Mitigando o Hacking

Sobre o que se trata essa reunião?

Vamos tentar diminuir um pouco a abstração do que é o hacking e apresentar alguns conceitos

- DDoS
- MITM
- Rogue Access Point
- Phishing
- APT


DDoS

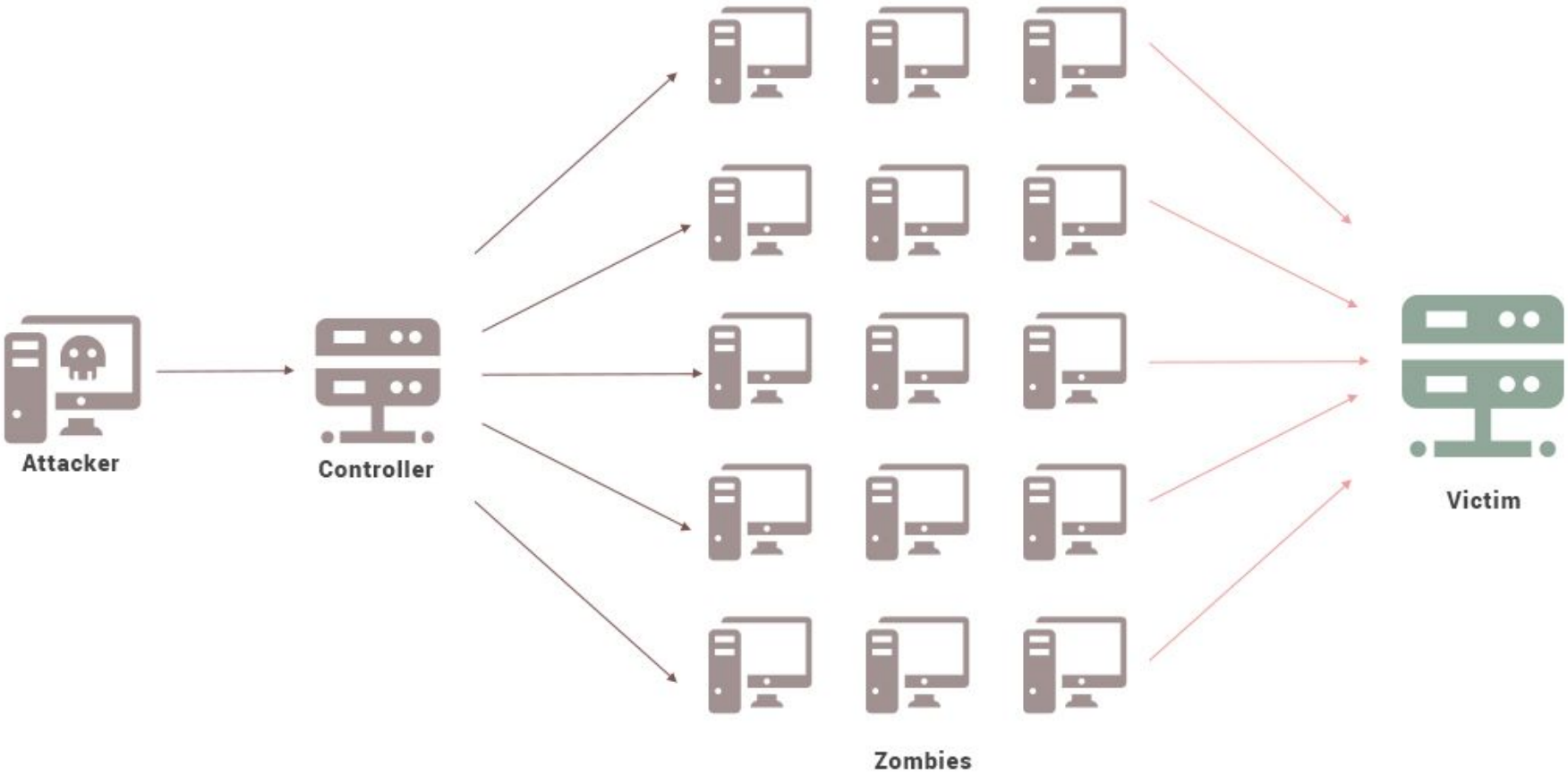
DDoS (Distributed Denial Of Service)

É o ataque mais simples, porém exige muito poder de banda

Requisições aos servidores consomem recursos, quando são feitas requisições em excesso e o servidor não é capaz de lidar com todas elas ele se torna indisponível

Ocorre de duas formas:

- Pode explorar alguma vulnerabilidade do serviço enviando um pacote mal formatado
- Pode consumir todos os recursos do servidor tornando-o lento ou indisponibilizando o serviço (mais usual)

