Prime

CCS-A

Ataques de Rede – 2

Sistema de Nomes de Domínio (DNS)

Catálogo telefônico para endereçamento, ou CEP para o endereço da pessoa.

O DNS fornece o endereço correto para levar o pacote ao seu destino.

O DNS é um dos principais alvos de invasores;

- Corrompê-lo leva a controlar todos os pacotes.

Sequestro de Domínio

- Ato de alterar o registro de um nome de domínio sem a permissão de seu titular original.
- Pode ter consequências graves.
  - O DNS espalhará automaticamente a localização do domínio falso.
- O proprietário original pode solicitar a correção, mas isso leva algum tempo.
- Pode iniciar com a Engenharia Social e depois trocar o nome de domínio.
- Ou explorar uma vulnerabilidade nas hospedagens do nome de domínio.

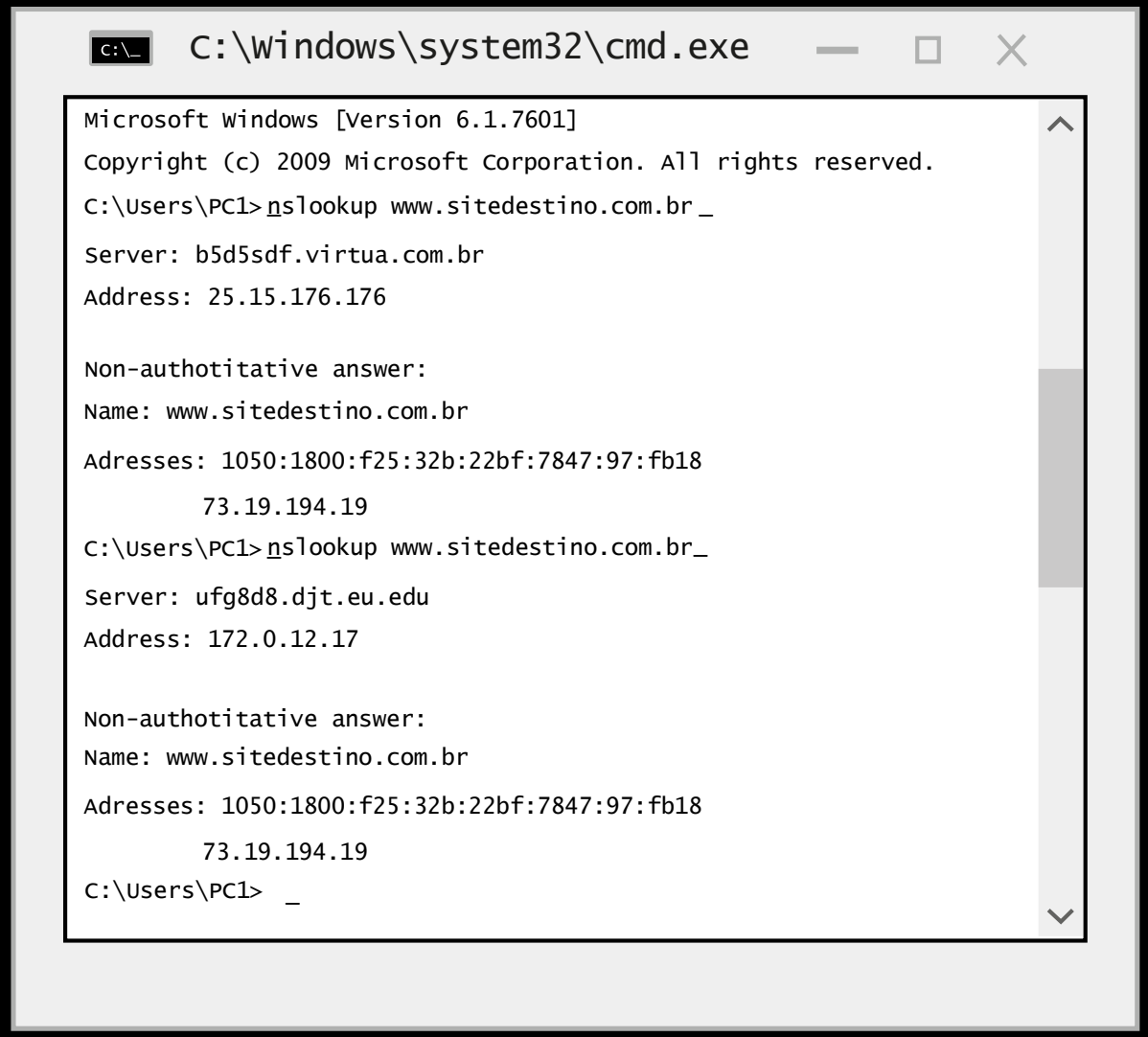
Envenenamento - Poisoning

- É colocar configurações incorretas, propositadamente (ARP e DNS).
- No DNS, é colocar entradas erradas apontando para outro IP.
- Cache DNS é o armazenamento local do histórico dos sites já visitados.
- Alteração local do arquivo hosts.
- Pharming é o termo usado para levar alguém ao site errado, modificando o DNS ou o arquivo hosts.

