr: * https://cert.microsoft.com</pre>	

Figura 5: Informações relativas ao endereço IP 51.124.82.43.

3.2.2 Análise da Página WEB

Para se analisar um página WEB de forma eficaz, pode recorrer-se à criação de um espelho do conteúdo local do *website*. Este tipo de análise tem como objetivo recolher informações empresariais que possam ser úteis no planeamento de um ataque.

Assim sendo, utilizou-se uma extensão do Google Chrome, "*Email Extractor*" que permite realizar um *scan* dos emails que existem na página mas não estão visíveis na abordagem do visitante. Além disto, descarrega-se o conteúdo da página para uma análise detalhada fora da rede.



Figura 6: Website da EDP.

Pela observação a "olho nu" do website não se retiram quaisquer informações, contrariamente ao que aconteceu nas visitas anteriores de empresas locais.

Pelas estratégias explicadas nesta secção também não se conseguiram informações relevantes, uma vez que não se obtiveram quaisquer emails ocultos; a análise do código HTML não mostrou código comentado, que por vezes ajuda neste tipo de abordagens; não se encontraram *links* para conteúdos de dados ou informações pessoais. A única ponta solta será a existência de *links* externos, como o LinkedIn.

Ao aceder a essa rede social podem ser reconhecidas algumas informações que potenciem o ataque, nomeadamente várias localidades onde a empresa tem instalações e um vasto conjunto de nomes de funcionários de várias nacionalidades, que além de informações pessoais identificam os cargos que ocupam na organização da empresa.

3.2.3 Estratégias de Segurança

Visto que ao nível desta página WEB não se encontraram grandes informações através da busca passiva, os autores não têm estratégias a recomendar, a não ser uma das que foi mencionada na análise anterior. Ou seja, não associar a empresa a que se trabalha ao perfil pessoal, num contexto de rede social, nem os mesmos nomes em diversas redes.

Porém nada garante que dada a dimensão desta empresa, estas recomendações já não estejam a ser seguidas, o que dificulta bastante a sugestão.

3.3 Diferenças entre as duas empresas

Relativamente à comparação dos resultados obtidos entre as duas empresas, é possível inferir que a empresa local tem menos preocupação de se proteger de ataques uma vez que o seu público alvo também é inferior. Por exemplo, no caso da Câmara Municipal o seu website tem informação de morada, contactos, criadores do site e tecnologias associadas, enquanto que na página da EDP não se consegue obter nenhuma dessas informações. Este exercício é fundamental para entender que toda e qualquer empresa, independentemente da sua dimensão se deve proteger de futuros ataques, e não mostrar mais do que é essencial.

4 Parte B

4.1 Questão 1

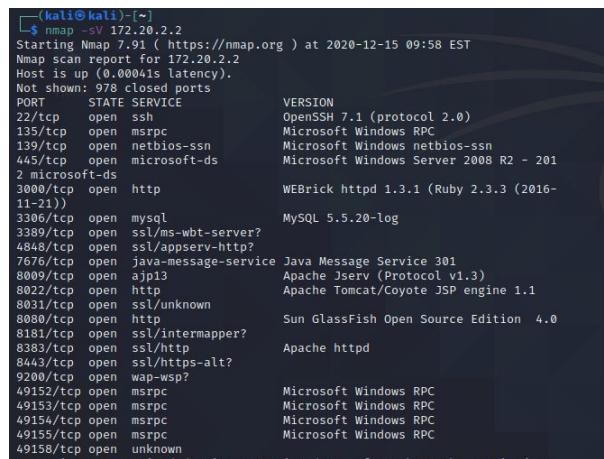
Selecione um conjunto de ferramentas e técnicas de varredura activa para identificar e detalhar vulnerabilidades e fraquezas para as quais o Sistema *Metasploitable 3* está exposto.

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.

Importante: Para esta questão, não será permitido o uso de *Scanners de Vulnerabilidades* (por exemplo, OpenVAS ou Nessus). Uma lista abrangente de ferramentas pode ser consultada em www.sectools.org

Para dar resposta a esta questão, e consultando o *link* fornecido optou-se por utilizar a ferramenta **nmap**.

Por forma a listar os serviços do sistema, e as suas respetivas versões recorreu-se ao comando **nmap** com a *flag* **-sV**. A execução do mesmo e os seus resultados, são apresentados nas figuras seguintes.



```
(kali㉿kali)-[~]
$ nmap -sV 172.20.2.2
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-15 09:58 EST
Nmap scan report for 172.20.2.2
Host is up (0.00041s latency).
Not shown: 978 closed ports
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 - 201
2/microsoft-ds
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  ssl/ms-wbt-server?
4848/tcp  open  ssl/appserv-https?
7676/tcp  open  java-message-service Java Message Service 3.01
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  ssl/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
49158/tcp open  unknown
```

Figura 7: Execução e resultados do comando **nmap -sV 172.20.2.2**

Figura 8: Continuação dos resultados do comando nmap -sV 172.20.2.2

Os resultados obtidos e considerados relevantes, são apresentados de seguida, bem como uma vulnerabilidade associada a cada um deles, sendo que por sugestão da equipa docente, foi analisada a vulnerabilidade mais grave ou mais recente.