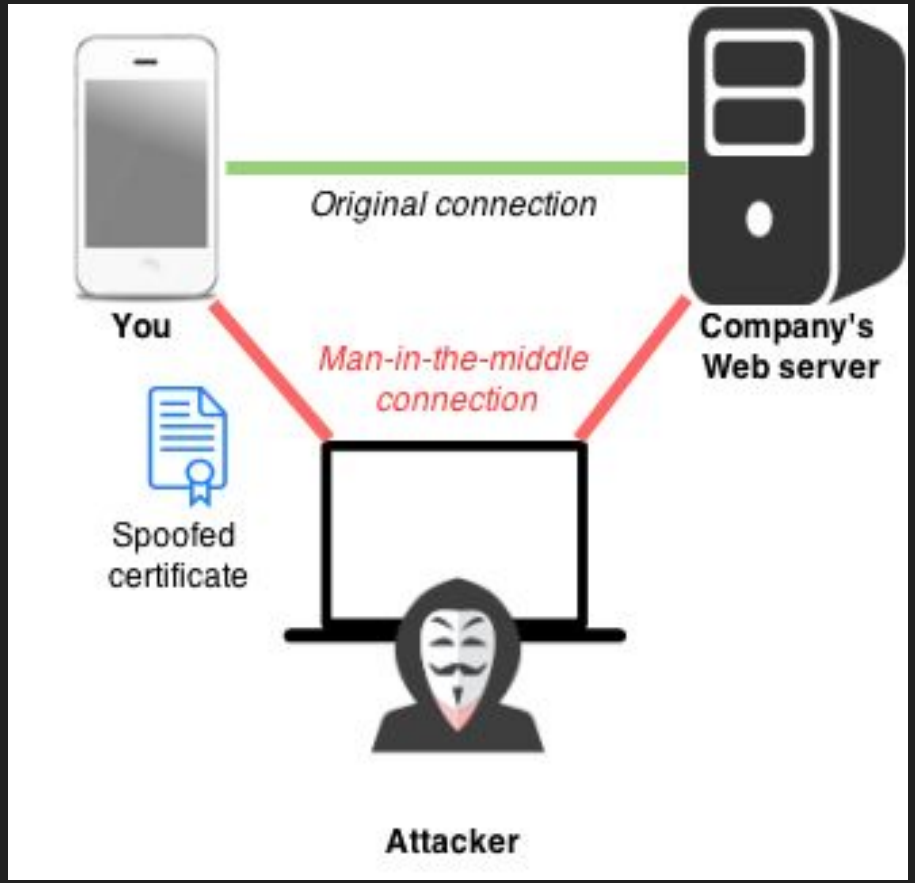

Attacker
Controller
Zombies
Victim

MITM (Man-In-The-Middle)

1. Existe muita troca de informação entre o servidor e os usuários, nesse processo são enviadas senhas e outros dados “sensíveis”

