Tecnologias de Segurança
Trabalho Prático 1

Duarte Oliveira, Melânia Pereira e Paulo R. Pereira
{pg47157, pg47520, pg47554}@alunos.uminho.pt
Grupo 16

27 de março de 2022

1 Perguntas e Respostas

Parte A: Escolha duas empresas com operação comercial suportada por serviços on-line (uma grande corporação e um negócio local) e utilize técnicas de busca passiva de informação que permitam identificar detalhes sobre os seus sistemas e infra-estrutura. Descreva as estratégias usadas, os resultados obtidos e as possíveis diferenças de postura adoptadas pelos administradores dos domínios estudados. Forneça uma análise crítica sobre os riscos associados às práticas identificadas. Enriqueça a sua análise apontando estratégias destinadas a fortalecer a postura de segurança destes domínios, especificamente, como resposta às técnicas e ferramentas de busca passiva.

Resposta: As empresas escolhidas para esta parte do trabalho foram a *Farfetch* - uma grande corporação - e o jornal MAIS/Semanário - um negócio local em Póvoa de Varzim.
Começou por se usar a ferramenta `whois` para descobrir informações sobre os domínios em questão. Pode verificar-se uma grande diferença entre os serviços *online* dos dois negócios, como seria de esperar, todas as informações para o domínio *farfetch.com* encontram-se privadas enquanto que para o domínio *maissemanario.pt* já foi possível adquirir alguma informação, como a data de criação e de "validade"do domínio, o nome do dono do domínio e a sua morada e email e, ainda, o nome do administrador do domínio, a sua morada e também o seu email. Neste último é ainda possível encontrar os *name server*'s disponíveis e respetivos IP's.
Percebe-se, com esta diferença, que a postura dos administradores dos domínios é muito mais relaxada quando se trata de um negócio mais "pequeno"e que não se baseia apenas no serviço *online* como é o caso da *Farfetch*, o que é normal pois é necessário perceber um equilíbrio para investir em coisas que não são tão necessárias, no caso da *Farfetch* a segurança e privacidade do serviço *online* e do domínio são essenciais e investir nisso é algo extremamente necessário, no entanto, para o jornal MAIS/Semanário não se justifica um investimento em segurança e privacidade tão grande.

```
Domain Name: FARFETCH.COM
Registry Domain ID: 98487148_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2017-09-20T17:10:14Z
Creation Date: 2003-05-29T00:20:35Z
Registrar Registration Expiration Date: 2026-05-29T00:20:35Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibit
ed
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US
Registrant Phone: +1.5707088622
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: x799z32u5pj@networksolutionsprivateregistration.com
Registry Admin ID:
Admin Name: PERFECT PRIVACY, LLC
Admin Organization:
Admin Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Admin City: Jacksonville
Admin State/Province: FL
Admin Postal Code: 32256
Admin Country: US
Admin Phone: +1.5707088622
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: x799z32u5pj@networksolutionsprivateregistration.com
Registry Tech ID:
Tech Name: PERFECT PRIVACY, LLC
Tech Organization:
Tech Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Tech City: Jacksonville
Tech State/Province: FL
Tech Postal Code: 32256
Tech Country: US
Tech Phone: +1.5707088622
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: x799z32u5pj@networksolutionsprivateregistration.com
Name Server: NS0.DNSMADEEASY.COM
Name Server: NS1.DNSMADEEASY.COM
Name Server: NS2.DNSMADEEASY.COM
Name Server: NS3.DNSMADEEASY.COM
Name Server: NS4.DNSMADEEASY.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: domain.operations@web.com
Registrar Abuse Contact Phone: +1.8777228662
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
```

