

Universidade do Minho
Mestrado Integrado em Engenharia Informática
Segurança de Sistemas Informáticos
Relatório do Trabalho Prático 2

Grupo 11
Lázaro Pinheiro (A86788)
Luis Ramos (A83930)

1 de julho de 2021

Conteúdo

1	Introdução	5
2	Contextualização	6
3	Parte A	8
4	Parte B	13
4.1	Ambiente de testes	13
4.1.1	Sistema Alvo	15
4.1.2	Sistema Auditor	15
4.2	Questão 1	15
4.2.1	Varredura de portas TCP	16
4.2.2	Varredura de portas UDP	19
4.3	Questão 2	22
4.4	Questão 3	23
4.5	Questão 4	24
4.6	Questão 5	25
5	Conclusão	32
Appendices		34
A	Output do comando <i>snmp-check</i> direcionado ao servidor alvo	34

Lista de Figuras

1	Os cinco estágios do teste de intrusão.	6
2	Comando nslookup	8
3	IP2Location do IP 109.237.24.222	9
4	IP2Location do IP 35.244.167.140	9
5	Comando <i>whois</i> da empresa Benda	10
6	Comando <i>whois</i> da empresa Continente	10
7	Comando host	11
8	Comando dig da empresa Benda	11
9	Comando dig da empresa Continente	12
10	Arquitetura do ambiente de testes.	13
11	Comando <i>ifconfig</i> , que permite listar todas as interfaces de rede presentes no Sistema Auditor.	14
12	Comando <i>ipconfig</i> , que permite listar todas as interfaces de rede presentes no Sistema Alvo.	14
13	<i>Vagrantfile</i> de instalação do sistema alvo.	15
14	<i>Nmap</i> usando o modo de <i>scan -sn</i>	16
15	<i>Nmap</i> usando o modo de <i>scan -sV -O</i>	17
16	<i>Nmap</i> usando o modo de <i>scan -sUV</i>	20
17	Número de vulnerabilidades por nível de gravidade, obtido através do relatório emitido pelo <i>Nessus</i>	22
18	Notificação de tráfego anómalo, presente no ficheiro <i>alert.full</i> , gerado pelo <i>Snort</i>	23
19	Pacote correspondente à entrada identificada no ficheiro <i>alert.full</i> , gerado pelo <i>Snort</i> , capturado via <i>Wireshark</i>	23
20	Notificação de tráfego anómalo, presente no ficheiro <i>alert.full</i> , gerado pelo <i>Snort</i>	24
21	Pacote correspondente à entrada identificada no ficheiro <i>alert.full</i> , gerado pelo <i>Snort</i> , capturado via <i>Wireshark</i>	24
22	Exemplo de notificações do <i>Snort</i> sem correspondência direta a vulnerabilidade do <i>Nessus</i>	25
23	Alterações efetuadas no Sistema <i>Metasploitable3</i>	26
24	Resultados da varredura do <i>Nessus</i> após implementação para a vulnerabilidade descrita.	26
25	Execução do comando <i>gpedit</i> na <i>Powershell</i> , com o intuito de abrir <i>Group Policy Editor</i>	27
26	Menu do <i>Group Policy Editor</i>	28
27	Ativação autenticação do utilizador para conexões remotas usando autenticação de nível de rede.	29
28	Resultados da varredura do <i>Nessus</i> após implementação para a vulnerabilidade descrita.	29
29	Lista de Vulnerabilidades com fator de risco CRITICAL e HIGH antes da alteração no sistem alvo.	30

30	Lista de Vulnerabilidades com fator de risco CRITICAL e HIGH após da alteração no sistem alvo.	31
----	---	----

1 Introdução

O presente relatório desenvolve-se no âmbito da Unidade Curricular Segurança de Sistemas Informáticos, tendo como principal objetivo consolidar e aplicar a fase de *Footprinting* bem como os dois processos que a constituem (i.e., *reconnaissance* e *scanning*). Este encontra-se dividido em duas partes.

Na primeira parte serão escolhidas duas empresas com serviços on-line, com o objetivo de, através de uma busca passiva, recolher informação sobre os sistemas e infra-estruturas das mesmas.

Na segunda parte será configurado um ambiente de testes, constituído por duas entidades, com o objetivo de, através de uma busca ativa, identificar vulnerabilidades e fraquezas do sistema alvo.

2 Contextualização

O principal objetivo deste trabalho prático é aplicar e consolidar os construtos teóricos e também pôr em prática alguns dos temas abordados em contexto sala de aula.

Sendo que as duas partes deste trabalho estão enquadradas na fase de *footprinting* da atividade de testes de penetração e, de forma a agilizar as partes práticas do trabalho, o grupo apresenta de seguida um breve resumo teórico.

Penetration Testing - Pentest

O método apresentado consiste na tentativa **autorizada** de aceder a um sistema, com o intuito de identificar e recomendar possíveis soluções para vulnerabilidades que existam.

Os testes de intrusão consistem num processo cíclico de 5 estágios, os quais estão identificados na figura seguinte.

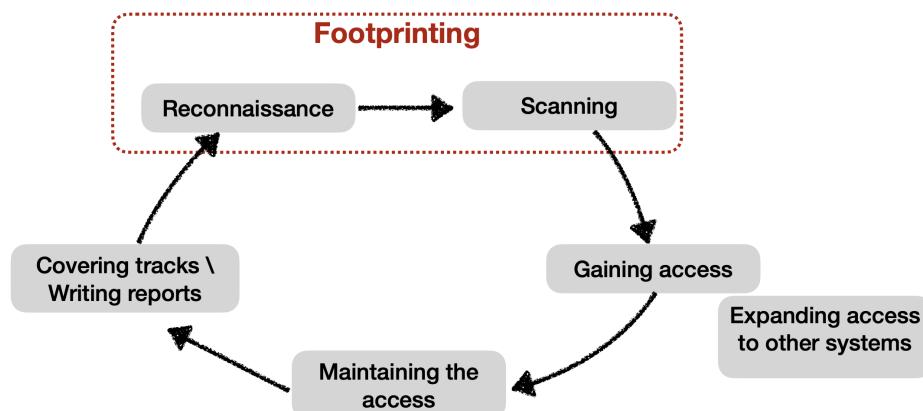


Figura 1: Os cinco estágios do teste de intrusão.

O trabalho versará na fase de ***Footprinting***. Esta fase, permite ao atacante a criação de um repertório da postura de segurança do sistema em análise. Por forma a facilitar a obtenção de informações do sistema, esta encontra-se subdividida nos processos de:

- Coleta Passiva de Informação(***Reconnaissance***) - Processo cujo o intuito é obter o máximo de informação(e.g., informação do **DNS**, *websites* privados...) sem estabelecer contacto entre o sistema alvo e o atacante, sem existir uma comunicação ”direta”entre os intervenientes.
- Coleta Ativa de Informação(***Scanning***) - Este processo utiliza as informações, obtidas através do processo referido anteriormente, com a finalidade de comunicar diretamente com o sistema alvo com a intenção de identificar potenciais ameaças e vulnerabilidades suscetíveis de serem atacadas.

3 Parte A

Esta parte do trabalho prático consiste no uso de técnicas para coleta passiva de informação como ferramenta de análise da postura de segurança em sistemas e infra-estruturas reais.

Para isso, escolhemos duas empresas sendo uma delas de maior dimensão "Continente" e outra de menor dimensão "Benda".

De seguida serão apresentados os resultados dos testes efectuados.

```
luisramos@luisramos-GL552VX ~ $ nslookup benda.pt
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
Name:   benda.pt
Address: 109.237.24.222

luisramos@luisramos-GL552VX ~ $ nslookup continente.pt
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
Name:   continente.pt
Address: 35.244.167.140
```

Figura 2: Comando nslookup

O primeiro comando efetuado foi o comando "nslookup" de modo a determinar qual o *Ip Address* de cada empresa.

No comando **nslookup benda.pt** obtemos como resposta o *Ip Address*: **109.237.24.222**. Já no comando **nslookup continente.pt** obtemos como resposta o *Ip Address*: **35.244.167.140**, como é visível na imagem acima (Figura 2).

Através dos *IP's* obtidos, e recorrendo ao **IP2Location**, podemos obter informações sobre a localização do *IP Address*, *ISP* e número do *ASN*, de cada empresa.

<input checked="" type="checkbox"/> IP Address	109.237.24.222
<input checked="" type="checkbox"/> Country	 United Kingdom of Great Britain and Northern Ireland [GB] ⓘ
<input type="checkbox"/> Region	England
<input type="checkbox"/> City	London
<input type="checkbox"/> Coordinates of City	51.508530, -0.125740 (51°30'31"N 0°7'33"W)
<input type="checkbox"/> ISP	Linode LLC
<input type="checkbox"/> ASN	63949 Linode LLC

Figura 3: IP2Location do IP 109.237.24.222

<input checked="" type="checkbox"/> IP Address	35.244.167.140
<input checked="" type="checkbox"/> Country	 United States of America [US] ⓘ
<input type="checkbox"/> Region	Missouri
<input type="checkbox"/> City	Kansas City
<input type="checkbox"/> Coordinates of City	39.099730, -94.578570 (39°5'59"N 94°34'43"W)
<input type="checkbox"/> ISP	Google LLC
<input type="checkbox"/> ASN	15169 Google

Figura 4: IP2Location do IP 35.244.167.140

Recorrendo ao domínio de cada empresa, <https://benda.pt> e <https://continente.pt>, procedeu-se à utilização do comando *whois*, com a finalidade de obter informações relativas ao domínio em si, permitindo uma resposta detalhada que permitirá reproduzir um conjunto de observações inerentes ao processo de coleta passiva. Informações estas que podem ser quem registou e administrou o registo, o local onde o mesmo se encontra registado e os contactos relativos a todo este processo (Figura 5 e 6).

```

luisramos@luisramos-GL552VX ~ $ whois benda.pt
Domain: benda.pt
Domain Status: Registered
Creation Date: 15/04/2020 16:42:27
Expiration Date: 15/04/2021 16:42:27
Owner Name:
Owner Address:
Owner Locality:
Owner ZipCode:
Owner Locality ZipCode:
Owner Country Code:
Owner Email:
Admin Name: AMENWORLD Serviços Internet - Sociedade Unipessoal Lda
Admin Address: Av. Duque D Alvalade, nº 185 4º A e B
Admin Locality: Lisboa
Admin ZipCode: 1050-082
Admin Locality ZipCode: Lisboa
Admin Country Code: PT
Admin Email: dominios@amen.pt,mailmanager@registryamen.com.pt
Name Server: ns2.amenworld.com | IPv4: and IPv6:
Name Server: ns1.amenworld.com | IPv4: and IPv6:

```

Figura 5: Comando *whois* da empresa Benda

```

luisramos@luisramos-GL552VX ~ $ whois continente.pt
Domain: continente.pt
Domain Status: Registered
Creation Date: 05/08/1998 00:00:00
Expiration Date: 02/11/2023 23:59:00
Owner Name: Modelo Continente Hipermercados S.A.
Owner Address: Rua Joao Mendonca No. 529 - 4º
Owner Locality: Senhora da Hora
Owner ZipCode: 4464-501
Owner Locality ZipCode: Senhora da Hora
Owner Country Code: PT
Owner Email: ajfranca@sonaemc.com,nsguerreiro@sonae.pt
Admin Name: Modelo Continente Hipermercados S.A.
Admin Address: Rua Joao Mendonca No. 529 - 4º
Admin Locality: Senhora da Hora
Admin ZipCode: 4464-501
Admin Locality ZipCode: Senhora da Hora
Admin Country Code: PT
Admin Email: ajfranca@sonaemc.com,nsguerreiro@sonae.pt
Name Server: rudy.ns.cloudflare.com | IPv4: and IPv6:
Name Server: amy.ns.cloudflare.com | IPv4: and IPv6:

```

Figura 6: Comando *whois* da empresa Continente

Olhando para o resultado do mesmo comando efetuado em domínios diferentes, podemos verificar que, neste caso, foi possível obter muita mais informação da empresa maior (Continente).