2. No MITM, o atacante se coloca entre o servidor e a vítima, fazendo a captura desses dados

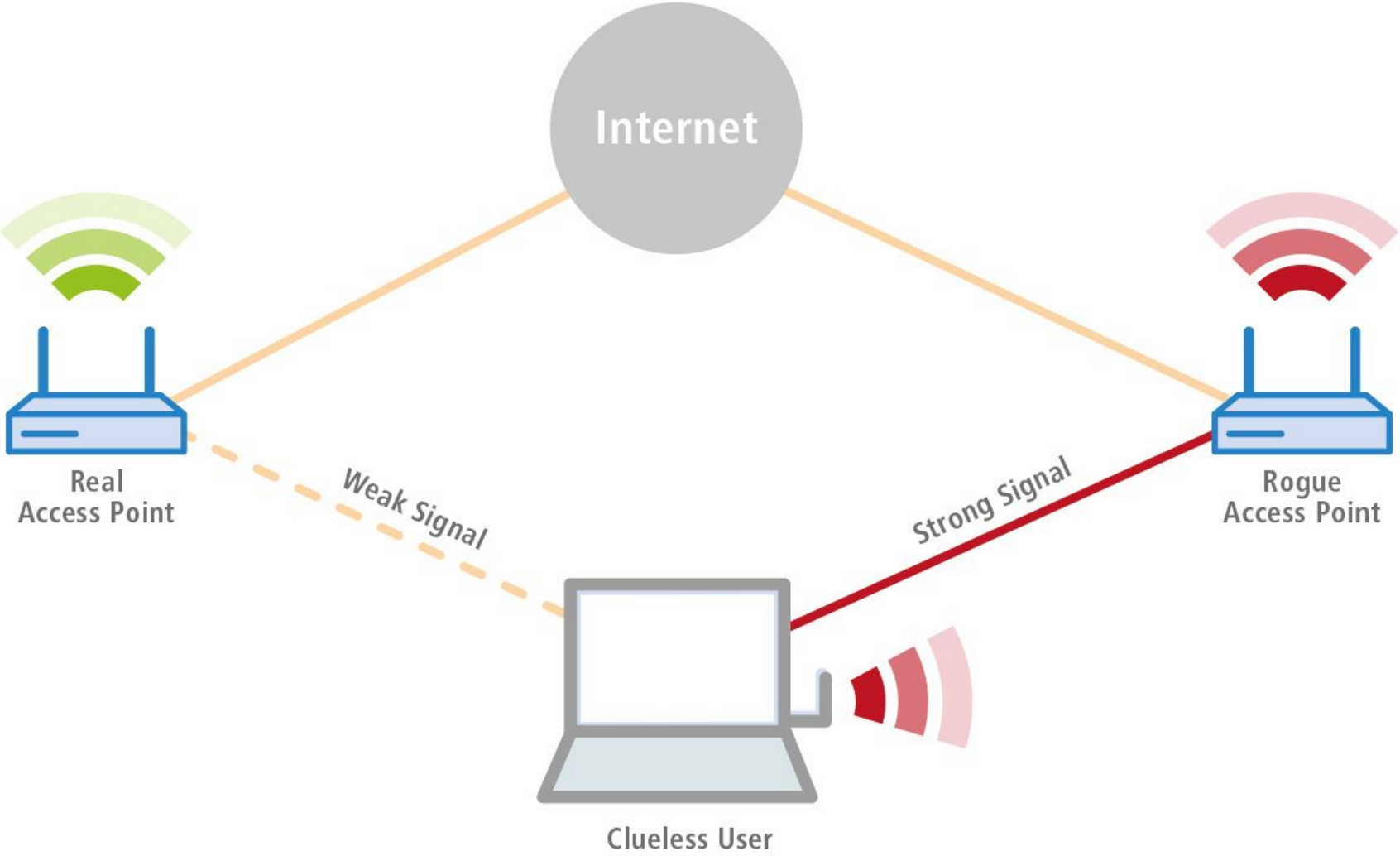
3. O MITM pode ser realizado de inúmeras formas, as mais comuns são nos protocolos DNS e ARP



Rogue Access Point: Aprendendo a pescar

Também chamado de Evil Twin

1. O hacker transforma o próprio computador em um roteador com nome e endereço IGUAIS ao roteador do ambiente (exemplo: DC-Grad)
2. Quando existem dois roteadores iguais, o computador se conecta ao que possui o sinal mais forte, quando esse sinal vem da máquina do hacker, a vítima se conecta a ele
3. Esse ataque pode funcionar como um Man-In-The-Middle em que o atacante transmite os pacotes da vítima para o roteador original interceptando e modificando esses dados de entrada e/ou de saída
4. O hacker pode manipular os dados que são transmitidos ao usuário e, em um local como o DC, pode iniciar uma página de autenticação falsa em que o RA e a senha da página de autenticação do DC-Grad são enviados ao atacante (phishing)
5. O hacker pode substituir os arquivos que a vítima baixa por arquivos que ele escolher, como um vírus
6. Sempre tome cuidado ao usar o wifi em aeroportos, cafeterias ou perto de mim ¯_(ツ)_/¯


Internet
Real
Access Point
Weak Signal
Strong Signal
Rogue
Access Point
Clueless User

APT: Advanced Persistent Threat

1. É uma arma muito usada na política
2. É como o pessoal tem obtido e divulgado os episódios de Game Of Thrones
3. Basicamente alguém quer te invadir, e vai conseguir fazer isso

Conclusão

O foco do grupo é segurança da informação, mas hacking não é invadir sistemas ou protegê-los. O hacking é a cultura da curiosidade, da disseminação de conhecimento. É explorar cada bit do seu sistema, conhecer cada lei do código penal, e tomar a atitude mais sensata baseada na informação acumulada. Hacking é aprender e ensinar, é dar o seu melhor pelo conhecimento. Uma pessoa interessada em aprender a fundo, seja lá o que ela gosta, esse é o hacker.

TO DO

Quando você tiver um tempo livre, baixe esses softwares para auxiliar nos próximos encontros! O VirtualBox é uma máquina virtual, ou seja ela permite que você simule outros sistemas operacionais dentro do seu. O Kali linux é um sistema linux com foco em segurança da informação

- VirtualBox
- Kali Linux (Uma boa ideia é baixar uma imagem já configurada para o VirtualBox)
- Configurar um ambiente Kali no Virtual Box

Vídeo:
https://www.youtube.com/watch?v=ukH0Ox1x-lc