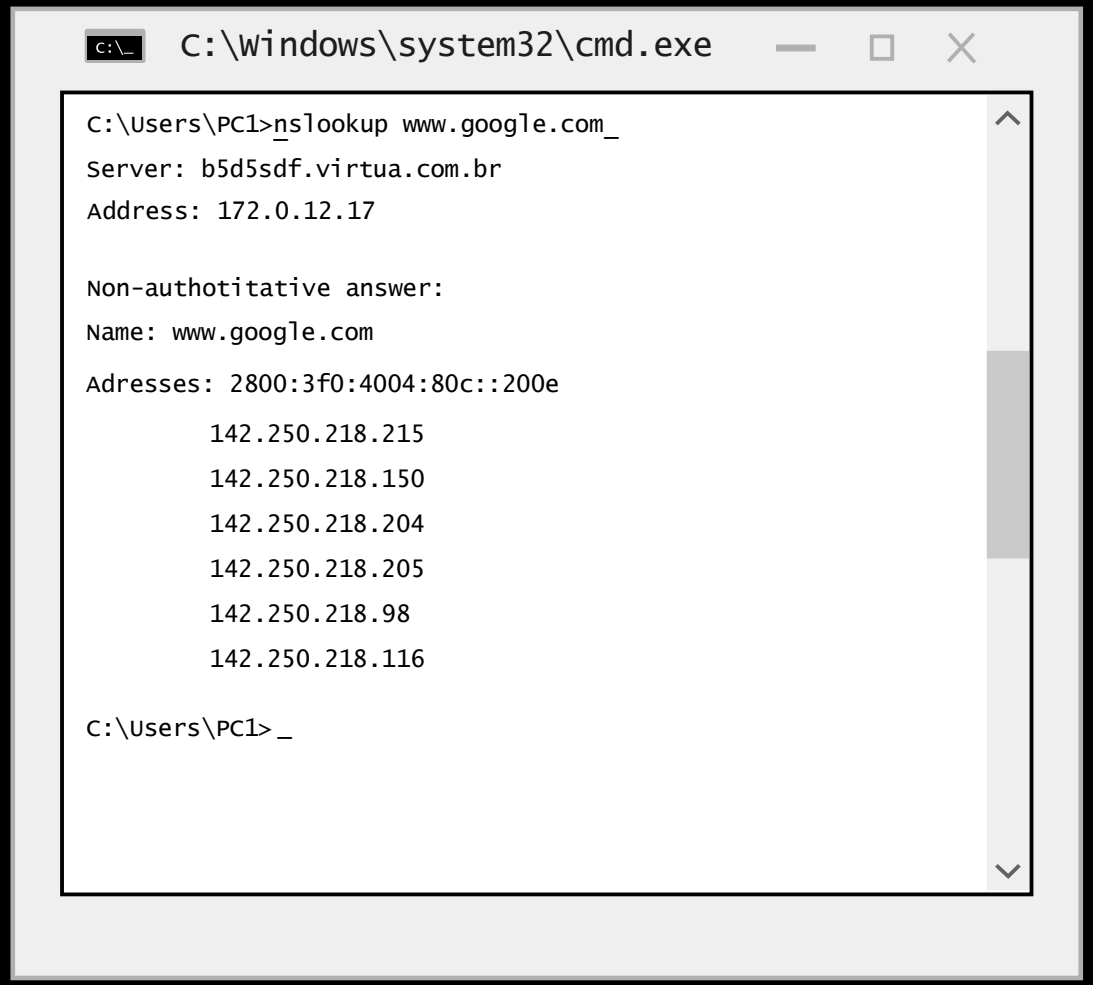
DNS Poisoning

- Um ataque no DNS é extremamente difícil de ser detectado e, na prática, impossível de ser prevenido.
- O DNS é composto por uma hierarquia de servidores master (root) no backbone da Internet e cópias no ISP.
- Roteadores domésticos e a máquinas locais têm um cache DNS (nslookup).
- Envenenar o DNS é uma variante de um vetor de ataque chamado falsificação de DNS.
- Domain Name System Security Extensions (DNSSEC) - Proteção da infraestrutura do DNS com assinatura digital.
  - Os solicitantes podem ter certeza de que as informações que recebem estão corretas.
  - Impedi ataques validando os dados e garantindo a origem das informações.