De notar que a falta de informação da empresa Benda, poderá ser um problema, pois caso seja detetado um erro no seu serviço, não haverá forma de contactar a empresa. Já no caso da empresa Continente, seria aconselhável alterar o email de *ajfranca@sonaemc.com* para *suporte@sonaemc.com*. Desta forma não estaria a expor informação nenhuma e poderia ser contactado sempre que necessário.

De seguida, recorremos à utilização do comando *host*, que permite identificar o **IPV4** e os servidores de *mail* e quais os portos utilizados, como é visível na figura abaixo.

```
luisramos@luisramos-GL552VX ~ $ host continente.pt
continente.pt has address 35.244.167.140
continente.pt mail is handled by 0 continente-pt.mail.protection.outlook.com.
luisramos@luisramos-GL552VX ~ $ host benda.pt
benda.pt has address 109.237.24.222
benda.pt mail is handled by 10 mail-pt.securemail.pro.
```

Figura 7: Comando host

A utilização do comando *dig*, permite identificar o **IPV4** dos servidores e **IPV4** e **IPV6** dos *domain servers* bem como os seus portos utilizados.

```
luisramos@luisramos-GL552VX ~ $ dig benda.pt

; <>> DiG 9.10.3-P4-Ubuntu <>> benda.pt
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42104
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; QUESTION SECTION:
;benda.pt.           IN      A

; ANSWER SECTION:
benda.pt.          631     IN      A      109.237.24.222

; AUTHORITY SECTION:
benda.pt.          2034    IN      NS      ns1.amenworld.com.
benda.pt.          2034    IN      NS      ns2.amenworld.com.

; ADDITIONAL SECTION:
ns2.amenworld.com. 745     IN      A      81.88.63.40
ns1.amenworld.com. 745     IN      A      81.88.63.34

; Query time: 3 msec
; SERVER: 127.0.1.1#53(127.0.1.1)
; WHEN: Wed Dec 16 19:09:50 WET 2020
; MSG SIZE  rcvd: 134
```

Figura 8: Comando dig da empresa Benda

```

luisramos@luisramos-GL552VX ~ $ dig continente.pt

; <>> DiG 9.10.3-P4-Ubuntu <>> continente.pt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29771
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
continente.pt.          IN      A

;; ANSWER SECTION:
continente.pt.      72      IN      A      35.244.167.140

;; AUTHORITY SECTION:
continente.pt.      3525    IN      NS      rudy.ns.cloudflare.com.
continente.pt.      3525    IN      NS      amy.ns.cloudflare.com.

;; ADDITIONAL SECTION:
amy.ns.cloudflare.com. 368     IN      A      108.162.192.101
amy.ns.cloudflare.com. 368     IN      A      172.64.32.101
amy.ns.cloudflare.com. 368     IN      A      173.245.58.101
rudy.ns.cloudflare.com. 510    IN      A      172.64.33.229
rudy.ns.cloudflare.com. 510    IN      A      173.245.59.229
rudy.ns.cloudflare.com. 510    IN      A      108.162.193.229
amy.ns.cloudflare.com. 368     IN      AAAA    2606:4700:50::adf5:3a65
amy.ns.cloudflare.com. 368     IN      AAAA    2803:f800:50::6ca2:c065
amy.ns.cloudflare.com. 368     IN      AAAA    2a06:98c1:50::ac40:2065
rudy.ns.cloudflare.com. 1833   IN      AAAA    2606:4700:58::adf5:3be5
rudy.ns.cloudflare.com. 1833   IN      AAAA    2803:f800:50::6ca2:c1e5
rudy.ns.cloudflare.com. 1833   IN      AAAA    2a06:98c1:50::ac40:21e5

;; Query time: 4 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Wed Dec 16 19:09:29 WET 2020
;; MSG SIZE  rcvd: 376

```

Figura 9: Comando dig da empresa Continente

4 Parte B

Nesta parte do trabalho prático, foi configurado um ambiente de testes. Ambiente este, constituído por as entidades *Sistema Auditor* e *Sistema Alvo*. Por forma a identificar vulnerabilidades e fraquezas no *Sistema Alvo*, foram utilizadas técnicas e ferramentas de *active scanning*.

4.1 Ambiente de testes

O ambiente de testes criado é composto por dois sistemas, pelo que, por forma a facilitar a interpretação e compreensão deste, recomenda-se a visualização da figura 10. Os dois sistema que constituem o ambiente de testes são:

- Sistema Alvo (i.e., Sistema *Metasploitable*)
- Sistema Auditor

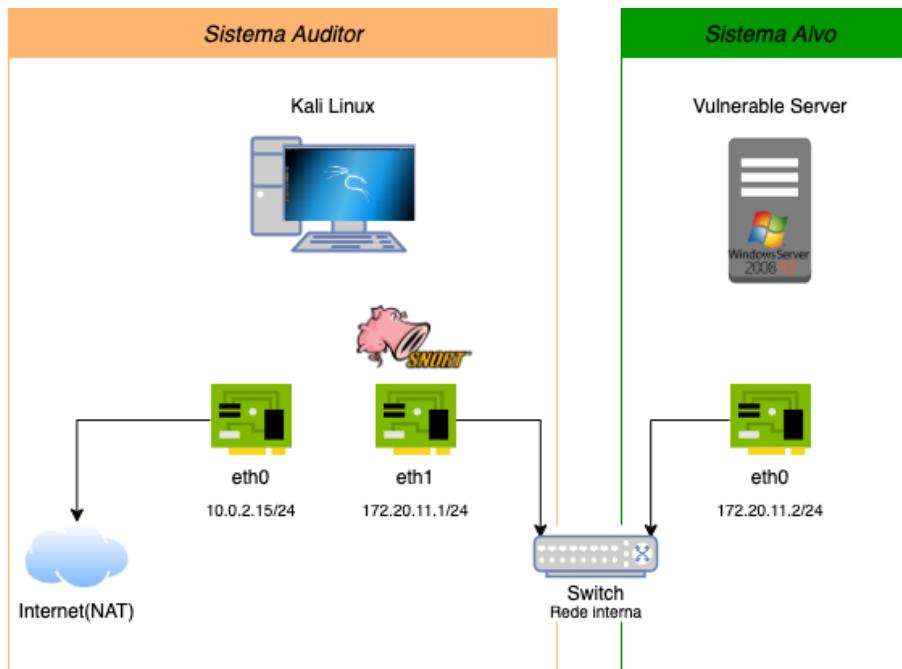


Figura 10: Arquitetura do ambiente de testes.

De notar também que, tal como referido no enunciado, é suposto criar uma topologia de rede onde o Sistema Auditor possui duas interfaces de rede(Figura 11), onde uma (*eth0*) segue uma configuração **NAT** com o IP *10.0.2.15/24* e outra (*eth1*) adota uma configuração "rede interna" com o IP *172.20.11.1/24*. De salientar que este último é atribuído com base nas restrições avançadas no enunciado facultado.

```

(lazaro@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe18:ec:e9 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:18:ec:e9 txqueuelen 1000 (Ethernet)
            RX packets 13 bytes 1744 (1.7 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 1039 bytes 62994 (61.5 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.20.11.1 netmask 255.255.255.0 broadcast 172.20.11.255
        inet6 fe80::a00:27ff:fe48:17e1 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:48:17:e1 txqueuelen 1000 (Ethernet)
            RX packets 1109 bytes 202885 (198.1 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 7470 bytes 636332 (621.4 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Loopback Local)
            RX packets 2462 bytes 140200 (136.9 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 2462 bytes 140200 (136.9 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figura 11: Comando *ifconfig*, que permite listar todas as interfaces de rede presentes no Sistema Auditor.

Tendo em consideração que o sistema *Metasploitable* representa um sistema *reconhecidamente vulnerável*, foi definida uma interface de rede que adota uma configuração de "rede interna", conectada a um *switch*, que se encontra igualmente conectado, tal como anteriormente referido, à interface de rede com a mesma configuração do Sistema Auditor, mas com o endereço **IP 172.20.11.2/24**(Figura 12), evidenciando a possibilidade de criação de uma rede interna, que se reveste de medida de prevenção, isolando o ambiente de testes da rede local pessoal.

```

PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::10a5:3cec:540d:5e19%11
    IPv4 Address . . . . . : 172.20.11.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Tunnel adapter isatap.{DE6858F3-C12B-44C3-9095-41B1E1CDCCDA}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

```

Figura 12: Comando *ipconfig*, que permite listar todas as interfaces de rede presentes no Sistema Alvo.

4.1.1 Sistema Alvo

Este sistema corresponde a uma instância do projeto *Metasploitable 3* mantido pela *Rapid7*, configurado a partir de uma *Vagrantfile*[1], conforme a figura 13.