- **OpenSSH 7.1 (protocol 2.0)** Para este *software* não foram encontradas vulnerabilidades que correspondessem à versão e protocolo utilizados, deste modo, estudou-se uma que acontece nas versões 5.x, 6.x, 7.x antes da 7.1p2. Esta apresenta uma pontuação de 8.1 (alta) uma vez que as funções *roaming_read* e *roming_write*, em certas opções de proxy e encaminhamento, não mantêm adequadamente a conexão aos descritores de ficheiro. Isto permite que servidores remotos causem uma negação de serviço (*buffer overflow*).

Este ataque é realizado através da rede, e apresenta um nível de complexidade alto, pelo que tem menos probabilidade de ter sucesso. No entanto, se acontecer, põe em alto risco a integridade, confidencialidade e disponibilidade dos dados.

CVE-2016-0778 Detail			
<h2>Current Description</h2> <p>The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.</p>			
View Analysis Description			
<table><thead><tr><th>Severity</th><th>CVSS Version 3.x</th><th>CVSS Version 2.0</th></tr></thead></table> <p>CVSS 3.x Severity and Metrics:</p> <p> NIST: NVD</p> <p>Base Score: 8.1 HIGH</p> <p>Vector: CVSS:3.0/AV:N/AC:H/PR:N/U:N/S:U/C:H/I:H/A:H</p>	Severity	CVSS Version 3.x	CVSS Version 2.0
Severity	CVSS Version 3.x	CVSS Version 2.0	

Figura 9: Vulnerabilidade referente ao OpenSSH.

- **Microsoft Windows RPC**

A vulnerabilidade mais grave apresenta um *base score* de 7.5 na CVSS versão 3.x e 9.3 na 2.0, ambas com elevado risco. Esta acontece porque existe uma vulnerabilidade de desvio de recurso de segurança no *Microsoft Windows* quando o serviço de Agendamento de Tarefas falha em verificar corretamente as conexões do cliente por RPC. Isto acontece através da rede e apresenta uma complexidade bastante elevada o que dificulta o ataque. No entanto, uma vez conseguido há uma alta probabilidade de perda da confidencialidade, integridade e negação total de acesso aos dados.

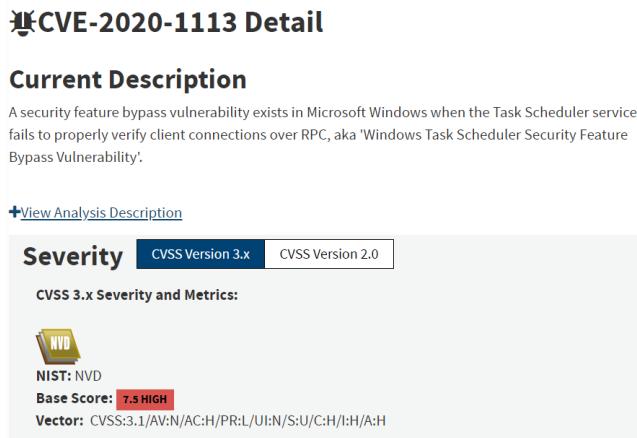


Figura 10: Vulnerabilidade referente ao Microsoft Windows RPC.

- **WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016-11-21))**

A vulnerabilidade encontrada para WEBrick httpd 1.3.1 não é compatível para a versão do Ruby 2.3.3. Portanto, para versões anteriores do *Ruby* (especificadas na imagem abaixo) são gravados dados num ficheiro de *logs*, sem eliminar os caracteres de lixo. Esta situação pode permitir a atacantes remotos: modificar o título de uma janela; executar comando arbitrários; ou substituir ficheiros por meio de um pedido HTTP.

Este ataque, quando executado, põe apenas e parcialmente em risco a confidencialidade dos dados, pelo que tem um *base score* de 5.0 (médio) e um acesso fácil.

CVE-2009-4492 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

WEBrick 1.3.1 in Ruby 1.8.6 through patchlevel 383, 1.8.7 through patchlevel 248, 1.8.8dev, 1.9.1 through patchlevel 376, and 1.9.2dev writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.

[+View Analysis Description](#)

Severity	CVSS Version 3.x	CVSS Version 2.0
CVSS 2.0 Severity and Metrics:		
 NIST: NVD	Base Score: 5.0 MEDIUM	Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Figura 11: Vulnerabilidade referente ao WEBrick httpd.

- **MySQL 5.5.20**

A única vulnerabilidade encontrada para este *software* e respetiva versão diz respeito a um *buffer overflow*, isto permite que atacantes remotos executem código arbitrário através de vetores não especificados. Esta exploração é realizada através da rede e que as condições de ataque são baixas, o que significa que aumenta a probabilidade de sucesso. Sabe-se também que há uma perda parcial da confidencialidade, da integridade e do acesso aos recursos.

CVE-2012-0882 Detail

Current Description

Buffer overflow in yaSSL, as used in MySQL 5.5.20 and possibly other versions including 5.5.x before 5.5.22 and 5.1.x before 5.1.62, allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by VulnDisko Pack Professional 9.17. NOTE: as of 20120224, this disclosure has no actionable information. However, because the module author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes. NOTE: due to lack of details, it is not clear whether this issue is a duplicate of CVE-2012-0492 or another CVE.

[+View Analysis Description](#)

Severity	CVSS Version 3.x	CVSS Version 2.0
CVSS 3.x Severity and Metrics:		
 NIST: NVD	Base Score: N/A	NVD score not yet provided.