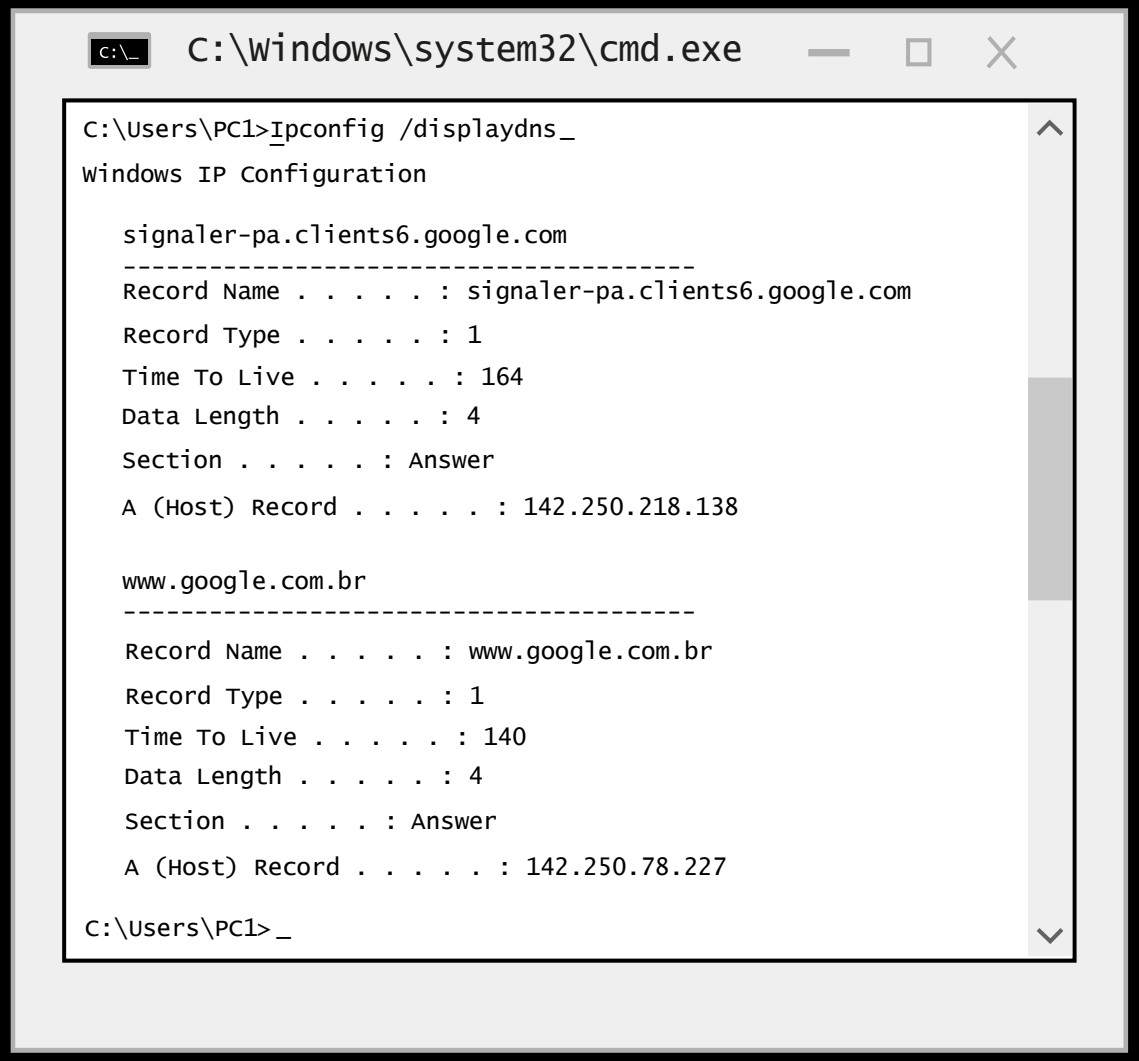
DNS Poisoning



DNS Poisoning

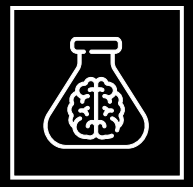


DNS Poisoning



Redirecionamento do Universal Resource Locator (URL)

Redirecionamento de Universal Resource Locator (URL) é um ataque de DNS que envia uma solicitação de nome DNS para um local diferente.



Os engenheiros sociais usam a psicologia e ciência cognitiva para adulterar um endereço.

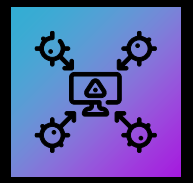
Muitos fornecedores de segurança e de e-mail têm suporte integrado que procura as diferenças entre uma URL adulterada e alerta o usuário.

