Universidade Presbiteriana Mackenzie

Computação Forense

Relatório Técnico Pericial

***Turma J – 1º Semestre***

*Cássio B. Pereira*

*Luzia Aparecida de Moraes*

*Renato Silva*

São Paulo

19 de junho de 2014

Sumário

[Objetivo 3](#_Toc390730295)

[Arquitetura 3](#_Toc390730296)

[Cenário 3](#_Toc390730297)

[Ataque realizado 3](#_Toc390730298)

[Exploit 3](#_Toc390730299)

[Métodos de detecção 4](#_Toc390730300)

[Métodos de remediação 4](#_Toc390730301)

[Conclusão dos ataques 4](#_Toc390730302)

[Impactos 4](#_Toc390730303)

[Furto de dados 4](#_Toc390730304)

[Indisponibilidade 5](#_Toc390730305)

[Conclusões da defesa 5](#_Toc390730306)

[Tempo de detecção 5](#_Toc390730307)

[Análise forense 5](#_Toc390730308)

Relatório Técnico Pericial

# Objetivo

Através de um ambiente de testes, realizar ataques e implementar defesas através de métodos de detecção e remediação, analisando os efeitos e consequências das referidas ações, finalizando com a apresentação dos resultados.

Arquitetura



**VMware-1:** SO-Windows XP Professional SP3

**Rede:**

**Atacante** VMware2 IP: 172.16.10.84.

**Vítima** VMware1 IP: 172.16.10.77

**Conexão** - internet: Bridge

**VMware-2:** SO-Backtrack5 R3

**HOST** IP: 172.16.10.50

# 

# Cenário

Um funcionário terceiro foi contratado na empresa “Turma J”, mal-intencionado e com acesso livre dentro da empresa, consegue obter os IP de computadores da rede facilmente, uma vez que trabalha no departamento de TI da empresa. Ele elabora e executa um ataque a determinada máquina, cujo usuário reporta arquivos estranhos presentes no disco.

# Ataque realizado

## Exploit

Foi criado um exploit através da ferramenta Metasploit contida no Backtrack versão 5 R3, que explorou uma falha em uma dll contida no Windows XP da máquina vítima, denominada “netapi32.dll”. Essa vulnerabilidade, permitiu o acesso e controle da máquina alvo via TCP Reverso.

