Exploração

Cassiano Peres

DIO Tech Education Analyst

cassiano-dio

peres-cassiano

Objetivo Geral

Explorar falhas, garantir acesso, executar ações e extrair dados de computadores vulneráveis.

Pré-requisitos

Conhecimento adquirido ao longo da trilha.

Percurso

Etapa 1 Explorando falhas no FTP

Etapa 2 Ataque DoS no RDP

Etapa 3 Explorando falhas no SSH

Percurso

Etapa 4 Adicionando backdoor em um executável

Etapa 1

Explorando falhas no FTP

Introdução

O FTP é um dos métodos de compartilhamento de dados mais antigos e ainda usados.

Introdução

Embora as equipes de TI e os usuários de negócios estejam familiarizados com isso, o FTP carece de muitos requisitos vitais de segurança, conformidade e fluxo de trabalho nas organizações modernas, especialmente em segurança de dados.

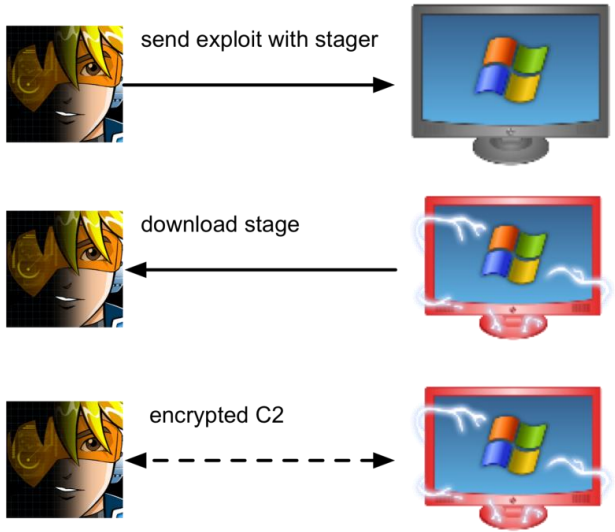
Vulnerabilidades no FTP

- Anonymous authentication;
- Directory traversal attack;
- Cross-site scripting;
- Dridex.

Metasploit

É uma ferramenta utilizaza por cibercriminosos e hackers éticos para investigar vulnerabilidades em redes e servidores.

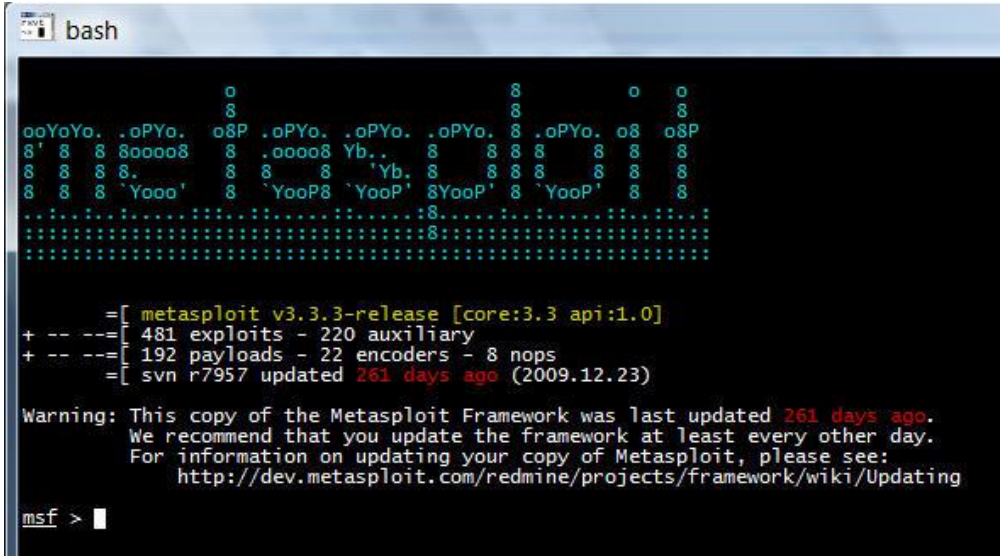
Metasploit



Ferramentas do Metasploit

- **msfconsole**: modo console;
- **msfweb**: Interface gráfica via browser;
- **msfplayload**: gerar e customizar payloads;
- **msfcli**: Interface de automatização de invasão;
- **msflogdump**: exibirá as sessões de arquivos de log.

