Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Blue – Eike G. Barbosa

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Blue – Eike G. Barbosa |
| **N° Revisão** | 1 |
| **Data de publicação** | 17/10/2024 |
| **Link** | https://tryhackme.com/r/room/blue |

|  |  |  |
| --- | --- | --- |
| **Redação** | Eike G. Barbosa | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | DD/MM/AAAA | Produção |
| **1** | 22/10/2024 | Revisão |
| **2** | DD/MM/AAAA | Aprovação |
| **3** | 04/11/2024 | 2° Revisão |

**Sumário**

[Contextualização 3](#_heading=h.gjdgxs)

[Desenvolvimento 3](#_heading=h.1fob9te)

[Scan the machine. (If you are unsure how to tackle this, I recommend checking out the Nmap room) 3](#_heading=h.3znysh7)

[How many ports are open with a port number under 1000? 3](#_heading=h.2et92p0)

[What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)](#_heading=h.tyjcwt) 4

[Find the exploitation code we will run against the machine. What is the full path of the code? (Ex: exploit/........)](#_heading=h.3dy6vkm) 4

Show options and set the one required value. What is the name of this value? (Allcaps for submission) 5

If you haven't already, background the previously gained shell (CTRL + Z). Research online how to convert a shell to meterpreter shell in metasploit. What is the name of the post module we will use? (Exact path, similar to the exploit we previously selected) 6

Select this (use MODULE\_PATH). Show options, what option are we required to change? 7

Within our elevated meterpreter shell, run the command 'hashdump'. This will dump all of the passwords on the machine as long as we have the correct privileges to do so. What is the name of the non-default user? 7

Copy this password hash to a file and research how to crack it. What is the cracked password? 8

Flag1? This flag can be found at the system root. 8

Flag2? This flag can be found at the location where passwords are stored within Windows. 8

flag3? This flag can be found in an excellent location to loot. After all, Administrators usually have pretty interesting things saved. 9

[Conclusão](#_heading=h.1t3h5sf) 9

[Referências](#_heading=h.4d34og8) 9

**Contextualização**

Um CTF simples treinar invasão em máquinas Windows e como funciona.

**Desenvolvimento**

**Scan the machine. (If you are unsure how to tackle this, I recommend checking out the Nmap room)**

***Comando usado:*** nmap –sS <ip\_target>

**How many ports are open with a port number under 1000?**

É possível perceber que há 3 portas embaixo da porta 1000, com o comando do nmap, portas essas que são: 135, 149 e 445.

Texto

Descrição gerada automaticamente

**What is this machine vulnerable to? (Answer in the form of: ms??-???, ex: ms08-067)**

Usando um script básico do nmap, é possível ver que a máquina é vulnerável a ms17–010

***Comando usado:*** sudo nmap -sS -Pn -p 445 10.10.100.64 --script smb-vuln-ms17-010.nse

Texto

Descrição gerada automaticamente

**Find the exploitation code we will run against the machine. What is the full path of the code? (Ex: exploit/........)**

Utilizando o Searchsploit para descobrir um exploit com esse código, descobrimos que há várias opções, mas apenas iremos utilizar o Eternal Blue.

***Comando usado:*** searchsploit ms17-010

Tela preta com letras brancas

Descrição gerada automaticamente

**Show options and set the one required value. What is the name of this value? (All caps for submission)**

Agora utilizando o melhor amigo do homen, o Metasploit Framework, vamos tentar criar uma shell para ter acesso.

Comando usado: msfconsole

Primeiro buscamos por eternal blue, então escolhemos o de número 0.

Interface gráfica do usuário, Aplicativo, Site

Descrição gerada automaticamente



Após isso, é necessário a gente saber o que o exploit necessita e mudar tudo o que for preciso.

Texto

Descrição gerada automaticamente



Agora é só rodar o exploit com “run” (Caso haja alguma falha, muda a LPORT para outra, eu recomendo 4445)

**Texto

Descrição gerada automaticamente**

**If you haven't already, background the previously gained shell (CTRL + Z). Research online how to convert a shell to meterpreter shell in metasploit. What is the name of the post module we will use? (Exact path, similar to the exploit we previously selected)**

Agora é preciso achar uma shell para o menterpreter, então vou deixar de backgroud esse exploit e procurar no Metasploit framework.

post/multi/manage/shell\_to\_meterpreter

***Comando usado:*** search shell\_to\_meterpreter

**Select this (use MODULE\_PATH). Show options, what option are we required to change?**

Como da última vez, também precisamos mudar algumas coisas aqui e também colocar o número da sessão , que no caso foi a “1”.ls

**Texto

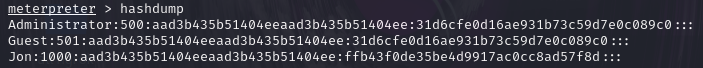
Descrição gerada automaticamente**

**Texto

Descrição gerada automaticamente**

**Within our elevated meterpreter shell, run the command 'hashdump'. This will dump all of the passwords on the machine as long as we have the correct privileges to do so. What is the name of the non-default user?**

Agora como pedido, usamos o comando Hashdump para conseguir a hash do usuário, que no caso é o jon. Com o JohnTheRipper é possível quebrar essa hash.



**Copy this password hash to a file and research how to crack it. What is the cracked password?**

Com o JohnTheRipper é possível quebrar essa hash.

***Comando usado:*** sudo john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt Jon.hash

**Texto

Descrição gerada automaticamente**

**Flag1? This flag can be found at the system root.**

Acessando a raiz do sistema, é possível encontrar a primeira flag que precisamos.

**Texto

Descrição gerada automaticamente com confiança média**

**Flag2? This flag can be found at the location where passwords are stored within Windows.**

O CTF dá uma dica muito valiosa, e com ela podemos achar facilmente o local da segunda

Comando usado: search -f flag2.txt

**Interface gráfica do usuário

Descrição gerada automaticamente com confiança baixa**

**flag3? This flag can be found in an excellent location to loot. After all, Administrators usually have pretty interesting things saved.**

O Apenas procurando nos diretórios do Jon, é possível achar a terceira e última flag.

**Calendário

Descrição gerada automaticamente**

**Conclusão**

O CTF Blue, é muito útil para entender um exemplo de como invadir uma máquina Windows, ele é simples, bem detalhado e fácil de entender.

**Referências**

https://www.exploit-db.com/