```
## -*- mode: ruby -*-
# vi: set ft=ruby :

Vagrant.configure("2") do |config|
  config.vm.synced_folder '.', '/vagrant', disabled: true
  config.vm.define "win2k8" do |win2k8|
    # Base configuration for the VM and provisioner
    win2k8.vm.box = "rapid7/metasploitable3-win2k8"
    win2k8.vm.hostname = "metasploitable3-win2k8"
    win2k8.vm.communicator = "winrm"
    win2k8.winrm.retry_limit = 60
    win2k8.winrm.retry_delay = 10

    win2k8.vm.network "private_network", type: "dhcp"

    win2k8.vm.provider "libvirt" do |v|
      v.memory = 4096
      v.cpus = 2
      v.video_type = 'qxl'
      v.input :type => "tablet", :bus => "usb"
      v.channel :type => 'unix', :target_name => 'org.qemu.guest-agent.0', :target_type => 'virtio'
      v.channel :type => 'spicevmc', :target_name => 'com.redhat.spice.0', :target_type => 'virtio'
      v.graphics_type = "spice"

      # Enable Hyper-V enlightenments: https://blog.wikichoos.com/2014/07/enabling-hyper-v-enlightenments-with-kvm.html
      v.hyperv_feature :name => 'stimer', :state => 'on'
      v.hyperv_feature :name => 'relaxed', :state => 'on'
      v.hyperv_feature :name => 'vapic', :state => 'on'
      v.hyperv_feature :name => 'syncic', :state => 'on'
    end

    # Configure Firewall to open up vulnerable services
    case ENV['MS3_DIFFICULTY']
    when 'easy'
      win2k8.vm.provision :shell, inline: "C:\\\\startup\\\\disable_firewall.bat"
    else
      win2k8.vm.provision :shell, inline: "C:\\\\startup\\\\enable_firewall.bat"
      win2k8.vm.provision :shell, inline: "C:\\\\startup\\\\configure_firewall.bat"
    end

    # Insecure share from the Linux machine
    win2k8.vm.provision :shell, inline: "C:\\\\startup\\\\install_share_autorun.bat"
    win2k8.vm.provision :shell, inline: "C:\\\\startup\\\\setup_linux_share.bat"
    win2k8.vm.provision :shell, inline: "rm C:\\\\startup\\\\*" # Cleanup startup scripts
  end
end

Vagrantfile
```

Figura 13: *Vagrantfile* de instalação do sistema alvo.

4.1.2 Sistema Auditor

Este sistema corresponde ao sistema criado para executar varreduras ativas ao sistema *Metasploitable3*. O grupo optou por configurar este sistema recorrendo a uma máquina virtual com o sistema operativo *Kali Linux* previamente configurada[2].

A configuração do sistema com a finalidade de efetuar varreduras ativas, teve lugar através da configuração de **IDS**(*Snort*) e um **Scanner** de Vulnerabilidades(*Nessus*). Não houve necessidade de um instalador de tráfego, visto que o sistema *Kali Linux* já possuí o *Wireshark Version 3.2.7*.

4.2 Questão 1

Para concretizar esta questão, de seguida serão apresentados os procedimentos, os serviços em execução, a identificação e detalhe das vulnerabilidades

e/ou fraquezas presentes no Sistema Alvo, para cada uma das ferramentas utilizadas.

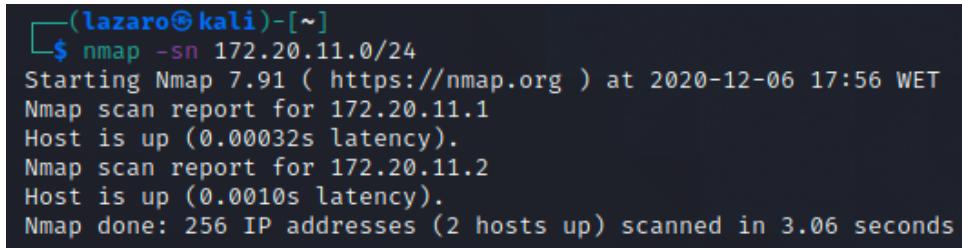
Para realizar esta questão optou-se por selecionar a ferramenta *Nmap*, a qual é usada para executar *port scanning*, enumeração de serviços, detecção de sistema operativo, identificação de vulnerabilidades, entre outros.

Recorrendo à documentação oficial do **Nmap** percebeu-se que a flag *-sn* permite realizar uma varredura de *hosts*, permitindo determinar quais os hosts(endereços **IP**) presentes na rede, o que acaba por ser muito semelhante ao comando *ping*.

Utilizando o comando (Figura 14):

```
nmap -sn 172.20.11.0/24
```

Pode-se constatar que a rede é constituída pelo Sistema Auditor (*172.20.11.1*) e pelo Sistema Alvo (*172.20.11.2*).



```
(lazaro㉿kali)-[~]
$ nmap -sn 172.20.11.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-06 17:56 WET
Nmap scan report for 172.20.11.1
Host is up (0.00032s latency).
Nmap scan report for 172.20.11.2
Host is up (0.0010s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 3.06 seconds
```

Figura 14: *Nmap* usando o modo de *scan -sn*.

4.2.1 Varredura de portas TCP

A flag *-O* permitiu a deteção de todas as portas **TCP** existentes, assumindo resultados complementares aos obtidos com a flag *-sS* e *-sT*, bem como a deteção do sistema operativo presente na máquina. O uso da flag *-sV* permitiu determinar as versões associadas aos serviços em execução nas portas apresentadas(Figura 15).

Com o intuito de efetuar a varredura nas portas **TCP** utilizou-se o comando:

```
nmap -sUV 172.20.11.2
```

que conjuga as duas flags acima mencionadas.

- *Microsoft IIS*
 - CVE-2020-0645
 - Este serviço apresenta vulnerabilidade, visto que adultera os dados(*tampering*) quando lida com *headers* de pacotes **HTTP** mal-formados.
 - *CVSS Version 2.x* : 5.0(**MEDIUM**)
 - *CVSS Version 3.x* : 7.5(**HIGH**)
- *Apache Tomcat*
 - CVE-2020-17527
 - Este serviço apresenta vulnerabilidade, visto que poderia reutilizar o *header* de um pacote **HTTP** de um fluxo anterior, numa conexão **HTTP/2**, na solicitação do fluxo seguinte.
 - *CVSS Version 2.x* : 5.0(**MEDIUM**)
 - *CVSS Version 3.x* : 7.5(**HIGH**)
- *Sun GlassFish*
 - CVE-2012-1712
 - Este serviço apresenta vulnerabilidade transversal do diretório na componente *Liferay*.
 - *CVSS Version 2.x* : 10.0(**CRITICAL**)
 - *CVSS Version 3.x* : **N/A**
- *Apache httpd*
 - CVE-2018-11803
 - Este serviço apresenta falha após a desreferenciação de um apontador não inicializado se o cliente omitir o *path* numa operação de listagem de diretório recursiva.
 - *CVSS Version 2.x* : 5.0(**MEDIUM**)
 - *CVSS Version 3.x* : 7.5(**HIGH**)
- *Microsoft Windows RPC*
 - CVE-2019-1089
 - Este serviço apresenta elevação de privilégios quando o *kernel* de ativação do serviço **RPC** lida incorretamente com uma solicitação **RPC**.
 - *CVSS Version 2.x* : 7.2(**MEDIUM**)
 - *CVSS Version 3.x* : 7.8(**HIGH**)

- *Java RMI*
 - CVE-2020-9761
 - Este serviço tem uma configuração padrão insegura, levando à execução de código **Java** a partir de um **URL**, através da invocação de um método do *Garbage Collector*.
 - *CVSS Version 2.x* : 7.5(**MEDIUM**)
 - *CVSS Version 3.x* : 9.8(**CRITICAL**)

Para o sistema operativo selecionado no conjunto dado como *output*, apresenta-se uma das suas vulnerabilidades:

- *Microsoft Windows Server 2008 R2*
 - CVE-2019-0584
 - Existe uma vulnerabilidade de execução remota de código quando o *Windows Jet Database Engine* manipula indevidamente objetos na memória.
 - *CVSS Version 2.x* : 9.3(**HIGH**)
 - *CVSS Version 3.x* : 7.8(**HIGH**)

4.2.2 Varredura de portas UDP

Para efetuar a varredura nas portas **UDP** utilizou-se o comando:

```
nmap -sUV 172.20.11.2
```

o qual permite conhecer as portas **UDP** existentes. De realçar ainda que, os tempos de varredura são exageradamente superiores aos da varredura das portas **TCP**, situação já esperada pelo grupo. Todavia, não era expectável tempos de espera superiores a uma hora. A utilização da flag *-sUV* permitiu a coleta da informação da porta, bem como da versão em execução do serviço.

```
(lazaro㉿kali)-[~]
$ sudo nmap -sUV 172.20.11.2
[sudo] senha para lazaro:
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-06 21:37 WET
Stats: 0:25:23 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 30.20% done; ETC: 23:01 (0:57:47 remaining)
Stats: 0:47:40 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 56.30% done; ETC: 23:02 (0:36:43 remaining)
Stats: 0:47:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 57.60% done; ETC: 23:00 (0:34:53 remaining)
Stats: 0:47:50 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 58.20% done; ETC: 22:59 (0:34:05 remaining)
Stats: 0:47:55 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 58.20% done; ETC: 22:59 (0:34:09 remaining)
Stats: 1:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 74.20% done; ETC: 23:00 (0:21:07 remaining)
Stats: 1:05:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 78.20% done; ETC: 23:01 (0:18:04 remaining)
Stats: 1:21:46 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 98.20% done; ETC: 23:01 (0:01:30 remaining)
Nmap scan report for 172.20.11.2
Host is up (0.00036s latency).
Not shown: 998 open|filtered ports
PORT      STATE SERVICE      VERSION
137/udp  open  netbios-ns Microsoft Windows netbios-ns (workgroup: WORKGROUP)
161/udp  open  snmp   SNMPv1 server (public)
MAC Address: 08:00:27:44:FE:EB (Oracle VirtualBox virtual NIC)
Service Info: Hosts: METASPLOITABLE3, metasploitable3-win2k8; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5003.75 seconds
```

Figura 16: *Nmap* usando o modo de *scan -sUV*.

No que respeita às vulnerabilidades encontradas nos serviços desta varredura, importa referir que foram descritas apenas aquelas em que se reconheceu a criticidade das mesmas. Assim sendo:

- *Microsoft Windows netbios-ns*
 - CVE-2017-0174
 - Existe uma vulnerabilidade de negação de serviço quando manipula incorretamente pacotes **NetBIOS**.
 - *CVSS Version 2.x* : 6.1(**MEDIUM**)
 - *CVSS Version 3.x* : 6.5(**MEDIUM**)

Para grande felicidade do grupo a porta *161/udp* encontra-se aberta e a executar o serviço **SNMP** (*Simple Network Management Protocol*), que é um protocolo que permite a gestão de objetos conectados, tipicamente usado em dispositivos (i.e., *routers*; computadores; servidores; impressoras; entre outros) de rede. Quando bem configurado, o *snmp walk* (sobre o qual o *snmp-check*) deve revelar apenas para utilizadores autenticados quais os objetos que este pode gerir.

Um serviço **SNMP** mal configurado é uma ótima fonte de informação, informações valiosas para os atacantes. Este caso é um exemplo no qual o software em si possuí vulnerabilidades, mas a sua má configuração torna o sistema vulnerável.

Executou-se o comando:

snmp—check 172.20.11.2

o qual permitiu obter informações dos seguintes tipos:

- Informações do sistema;
- Contas dos Utilizadores;
- Informações da rede;
- Interfaces de rede;
- Endereços **IP** da rede;
- Informações de *routing*;
- Portas **TCP** à "escuta";
- Portas **UDP** à "escuta";
- Serviços de rede;
- Quais os processos em execução;
- Informações do armazenamento;
- Informações do sistema de ficheiros;
- Componentes Software;
- Informações do servidor **ISS**(*Internet Information Services*).

É importante realçar a quantidade de informação que este comando permite obter. Por forma a obter mais informação do *output* deste comando, consultar Anexo A.

Configuração das Ferramentas no Sistema Auditor

Para a realização das seguintes questões, primeiramente, inicializou-se a ferramenta *Snort* via linha de comandos, a partir do comando:

```
/etc/init.d/snort start
```

Ainda foi executado o comando:

```
snort -l /var/log/snort -c /etc/snort/snort.conf -i eth1
```

Este iniciou o *scan* na ferramenta *Snort*, onde foram usadas as seguintes *flags* com o intuito de:

- **-l** : *Path* onde os *logs* do *Snort* serão armazenados;
- **-c** : *Path* do ficheiro de configuração do *Snort*;
- **-i** : Interface que será utilizada para a captura de tráfego;

Ainda se iniciou o *Wireshark*, escolhendo a interface *eth1*(*172.20.11.1*).

Tendo estas duas ferramentas inicializadas, iniciou-se o *Nessus* com o comando:

```
/bin/systemctl start nessusd.service
```

O *Nessus* e o *Snort* permitiram observar as vulnerabilidades do Sistema Alvo, através da catalogação das mesmas em gráficos e níveis de gravidade.

O *Wireshark* permitiu capturar os pacotes transacionados entre os dois sistemas no decorrer da varredura.

4.3 Questão 2

Após a inicialização de todas as ferramentas e do Sistema Alvo, começou-se o processo de *scanning*, o qual consistia num *Basic Network Scan*, onde no final foram obtidas as vulnerabilidades presentes na máquina *Metasploitable3* bem como as suas informações(*Severity, CVSS, Plugin, Name*), através de um relatório emitido pelo *Nessus*. Importa salientar que, com este *scanning*, foram descobertas 93 vulnerabilidades (Figura 17), sendo que 6 delas são *CRITICAL* e todas cotadas com um *CVSS* de 10.0.

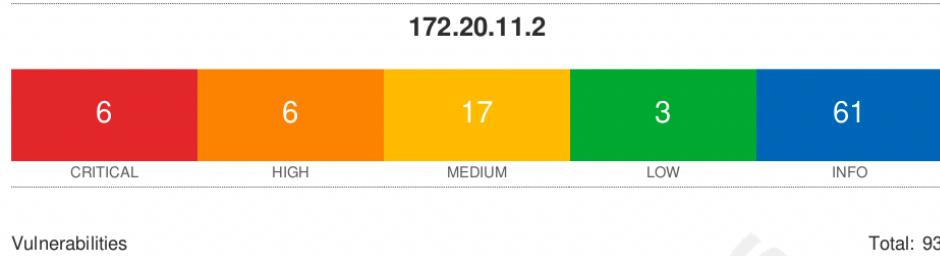


Figura 17: Número de vulnerabilidades por nível de gravidade, obtido através do relatório emitido pelo *Nessus*.

Não é possível efetuar uma comparação de resultados encontrados no sistema automático de identificação de vulnerabilidades, quando comparado com o manual(Secção 4.2), uma vez que neste último foram varridas as portas **TCP** e **UDP**, sendo que para cada serviço em execução numa destas portas *aberta*, foram procuradas vulnerabilidades mais recentes ou mais críticas, quando esta não é única, o que não garante que esta vulnerabilidade esteja presente no serviço em execução, uma vez que não foi identificada a versão do mesmo. A vantagem do sistema *Nessus* é a sua automatização, uma vez que executa a varredura de todas as portas, identifica os serviços em execução bem como as um intervalo de versões possíveis. Num caso real, não seria utilizado o *Nessus*, pois se o sistema alvo estivesse a executar um *Snort*, facilmente detetaria que estavam a ser recebido demasiados pacotes de um mesmo endereço IP, o que resultaria no bloqueio deste.

4.4 Questão 3

Para a realização desta questão os eventos foram selecionadas as seguintes entradas do ficheiro *alert.full*, no qual estão listados *logs* adicionais que facilitarão o entendimento do alerta gerado.

O primeiro evento de tráfego anómalo selecionado possuí a descrição ”*DDOS mstream client to handler*”, podendo ser consultado na Figura 18, o qual é identificado com **CVE-2000-0138**.

```
[**] [1:249:8] DDOS mstream client to handler [**]
[Classification: Attempted Denial of Service] [Priority: 2]
12/20/2018:52:460265 172.20.11.1:32073 -> 172.20.11.2:15104
TCP TTL:64 TOS:0x0 ID:0 Iplen:20 DgmLen:48 DF
*****$* Seq: 0x93F802F1 Ack: 0x0 Win: 0x1000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
[Xref = http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0138][Xref => http://www.whitehats.com/info/IDS111]
```

Figura 18: Notificação de tráfego anómalo, presente no ficheiro *alert.full*, gerado pelo *Snort*.

Esta notificação corresponde a uma tentativa de *Denial of Service*, isto é, uma tentativa de tornar os recursos do sistema alvo indisponível para os seus utilizadores. Esta foi capturada através do *Wireshark* através da porta da fonte e do destino(Figura 19).

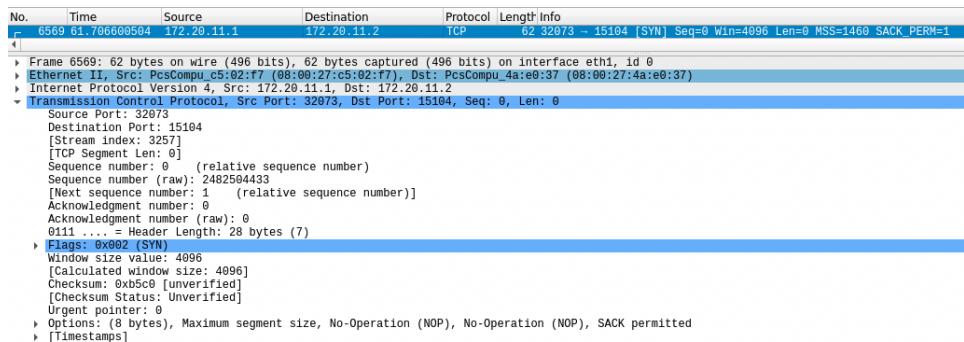


Figura 19: Pacote correspondente à entrada identificada no ficheiro *alert.full*, gerado pelo *Snort*, capturado via *Wireshark*.

O segundo evento de tráfego anómalo selecionado possuí a descrição ”*MISC UPnP malformed advertisement*”, podendo ser consultado na Figura 20, o qual é identificado com **CVE-2001-0876** e **CVE-2001-0877**.

```
[**] [1:1384:8] MISC UPnP malformed advertisement [**]
[Classification: Misc Attack] [Priority: 2]
12/20-02:20:21.396209 172.20.11.1:51761 → 172.20.11.2:1900
UDP TTL:64 TOS:0x0 ID:31337 IpLen:20 DgmLen:282
Len: 254
[Xref ⇒ http://www.microsoft.com/technet/security/bulletin/MS01-059.mspx][Xref ⇒ http://cve.mitre.org/cgi-bin/cvename.cgi?name=2001-0876]
[Xref ⇒ http://cve.mitre.org/cgi-bin/cvename.cgi?name=2001-0876][Xref ⇒ http://www.securityfocus.com/bid/3723]
```

Figura 20: Notificação de tráfego anómalo, presente no ficheiro *alert.full*, gerado pelo *Snort*.

Esta notificação corresponde a um *Buffer overflow Universal Plug and Play(UPnP)*, o qual consiste num conjunto de protocolos de rede de computadores que permitem a conexão direta e simplificação da implementação de redes em casa e em escritórios, onde o protocolo de comunicação é o *Simple Service Discovery Protocol(SSDP)*, o qual é baseado no **UPnP**(Figura 21).

No.	Time	Source	Destination	Protocol	Length	Info
13171	150.642544245	172.20.11.1	172.20.11.2	SSDP	296	NOTIFY * HTTP/1.1
▶ Frame 13171: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interface eth1, id 0						
▶ Ethernet II, Src: PcsCompu_c5:02:f7 (08:00:27:c5:02:f7), Dst: PcsCompu_4a:e0:37 (08:00:27:4a:e0:37)						
▶ Internet Protocol Version 4, Src: 172.20.11.1, Dst: 172.20.11.2						
0100 = Version: 4						
.... 0101 = Header Length: 20 bytes (5)						
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 282						
Identification: 0x7a69 (31337)						
Flags: 0x0000						
Fragment offset: 0						
Time to live: 64						
Protocol: UDP (17)						
Header checksum: 0x913e [validation disabled]						
[Header checksum status: Unverified]						
Source: 172.20.11.1						
Destination: 172.20.11.2						
▶ User Datagram Protocol, Src Port: 51761, Dst Port: 1900						
▶ Simple Service Discovery Protocol						

Figura 21: Pacote correspondente à entrada identificada no ficheiro *alert.full*, gerado pelo *Snort*, capturado via *Wireshark*.

4.5 Questão 4

Esta questão procura dar resposta ao facto de, no ficheiro de *logsalert.full* resultante do *Snort* existirem algumas notificações que não possuem correspondência direta no relatório de vulnerabilidades, emitido pela ferramenta *Nessus*.

Na consulta do ficheiro *alert.full* é perceptível a existência de notificações que não possuem qualquer correspondência com uma vulnerabilidade. De destacar a Figura 22 na qual se verificam entradas no ficheiro descrito, que não correspondem a uma vulnerabilidade em si, mas a pacotes enviados pelo *localhost* (*0.0.0.0*) em modo *broadcast* (*255.255.255.255*). Esta notificação ocorre sempre que há uma tentativa de conexão à rede, com o intuito de reconhecer todas as máquinas presentes numa determinada rede, o qual recorre ao envio de pacotes **UDP**, em modo *broadcast*.

