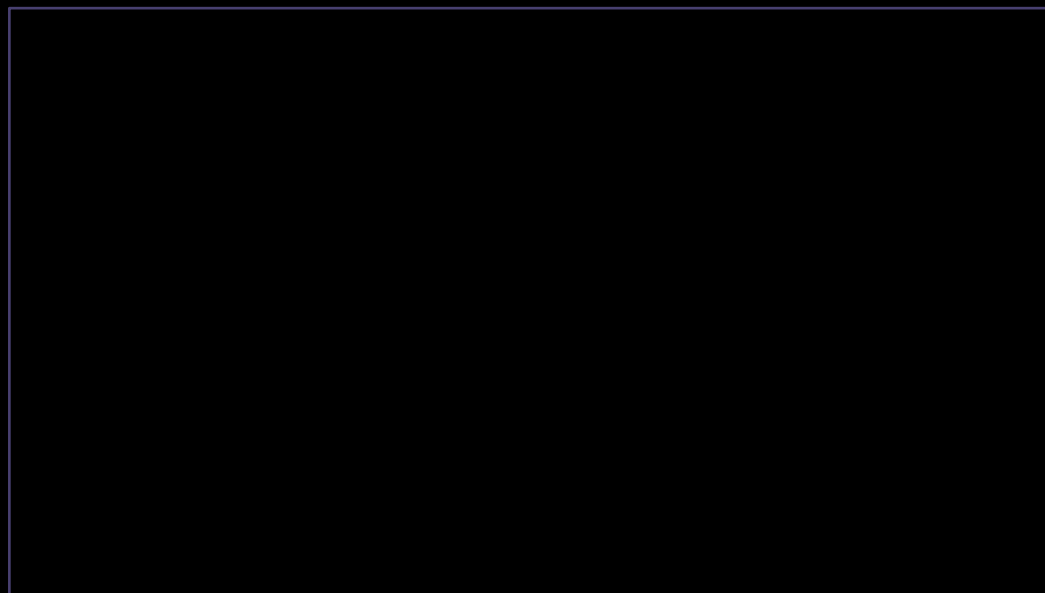




Prime

CCS-A

Indicadores de
Ataque de Rede



Wireless



Tecnologia de rede que possui um número substancial de processos e padrões para conexão de usuários à rede por meio de sinal de rádio.



É um alvo para hackers.
Remove a barreira física.

Vulnerabilidades

- **Emanação de dados:** Coleta de dados devido emissões dos componentes elétricos.
- **Jamming/interferência:** Faz a rede sem fio cair, por exemplo, interferência de telefones sem fio.
- **Sniffing de pacotes** Qualquer pessoa com uma placa de rede sem fio e um sniffer pode facilmente capturar dados.