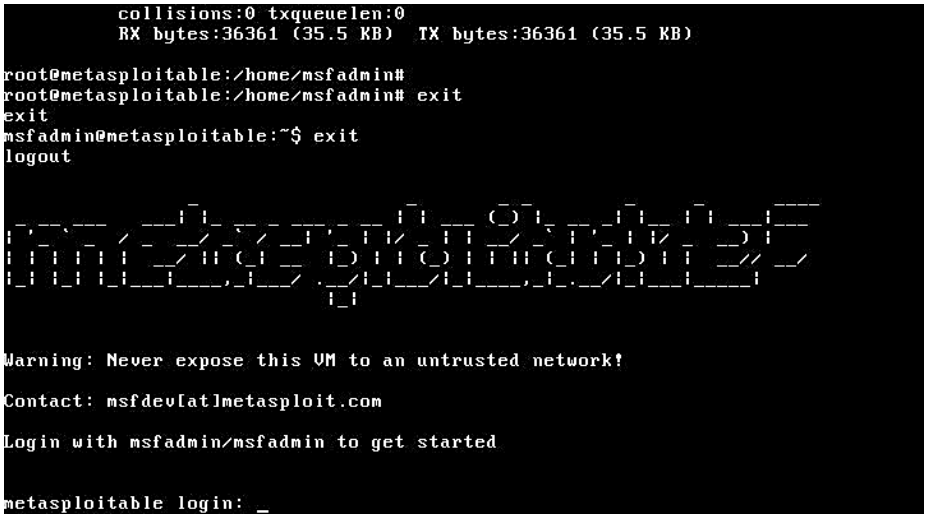
Metasploit


bash
=[metasploit v3.3.3-release [core:3.3 api:1.0]
+ -- --=[481 exploits - 220 auxiliary
+ -- --=[192 payloads - 22 encoders - 8 nops
=[svn r7957 updated 261 days ago (2009.12.23)
Warning: This copy of the Metasploit Framework was last updated 261 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
http://dev.metasploit.com/redmine/projects/framework/wiki/Updating
msf >

Metasploitable

Vamos realizar o ataque contra a máquina VM do Metaspoitable com os serviços vulneráveis.

Metasploitable



Payloads

Módulos para exploit, sendo de três tipos:

- Singles;
- Stagers;
- Stages.

Prática

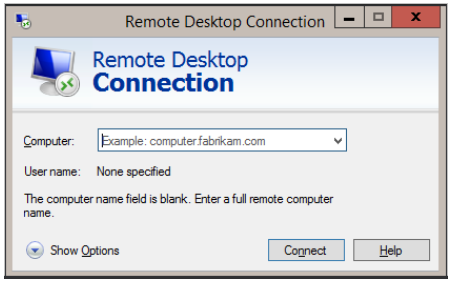
Vamos explorar vulnerabilidades do protocolo FTP com o Metasploit.

Etapa 2

Ataque DoS no RDP

Introdução

RDP é a abreviação de *Remote Desktop* Protocol, sendo uma opção para controlar um sistema de computador remotamente.



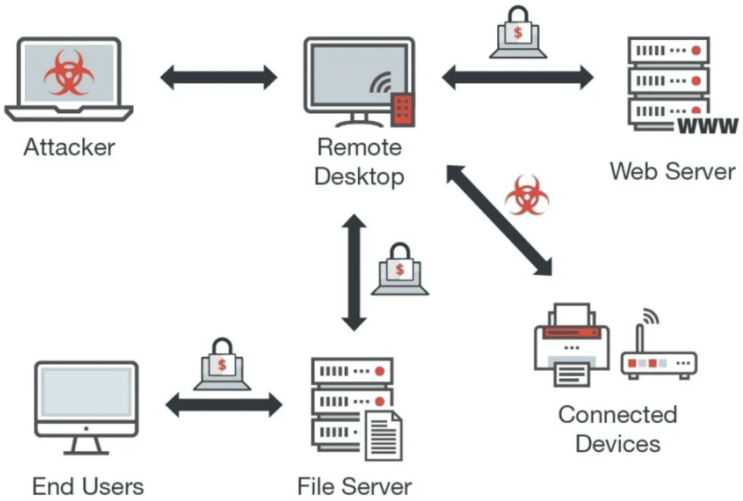
RDP

O serviço RDP pode ser configurado por administradores de sistemas Windows para ser executado em TCP (geralmente na porta 3389) e/ou na porta UDP (3389).

Ataques RDP

Os ataques RDP são tentativas de agentes de ameaças de acessar um host de desktop remoto ou privilégios administrativos do cliente para reconhecimento, comando e controle e movimentação lateral.