```
[**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
12/20-02:20:08.020404 0.0.0.0:40214 -> 255.255.255.255:20561
UDP TTL:128 TOS:0x0 ID:343 IPlen:20 DgmLen:50 DF
Len: 22
[Xref => http://www.cert.org/advisories/CA-1997-28.html][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0016][Xref => http://www.securityfocus.com/bid/2666]
[**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
12/20-02:20:10.096368 0.0.0.0:40214 -> 255.255.255.255:20561
UDP TTL:128 TOS:0x0 ID:343 IPlen:20 DgmLen:50 DF
Len: 22
[Xref => http://www.cert.org/advisories/CA-1997-28.html][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0016][Xref => http://www.securityfocus.com/bid/2666]
[**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
12/20-02:20:12.228464 0.0.0.0:40214 -> 255.255.255.255:20561
UDP TTL:128 TOS:0x0 ID:343 IPlen:20 DgmLen:50 DF
Len: 22
[Xref => http://www.cert.org/advisories/CA-1997-28.html][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0016][Xref => http://www.securityfocus.com/bid/2666]
```

Figura 22: Exemplo de notificações do *Snort* sem correspondência direta a vulnerabilidade do *Nessus*.

4.6 Questão 5

Para a realização desta questão efetuou-se o *download* dos relatórios emitidos pelo *Nessus*, com maior e menor detalhe. A partir destes foram selecionadas três vulnerabilidades com o intuito de as corrigir, aplicando procedimentos escolhidos com base na documentação, efetuando uma nova varredura posteriormente às respetivas correções.

SMB Signing not required

Descrição/Detalhe

Esta vulnerabilidade é classificada com um grau de 5.3, com um fator de risco **MEDIUM**. Uma vez que a assinatura não é necessária no servidor **SMB** remoto, um atacante remoto não autenticado pode explorar isso para conduzir ataques do tipo *man-in-the-middle* contra o servidor **SMB**.

- Problema: Assinatura não necessária no servidor **SMB** remoto.
- Solução: Impor a assinatura de mensagem na configuração do *host*.

Implementação da solução

Como tentativa de resolução da vulnerabilidade encontrada, no sistema alvo, nas *Security Options* das *Local Policies* na definição *Local Security Policy* para a chave *Microsoft network server: Digitally sign communications (always)*, procedeu-se a alteração do valor de *Disabled* para *Enabled*, na tentativa de obrigar a assinatura de mensagem na configuração.(cf. Figura 23).

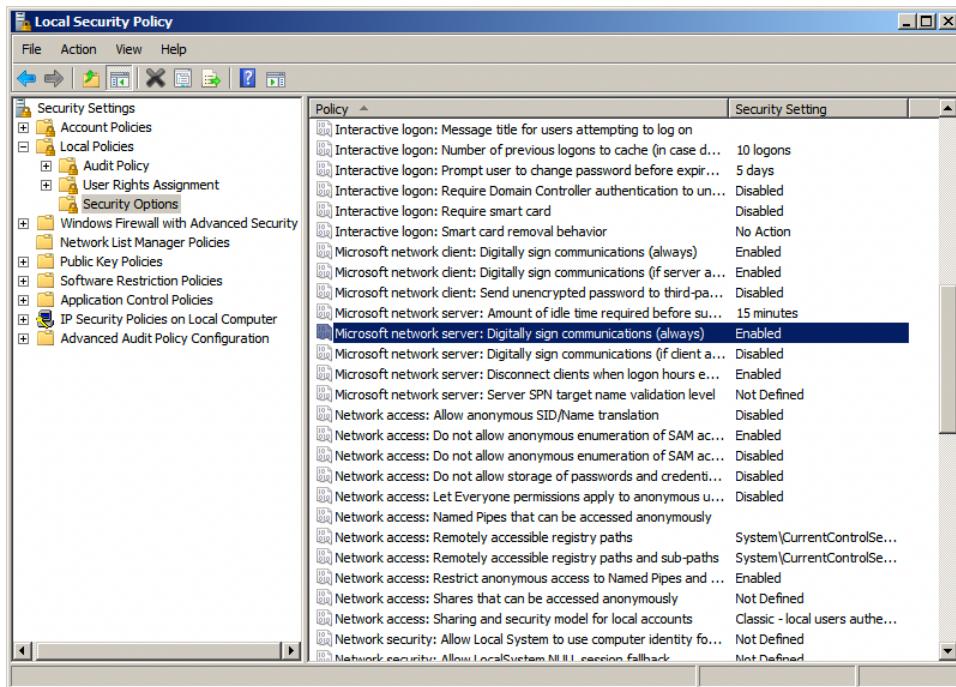


Figura 23: Alterações efetuadas no Sistema *Metasploitable3*.

Através da aplicação da solução desapareceu a vulnerabilidade em causa, sendo evidente o decréscimo do grau de vulnerabilidades e do fator de risco em causa(cf. Figura 24), face à primeira varredura prévia à implementação da solução (cf. Figura 17) e a vulnerabilidade em si deixa de estar presente no detalhe de cada uma das vulnerabilidades do relatório de *Nessus*.

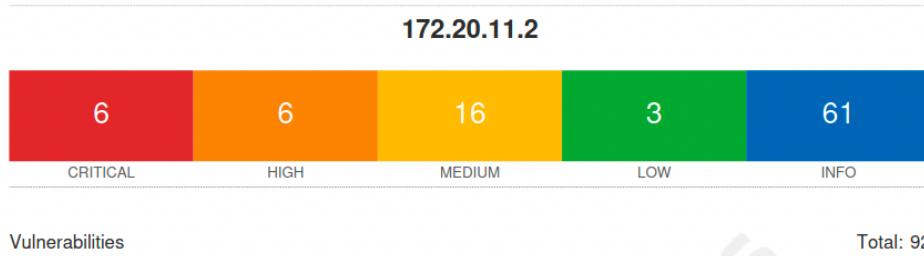


Figura 24: Resultados da varredura do *Nessus* após implementação para a vulnerabilidade descrita.

Terminal Services Doesn't Use NLA Only

Descrição/Detalhe

Esta vulnerabilidade é classificada com um grau de 4.0, com um fator de risco **MEDIUM**. Os serviços de terminal remotos não estão configurados para usar apenas a autenticação no nível da rede. O *Network Level Authentication(NLA)* usa o protocolo *Credential Security Support Provider(CredSSP)* para executar autenticação forte do servidor por meio de mecanismos **TLS/SSL** ou **Kerberos**, que protegem contra ataques *man-in-the-middle*. Além de melhorar a autenticação, o **NLA** também ajuda a proteger o computador remoto de utilizadores e *softwares* maliciosos, concluindo a autenticação do utilizador antes que uma conexão **RDP** completa seja estabelecida.

- Problema: Os serviços de terminal remotos não usam apenas autenticação de nível de rede.
- Solução: Ativação da autenticação no nível da rede (**NLA**) no servidor **RDP** remoto.

Implementação da solução

Como tentativa de resolução da vulnerabilidade encontrada, no sistema alvo, recorreu-se à *Powershell*, na qual foi executado o comando:

```
gpedit
```

o qual abriu uma janela *Group Policy Editor*(cf. Figura 25).

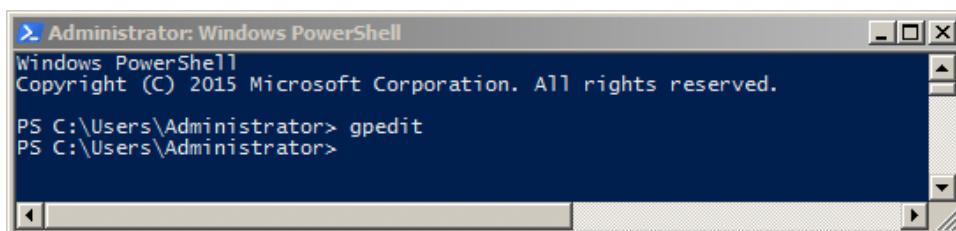


Figura 25: Execução do comando *gpedit* na *Powershell*, com o intuito de abrir *Group Policy Editor*.

Posteriormente, navegou-se por *Computer Configuration* → *Administrative Templates* → *Windows Components* → *Remote Desktop Services* → *Remote Desktop Session Host* → *Security* (cf. Figura 26).

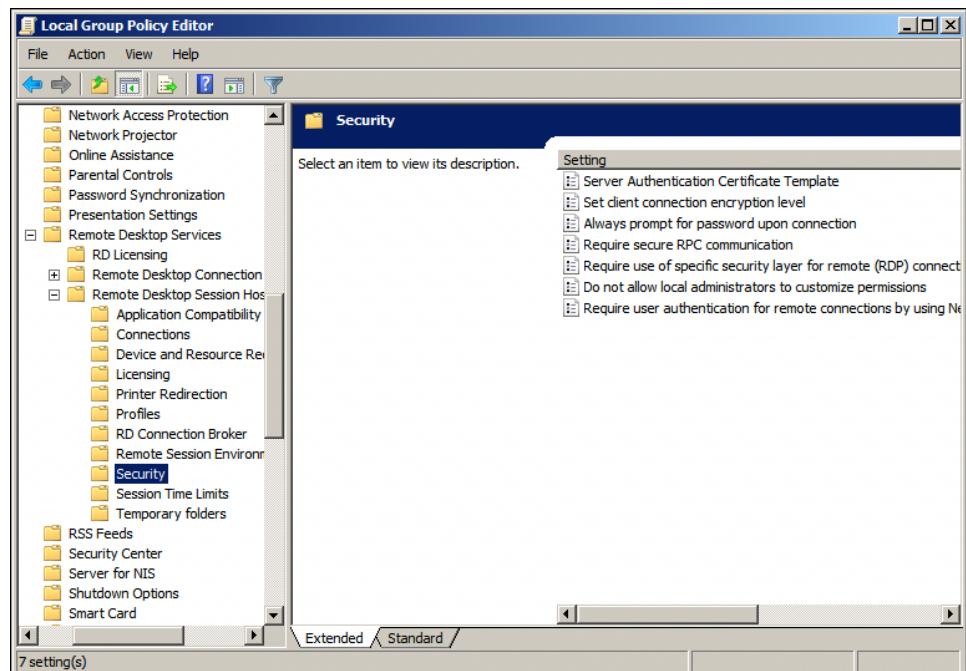


Figura 26: Menu do *Group Policy Editor*.

Neste seleciona-se o item *Require user authentication for remote connections by using Network Level Authentication* e alterou-se de *Disabled* para *Enabled*(cf. Figura 27).

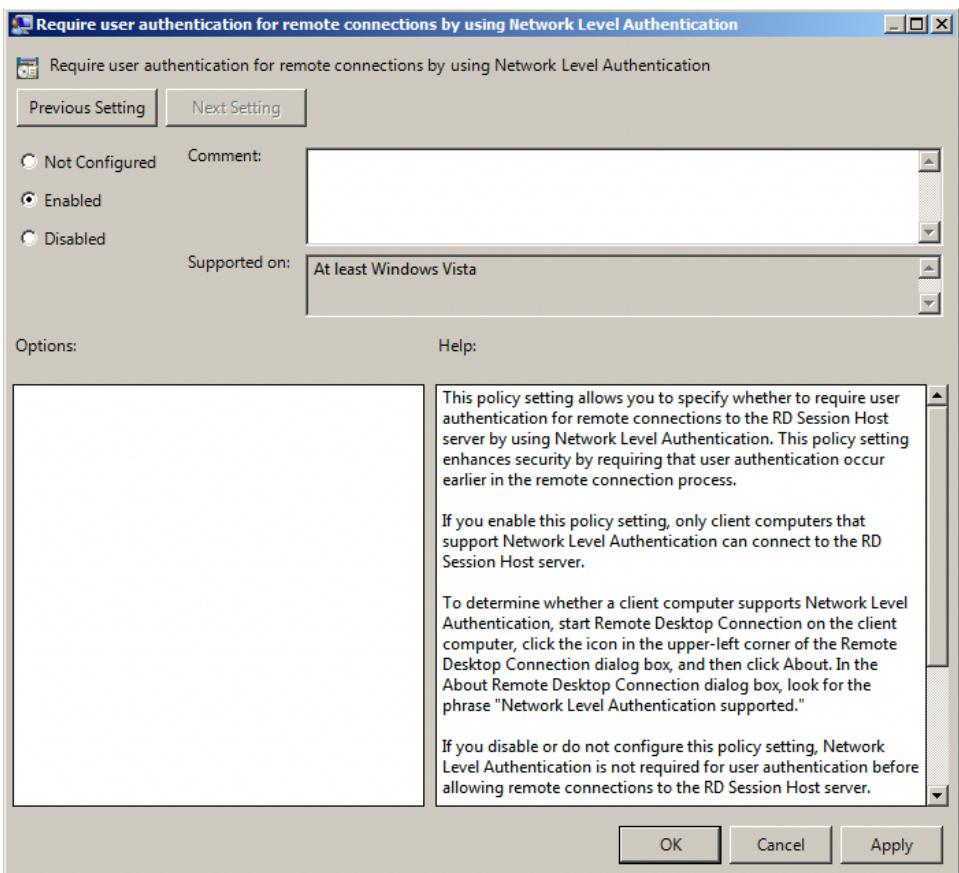


Figura 27: Ativação autenticação do utilizador para conexões remotas usando autenticação de nível de rede.

Através da aplicação da solução desapareceu a vulnerabilidade em causa, sendo evidente o decréscimo do grau de vulnerabilidades e do fator de risco em causa(cf. Figura 28), face à primeira varredura prévia à implementação da solução (cf. Figura 24) e a vulnerabilidade em si deixa de estar presente no detalhe de cada uma das vulnerabilidades do relatório de *Nessus*.

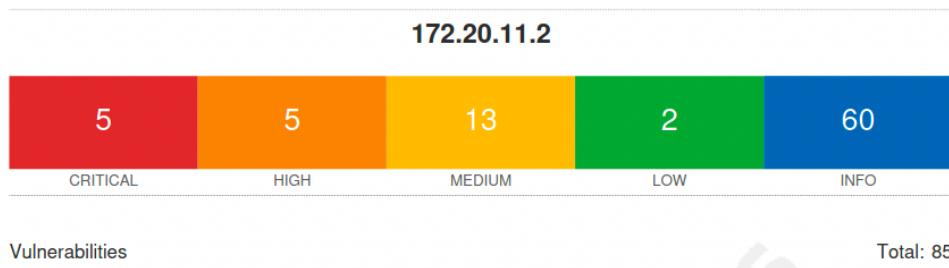


Figura 28: Resultados da varredura do *Nessus* após implementação para a vulnerabilidade descrita.

De salientar ainda que esta alteração resolveu uma vulnerabilidade com um fator de risco **CRITICAL** e uma outra com fator de risco **HIGH**, bem como muitas outras com diferentes fatores, para maior detalhe podemos consultar a Figura 29 e a Figura 30. De salientar que as duas vulnerabilidades que desapareceram foram ***Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unprivileged check)*** a qual era altamente crítica, pontuando 9.8 no *CVSS v3.0 Base Score* e a ***MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (unprivileged check)*** que pontuava 9.3 no *CVSS Base Score*.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (unprivileged check)
CRITICAL	10.0	135293	ManageEngine Desktop Central 10 < Build 100479 Remote Code Execution (direct check)
CRITICAL	10.0	90192	ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE
CRITICAL	10.0	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unprivileged check)
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	9.3	58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (unprivileged check)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unprivileged check)
HIGH	7.8	110612	Oracle GlassFish Server URL normalization Denial of Service
HIGH	7.5	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
HIGH	7.5	119499	Elasticsearch ESA-2015-06
HIGH	7.5	105752	Elasticsearch Transport Protocol Unspecified Remote Code Execution

Figura 29: Lista de Vulnerabilidades com fator de risco **CRITICAL** e **HIGH** antes da alteração no sistema alvo.

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0	79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (unprivileged check)
CRITICAL	10.0	135293	ManageEngine Desktop Central 10 < Build 100479 Remote Code Execution (direct check)
CRITICAL	10.0	90192	ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unprivileged check)
HIGH	7.8	110612	Oracle GlassFish Server URL normalization Denial of Service
HIGH	7.5	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
HIGH	7.5	119499	Elasticsearch ESA-2015-06
HIGH	7.5	105752	Elasticsearch Transport Protocol Unspecified Remote Code Execution

Figura 30: Lista de Vulnerabilidades com fator de risco **CRITICAL** e **HIGH** após da alteração no sistema alvo.

5 Conclusão

Culminada a elaboração deste trabalho prático, importa referir que a execução do mesmo permitiu aos elementos do grupo compreender o funcionamento de *Footprinting*.

A execução desta fase do trabalho prático permitiu uma melhor consolidação dos construtos teóricos através dos dois processos utilizados, *reconnaissance* e *scanning*.

No ímpeto geral o desenvolvimento desta fase do trabalho decorreu como planeado, alcançando os objetivos delineados pelo enunciado.

Referências

- [1] *Metasploitable3*,
<https://github.com/rapid7/metasploitable3>
- [2] *Download Kali Linux Images*,
<https://www.kali.org/downloads/>

Appendices

A Output do comando *snmp-check* direcionado ao servidor alvo