Reputação do Domínio

Seu endereço IP pode ter uma reputação.

- Se você não protege seu endereço, ele pode ter a reputação prejudicada.

Empresas de segurança rastreiam a origem do spam ou botnet e, se o endereço IP for associado a comportamentos negativos, a reputação cai.



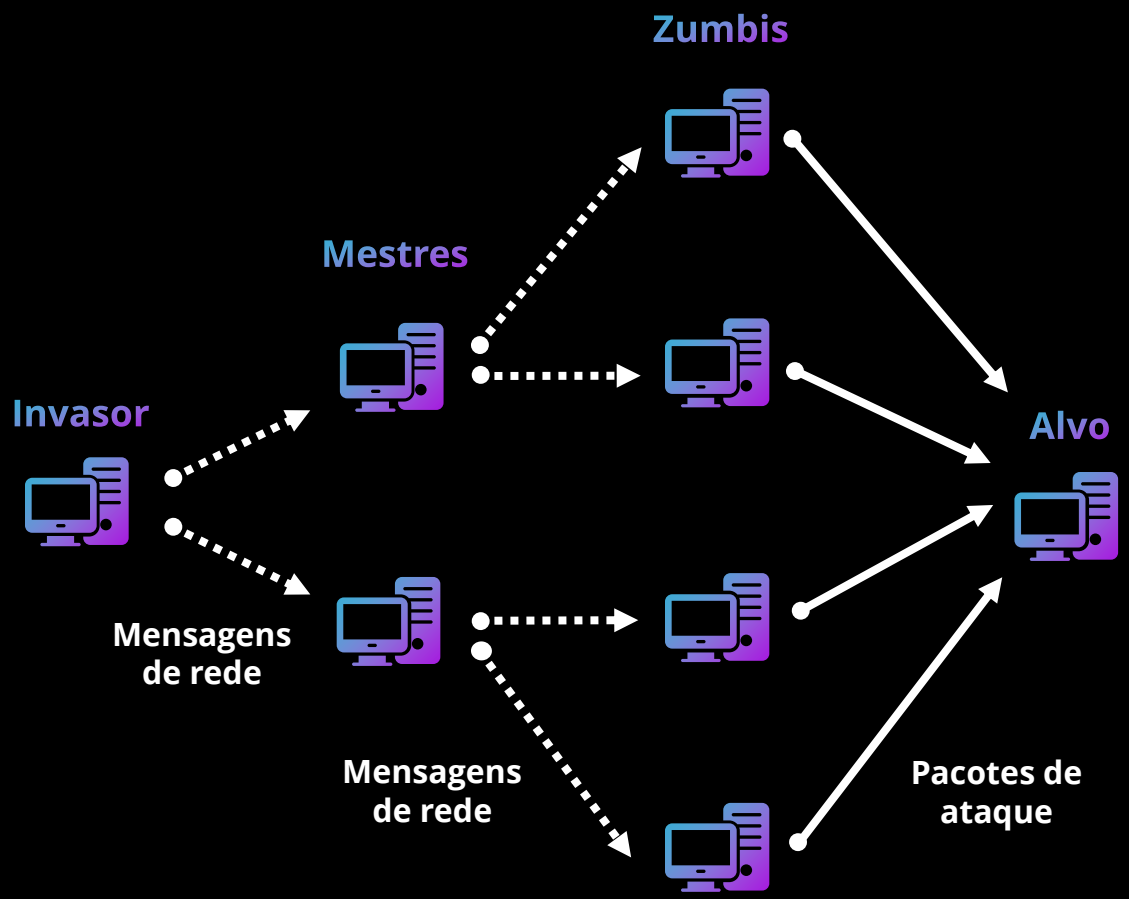
Os atacantes usam esses canais e não se importam com a reputação do seu domínio.

Violar regras contra uma API do Google ou do Amazon Web Services (AWS) pode ocasionar em baixa reputação ou suspensão.

Negação de Serviço Distribuído (DDoS)

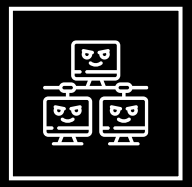
- Ocorre quando o hacker usa vários sistemas para realizar o ataque;
- Etapas:
  - Hacker assume o controle de vários sistemas;
  - Usa esses sistemas para ajudar no ataque.
- Sistemas comprometidos são conhecidos como zumbis.
- O objetivo é deixar os sistemas sobrecarregados e offline, é negar o serviço.
- A criação da rede de ataque pode conter um processo de várias etapas.