Figura 1: Resultado da pesquisa com 'whois' para *farfetch.com*

```
# whois.dns.pt

Domain: maissemanario.pt
Domain Status: Registered
Creation Date: 22/06/2012 10:33:19
Expiration Date: 21/06/2022 23:59:19
Owner Name: ILUSTREPÁGINA  UNIPESSOAL LDA
Owner Address: Praça do Almada, nº 10, 1º, Póvoa de Varzim
Owner Locality: Póvoa de Varzim
Owner ZipCode: 4490-438
Owner Locality ZipCode: Póvoa de Varzim
Owner Country Code: PT
Owner Email: multimedia@maissemanario.pt,maissemanario@gmail.com
Admin Name: AMENWORLD Serviços Internet - Sociedade Unipessoal Lda
Admin Address: Rua do Pólo Sul   Nº 2 - 3ºB-1 - Parque Expo
Admin Locality: Lisboa
Admin ZipCode: 1990-273
Admin Locality ZipCode: LISBOA
Admin Country Code: PT
Admin Email: dominios@amen.pt,mailmanager@registryamen.com.pt
Name Server: ns2.solucoesdigitais.com.pt | IPv4: 85.234.159.44 and IPv6:
Name Server: ns1.solucoesdigitais.com.pt | IPv4: 151.236.39.213 and IPv6:
```

Figura 2: Resultado da pesquisa com 'whois' para *maissemanario.pt*

Em contrapartida, o facto de não haver uma segurança tão grande nesses domínios permite a que muita informação possa ser encontrada muito facilmente e, mesmo que isso não seja um problema para o negócio em si, pode tornar-se um problema a nível pessoal para quem está à frente do negócio. Muitas informações sobre uma pessoa podem ser encontradas *online* e, às vezes, com apenas alguma pesquisa torna-se possível conhecer muitas rotinas e informações íntimas sobre alguém. Isto pode ser uma enorme violação à privacidade das pessoas e, no entanto, tudo está público e pode ser acedido por qualquer pessoa no mundo. Além disto, há muitos ataques que se tornam possíveis com a informação recolhida, por exemplo um ataque de negação de serviço, depois de saber quais os IP's e *name server*'s onde o domínio está alojado.

Parte B: Para esta parte do trabalho prático, certifique-se que tem o ambiente de testes instalado e configurado de acordo com as instruções da Secção 5 deste enunciado. Todas as tarefas listadas nesta parte do trabalho deverão usar ferramentas de varredura activa instaladas no Sistema Auditor e terá como alvo, apenas, o Sistema Mestasploitable 3.

Q1: 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

Resposta: Para esta varredura, decidimos usar a ferramenta `nmap`, que nos permite fazer um *scan* a uma máquina alvo e obter informações que podem ajudar a identificar vulnerabilidades. Com o comando `nmap` conseguimos então descobrir quais as portas vulneráveis no Sistema Metasploitable 3, como podemos ver na imagem:

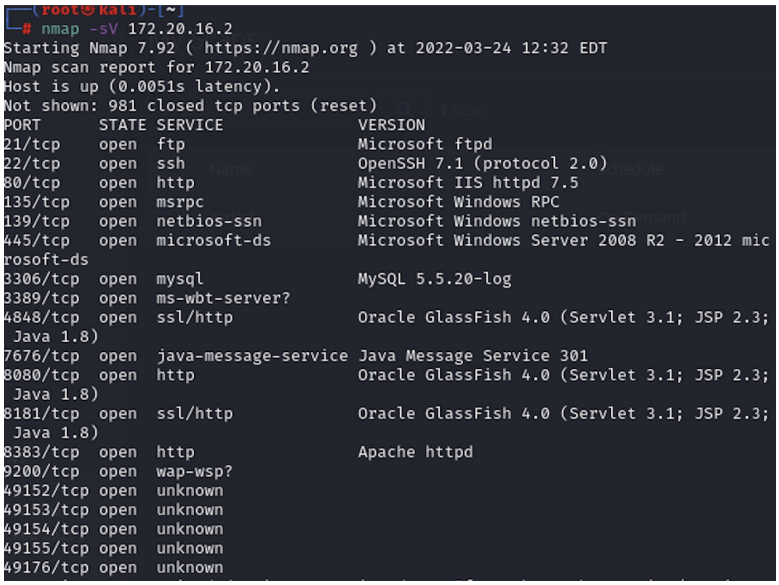


Figura 3: Resultado do comando *nmap -sV 172.20.16.2*

Podemos notar que, para além das portas, obtemos ainda informação sobre quais são os serviços que estão a correr em cada uma dessas portas (isto é conseguido com a flag -sV).
Passamos então a listar os serviços encontrados e quais as vulnerabilidades associadas a cada um.