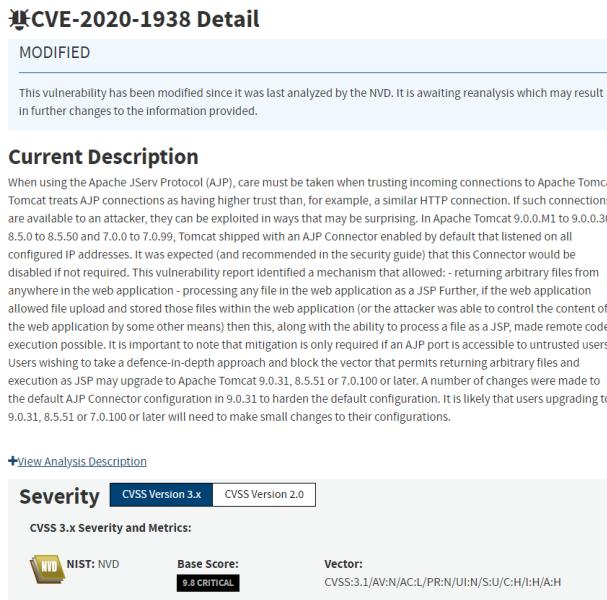
Figura 12: Vulnerabilidade referente ao MySQL.

- **Apache JServ (Protocol v1.3) e Apache Tomcat/Coyote JSP engine 1.1**

A vulnerabilidade estudada não é compatível com as versões e protocolos utilizados, porém permite entender quais os tipos de problemas que podem surgir com a utilização destes *softwares*.

Assim sendo, ao usar o protocolo Apache JServ (AJP) deve ter-se em atenção a confiabilidade nas conexões de entrada para o Apache Tomcat uma vez que este é fornecido com um conector AJP ativo que escuta em todos os endereços IP configurados. Por consequência podem ser retornados ficheiros arbitrários na aplicação *web*, e posteriormente executar código remotamente.

Esta vulnerabilidade é bastante crítica, tendo uma pontuação de 9.8, é realizada através da rede e tem uma complexidade baixa (aumenta a facilidade do ataque). Não obstante, coloca em alto risco os três pilares de segurança: integridade, confidencialidade e disponibilidade.



CVE-2020-1938 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP. Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.

+View Analysis Description

Severity	CVSS Version 3.x	CVSS Version 2.0
CVSS 3.x Severity and Metrics:		
NVD NIST: NVD	Base Score: 9.8 CRITICAL	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Figura 13: Vulnerabilidade referente ao Apache JServ.

- **Sun GlassFish Open Source Edition 4.0**

Para este *software* não foi encontrada uma vulnerabilidade compatível a cem por cento. Portanto, considerou-se interessante especificar a mais grave àcerca do Sun GlassFish, com a pontuação máxima de *base score*, ou seja, 10. No Oracle Sun GlassFish Web Space Server, antes da versão 10.0, atualização 7, patch 2, existem vetores de ataque e um impacto desconhecido na travessia da diretoria, na componente *Liferay*.

Este ataque, com recurso à rede, causa perda completa da integridade, confidencialidade e disponibilidade dos dados.

The screenshot shows the NVD detail page for CVE-2012-1712. The title is "CVE-2012-1712 Detail". Under "Current Description", it states: "Directory traversal vulnerability in the Liferay component in Oracle Sun GlassFish Web Space Server before 10.0 Update 7 Patch 2 has unknown impact and attack vectors." Below this is a link to "View Analysis Description". A "Severity" section contains tabs for "CVSS Version 3.x" (selected) and "CVSS Version 2.0". The CVSS 2.0 section shows a "Base Score: 10.0 HIGH" with a "NIST: NVD" icon. The "Vector" is listed as (AV:N/AC:L/Au:N/C:C/I:C/A:C).

Figura 14: Vulnerabilidade referente ao Sun GlassFish.

- **Apache httpd**

A vulnerabilidade mais grave deste *software* tem pontuação de 9.8, ou seja, está bastante perto do limite da escala e portanto é considerada crítica. São divulgadas informações do servidor Apache HTTP e é possível que haja execução remota de código. Esta é executada através da rede, tem baixa complexidade de ataque, não há privilégios requeridos e ameaça fortemente a integridade, confidencialidade bem como a negação total de acesso aos dados.

The screenshot shows the NVD detail page for CVE-2020-11984. The title is "CVE-2020-11984 Detail". A "MODIFIED" status bar is visible. Below it, a message states: "This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis information provided." Under "Current Description", it says: "Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE". Below this is a link to "View Analysis Description". A "Severity" section contains tabs for "CVSS Version 3.x" (selected) and "CVSS Version 2.0". The CVSS 3.0 section shows a "Base Score: 9.8 CRITICAL" with a "NIST: NVD" icon. The "Vector" is listed as CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

Figura 15: Vulnerabilidade referente ao Apache HTTP.

4.2 Questão 2

Discuta os resultados globais do processo de varredura activa ao Sistema Metasploitable 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.

Com o auxílio da ferramenta Nessus, realizou-se o processo de *scanning* ao sistema da máquina virtual *Metasploitable 3*. Através deste, verificou-se que o sistema apresenta 195 vulnerabilidades.

Destas vulnerabilidades, 8 exibem gravidade crítica, 6 elevada, 34 média, 5 baixa gravidade e 142 fornecem informações, como pode ser inferido pela figura 16.