Jamming Attack

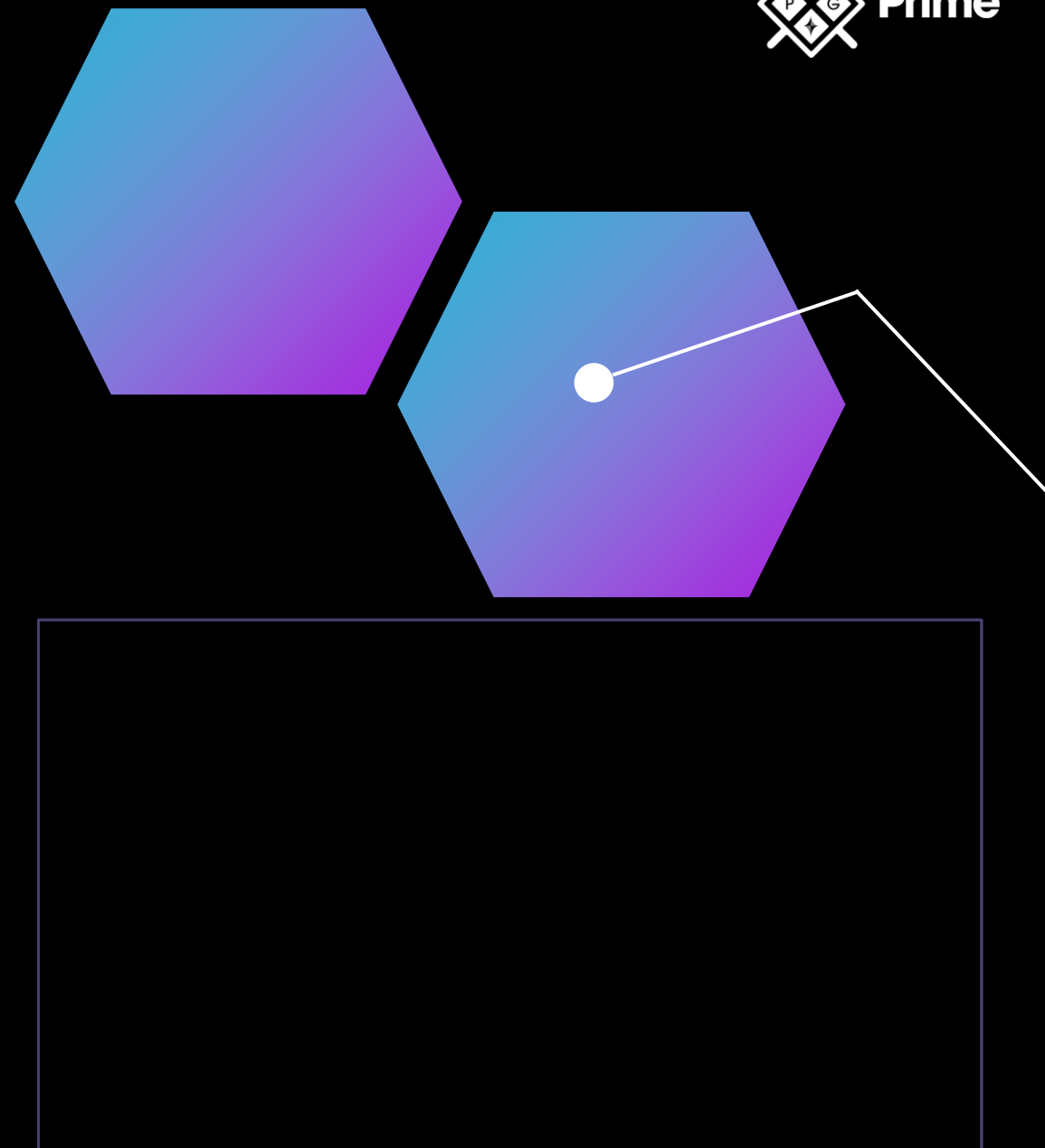
- ▶ Forma de negação de serviço que visa o espectro de rádio da rede sem fio.
- ▶ Objetivo simples: Paralisar a rede Wireless
- ▶ Características:



Manipulação de forma discreta;



Interferência em um ponto de acesso sem fio, através de conexão com pontos de acesso não autorizados.



Ataque Evil Twin

- ▶ Ataque contra o protocolo sem fio via hardware substituto.

- ▶ Características:



Usa um ponto de acesso de propriedade de um invasor que geralmente foi aprimorado;



Os invasores podem analisar o tráfego e realizar ataques man-in-the-middle.

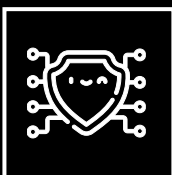


Pode bloquear o sinal sem fio.

Ponto de Acesso Não Autorizado



Na configuração de um ponto de acesso não autorizado, um invasor pode fazer com que clientes se conectem a ele como se estivessem autorizados, e autenticar no ponto de acesso real.



Método de defesa:

Empresas com pontos de acesso sem fio devem verificar e remover pontos de acesso invasores.



Um ponto de acesso que geralmente é colocado em uma rede interna por acidente ou propositalmente.



Não é administrado pelo proprietário da rede, mas pelo espião.

Bluejacking

Envio de mensagens não autorizadas para outro dispositivo Bluetooth

Funcionamento:



O invasor verifica ao seu redor um dispositivo habilitado para Bluetooth

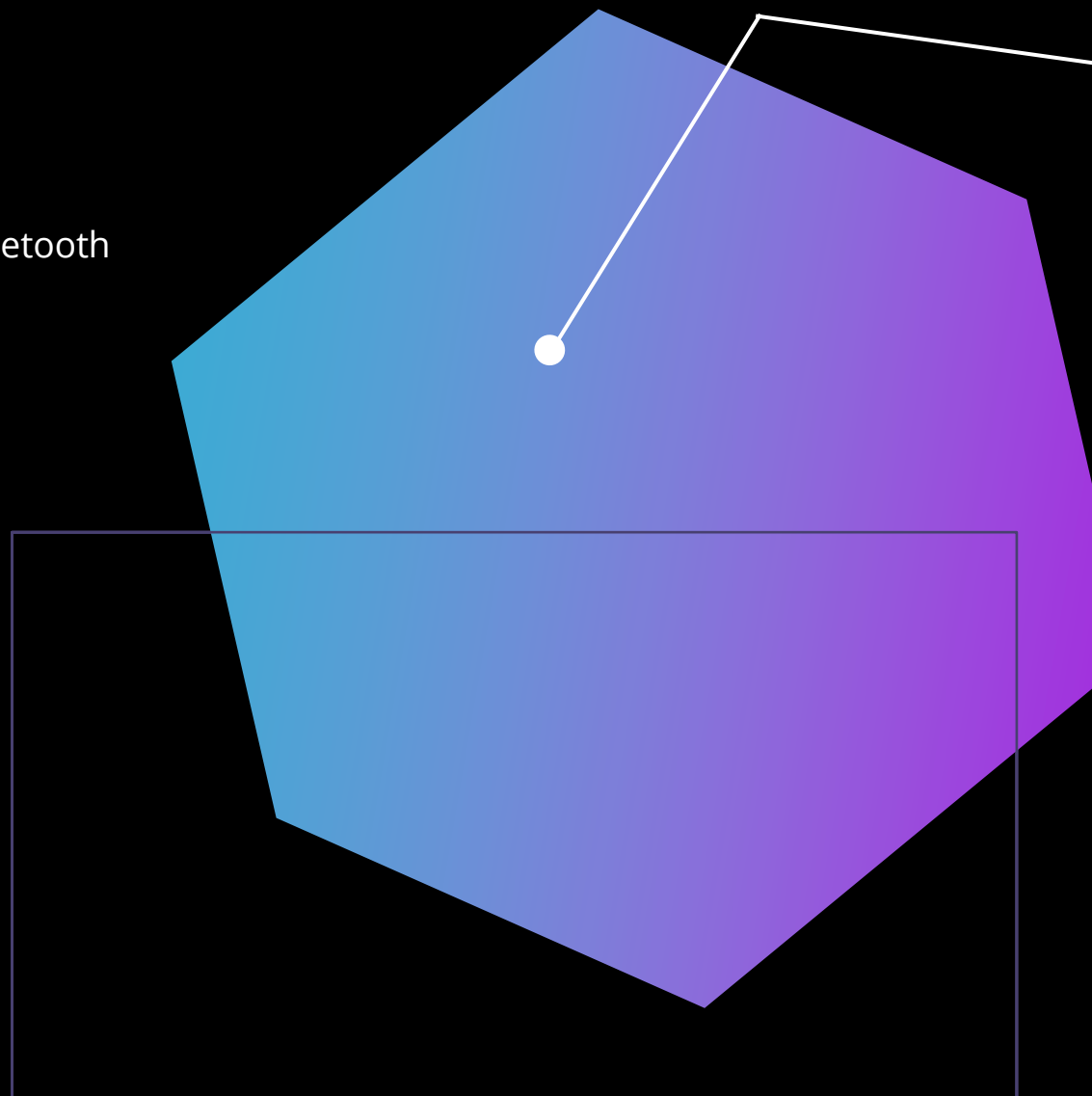


Envia a mensagem para o possível destinatário via Bluetooth

Envio de Mensagens de texto e imagens chocantes.

Smartphones mais antigos o Bluetooth é ativado por padrão.

O ataque e a vítima devem estar a aproximadamente 10 metros um do outro.



Bluesnarfing



Semelhante ao bluejacking.



O invasor copia as informações da vítima.



Os aplicativos de bluesnarfing estão disponíveis para dispositivos móveis.



Os telefones bluetooth precisam ser detectáveis para que o ataque bluesnarf funcione.

Ataques de Desassociação

- ▶ Ataques projetados para desassociar um host do ponto de acesso e rede sem fio.
- ▶ Características:



Sempre em sintonia com outro tipo de ataque.



Oferece ao hacker a chance de dar o primeiro passo na coleta de informações.