Negação de Serviço Distribuído (DDoS)



Proteção Contra DDoS

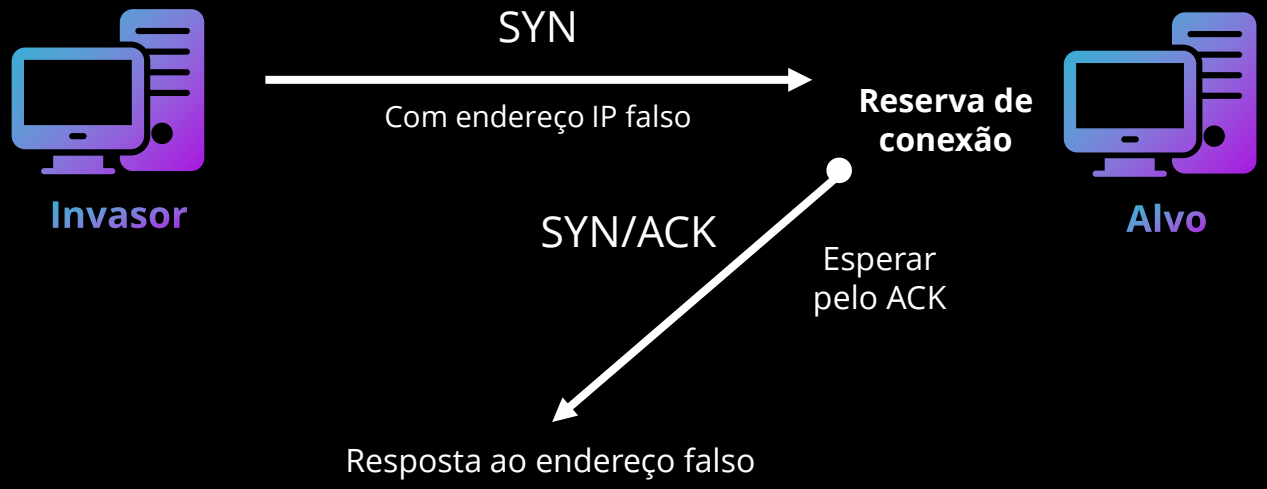
Alteração da opção de tempo limite para conexões TCP. Conexões não utilizadas são descartadas rapidamente.



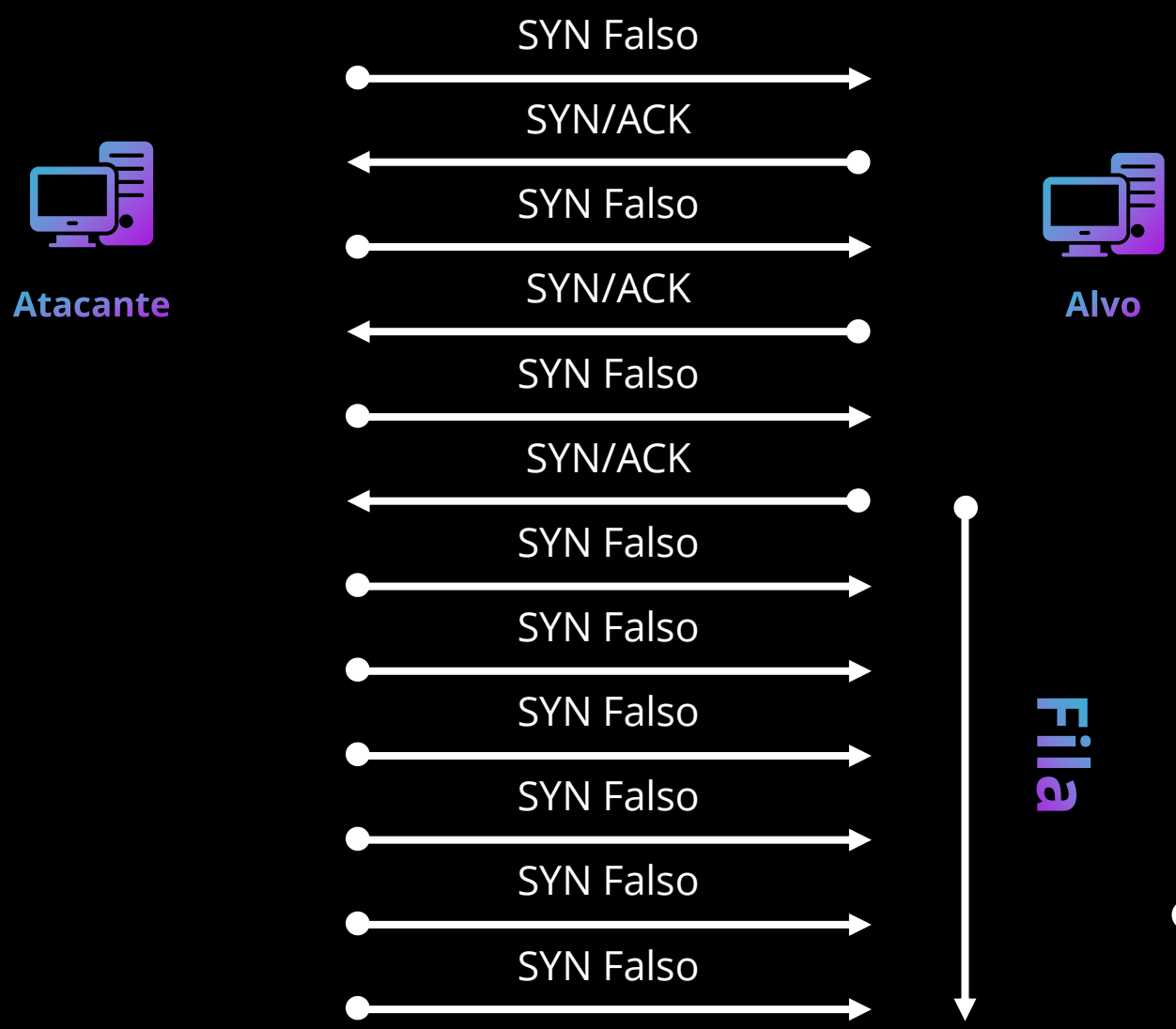
É mais fácil evitar ser um zumbi do que impedir ou interromper um ataque DDoS.