- **Oracle GlassFish 4.0** – nas portas 4848, 8080, 8181

  Este serviço tem uma vulnerabilidade conhecida - CVE-2011-0807 - que permita atacantes remotos de afetar a confidencialidade, integridade e disponibilidade através de vetores de ataque desconhecidos relacionados com Administração.

- **Microsoft IIS httpd 7.5** – na porta 80

  A vulnerabilidade encontrada para o IIS (CVE-2015-1635) foi a *HTTP.sys Remote Code Execution Vulnerability*, que, nas versões 7 SP11, Server 2008 R2 SP1, 8, 8.1 e Server 2012 Gold e R2 do Windows permite a atacantes remotos a execução de código arbitrário através de pedidos HTTP criados.

- **Microsoft ftpd** – na porta 21

  No serviço ftpd, o comando CWD root permite acesso de *root* sem ser necessária qualquer autenticação. É uma vulnerabilidade muito perigosa e que dá completo acesso ao sistema a qualquer pessoa. (CVE-1999-0082)

- **OpenSSH 7.1 (protocol 2.0)** – na porta 22

  Uma das vulnerabilidades deste serviço (CVE-2017-15906) é que a função `process_open` em `sftp.server.c` não previne corretamente operações de escrita em modo de leitura, permitindo aos atacantes criar ficheiros de tamanho 0.

- **Microsoft Windows RPC** – na porta 135

Este serviço com *routing* e acesso remoto permite a um atacante executar código num servidor RPC alvo que tem *routing* e acesso remoto ativo através de uma aplicação especialmente desenvolvida. Esta vulnerabilidade (CVE-2017-8461) é conhecida por "*Windows RPC Remote Code Execution Vulnerability*"

- **Microsoft Windows netbios-ssn** – na porta 139

  Windows NetBIOS Denial of Service Vulnerability é uma vulnerabilidade (CVE-2017-0174) que permite um ataque de negação de serviço quando trata pacotes NetBios de forma incorreta.

- **Microsoft Windows Server 2008 R2 - 2012 microsoft-ds** – na porta 445

  A configuração *default* do Microsoft Windows usa o *Web Proxy Autodiscovery Protocol* (WPAD) sem entradas estáticas, o que pode permitir atacantes remotos a intercetar tráfego*web* ao registar um servidor *proxy* usando WINS ou DNS e, depois, responder a pedidos WPAD. Esta vulnerabilidade tem o CVE-2007-1692.

- **MySQL 5.5.20-log** – na porta 3306

  Um *buffer overflow* no Oracle MySQL e na MariaDB em versões anteriores à 5.5.35 permitem que servidores da base de dados remotos causem uma negação de serviço (*crash*) e ainda, possivelmente, que possam executar código arbitrário através de uma cadeia longa de versão do servidor (CVE-2014-0001).

- **Apache httpd** – na porta 8383

  Um corpo de pedido cuidadosamente criado pode causar um *buffer overflow* no *parser multipart* `mod_lua` (`r:parsebody()` chamado desde *scripts* Lua) - CVE-2021-44790.

Conseguimos ainda saber com pormenor qual é o sistema operativo da máquina alvo, através da flag *-O*, assim como a distância na rede a que nos encontramos da máquina e ainda o tipo de dispositivo e o seu *MAC Adress*:

```
┌──(root㉿kali)-[~]
└─# nmap -O 172.20.16.2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-24 12:46 EDT
Nmap scan report for 172.20.16.2
Host is up (0.00034s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49176/tcp open  unknown
MAC Address: 08:00:27:27:45:2D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.45 seconds
```

Figura 4: Resultado do comando *nmap -O 172.20.16.2*

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.