Ataques RDP


Attacker
Remote Desktop
Web Server
WWW
Connected Devices
End Users
File Server

Tipos de taques RDP

- Calling Into Robinhood
- SamSam Ransomware

Prevenção

- Autenticação multifator e requisitos complexos de credenciais de acesso
- Estabelecer políticas de bloqueio de conta para tentativas de força bruta;
- Controle de acesso baseado em função (RBAC) para consoles RDP;
- Restrições de acesso RDP baseadas em firewall.

Prática

Vamos simular um ataque em nossa máquina virtual Windows.

Etapa 3

Explorando falhas no SSH

Introdução

Nesta aula vamos abordar as falhas no SSH e explorá-las com o Metasploit.

SSH

O protocolo SSH é utilizado para a comunicação remota entre dispositivos, sendo executado na porta 22.

Metasploit SSH

Utilizaremos o ataque de força bruta com arquivos de usuários e senhas para encontrar credenciais.

Prática

Vamos ao nosso laboratório executar o Metasploit para explorar as vulnerabilidades em uma VM.

Etapa 4

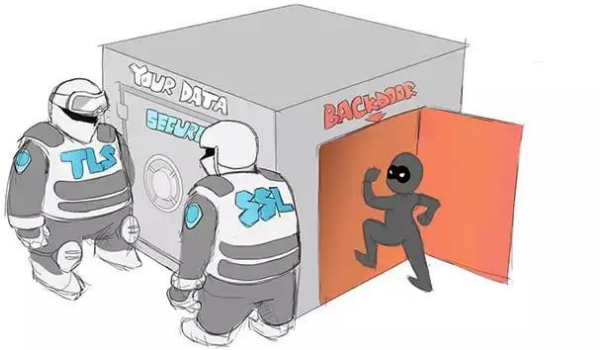
Adicionando backdoor em um executável

Introdução

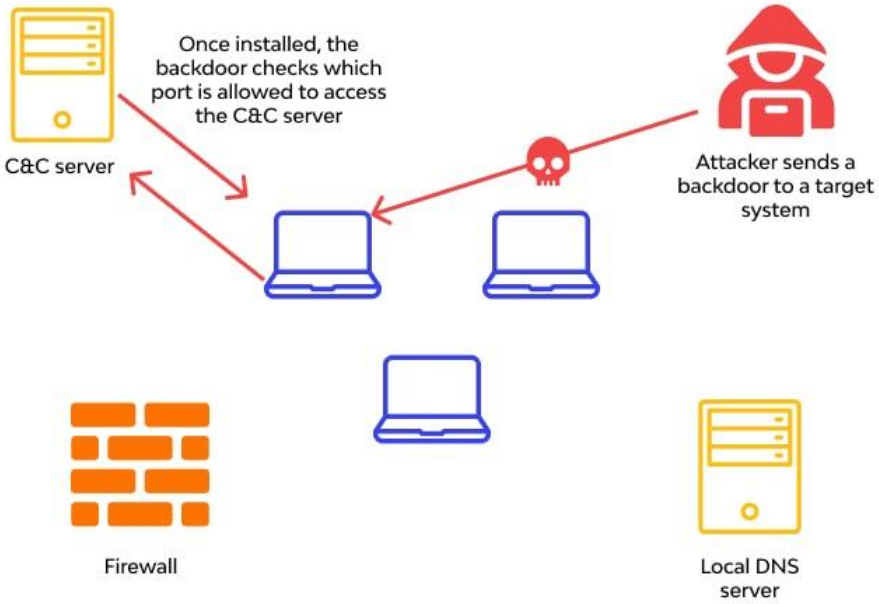
Nesta aula vamos mascarar um backdoor para varredura em um arquivo executável.

Backdoor

É definido como o uso de qualquer malware/vírus/tecnologia para obter acesso não autorizado ao aplicativo/sistema/rede driblando a segurança implementada.



Backdoor


Once installed, the backdoor checks which port is allowed to access the C&C server
C&C server
Attacker sends a backdoor to a target system
Firewall
Local DNS server

Tipos de ataques com backdoor

- Spyware;
- Ransomware;
- DDoS;
- Cryptojacking.

Proteção contra backdoor

- Rotatividade de senhas;
- Monitoramento de atividades da rede;
- Cautela ao instalar programas;
- Antivirus.

Meterpreter

Ou Meta-Interpreter, é um payload que funciona por **injecção dll**.

O meterpreter reside inteiramente na **memória** do anfitrião e não deixa vestígios no disco rígido (o que a torna de difícil detecção nas técnicas forenses).

Prática

Vamos criar um backdoor embarcado em um executável e testar o ataque em uma VM.

Dúvidas?

> Fórum/Artigos

> Comunidade Online (Discord)