Algumas ferramentas escaneiam sistemas, procurando **por zumbis** adormecidos esperando por um sinal de ataque.

Inundação SYN

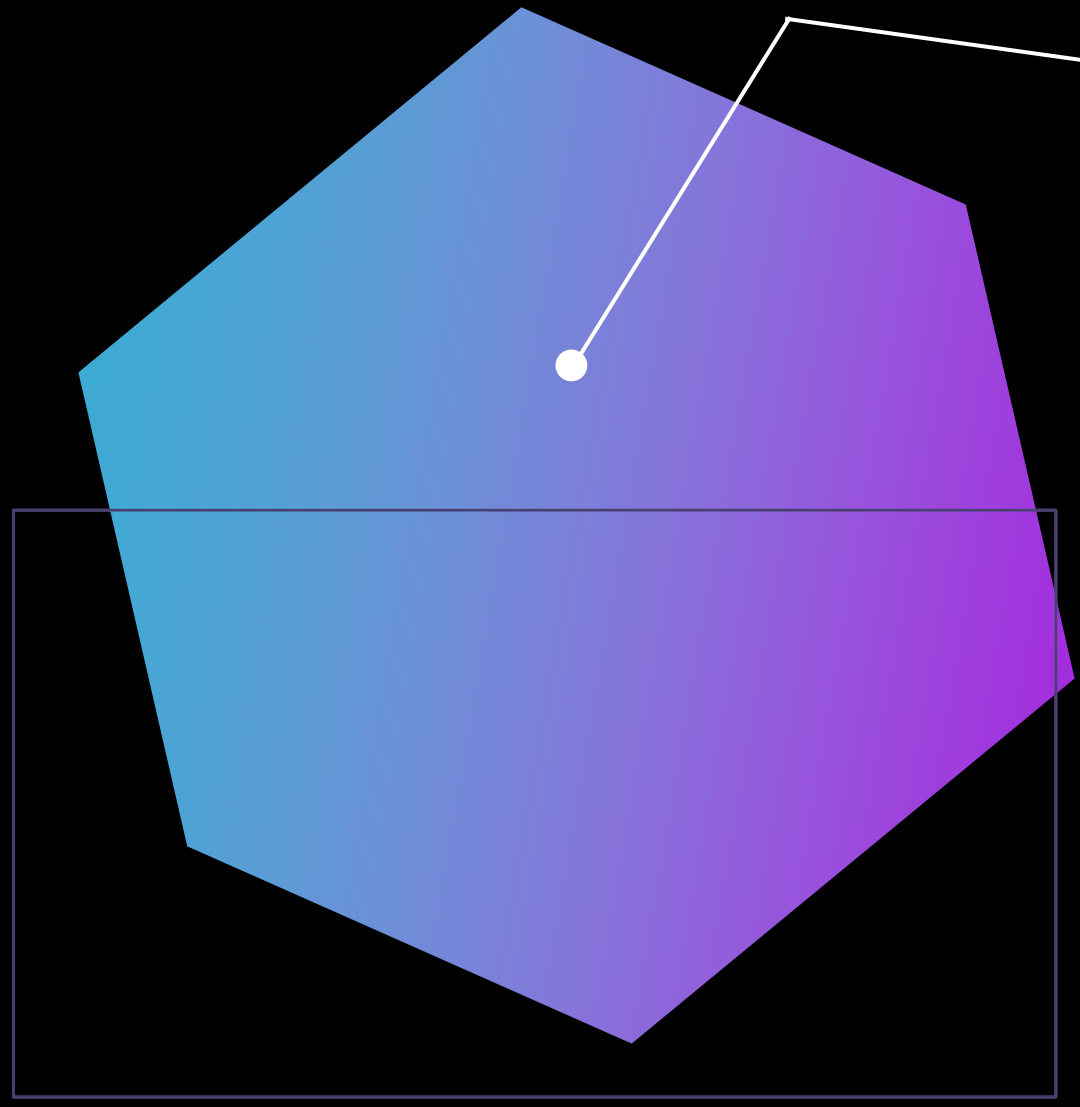


SYN Flooding em Ação



Vetor de Ataque DDoS

- Ping of Death (POD) - O invasor envia um pacote de ping ICMP igual ou superior a 64 kB (Não natural).
- Connectionless Lightweight Directory Access Protocol (CLDAP) - Forma mais recente de ataque. (O mais procurado).
  - No CLDAP, o invasor solicita informações de todas as contas do Active Directory, apontando para a máquina da vítima.
  - Fácil proteção: Bloquear a porta 389 para evitar solicitações fora da rede interna.



DDoS em Aplicativo

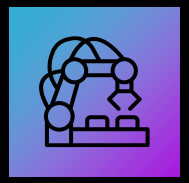
Aplicativos estão sujeitos a DDoS, pois recebem entradas do usuário, processam dados e criam saídas.

O objetivo é consumir todos os recursos ou colocar o sistema em falha. HTTP é o alvo pelo anonimato.

Para detectar esse tipo de ataque, utilize firewalls de última geração (new Generation) de aplicativos Web.

Ataques DDoS funcionam contra interfaces de API. O esforço computacional do invasor é mínimo.

Tecnologia Operacional (TO)



Ataque DDoS contra hardware ou software de dispositivos industriais em sistemas ciberfísicos.

Diferença entre os sistemas de TO e TI: protocolos.

- TO possuem protocolos específicos que são usados para realizar comunicações de controle de equipamentos.

Os ataques de negação de serviço são utilizados como parte de um conjunto de ataques, ou seja, podem interagir com outras partes da empresa.

Código Malicioso e Execução de Script

- Automação em sistemas promovem velocidade, precisão, reprodutibilidade e portabilidade.

Muitos desses motivos são fatores para invasores para automatizar seus ataques.

- Tecnologias para automatizar ataques com código malicioso e execução de script:

PowerShell;

Python;

Bash;

Macros;

Visual Basic for Applications.