Resposta: Os resultados da varredura ativa ao Sistema Metasploitable 3 com a ferramenta *Nessus* foram muito completos e detalhados, deu para perceber que estamos perante um sistema com imensas falhas de segurança, as quais podem ser facilmente exploradas. Em relação à pesquisa feita na questão anterior, é fácil perceber que a varredura automática é muito mais completa e eficiente, começando pelo facto de que para a questão 1 foi necessário ter um trabalho intenso de pesquisa para perceber as vulnerabilidades às quais cada serviço está sujeito e, mesmo assim, no fim concordamos que se trata de uma avaliação "pobre"das falhas de segurança do sistema, comparando com os resultados obtidos no sistema automático de identificação de vulnerabilidades.

Q3: 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.

Resposta: Como resultado do IDS escolhido (*snort*) foram obtidos os seguintes alertas[1]:

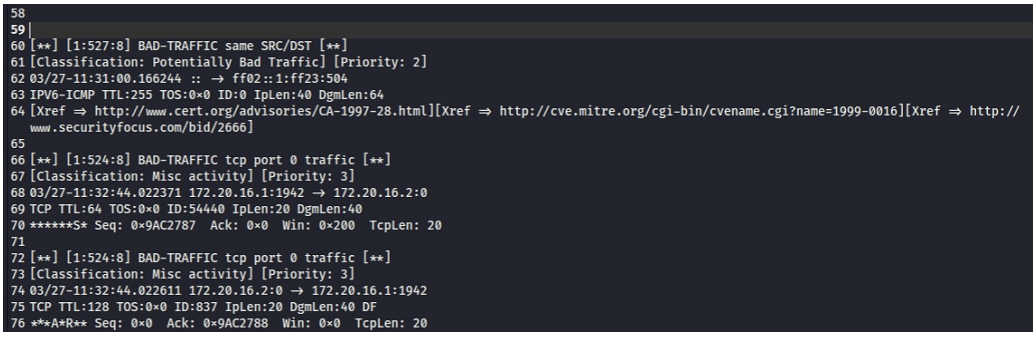


Figura 5: Alertas dadas pelo *snort*

Os eventos escolhidos são os primeiros dois da imagem acima e mostramos, de seguida, o tráfego capturado no *wireshark* para cada um deles.

[1]**NOTA**: mesmo depois de muitas tentativas de perceber o porquê e de muita pesquisa e reconfiguração do *snort*, não conseguimos obter muitos resultados. Como se pode notar, em cada *scan*, apenas eram gerados estes alertas, o que consideramos estranho sendo que no *scanner* é possível encontrar muitas vulnerabilidades. Assim, temos noção que algo de errado aconteceu e que deveríamos ter tido mais alertas.