- ▶ Exemplo: Wifiphisher (usado por Red Team)

Identificação por Radiofrequência (RFID)

— São usadas em vários casos. Alguns centímetros até 200 metros.

— Características:



Etiquetas RFID vêm em várias formas diferentes como crachás e *smartcards* (Ativo e Passivo).



Possuem várias preocupações de segurança.

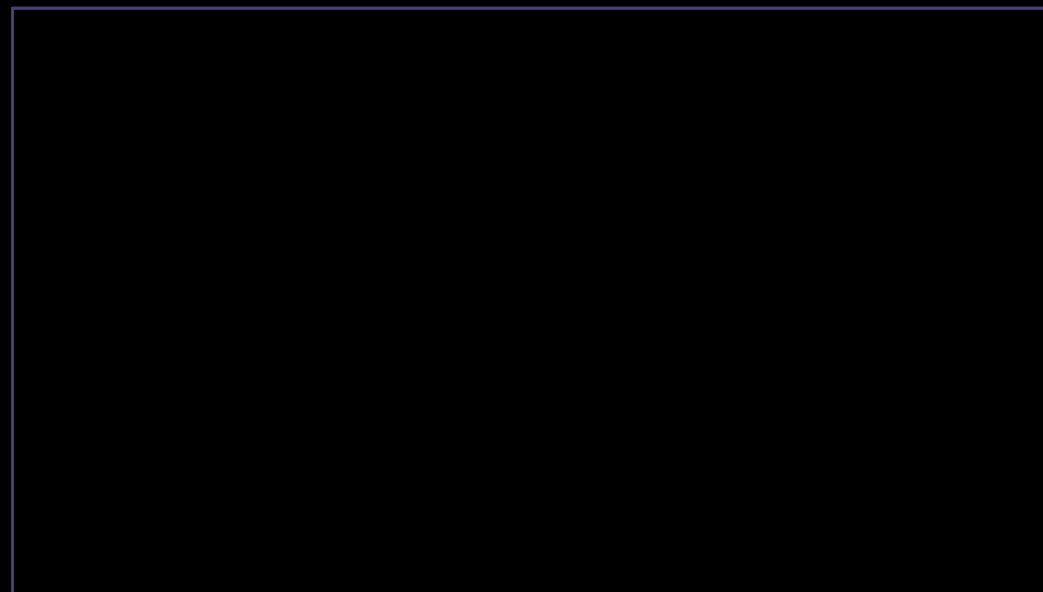
— Possíveis ataques contra o RFID:

— Ataques contra os próprios dispositivos RFID, como clonagem e Skimming;

— Canal de comunicação (ataques de repetição, *eavesdropping* seguida de *spoofing* e *man-it-the-middle*);

— Sistema de back-end podem ser realizados.

— Carteiras com bloqueio de frequências.



Comunicação de Campo Próximo (NFC)



Conjunto de tecnologias sem fio que permite que smartphones e outros dispositivos estabeleçam comunicação de rádio a uma curta distância.



Não teve muito uso até pouco tempo

Começou a ser utilizada para mover dados entre telefones celulares e em sistemas de pagamento móvel.



RFID

Processo pelo qual um cartão de crédito ou telefone se comunica com um leitor usando ondas de rádio;