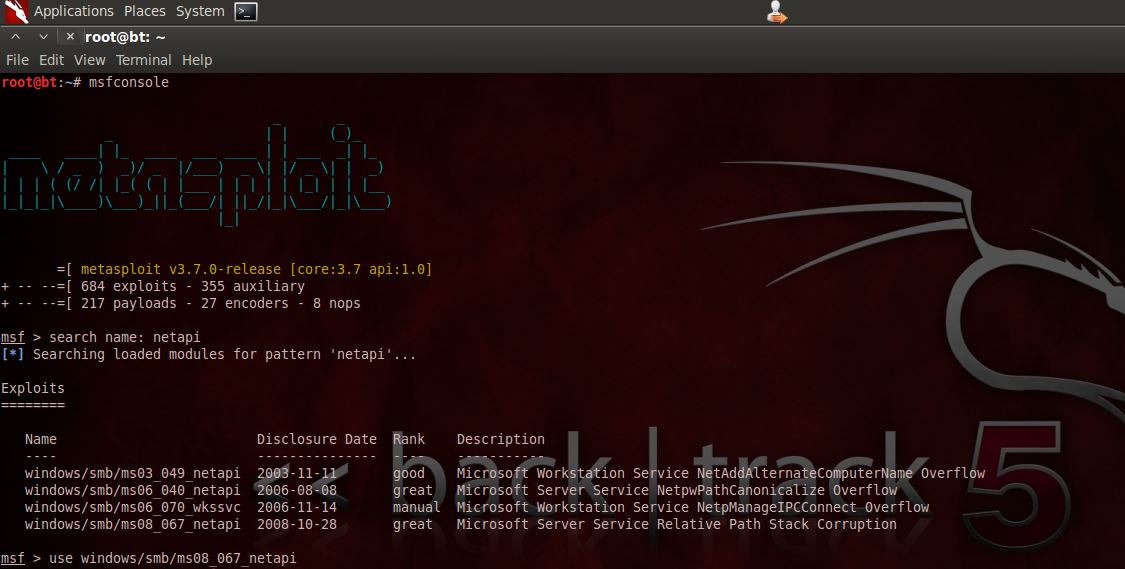


Figura 1- Metasploit - início- seleção do exploit

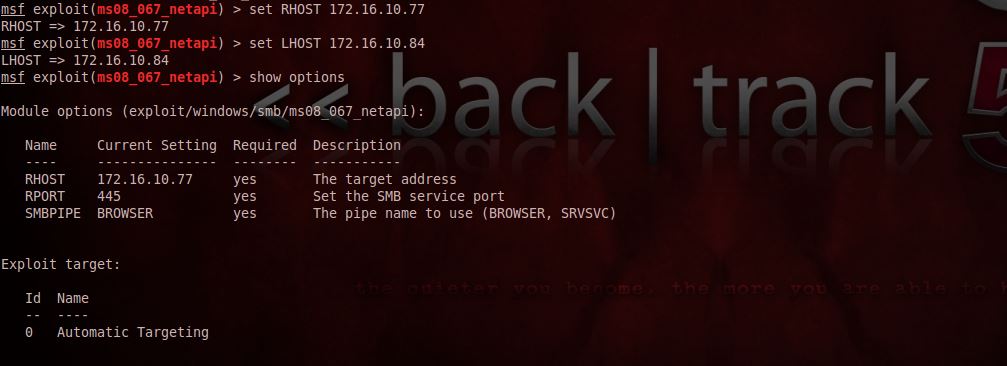


Figura 2- Configuração dos parâmetros

C:\Temp\re prints\Metasploit - configuração do payload.JPG

Figura - Configuração do payload - TCP Reverso



Figura 4- Execução do exploit e acesso a máquina alvo

# Métodos de detecção

O usuário percebeu a presença de um arquivo estranho em sua máquina, conforme caminho a seguir: “C:\Documents and Settings\ UsuarioForense\ ConteudoMaquina.txt”. Após notar essa anomalia, o usuário reportou o problema para a área segurança da empresa, que abriu um processo de análise de incidentes.

# 

# Métodos de remediação

O hacker aproveitou a vulnerabilidade do Windows XP (mais detalhes na página <https://technet.microsoft.com/en-us/library/security/ms08-067.aspx> e http:// cvedetails.com/ cve/ 2008-4250) no processo de Serviço de Servidor, fato que provocou uma varredura e a atualização de todas as máquinas que tinha instalado o referido sistema operacional na versão XP sem o último Service Pack a Hotfix, com objetivo de prevenir problemas futuros do mesmo tipo.

# 

# Conclusão dos ataques

## Impactos

Uma análise detalhada da atividade do exploit criado pode ser vista no link seguinte: (<http://home.mcafee.com/virusinfo/virusprofile.aspx?key=977860#none>), basicamente, o exploit gera uma falha de memória o que permite ao seu criador acesso total a máquina via terminal shell.

Com esse acesso, muitos impactos podem acontecer, dentre eles, o roubo de arquivos, que no nosso cenário era o objetivo do hacker, que gerou um arquivo chamado ConteudoMaquina.txt, que continha todas as informações relevantes para ele sobre aquela máquina como um mapeamento, o que fez o usuário identificar o ataque.

## 

## Furto de dados

Nosso cenário é bem flexível no caso do hacker, no entendimento do grupo muitos arquivos e ou informações podem ter sido coletados após o acesso, visto que a data de criação do arquivo encontrado pelo usuário tinha 3 dias a contar da data de detecção, portanto, o hacker pode ter coletado diversas informações, bem como, feito outros ataques utilizando a máquina vítima.

## 

## Indisponibilidade

Não foi causada indisponibilidade da máquina da vítima.

# 

# Conclusões da defesa

## Tempo de detecção

Pelo cenário proposto, nosso usuário demorou aproximadamente três dias para detectar o incidente e informar a área responsável que, imediatamente, iniciou a análise.