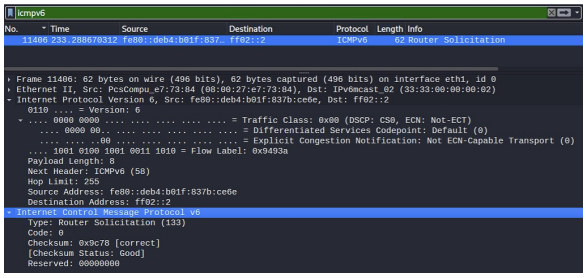


Figura 6: Pacote correspondente ao primeiro alerta escolhido

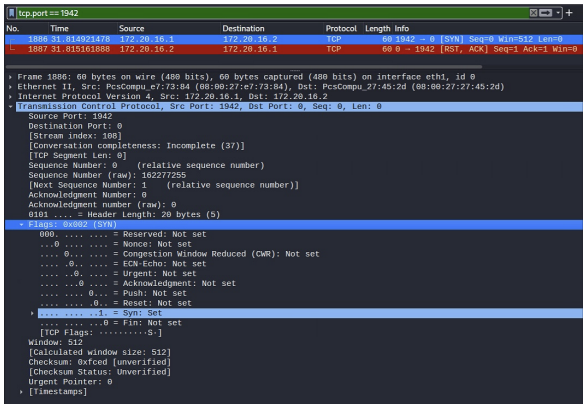


Figura 7: Pacote correspondente ao segundo alerta escolhido

Na primeira imagem, temos um alerta de tráfego potencialmente anómalo que é indicado no *wireshark* como uma solicitação do *router*. Seguindo o *link* do CVE indicado no alerta: `http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0016`, somos levados à página de descrição da vulnerabilidade associada a este alerta, que nos indica que se trata de uma negação de serviço, como podemos ver na imagem seguinte.

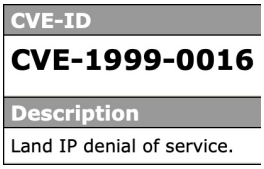


Figura 8: Descrição do CVE para o alerta

Na segunda imagem, vemos um alerta para tráfego na porta TCP 0, que é uma porta reservada e que deve estar fora de serviço, portanto, tentativas de tráfego para esta porta devem, claramente, ser suspeitas.

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.

Resposta: No *snort* podemos ver um alerta para uma vulnerabilidade a um ataque de negação de serviço, vulnerabilidade essa que não encontramos nos resultados do *Nessus*. Depois de alguma pesquisa, percebemos que isto se deve ao facto de que o *Nessus* é uma ferramenta que faz interação com o sistema alvo para detetar aspetos que possam ser uma vulnerabilidade, como o *snort* é uma ferramenta que está à espreita dos pacotes da rede e os analisa, é possível que este detete uma situação anómala que pelo *Nessus* não seja percebida como um risco de ataque.

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.

Resposta: Apresentamos de seguida as três vulnerabilidades escolhidas e, depois de cada uma, uma breve explicação dos procedimentos efetuados para a sua correção.
Começamos pela vulnerabilidade **41028 - SNMP Agent Default Community Name (public)**.

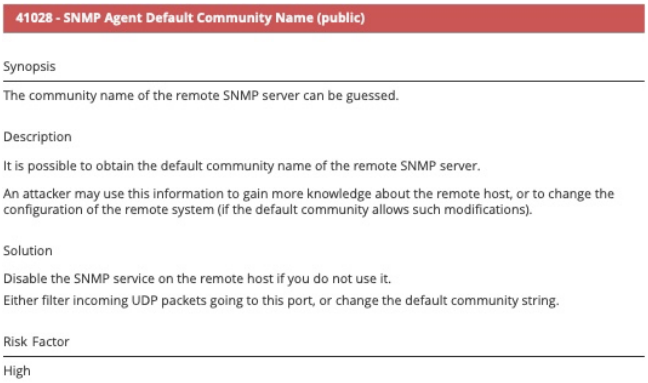


Figura 9: Detalhes da vulnerabilidade 41028

Tal como detalhado na imagem acima, a solução para esta vulnerabilidade passa por desativar o serviço SNMP no caso de este não ser usado, então, depois de alguma pesquisa, efetuamos esse procedimento.

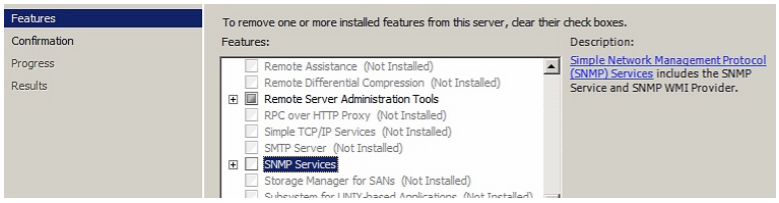


Figura 10: Desativação da *feature* SNMP Services no *server manager* do dispositivo

Passamos então para a vulnerabilidade **18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness**.