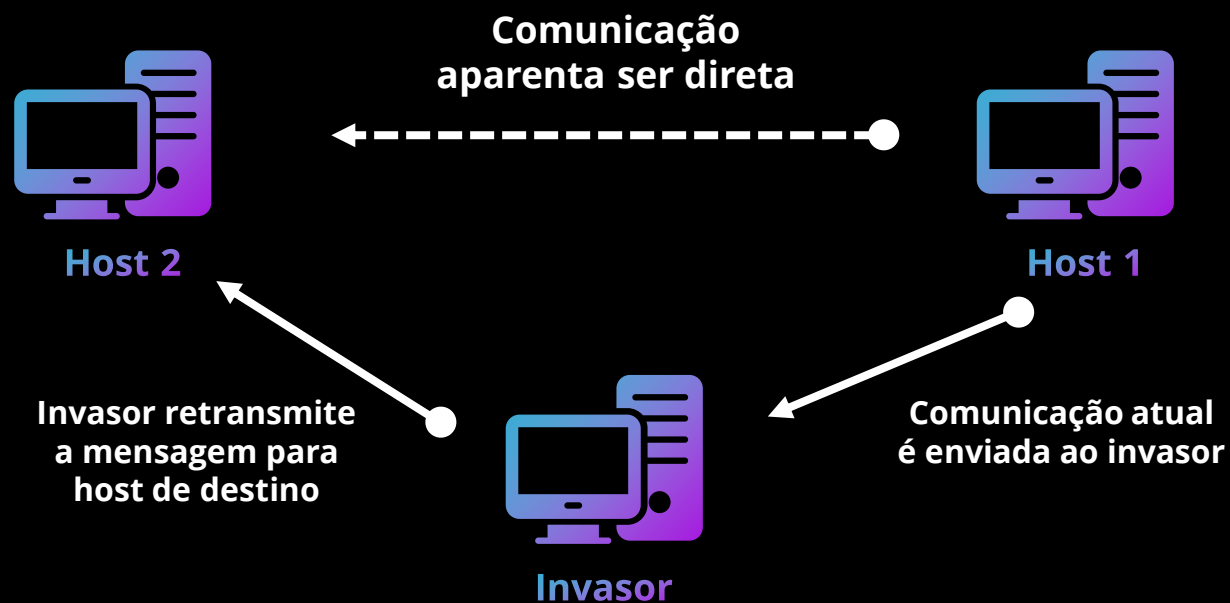
NFC

Subconjunto do RFID, atuando em uma distância bem menor.

Vetor de Inicialização (IV)

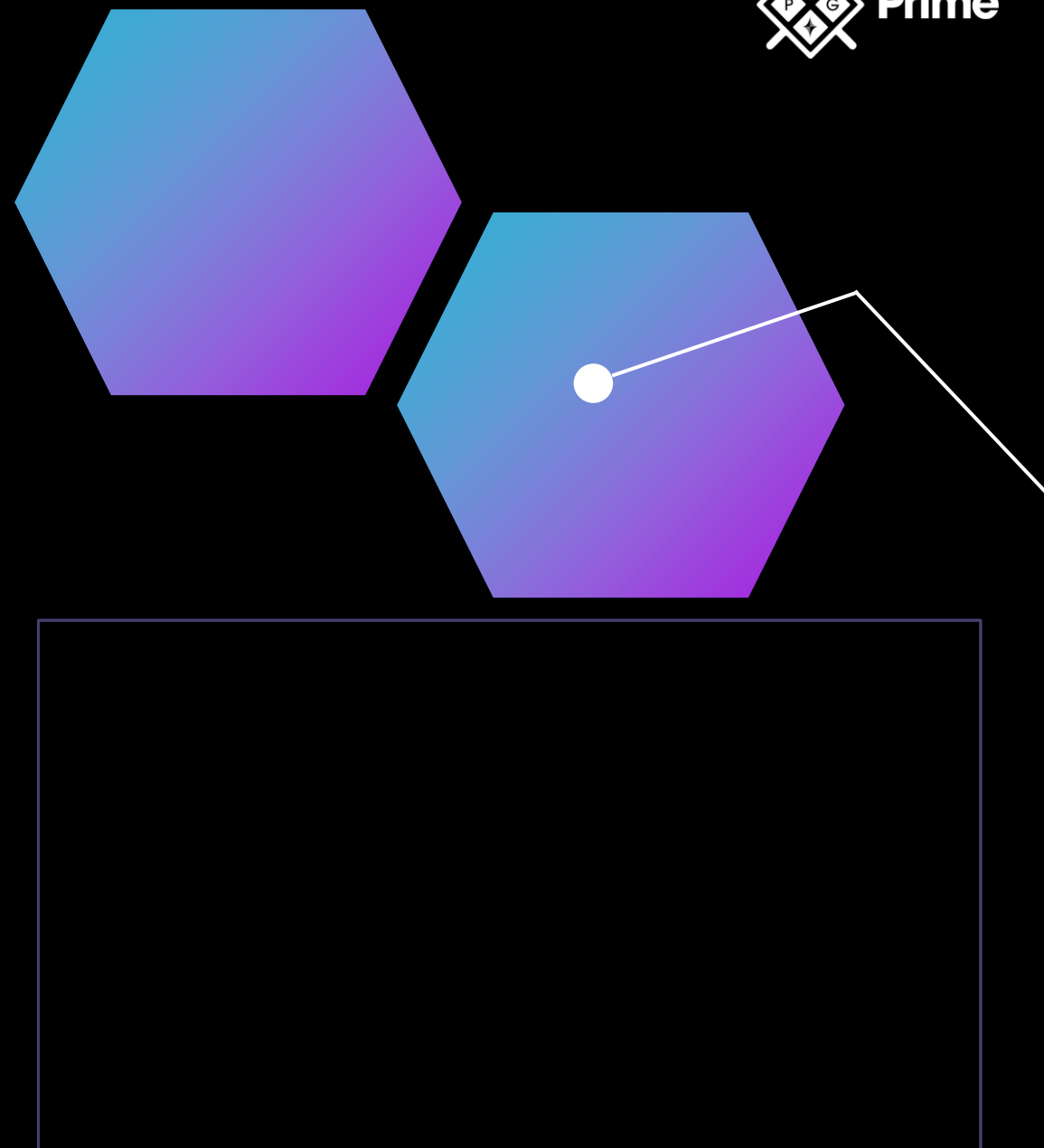
- ▶ Usado em sistemas sem fio como elemento de randomização (limitado) no início de uma conexão.
- ▶ Principal razão para as fraquezas de **Wired Equivalent Privacy (WEP)**:
 - ▶ Autenticação + Criptografia fraca (simétrica);
 - ▶ Independente do tamanho da criptografia, 24 bits é para o IV;
 - ▶ Devido a vulnerabilidade do IV, quebra-se em menos de 1 dia.
- ▶ IV tem apenas 16 milhões de chaves que é reutilizada. O invasor pode examinar o texto e quebrar a chave.