```
snmp-check v1.9 – SNMP enumerator
Copyright (c) 2005–2015 by Matteo Cantoni (www.nothink.org)
```

```
[+] Try to connect to 172.20.11.2:161 using SNMPv1 and community 'public'
```

```
[*] System information:
```

```
Host IP address : 172.20.11.2
Hostname : metasploitable3-win2k8
Description : Hardware: Intel64 Family 6 Model 158 Stepping 10 AT/AT
              COMPATIBLE – Software: Windows Version 6.1 (Build 7601 Multiprocessor
              Free)
Contact : –
Location : –
Uptime snmp : 01:08:09.85
Uptime system : 01:07:56.86
System date : 2020–12–8 09:09:27.1
Domain : WORKGROUP
```

```
[*] User accounts:
```

```
sshd
Guest
greedo
vagrant
han_solo
kylo_ren
boba_fett
chewbacca
ben_kenobi
jabba_hutt
artoo_detoo
c_three_pio
darth_vader
leia_organa
sshd_server
jarjar_binks
Administrator
luke_skywalker
anakin_skywalker
lando_calrissian
```

```
[*] Network information:
```

```
IP forwarding enabled : no
Default TTL : 128
```

```
TCP segments received : 1779730  
TCP segments sent : 1779722  
TCP segments retrans : 8  
Input datagrams : 490  
Delivered datagrams : 631  
Output datagrams : 1331466
```

[*] Network interfaces:

```
Interface : [ up ] Software Loopback Interface 1
```

```
Id : 1  
Mac Address : :::::  
Type : softwareLoopback  
Speed : 1073 Mbps  
MTU : 1500  
In octets : 0  
Out octets : 0
```

```
Interface : [ up ] WAN Miniport (SSTP)
```

```
Id : 2  
Mac Address : :::::  
Type : unknown  
Speed : 1073 Mbps  
MTU : 4091  
In octets : 0  
Out octets : 0
```

```
Interface : [ up ] WAN Miniport (L2TP)
```

```
Id : 3  
Mac Address : :::::  
Type : unknown  
Speed : 1073 Mbps  
MTU : 1460  
In octets : 0  
Out octets : 0
```

```
Interface : [ up ] WAN Miniport (PPTP)
```

```
Id : 4  
Mac Address : :::::  
Type : unknown  
Speed : 1073 Mbps  
MTU : 1464  
In octets : 0  
Out octets : 0
```

```
Interface : [ up ] WAN Miniport (PPPOE)
```

```
Id : 5  
Mac Address : :::::  
Type : ppp  
Speed : 1073 Mbps  
MTU : 1494  
In octets : 0  
Out octets : 0
```

Interface : [up] WAN Miniport (IPv6)
Id : 6
Mac Address : d8:1a:20:52:41:53
Type : ethernet—csmacd
Speed : 1073 Mbps
MTU : 1500
In octets : 0
Out octets : 0

Interface : [up] WAN Miniport (Network Monitor)
Id : 7
Mac Address : d6:b9:20:52:41:53
Type : ethernet—csmacd
Speed : 1073 Mbps
MTU : 1500
In octets : 0
Out octets : 0

Interface : [up] WAN Miniport (IP)
Id : 8
Mac Address : d6:b9:20:52:41:53
Type : ethernet—csmacd
Speed : 1073 Mbps
MTU : 1500
In octets : 0
Out octets : 0

Interface : [down] RAS Async Adapter
Id : 9
Mac Address : 20:41:53:59:4e:ff
Type : ppp
Speed : 0 Mbps
MTU : 0
In octets : 0
Out octets : 0

Interface : [up] WAN Miniport (IKEv2)
Id : 10
Mac Address : 00:00:00:00:00:00
Type : unknown
Speed : 0 Mbps
MTU : 1480
In octets : 0
Out octets : 0

Interface : [up] Intel(R) PRO/1000 MT Desktop Adapter
Id : 11
Mac Address : 08:00:27:44:fe:eb
Type : ethernet—csmacd
Speed : 1000 Mbps
MTU : 1500
In octets : 79184
Out octets : 117873

```
Interface : [ up ] Microsoft ISATAP Adapter
Id : 12
Mac Address : 00:00:00:00:00:00
Type : unknown
Speed : 0 Mbps
MTU : 1280
In octets : 0
Out octets : 0

Interface : [ up ] Microsoft ISATAP Adapter #2
Id : 13
Mac Address : 00:00:00:00:00:00
Type : unknown
Speed : 0 Mbps
MTU : 1280
In octets : 0
Out octets : 0

Interface : [ down ] Intel(R) PRO/1000 MT Desktop Adapter #2
Id : 14
Mac Address : 08:00:27:a4:a3:db
Type : ethernet—csmacd
Speed : 0 Mbps
MTU : 0
In octets : 0
Out octets : 0

Interface : [ up ] Intel(R) PRO/1000 MT Desktop Adapter—QoS Packet Scheduler
           —0000
Id : 15
Mac Address : 08:00:27:44:fe:eb
Type : ethernet—csmacd
Speed : 1000 Mbps
MTU : 1500
In octets : 79184
Out octets : 117873

Interface : [ up ] Intel(R) PRO/1000 MT Desktop Adapter—WFP LightWeight Filter
           —0000
Id : 16
Mac Address : 08:00:27:44:fe:eb
Type : ethernet—csmacd
Speed : 1000 Mbps
MTU : 1500
In octets : 79184
Out octets : 117873