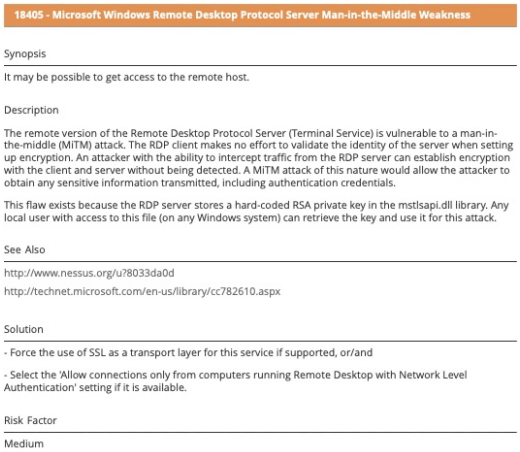


Figura 11: Detalhes da vulnerabilidade 18405

Mais uma vez, depois de alguma pesquisa e tendo em conta a solução recomendada no relatório do *Nessus*, decidimos selecionar a definição especificada neste último, como se mostra a seguir.

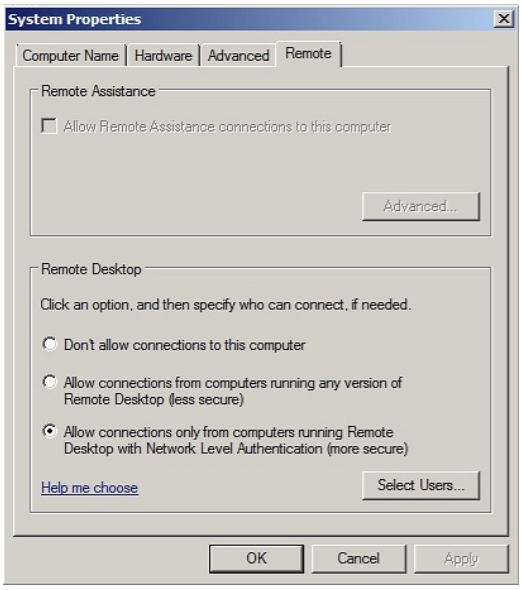


Figura 12: Seleção da opção que permite conexões remotas apenas a computadores que correm o *Remote Desktop* com *Network Level Authentication*

Finalmente, a vulnerabilidade **57608 - SMB Signing not required**.

Figura 13: Detalhes da vulnerabilidade 57608

Para corrigir esta vulnerabilidade, efetuamos mais uma vez alguma pesquisa e tivemos em conta a solução dada pelo Nessus. Procedemos então à imposição de assinatura de mensagens.

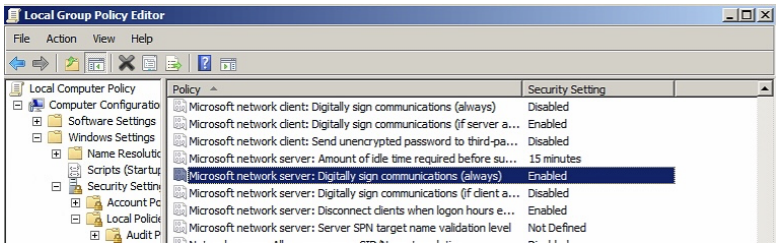
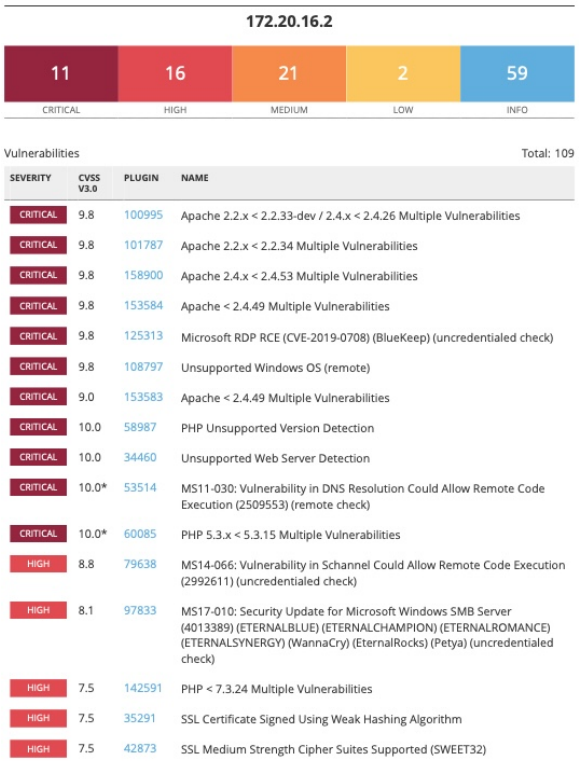