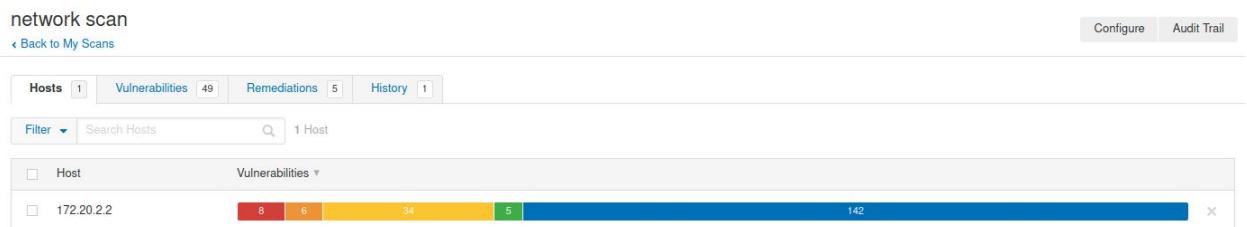


Figura 16: Contagem das vulnerabilidades do Sistema *Metasploitable 3*.

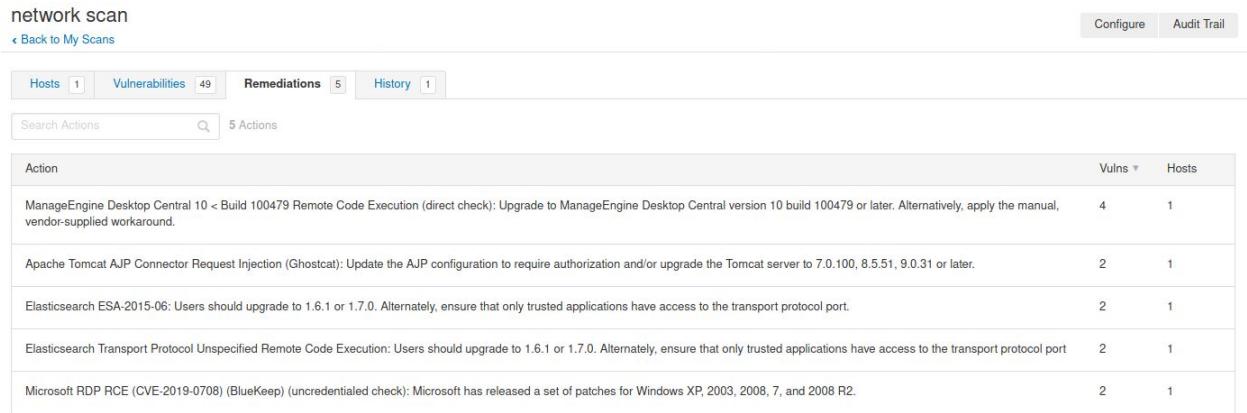
The screenshot shows the Nessus interface with the following details:

- Hosts: 1
- Vulnerabilities: 49
- Remediations: 5
- History: 1

Under the 'Vulnerabilities' tab, a detailed list of findings is displayed:

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

Figura 17: Listagem de algumas vulnerabilidades do Sistema *Metasploitable 3*.



The screenshot shows a network scan interface with the following details:

- Hosts:** 1
- Vulnerabilities:** 49
- Remediations:** 5
- History:** 1

Search Actions: 5 Actions

Action	Vulns	Hosts
ManageEngine Desktop Central 10 < Build 100479 Remote Code Execution (direct check): Upgrade to ManageEngine Desktop Central version 10 build 100479 or later. Alternatively, apply the manual, vendor-supplied workaround.	4	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) (unauthenticated check): Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.	2	1

Figura 18: Remediações do Sistema *Metasploitable 3*.

Comparativamente com os resultados obtidos na questão anterior, no que concerne às vulnerabilidades, podemos concluir que estes apresentam uma especificidade maior, pois são mais concretos e objetivos em relação à máquina virtual.

Na questão 1, as vulnerabilidades estudadas eram mais abrangentes e não se relacionavam diretamente com as versões e protocolos utilizados nos *softwares*. Apesar de se considerar que as questões se completam, é seguro afirmar que é mais fiável recorrer a uma ferramenta deste tipo.

4.3 Questão 3

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

Examinando o output do IDS Suricata verifica-se que existem bastantes entradas no ficheiro `eve.json`. De modo a encontrar eventos identificados como anómalos, usou-se a ferramenta "jq", que é recomendada na documentação do Suricata, e executou-se o comando `sudo cat /var/log/suricata/eve.json | jq 'select(.event_type=="alert")' > alertas.json`. Neste IDS, todo o tráfego anómalo que tenha correspondência com uma regra, gera um alerta.

Depois de se obter o ficheiro com todos os alertas gerados durante o *scan network* do Nessus, escolhem-se dois e através do *timestamp* encontra-se o pacote correspondente no Wireshark.