Man-In-The-Middle



Ataque Man-In-The-Middle

- ▶ O invasor pode observar todo o tráfego, retransmitir, modificar ou bloquear.
- ▶ Um dos métodos comuns de instanciar um ataque é o sequestro de sessão através do roubo do cookie.
- ▶ A quantidade de informação que pode ser obtida será limitada se a comunicação for criptografada.
- ▶ Variação do MITM: Man-in-the-browser (MITB):
 - ▶ Primeiro com ataque de Malware;
 - ▶ Imputa um trojan que atua como proxy;
 - ▶ Intercepta as teclas digitadas pelo usuário.



Ataques Camada 2

- ▶ A camada 2 é onde as decisões de endereçamento local são tomadas.
- ▶ Switches operam na camada 2;
- ▶ E protocolos, como o ARP e MAC Address.
- ▶ As três maneiras mais comuns de adulterar esse nível de endereçamento são:



Envenenamento ARP (ARP Poisoning);

MAC

Inundação do MAC (MAC Flooding);



Clonagem de MAC (MAC Cloning).

Envenenamento do Protocolo de Resolução de Endereços (ARP)

- ▶ O ARP mapeia endereços IP com os endereços MAC ou da camada 2 com quatro tipos de mensagens (sujeitas a ataque):



Solicitação ARP:

"Quem tem este endereço IP?"



Resposta ARP:

"Eu tenho esse endereço IP; meu endereço MAC é..."



Solicitação ARP reversa (RARP):

"Quem tem este endereço MAC?"