Figura 14: Ativação da política de assinatura digital de comunicações sempre

Depois destas alterações, procedemos então a uma nova varredura do Sistema Metasploitable 3. Varredura essa que, como seria de esperar, apresenta menos vulnerabilidades e nas quais

não está presente nenhuma das referidas acima. Com isto, concluímos que que as soluções que aplicamos foram efetivas e que a pesquisa efetuada foi correta.
Apresentamos de seguida imagens de parte do resultado da varredura antes e depois das correções efetuadas.



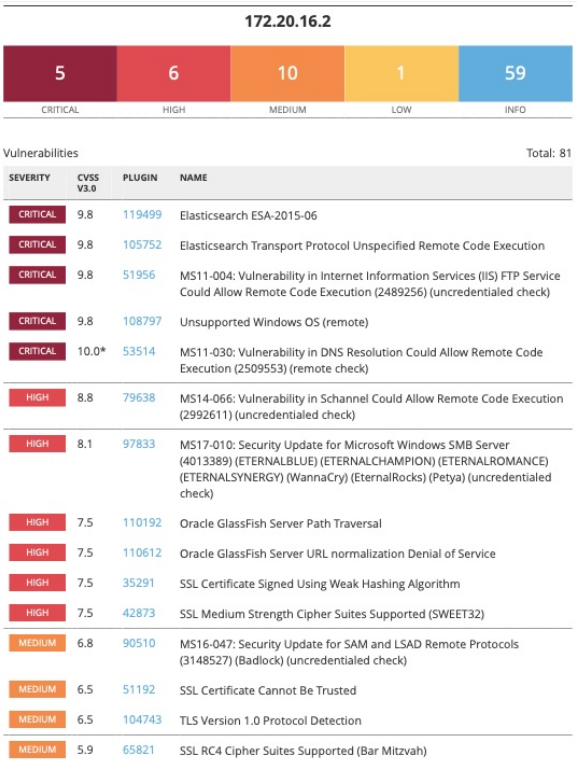
172.20.16.2

11	16	21	2	59
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 109

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	100995	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
CRITICAL	9.8	101787	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
CRITICAL	9.8	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	9.8	108797	Unsupported Windows OS (remote)
CRITICAL	9.0	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	58987	PHP Unsupported Version Detection
CRITICAL	10.0	34460	Unsupported Web Server Detection
CRITICAL	10.0*	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0*	60085	PHP 5.3.x < 5.3.15 Multiple Vulnerabilities
HIGH	8.8	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
HIGH	8.1	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.5	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)

Figura 15: Resultados antes das correções



172.20.16.2

5	6	10	1	59
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 81

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	119499	Elasticsearch ESA-2015-06
CRITICAL	9.8	105752	Elasticsearch Transport Protocol Unspecified Remote Code Execution
CRITICAL	9.8	51956	MS11-004: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256) (uncredentialed check)
CRITICAL	9.8	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
HIGH	8.8	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
HIGH	8.1	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.5	110192	Oracle GlassFish Server Path Traversal
HIGH	7.5	110612	Oracle GlassFish Server URL normalization Denial of Service
HIGH	7.5	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Figura 16: Resultados depois das correções