4.3.1 Heartbleed exploit

O primeiro alerta corresponde a uma tentativa de um *exploit* chamado *heartbleed* que consiste num *buffer overflow*, com o intuito de se obter informações privilegiadas. Deste modo, os autores consideram que o IDS detecta este tipo de ataque verificando o tamanho da mensagem, sendo este menor do que o *payload* do pacote. Nas versões OpenSSL vulneráveis tal não acontece, pois não é verificado o tamanho do *payload*.

```
[{"timestamp": "2020-12-26T10:51:38.219410-0500",
 "flow_id": 998858465878038,
 "in_iface": "eth0",
 "event_type": "alert",
 "src_ip": "172.20.2.2",
 "src_port": 8383,
 "dest_ip": "172.20.2.1",
 "dest_port": 59590,
 "proto": "TCP",
 "metadata": {
   "flowbits": [
     "ET.MalformedTLSHB",
     "ET.HB.Request.CI"
   ],
   "flowints": {
     "tls.anomaly.count": 1
   }
 },
 "tx_id": 0,
 "alert": {
   "action": "allowed",
   "gid": 1,
   "signature_id": 2230012,
   "rev": 1,
   "signature": "SURICATA TLS overflow heartbeat encountered, possible exploit attempt (heartbleed)",
   "category": "Generic Protocol Command Decode",
   "severity": 3
 }]
```

Figura 19: Anomalia *Heartbleed*.

```

"tls": {
    "subject": "C=US, ST=CA, L=Pleasanton, O=Zoho Corporation, OU=ManageEngine, CN=Desktop Central, Email=support@desktopcentral.com",
    "issuerdn": "C=US, ST=CA, L=Pleasanton, O=Zoho Corporation, OU=ManageEngine, CN=Desktop Central, Email=support@desktopcentral.com",
    "serial": "00:F5:9C:EF:71:E6:D8:72:A5",
    "fingerprint": "70:1e:2e:6d:f8:85:4c:4f:0b:29:8d:ff:03:a2:c6:f0:ba:c7:d3:15",
    "version": "TLS 1.2",
    "notbefore": "2010-09-08T12:24:44",
    "notafter": "2020-09-05T12:24:44",
    "ja3": {
        "hash": "494aba099c9f76a41d81968f2c00ff3b",
        "string": "771,29-28-65279-65504-65278-65505-162-163-49280-49281-49318-170-49319-171-49302-49296-49303-49297-52397-49310-49314-158
    },
    "ja3s": {
        "hash": "21f8297254a9f09a81eb8480cc1b7d8a",
        "string": "771,49200,11-15"
    }
},
"app_proto": "tls",
"flow": [
    {
        "pkts_toserver": 6,
        "pkts_toclient": 3,
        "bytes_toserver": 1197,
        "bytes_toclient": 1507,
        "start": "2020-12-26T10:51:38.008214-0500"
    }
]
}

```

Figura 20: Continuação da anomalia *Heartbleed*.

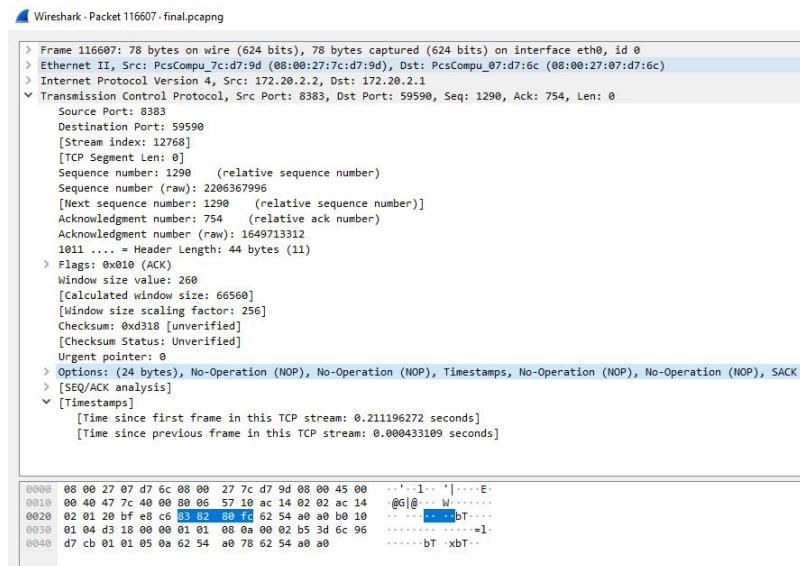


Figura 21: Wireshark da anomalia *Heartbleed*.

4.3.2 GhostCat LFI Attempt Inbound

O segundo alerta diz respeito a uma tentativa de ganho de privilégios administrativos, em que o alvo é o servidor *Apache Tomcat*. A vulnerabilidade está identificada com o **CVE-2020-1938** e está classificada com grande severidade, visto que permite ao atacante executar código remotamente além do acesso a páginas *web* do servidor.

Deste modo, os autores acreditam que o Suricata classifica este evento como anómalo porque reconhece a assinatura do mesmo, visto que retorna o código CVE correspondente.

```
"timestamp": "2020-12-26T10:53:50.322134-0500",
"flow_id": 514935919399914,
"in_iface": "eth0",
"event_type": "alert",
"src_ip": "172.20.2.1",
"src_port": 60620,
"dest_ip": "172.20.2.2",
"dest_port": 8009,
"proto": "TCP",
"alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2029533,
    "rev": 2,
    "signature": "ET EXPLOIT [401TRG] GhostCat LFI Attempt Inbound (CVE-2020-1938)",
    "category": "Attempted Administrator Privilege Gain",
    "severity": 1,
    "metadata": {
        "affected_product": [
            "Apache_Tomcat"
        ],
        "attack_target": [
            "Web_Server"
        ],
        "created_at": [
            "2020_02_25"
        ],
        "deployment": [
            "Perimeter"
        ],
        "former_category": [
            "EXPLOIT"
        ],
        "signature_severity": [
            "Major"
        ],
        "updated_at": [
            "2020_02_25"
        ]
    }
}
```