PowerShell

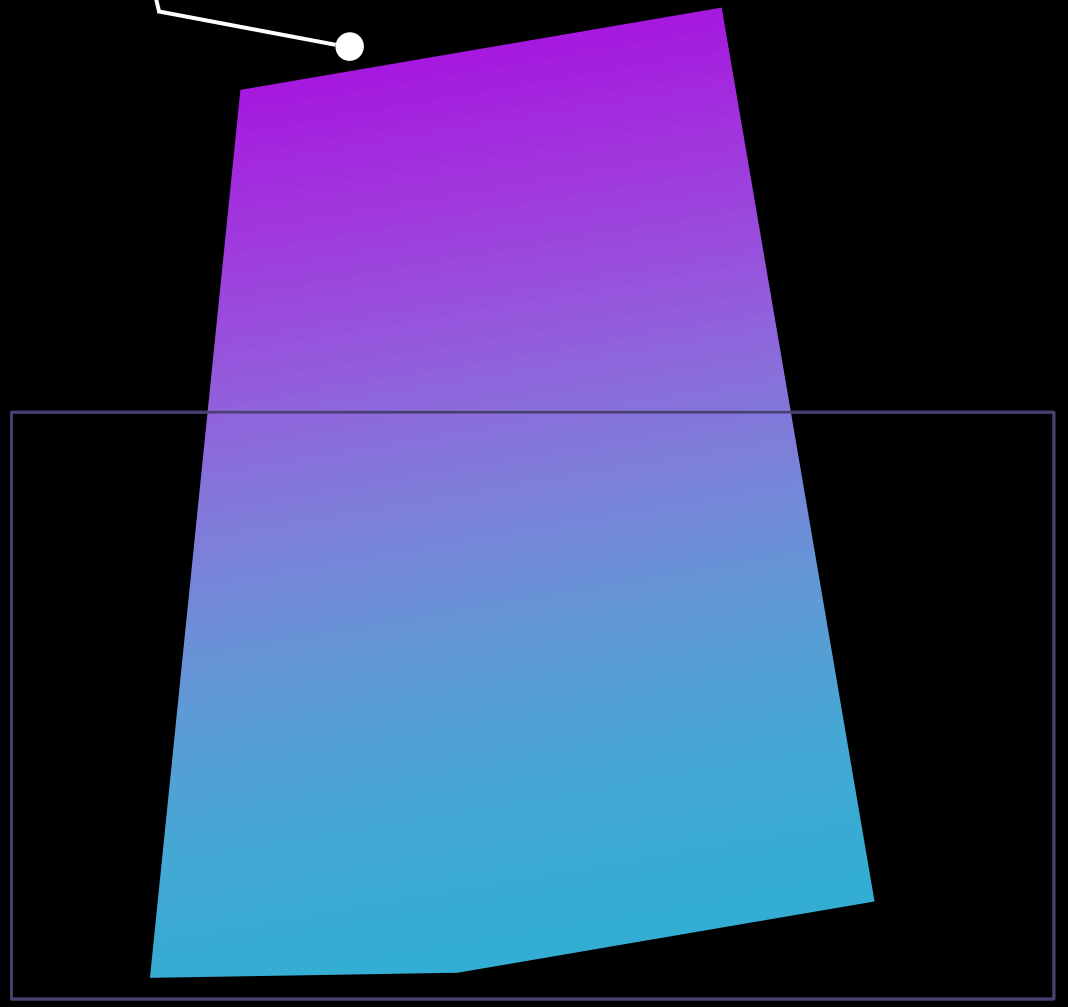
- Conjunto de ferramentas de linha de comando interno que possui um conjunto rico de comandos do Windows.

Totalmente integrado ao Windows.

Os invasores adoram o PowerShell!

- Você pode criar um arquivo de script do PowerShell, que tenha a extensão .ps1

Exemplo: PowerSploit (usado para ajudar no *pentest*)



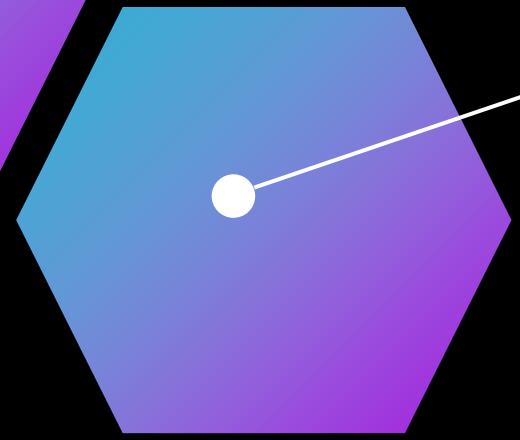
Python

- Linguagem de programação/script muito utilizada:
  - Ferramenta de script fácil de aprender;
  - Amplamente suportada;
  - Boa para automatizar tarefas.

Os hackers usam o Python pelos mesmos motivos.

Github
Biblioteca de conjuntos de ferramentas e utilitários de ataque orientados a Python.

- Você pode criar um arquivo de script do Phyton, que tenha a extensão .py



Bash

Um interpretador que processa comandos shell em sistemas Linux.

- Os hackers usam o Bash para pesquisar sistemas e executar tarefas em sistemas Linux.

A diferenciação entre o uso do PowerShell, Python e Bash está relacionada ao sistema operacional.

- Você pode criar um arquivo de script Bash, que tenha a extensão .sh

Macros

- Conjuntos de instruções gravados, normalmente apresentados a um aplicativo para automatizar sua função.
- O uso de macros permite uma grande quantidade de funcionalidades em produtos (PDF e Office).
  - Por isso, algumas restrições são necessárias.
- O atacante pode criar um arquivo do MS Office, inserir uma macro e enviar por e-mail para suas vítimas.

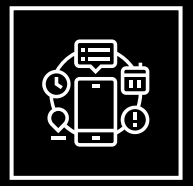
Visual Basic for Applications (VBA)

Uma tecnologia mais antiga da Microsoft que foi usada para automatizar muitos processos internos em aplicativos.

Ainda é válido em muitas plataformas

- É mais um vetor para invasores.

Forma de se proteger: desabilitando a execução de macros ou VBA em aplicativos.



Macros e VBA são utilizados por conta da automação dos aplicativos.

- O atacante pode criar um VBA em um arquivo no Excel.

OBRIGADO!

INDICADORES DE ATAQUES
DE REDE – PARTE 2