Interface : [ up ] WAN Miniport (IPv6)—QoS Packet Scheduler—0000
Id : 17
Mac Address : d8:1a:20:52:41:53
Type : ethernet—csmacd
Speed : 1073 Mbps
MTU : 1500
In octets : 0
```

Out octets : 0

Interface : [up] WAN Miniport (IP)—QoS Packet Scheduler—0000
Id : 18
Mac Address : d6:b9:20:52:41:53
Type : ethernet—csmacd
Speed : 1073 Mbps
MTU : 1500
In octets : 0
Out octets : 0

Interface : [up] WAN Miniport (Network Monitor)—QoS Packet Scheduler—0000
Id : 19
Mac Address : d6:b9:20:52:41:53
Type : ethernet—csmacd
Speed : 1073 Mbps
MTU : 1500
In octets : 0
Out octets : 0

[*] Network IP:

Id	IP Address	Netmask	Broadcast
1	127.0.0.1	255.0.0.0	1
11	172.20.11.2	255.255.255.0	1

[*] Routing information:

Destination	Next hop	Mask	Metric
127.0.0.0	127.0.0.1	255.0.0.0	306
127.0.0.1	127.0.0.1	255.255.255.255	306
127.255.255.255	127.0.0.1	255.255.255.255	306
172.20.11.0	172.20.11.2	255.255.255.0	266
172.20.11.2	172.20.11.2	255.255.255.255	266
172.20.11.255	172.20.11.2	255.255.255.255	266
224.0.0.0	127.0.0.1	240.0.0.0	306
255.255.255.255	127.0.0.1	255.255.255.255	306

[*] TCP connections and listening ports:

Local address	Local port	Remote address	Remote port	State
0.0.0.0	22	0.0.0.0	0	listen
0.0.0.0	135	0.0.0.0	0	listen
0.0.0.0	3306	0.0.0.0	0	listen
0.0.0.0	3389	0.0.0.0	0	listen
0.0.0.0	8009	0.0.0.0	0	listen
0.0.0.0	8019	0.0.0.0	0	listen
0.0.0.0	8020	0.0.0.0	0	listen
0.0.0.0	8022	0.0.0.0	0	listen
0.0.0.0	8027	0.0.0.0	0	listen
0.0.0.0	8028	0.0.0.0	0	listen
0.0.0.0	8031	0.0.0.0	0	listen
0.0.0.0	8032	0.0.0.0	0	listen

0.0.0.0 8282 0.0.0.0 0 listen
0.0.0.0 8383 0.0.0.0 0 listen
0.0.0.0 8443 0.0.0.0 0 listen
0.0.0.0 8444 0.0.0.0 0 listen
0.0.0.0 8585 0.0.0.0 0 listen
0.0.0.0 49152 0.0.0.0 0 listen
0.0.0.0 49153 0.0.0.0 0 listen
0.0.0.0 49154 0.0.0.0 0 listen
0.0.0.0 49159 0.0.0.0 0 listen
0.0.0.0 49166 0.0.0.0 0 listen
0.0.0.0 49206 0.0.0.0 0 listen
127.0.0.1 8005 0.0.0.0 0 listen
127.0.0.1 8028 127.0.0.1 49274 established
127.0.0.1 8028 127.0.0.1 49282 established
127.0.0.1 8028 127.0.0.1 49306 established
127.0.0.1 8028 127.0.0.1 49307 established
127.0.0.1 8028 127.0.0.1 49308 established
127.0.0.1 8028 127.0.0.1 49309 established
127.0.0.1 8028 127.0.0.1 49310 established
127.0.0.1 8028 127.0.0.1 49311 established
127.0.0.1 8028 127.0.0.1 49312 established
127.0.0.1 8028 127.0.0.1 49313 established
127.0.0.1 8028 127.0.0.1 49314 established
127.0.0.1 8028 127.0.0.1 49315 established
127.0.0.1 8028 127.0.0.1 49316 established
127.0.0.1 31000 127.0.0.1 32000 established
127.0.0.1 32000 0.0.0.0 0 listen
127.0.0.1 32000 127.0.0.1 31000 established
127.0.0.1 49157 127.0.0.1 49158 established
127.0.0.1 49158 127.0.0.1 49157 established
127.0.0.1 49160 127.0.0.1 49161 established
127.0.0.1 49161 127.0.0.1 49160 established
127.0.0.1 49162 127.0.0.1 49163 established
127.0.0.1 49163 127.0.0.1 49162 established
127.0.0.1 49164 127.0.0.1 49165 established
127.0.0.1 49165 127.0.0.1 49164 established
127.0.0.1 49167 127.0.0.1 49168 established
127.0.0.1 49168 127.0.0.1 49167 established
127.0.0.1 49169 127.0.0.1 49170 established
127.0.0.1 49170 127.0.0.1 49169 established
127.0.0.1 49171 127.0.0.1 49172 established
127.0.0.1 49172 127.0.0.1 49171 established
127.0.0.1 49173 127.0.0.1 49174 established
127.0.0.1 49174 127.0.0.1 49173 established
127.0.0.1 49175 127.0.0.1 49176 established
127.0.0.1 49176 127.0.0.1 49175 established
127.0.0.1 49177 127.0.0.1 49178 established
127.0.0.1 49178 127.0.0.1 49177 established
127.0.0.1 49195 127.0.0.1 49196 established
127.0.0.1 49196 127.0.0.1 49195 established
127.0.0.1 49197 127.0.0.1 49198 established
127.0.0.1 49198 127.0.0.1 49197 established
127.0.0.1 49199 127.0.0.1 49200 established
127.0.0.1 49200 127.0.0.1 49199 established

127.0.0.1 49201 127.0.0.1 49202 established
127.0.0.1 49202 127.0.0.1 49201 established
127.0.0.1 49203 127.0.0.1 49204 established
127.0.0.1 49204 127.0.0.1 49203 established
127.0.0.1 49210 127.0.0.1 49211 established
127.0.0.1 49211 127.0.0.1 49210 established
127.0.0.1 49212 127.0.0.1 49213 established
127.0.0.1 49213 127.0.0.1 49212 established
127.0.0.1 49214 127.0.0.1 49215 established
127.0.0.1 49215 127.0.0.1 49214 established
127.0.0.1 49216 127.0.0.1 49217 established
127.0.0.1 49217 127.0.0.1 49216 established
127.0.0.1 49218 127.0.0.1 49219 established
127.0.0.1 49219 127.0.0.1 49218 established
127.0.0.1 49220 127.0.0.1 49221 established
127.0.0.1 49221 127.0.0.1 49220 established
127.0.0.1 49222 127.0.0.1 49223 established
127.0.0.1 49223 127.0.0.1 49222 established
127.0.0.1 49224 127.0.0.1 49225 established
127.0.0.1 49225 127.0.0.1 49224 established
127.0.0.1 49226 127.0.0.1 49227 established
127.0.0.1 49227 127.0.0.1 49226 established
127.0.0.1 49229 127.0.0.1 49230 established
127.0.0.1 49230 127.0.0.1 49229 established
127.0.0.1 49231 127.0.0.1 49232 established
127.0.0.1 49232 127.0.0.1 49231 established
127.0.0.1 49233 127.0.0.1 49234 established
127.0.0.1 49234 127.0.0.1 49233 established
127.0.0.1 49235 127.0.0.1 49236 established
127.0.0.1 49236 127.0.0.1 49235 established
127.0.0.1 49237 127.0.0.1 49238 established
127.0.0.1 49238 127.0.0.1 49237 established
127.0.0.1 49239 127.0.0.1 49240 established
127.0.0.1 49240 127.0.0.1 49239 established
127.0.0.1 49241 127.0.0.1 49242 established
127.0.0.1 49242 127.0.0.1 49241 established
127.0.0.1 49243 127.0.0.1 49244 established
127.0.0.1 49244 127.0.0.1 49243 established
127.0.0.1 49247 127.0.0.1 49248 established
127.0.0.1 49248 127.0.0.1 49247 established
127.0.0.1 49249 127.0.0.1 49250 established
127.0.0.1 49250 127.0.0.1 49249 established
127.0.0.1 49251 127.0.0.1 49252 established
127.0.0.1 49252 127.0.0.1 49251 established
127.0.0.1 49253 127.0.0.1 49254 established
127.0.0.1 49254 127.0.0.1 49253 established
127.0.0.1 49255 127.0.0.1 49256 established
127.0.0.1 49256 127.0.0.1 49255 established
127.0.0.1 49257 127.0.0.1 49258 established
127.0.0.1 49258 127.0.0.1 49257 established
127.0.0.1 49262 127.0.0.1 49263 established
127.0.0.1 49263 127.0.0.1 49262 established
127.0.0.1 49264 127.0.0.1 49265 established
127.0.0.1 49265 127.0.0.1 49264 established

127.0.0.1 49266 127.0.0.1 49267 established
127.0.0.1 49267 127.0.0.1 49266 established
127.0.0.1 49268 127.0.0.1 49269 established
127.0.0.1 49269 127.0.0.1 49268 established
127.0.0.1 49274 127.0.0.1 8028 established
127.0.0.1 49276 127.0.0.1 49277 established
127.0.0.1 49277 127.0.0.1 49276 established
127.0.0.1 49278 127.0.0.1 49279 established
127.0.0.1 49279 127.0.0.1 49278 established
127.0.0.1 49280 127.0.0.1 49281 established
127.0.0.1 49281 127.0.0.1 49280 established
127.0.0.1 49282 127.0.0.1 8028 established
127.0.0.1 49306 127.0.0.1 8028 established
127.0.0.1 49307 127.0.0.1 8028 established
127.0.0.1 49308 127.0.0.1 8028 established
127.0.0.1 49309 127.0.0.1 8028 established
127.0.0.1 49310 127.0.0.1 8028 established
127.0.0.1 49311 127.0.0.1 8028 established
127.0.0.1 49312 127.0.0.1 8028 established
127.0.0.1 49313 127.0.0.1 8028 established
127.0.0.1 49314 127.0.0.1 8028 established
127.0.0.1 49315 127.0.0.1 8028 established
127.0.0.1 49316 127.0.0.1 8028 established
172.20.11.2 139 0.0.0.0 0 listen
172.20.11.2 9300 172.20.11.2 49182 established
172.20.11.2 9300 172.20.11.2 49183 established
172.20.11.2 9300 172.20.11.2 49184 established
172.20.11.2 9300 172.20.11.2 49185 established
172.20.11.2 9300 172.20.11.2 49186 established
172.20.11.2 9300 172.20.11.2 49187 established
172.20.11.2 9300 172.20.11.2 49188 established
172.20.11.2 9300 172.20.11.2 49189 established
172.20.11.2 9300 172.20.11.2 49190 established
172.20.11.2 9300 172.20.11.2 49191 established
172.20.11.2 9300 172.20.11.2 49192 established
172.20.11.2 9300 172.20.11.2 49193 established
172.20.11.2 9300 172.20.11.2 49194 established
172.20.11.2 49182 172.20.11.2 9300 established
172.20.11.2 49183 172.20.11.2 9300 established
172.20.11.2 49184 172.20.11.2 9300 established
172.20.11.2 49185 172.20.11.2 9300 established
172.20.11.2 49186 172.20.11.2 9300 established
172.20.11.2 49187 172.20.11.2 9300 established
172.20.11.2 49188 172.20.11.2 9300 established
172.20.11.2 49189 172.20.11.2 9300 established
172.20.11.2 49190 172.20.11.2 9300 established
172.20.11.2 49191 172.20.11.2 9300 established
172.20.11.2 49192 172.20.11.2 9300 established
172.20.11.2 49193 172.20.11.2 9300 established
172.20.11.2 49194 172.20.11.2 9300 established

[*] Listening UDP ports:

Local address Local port

0.0.0.0 161
0.0.0.0 500
0.0.0.0 4500
0.0.0.0 5353
0.0.0.0 5355
0.0.0.0 33848
0.0.0.0 54328
127.0.0.1 59767
172.20.11.2 137
172.20.11.2 138

[*] Network services:

Index	Name
0	jmx
1	Power
2	Server
3	jenkins
4	IP Helper
5	DNS Client
6	wampapache
7	wampmysqld
8	DHCP Client
9	Workstation
10	SNMP Service
11	Plug and Play
12	Print Spooler
13	OpenSSH Server
14	Task Scheduler
15	Windows Update
16	Remote Registry
17	Windows Firewall
18	COM+ Event System
19	Windows Event Log
20	IPsec Policy Agent
21	Group Policy Client
22	RPC Endpoint Mapper
23	Software Protection
24	Network List Service
25	User Profile Service
26	Base Filtering Engine
27	Microsoft FTP Service
28	TCP/IP NetBIOS Helper
29	Cryptographic Services
30	Certificate Propagation
31	Remote Desktop Services
32	SPP Notification Service
33	domain1 GlassFish Server
34	Apache Tomcat 8.0 Tomcat8
35	Diagnostic Policy Service
36	Security Accounts Manager
37	Network Location Awareness
38	Windows Font Cache Service
39	Remote Procedure Call (RPC)

40 DCOM Server Process Launcher
41 Remote Desktop Configuration
42 MEDC Server Component – Apache
43 Application Host Helper Service
44 Network Store Interface Service
45 Distributed Link Tracking Client
46 System Event Notification Service
47 World Wide Web Publishing Service
48 VirtualBox Guest Additions Service
49 Windows Management Instrumentation
50 Windows Process Activation Service
51 Distributed Transaction Coordinator
52 IKE and AuthIP IPsec Keying Modules
53 ManageEngine Desktop Central Server
54 Windows Licensing Monitoring Service
55 Desktop Window Manager Session Manager
56 Windows Remote Management (WS–Management)
57 MEDC Server Component – Notification Server
58 Elasticsearch 1.1.1 (elasticsearch–service–x64)
59 Remote Desktop Services UserMode Port Redirector

[*] Processes:

Id	Status	Name	Path	Parameters
1	running	System Idle Process		
4	running	System		
252	running	smss.exe	\SystemRoot\System32\	
276	running	svchost.exe		
324	running	csrss.exe	%SystemRoot%\system32\	ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:User
376	running	wininit.exe		
384	running	csrss.exe	%SystemRoot%\system32\	ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:User
412	running	winlogon.exe		
472	running	services.exe	C:\Windows\system32\	
480	running	lsass.exe	C:\Windows\system32\	
488	running	lsm.exe	C:\Windows\system32\	
588	running	svchost.exe		
648	running	VBoxService.exe	C:\Windows\System32\	
716	running	svchost.exe		
792	running	LogonUI.exe	/flags:0x0	
800	running	svchost.exe		
848	running	svchost.exe		
904	running	svchost.exe		
936	running	postgres.exe	--forkbackend" "9144"	
956	running	svchost.exe		
1000	running	svchost.exe		
1148	running	spoolsv.exe		
1176	running	postgres.exe	--forkbackend" "9144"	
1192	running	svchost.exe		
1224	running	wrapper.exe		
1248	running	postgres.exe	--forkbackend" "9144"	

1316 running conhost.exe \??\C:\Windows\system32\
1332 running domain1Service.exe
1376 running cygrunsrv.exe C:\Program Files\OpenSSH\bin\
1396 running elasticsearch—service—x64.exe C:\Program Files\elasticsearch—1.1.1\bin
 \ //RS//elasticsearch—service—x64
1404 running conhost.exe \??\C:\Windows\system32\
1436 running svchost.exe
1460 running jenkins.exe
1516 running cmd.exe /c ""C:/glassfish/glassfish4/glassfish/lib/nadmin.bat" start—
 domain --watchdog --domaindir C:\\glassfish\\glassfish4\\glassfish
1524 running conhost.exe \??\C:\Windows\system32\
1540 running cmd.exe C:\Windows\system32\ /c "C:\Program Files\jmx\start.jmx.
bat"
1580 running java.exe —jar "C:\glassfish\glassfish4\glassfish\lib\..\modules\admin—
cli.jar" start—domain --watchdog --domaindir C:\\glassfish\\glassf
1588 running java.exe
1616 running conhost.exe \??\C:\Windows\system32\
1620 running java.exe C:\openjdk6\openjdk—1.6.0—unofficial—b27—windows—amd64\
 jre\bin\ —Dcom.sun.management.jmxremote —Dcom.sun.management.
 jmxremote.port=1617 —Dcom.sun.management.jmxremote.authenticate=false —
 Dco
1816 running jmx.exe
1832 running conhost.exe \??\C:\Windows\system32\
1896 running dcnotificationserver.exe
1956 running dcserverhttpd.exe
2096 running svchost.exe
2116 running snmp.exe C:\Windows\System32\
2124 running conhost.exe \??\C:\Windows\system32\
2160 running sshd.exe C:\Program Files\OpenSSH\usr\sbin\
2172 running drotatelogs.exe C:\ManageEngine\DesktopCentral_Server\apache\bin\
 —l C:/ManageEngine/DesktopCentral_Server/logs/apache_errorlog_%Y-%m-%d
 -%H.%M.txt 5M
2184 running conhost.exe \??\C:\Windows\system32\
2208 running tomcat8.exe C:\Program Files\Apache Software Foundation\tomcat\
 apache—tomcat—8.0.33\bin\ //RS//Tomcat8
2216 running conhost.exe \??\C:\Windows\system32\
2268 running dcserverhttpd.exe C:\ManageEngine\DesktopCentral_Server\apache\bin
 \ —d C:/ManageEngine/DesktopCentral_Server/apache
2332 running httpd.exe
2348 running java.exe
2428 running conhost.exe \??\C:\Windows\system32\
2484 running drotatelogs.exe C:\ManageEngine\DesktopCentral_Server\apache\bin\
 —l C:/ManageEngine/DesktopCentral_Server/logs/apache_errorlog_%Y-%m-%d
 -%H.%M.txt 5M
2492 running conhost.exe \??\C:\Windows\system32\
2560 running mysqld.exe c:\wamp\bin\mysql\mysql5.5.20\bin\ wampmysqld
3304 running httpd.exe C:\wamp\bin\apache\apache2.2.21\bin\ —d C:/wamp/bin/
 apache/Apache2.2.21
3612 running svchost.exe C:\Windows\system32\ —k iissvcs
3668 running wlms.exe C:\Windows\system32\wlms\
3696 running postgres.exe "--forkbackend" "9108"
3976 running conhost.exe \??\C:\Windows\system32\
4100 running java.exe C:\Program Files (x86)\Common Files\Oracle\Java\javapath\
 —jar "C:\Program Files\jenkins.war" —httpPort=8484