Figura 22: Anomalia *GhostCat LFI*.

```
},
"flow": {
    "pkts_toserver": 3,
    "pkts_toclient": 1,
    "bytes_toserver": 604,
    "bytes_toclient": 74,
    "start": "2020-12-26T10:53:50.316394-0500"
}
```

Figura 23: Continuação da anomalia *GhostCat LFI*.

```

> Frame 138316: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits) on interface eth0, id 0
> Ethernet II, Src: PcsCompu_07:d7:6c (08:00:27:07:d7:6c), Dst: PcsCompu_7c:d7:9d (08:00:27:7c:d7:9d)
> Internet Protocol Version 4, Src: 172.20.2.1, Dst: 172.20.2.2
> Transmission Control Protocol, Src Port: 60620, Dst Port: 8009, Seq: 1, Ack: 1, Len: 398
  ▾ Apache Jserv Protocol v1.3
    Magic: 1234
    Length: 394
    Code: FORWARD REQUEST (2)
    Method: GET (2)
    Version: HTTP/1.1
    URI: /asdf/xxxxx.jsp
    RADDR: localhost
    RHOST:
    SRV: localhost
    PORT: 80
    SSLP: False
    NHDR: 9
    keep-alive
    Accept-Language: en-US,en;q=0.5
    0
    Accept-Encoding: gzip, deflate, sdch
    Cache-Control: max-age=0
    Mozilla
    Upgrade-Insecure-Requests: 1
    text/html
    localhost
    0000  08 00 27 7c d7 9d 08 00  27 07 d7 6c 08 00 45 00  ...|....'..1..E...
    0010  01 c5 cc cc 40 00 40 06  10 3e ac 14 02 01 ac 14  ..@. @. >.....
    0020  02 02 ec cc 1f 49 82 e1  d6 0d f7 71 ba f1 80 18  ..I. ....q....
    0030  01 f6 5d e0 00 00 01 01  08 0a 6c 98 dc 9f 00 02  .].....1.....
    0040  e8 d0 12 34 01 8a 02 02  00 08 48 54 54 50 2f 31  ..4.....HTTP/1
    0050  2e 31 00 00 0f 2f 61 73  64 66 2f 78 78 78 78 78  .1.../as df/xxxxx
    0060  2e 6a 73 70 00 00 00 6c  6f 63 61 6c 68 6f 73 74  .jsp..l ocalhost
    0070  00 ff ff 00 09 6c 6f 63  61 6c 68 6f 73 74 00 00  ....loc alhost..
    0080  50 00 00 09 a0 06 00 0a  6b 65 65 70 2d 61 6c 69  P.....keep-all
    0090  76 65 00 00 0f 41 63 63  65 70 75 2d 4c 61 6e 67  ve..Acc ept-Lang
    00a0  75 61 67 65 00 00 00 65  6e 2d 55 53 2c 65 6e 3b  usage..e n-US,en;
    00b0  71 3d 30 2e 35 00 a0 08  00 01 30 00 00 0f 41 63  q0.5....0..Ac
    00c0  63 65 70 74 2d 45 60 63  0f 64 69 6e 67 00 13  cept-Enc oding...
    00d0  67 7a 69 70 2c 20 64 65  66 6c 61 74 65 20 73  gzip, de flate, s
    00e0  64 63 68 00 00 0d 43 61  63 68 65 2d 43 6f 6e 74  dch..Ca che-Cont
    00f0  72 6f 6c 00 00 09 6d 61  78 2d 61 67 65 3d 30 00  rol..ma x-age=0
    0100  a0 0e 00 00 0f 6f 72 6c  5c 6c 61 00 00 15 55 70  ....Mozil lla..Up
    0110  67 72 61 64 65 2d 49 6e  73 65 63 75 72 65 2d 52  grade-In secur-R
    0120  65 71 75 65 73 74 73 00  00 01 31 00 a0 01 00 09  equests..I.....

```

Figura 24: Wireshark anomalia *GhostCat LFI*.

4.4 Questão 4

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.

Os IDS (Sistemas de Deteção de Intrusão) tem como função principal servir como uma segunda linha de defesa à invasão de atacantes, detetando atividades de risco numa rede ou *host*. Para conseguir combater os ataques, os IDS tentam impedir este tipo de atividades maliciosas (bloqueando sessões, p.e.) ou reportando os administradores através de notificações.

Estas notificações na sua maioria fazem-se acompanhar da vulnerabilidade que a atividade pode causar, para tal a ferramenta de *scan* observa pacotes de tráfego de rede e gera um alerta se este se enquadrar com aquilo que alberga na sua base de conhecimento.

Posto isto, põe-se a hipótese que as notificações que não possuem vulnerabilidades, digam respeito a pacotes iniciais de estabelecimento de ligação à rede, por exemplo pacotes de *request* e *reply*.

Este tipo de alertas são igualmente importantes, na medida que podem prevenir um possível ataque uma vez que através do tráfego da rede detetam sempre que alguém tenta estabelecer ligação ao sistema.

4.5 Questão 5

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.