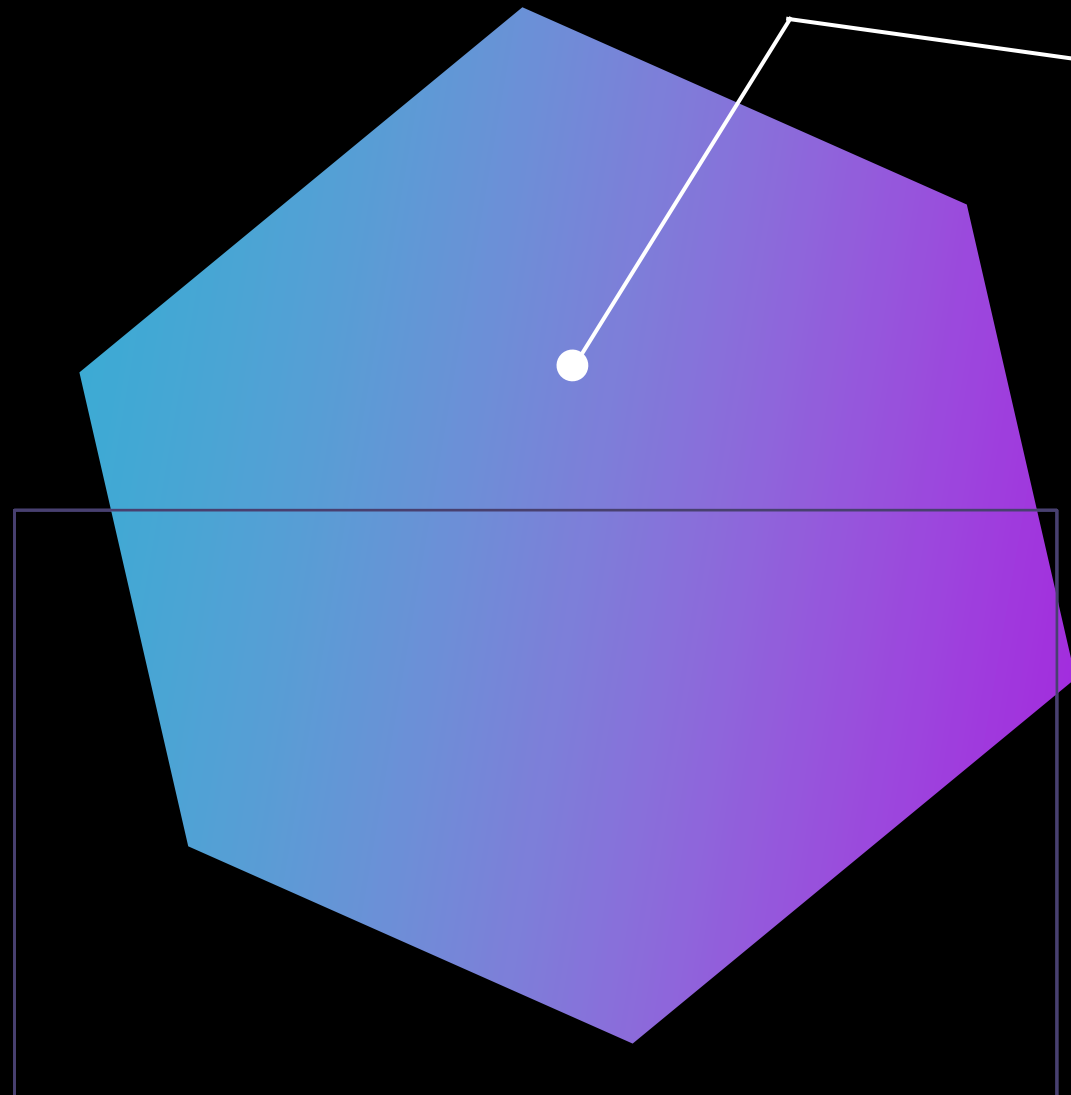
Resposta RARP:

"Eu tenho esse endereço MAC; meu endereço IP é..."

- ▶ Usadas em conjunto com a tabela ARP de um dispositivo.
- ▶ Quando a tabela ARP recebe uma resposta, ela confia automaticamente na resposta e atualiza a tabela.

Inundação de Controle de Acesso ao Meio (MAC)

- ▶ O endereçamento na interface da camada 2 é feito por MAC Address, switches e hubs.
- ▶ Como funciona o ataque:
 - ▶ O invasor inunda a tabela com endereços, tornando o **switch** incapaz de encontrar o endereço correto para um pacote;
 - ▶ Como resultado, remove os endereços MAC antigos e válidos, mas adicione os novos endereços MAC falsos;
 - ▶ O switch atua como hub (*failopen mode*) fazendo broadcast na rede em busca dos endereços;
 - ▶ Com um Sniffer em modo promíscuo, é possível capturar os dados na rede.



Clonagem de MAC

 MAC

- ▶ Quando o invasor copia o endereço MAC de outro sistema e o usa para comunicação de rede.
- ▶ Pode ser usado para contornar listas de controle de acesso e só permitir tráfego de um MAC específico.



Quando funciona:

A verificação de segurança é baseada em MAC Address.



Nem sempre essa clonagem é um ataque. Um firewall pode clonar o MAC para torná-lo transparente (conexão do modem a cabo).

OBRIGADO!

INDICADORES DE
ATAQUE DE REDE