```
4108 running cmd.exe /C ""C:/ManageEngine/DesktopCentral_Server/pgsql/bin/
    postgres.exe" -D "C:/ManageEngine/DesktopCentral_Server/pgsql/data" -
    p8028
4156 running postgres.exe -D "C:/ManageEngine/DesktopCentral_Server/pgsql/data"
    -p8028
4216 running sppsvc.exe
4224 running postgres.exe "--forklog" "9284" "9288"
4440 running svchost.exe
4456 running postgres.exe "--forkboot" "9156" "-x4"
4464 running postgres.exe "--forkboot" "9140" "-x3"
4472 running postgres.exe "--forkboot" "9156" "-x5"
4480 running postgres.exe "--forkavlauncher" "9140"
4488 running postgres.exe "--forkarch" "9156"
4496 running postgres.exe "--forkcol" "9140"
4632 running postgres.exe "--forkbackend" "9140"
4640 running postgres.exe "--forkbackend" "9108"
4660 running svchost.exe
4956 running postgres.exe "--forkbackend" "9120"
5592 running postgres.exe "--forkbackend" "9144"
5656 running msdtc.exe
5688 running svchost.exe
5728 running postgres.exe "--forkbackend" "9144"
5944 running postgres.exe "--forkbackend" "9140"
5960 running postgres.exe "--forkbackend" "9108"
6036 running postgres.exe "--forkbackend" "9140"
6136 running postgres.exe "--forkbackend" "9140"
```

[*] Storage information:

Description : ["C:\\ Label:Windows 2008R2 Serial Number 807fea50"]
Device id : [#<SNMP::Integer:0x000055c984a733e0 @value=1>]

Filesystem **type** : ["unknown"]

Device unit : [#<SNMP::Integer:0x000055c984a71180 @value=4096>]

Memory size : 60.00 GB

Memory used : 15.61 GB

Description : ["Virtual Memory"]

Device id : [#<SNMP::Integer:0x000055c984a5f138 @value=2>]

Filesystem **type** : ["unknown"]

Device unit : [#<SNMP::Integer:0x000055c984a5ce88 @value=65536>]

Memory size : 4.00 GB

Memory used : 3.40 GB

Description : ["Physical Memory"]

Device id : [#<SNMP::Integer:0x000055c9848b2bf0 @value=3>]

Filesystem **type** : ["unknown"]

Device unit : [#<SNMP::Integer:0x000055c98488fb78 @value=65536>]

Memory size : 2.00 GB

Memory used : 1.54 GB

[*] File system information:

Index : 1

Mount point :
Remote mount point : –
Access : 1
Bootable : 1

[*] Device information:

Id	Type	Status	Descr
1	unknown	running	Unknown Processor Type
2	unknown	running	Unknown Processor Type
3	unknown	unknown	Software Loopback Interface 1
4	unknown	unknown	WAN Miniport (SSTP)
5	unknown	unknown	WAN Miniport (L2TP)
6	unknown	unknown	WAN Miniport (PPTP)
7	unknown	unknown	WAN Miniport (PPPOE)
8	unknown	unknown	WAN Miniport (IPv6)
9	unknown	unknown	WAN Miniport (Network Monitor)
10	unknown	unknown	WAN Miniport (IP)
11	unknown	unknown	RAS Async Adapter
12	unknown	unknown	WAN Miniport (IKEv2)
13	unknown	unknown	Intel(R) PRO/1000 MT Desktop Adapter
14	unknown	unknown	Microsoft ISATAP Adapter
15	unknown	unknown	Microsoft ISATAP Adapter #2
16	unknown	unknown	Intel(R) PRO/1000 MT Desktop Adapter #2
17	unknown	unknown	Intel(R) PRO/1000 MT Desktop Adapter—QoS Packet Scheduler—0000
18	unknown	unknown	Intel(R) PRO/1000 MT Desktop Adapter—WFP Lightweight Filter—0000
19	unknown	unknown	WAN Miniport (IPv6)—QoS Packet Scheduler—0000
20	unknown	unknown	WAN Miniport (IP)—QoS Packet Scheduler—0000
21	unknown	unknown	WAN Miniport (Network Monitor)—QoS Packet Scheduler—0000
22	unknown	running	Fixed Disk
23	unknown	running	IBM enhanced (101—or 102—key) keyboard, Subtype=(0)

[*] Software components:

Index	Name
1	7-Zip 19.00 (x64)
2	OpenSSH for Windows 7.1p1—1 (remove only)
3	Oracle VM VirtualBox Guest Additions 6.0.8
4	Java 8 Update 251 (64-bit)
5	Microsoft Visual C++ 2008 Redistributable — x64 9.0.30729.6161
6	Java SE Development Kit 8 Update 211 (64-bit)
7	Microsoft .NET Framework 4.5.1
8	Microsoft .NET Framework 4.5.1

[*] IIS server information:

TotalBytesSentLowWord : 0
TotalBytesReceivedLowWord : 0
TotalFilesSent : 0
CurrentAnonymousUsers : 0
CurrentNonAnonymousUsers : 0

TotalAnonymousUsers : 0
TotalNonAnonymousUsers : 0
MaxAnonymousUsers : 0
MaxNonAnonymousUsers : 0
CurrentConnections : 0
MaxConnections : 0
ConnectionAttempts : 0
LogonAttempts : 0
Gets : 0
Posts : 0
Heads : 0
Others : 0
CGIRequests : 0
BGIRequests : 0
NotFoundErrors : 0