4.5.1 ManageEngine Desktop Central 10 < Build 100479 Remote Code Execution (direct check)

The screenshot shows the Nessus interface for a network scan. The title bar says "network scan / Plugin #135293" and "Back to Vulnerability Group". Below the title, there are tabs for "Hosts" (1), "Vulnerabilities" (49), "Remediations" (5), and "History" (1). The "Vulnerabilities" tab is selected. A red box highlights the first entry: "ManageEngine Desktop Central 10 < Build 100479 Remote Code Execution (direct check)". This entry is labeled "CRITICAL". The "Description" section states: "The ManageEngine Desktop Central application running on the remote host is version 10 prior to build 100479. It is, therefore, affected by a remote code execution vulnerability." The "Solution" section suggests upgrading to version 10 build 100479 or later, or applying a vendor-supplied workaround. The "See Also" section lists three URLs. The "Output" section shows the exploit request: "Nessus was able to exploit the issue using the following request :
GET /cewolf/?img=%5Clogger.zip HTTP/1.1
Host: 172.20.2.2:8022
Accept: */*
Accept-Language: en
Connection: Close
Cookie: DCJSESSIONID=A7EC7005CEA1751B27D596794B84C35B
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
more...". At the bottom, there are "Port" and "Hosts" filters, with "8022 /tcp /www" and "172.20.2.2" selected.

Figura 25: Vulnerabilidade 1 - *High/Critical*.

A vulnerabilidade escolhida como *High/Critical* é referente à aplicação *Desktop ManageEngine* versão 10, que é afetada por uma vulnerabilidade de execução de código remoto. A vulnerabilidade foi identificada com o código **CVE-2020-10189** e, depois de procurar na documentação, encontrou-se uma solução que envolvia alterar o ficheiro `web.xml` na diretoria `"/ManageEngine/DesktopCentral_Server/webapps/DesktopCentral/WEB-INF/"`.

Após alterado o ficheiro `web.xml` reiniciou-se o *ManageEngine* e correu-se de novo um *network scan* no *Nessus* e como se pode ver na próxima imagem, a vulnerabilidade

desaparece e apenas aparecem outras vulnerabilidades do *software*. Isto acontece devido à alteração do ficheiro, o que impossibilita a execução de código remoto, ponto fulcral e que era a origem da vulnerabilidade.

Sev	Name
CRITICAL	ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE
MEDIUM	ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities
INFO	ManageEngine Desktop Central Detection

Figura 26: Confirmação da resolução de uma vulnerabilidade 1 (*High/Critical*).

4.5.2 SMB Signing not required

Description
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

- <https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing>
- <http://technet.microsoft.com/en-us/library/cc731957.aspx>
- <http://www.nessus.org/u?74b80723>
- <https://www.samba.org/docs/current/man-html/smb.conf.5.html>
- <http://www.nessus.org/u?a3cac4ea>

Figura 27: Vulnerabilidade 2 - *Medium*.

A vulnerabilidade escolhida como *Medium* foi a que afeta o servidor SMB. Visto que não é necessária autenticação, um atacante remoto pode usar isto para realizar ataques do tipo *Man in the midle* contra o servidor SMB e roubar ou alterar informações. A solução para esta vulnerabilidade, tal como é sugerida, é obrigar a que todas as conexões com o servidor tenham autenticação, neste modo, o servidor sabe que está a falar com um cliente e não com um possível atacante.

A resolução da vulnerabilidade pode ser vista na seguinte imagem. Após essa configuração, reiniciou-se o serviço e correu-se um *basic network scan* no *Nessus*, o resultado foi o expectável e a vulnerabilidade desapareceu.

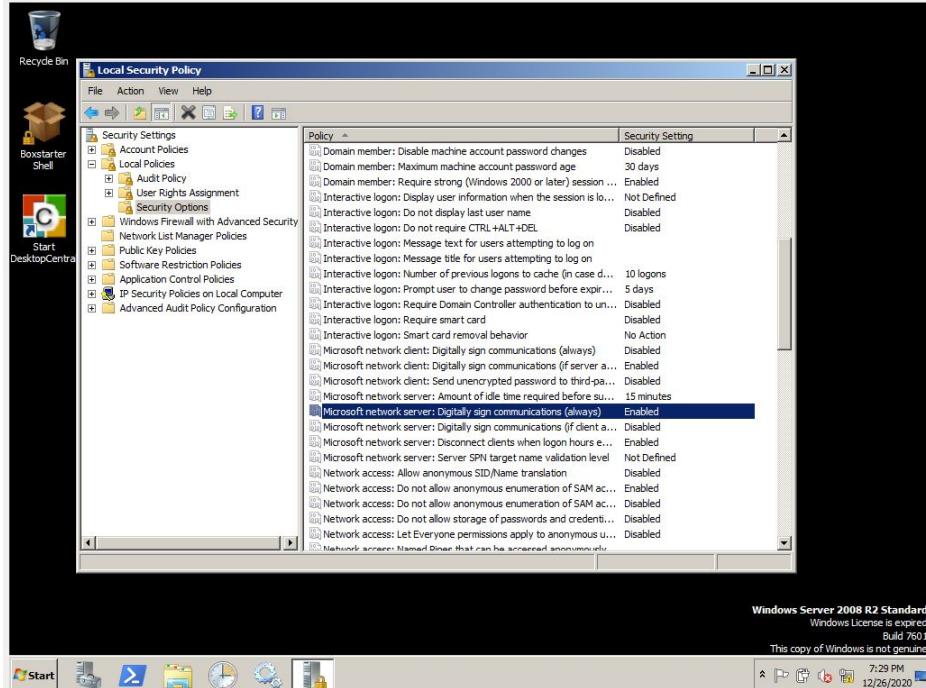


Figura 28: Resolução de uma vulnerabilidade 2 (*Medium*).