## 

## Análise forense

O time de resposta a incidentes iniciou uma análise na máquina da vítima e encontrou os seguintes artefatos:

* Análise de processos “suspeitos” no Windows, identificado o processo “cmd.exe” como sub-processo do “svchost.exe”, normalmente o cmd.exe é um processo pai e não sub-processo, destacados na figura 5, em vermelho e verde respectivamente;
* Foi feito um dump da memória e enviado ao Vírus Total, identificado como “Exploit.Call4\_Dword\_Xor”, mais detalhes em (http:// home.mcafee.com/ virusinfo/ virusprofile.aspx?key=977860#none), conforme figura 6;
* O vírus é catalogado em um site centralizador de falhas e vulnerabilidades, mais detalhes em (<http://cvedetails.com/cve/2008-4250>);

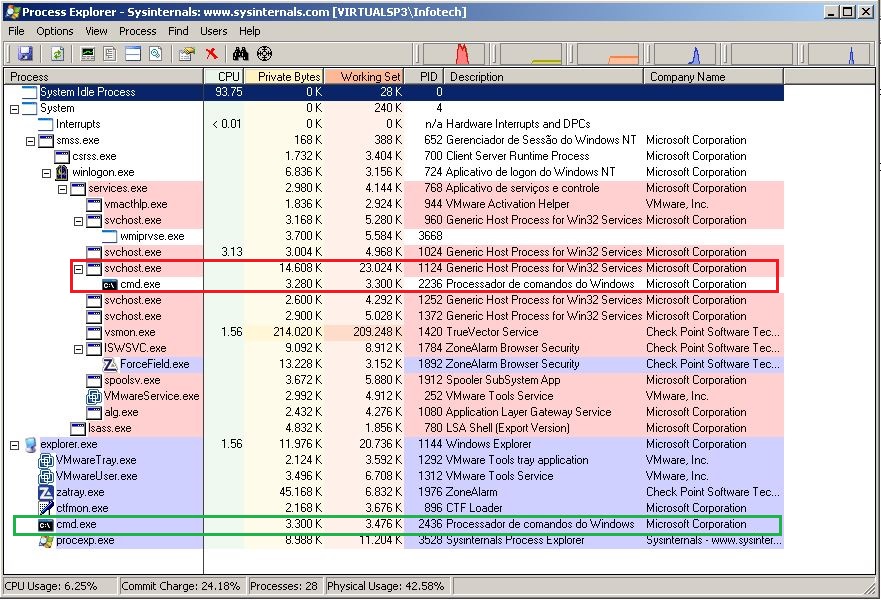


Figura 5- Process Explorer - Processo cmd malicioso e processo cmd do Windows

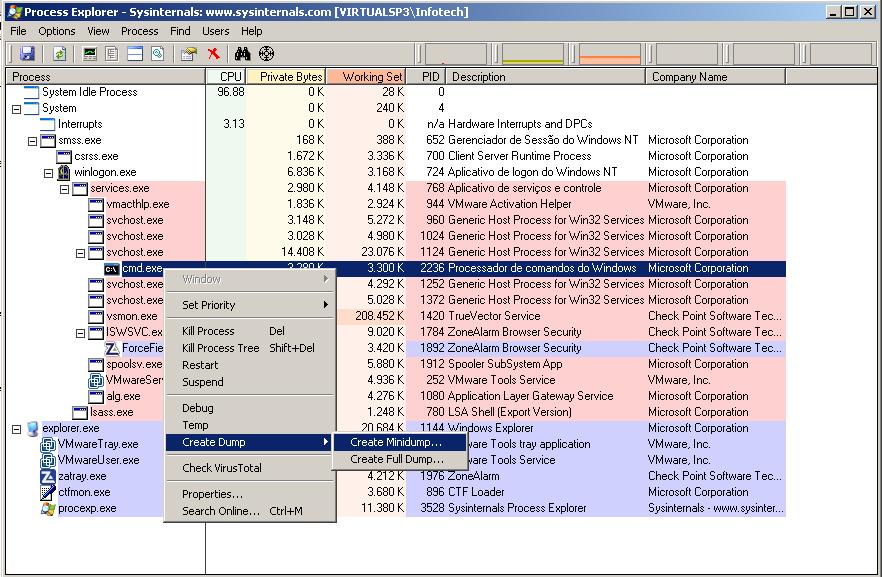


Figura 6- Process Explorer - Criação do dump do processo malicioso.