4.5.3 Terminal Services Doesn't Use Network Level Authentication (NLA) Only

network scan / Plugin #58453
[Back to Vulnerability Group](#)

Hosts	1	Vulnerabilities	49	Remediations	5	History	10
-----------------------	---	---------------------------------	----	------------------------------	---	-------------------------	----

MEDIUM Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Description
The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

Solution
Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

See Also
[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11))
<http://www.nessus.org/u?e2628096>

Figura 29: Vulnerabilidade 3 - *Medium*.

A última vulnerabilidade selecionada foi a que envolve os serviços remotos do terminal não usarem autenticação, ao nível da rede. Esta autenticação ao nível da rede usa TLS/SSL, o que leva a uma maior proteção contra ataques *Man in the middle*. Além disto, também protege contra ataques remotos de *malware*.

A solução para esta vulnerabilidade passa por possibilitar a *Network Level Authentication (NLA)* nas *system settings* do Windows e, de seguida, na *remote tab*, como pode ser verificado na figura 30. Depois de corrigir a vulnerabilidade, reiniciou-se o *Metasploitable* e verificou-se a inexistência da vulnerabilidade.

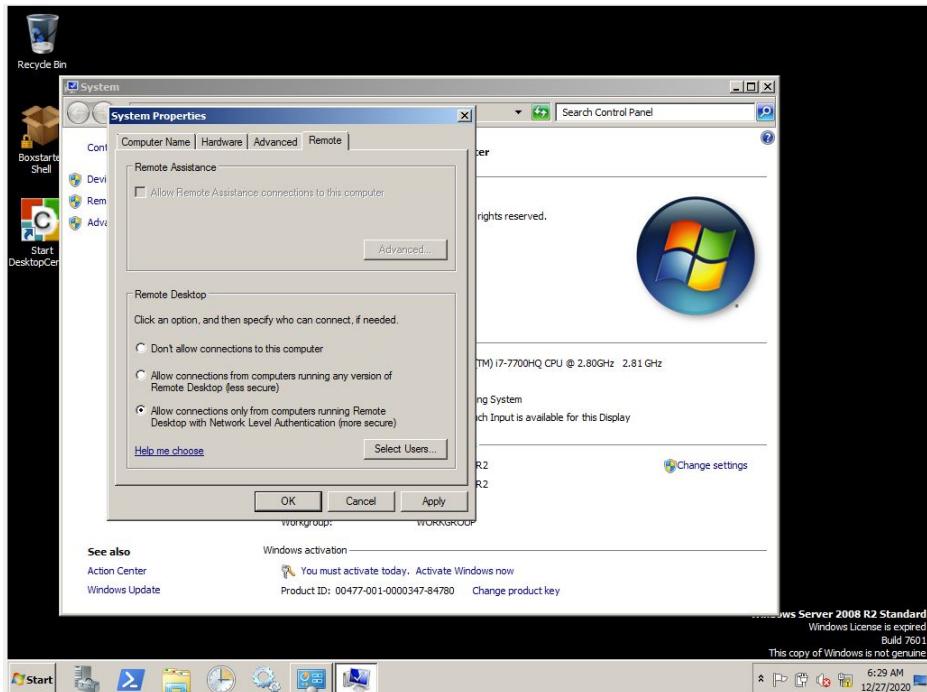


Figura 30: Resolução de uma vulnerabilidade 3 (*Medium*).

Os resultados da questão 5 podem ser consultados nos ficheiros `1st_network_scan.pdf` (antes) e `Last_network_scan.pdf` (depois), onde que se pode comprovar que as vulnerabilidades desaparecem depois das correções efetuadas. Estes ficheiros encontram-se na pasta de envio do projeto.

5 Conclusão

O *footprinting* é a técnica usada para adquirir informações sobre os sistemas de computadores e as entidades às quais estes pertencem. Pode considerar-se como a fase inicial quando um atacante planeia uma invasão, sendo que de forma passiva e ativa são reunidas o maior número de informações possíveis sobre o alvo.

Neste projeto prático, iniciou-se essa reunião de informações pela vertente passiva, sendo que se analisou ao detalhe dois *websites* por forma a obter endereços de email, dados sobre funcionários das empresas, linguagens utilizadas na sua criação, entre outros. Após concluída esta fase, seguiu-se uma recolha ativa, que visa a responder a uma série de questões recorrendo a um *scanner* de vulnerabilidades, a um Sistema de Detecção de Intrusão, e ainda um analisador de tráfego.

O grupo sentiu algumas dificuldades na instalação do IDS Snort, pelo que optou pelo Suricata para conseguir obter os alertas necessários para dar resposta às questões. Neste sentido, considerou-se este trabalho complexo e que requereu uma grande pesquisa por parte dos elementos do grupo, para serem atingidos os objetivos propostos.

Em suma, os autores compreenderam os conceitos chave deste trabalho prático e consideram terem atingido um nível satisfatório no que toca ao seu aproveitamento global.