INSTITUTO FEDERAL
São Paulo
Câmpus Barretos

Segurança da Informação

Aula 1

Prof. Lucas

Agenda

- Apresentação
- Ambiente Virtual de Aprendizagem
- Visão geral do curso
- Introdução

Introdução

- Identificação dos componentes em uma rede de computadores TCP/IP
- Entender os elementos básicos da segurança da informação
- Terminologia do hacker ético
- Classificação de hackers
- Descrição dos 5 estágios de ataques

Modelo OSI

- Modelo de referência

- O que é necessário para conectar 2 computadores?
  - Meio de transmissão (par trançado, coaxial, ondas de rádio, fibras, etc)
  - Camada 1 – Física (transmissão de bits: 0 e 1)
  - PDU: **bits**

Modelo OSI
7-Aplicação
6-Apresentação
5-Sessão
4-Transporte
3-Rede
2-Enlace
1-Física

Modelo OSI

- A camada 2 é responsável por encapsular os bits para as camadas superiores – frames
- Identifica um host dentro de uma rede local
- Endereços físicos – mac
- Switches
- PDU: **Frames**

Modelo OSI
7-Aplicação
6-Apresentação
5-Sessão
4-Transporte
3-Rede
2-Enlace
1-Física

Modelo OSI

- E o que acontece quando você precisa enviar uma informação para fora da sua rede local?
- Camada 3 (Rede) é responsável por encapsular a informação de roteamento – endereço IP
- PDU: **Pacote**

Modelo OSI
7-Aplicação
6-Apresentação
5-Sessão
4-Transporte
3-Rede
2-Enlace
1-Física

Modelo OSI

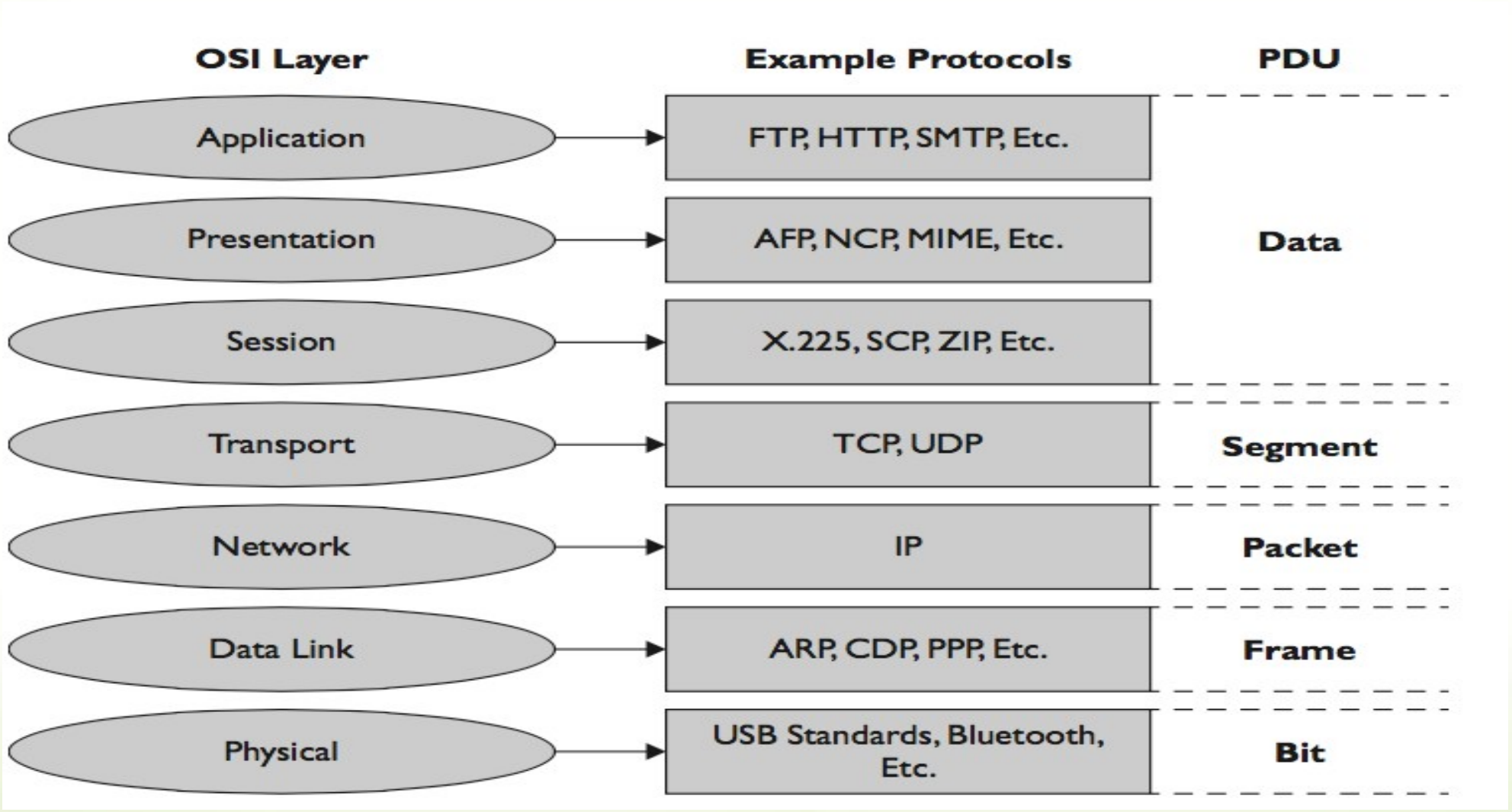
- Camada 4 (Transporte), segmentos são entregues ponto-a-ponto para o destino
- Determina que tipo de serviço será oferecido aos usuários da rede:
  - Ponto a ponto, livre de erros e na mesma ordem recebida
  - Mensagens isoladas sem garantia da ordem de entrega
- TCP e UDP
- PDU: **Segmento**

Modelo OSI
7-Aplicação
6-Apresentação
5-Sessão
4-Transporte
3-Rede
2-Enlace
1-Física

Modelo OSI

- As 3 últimas camadas (sessão, apresentação e aplicação) lidam com os dados em si
- Sessão: abrir, manter e fechar uma sessão
- Apresentação: Criptografia, compressão de caracteres; sintaxe e a semântica da informação
- Aplicação: Lida com os protocolos que permite ao usuário acessar informação através da rede (ftp, http, smtp,etc)
- PDU (*protocol data unit*) destas 3 camadas: **dado**

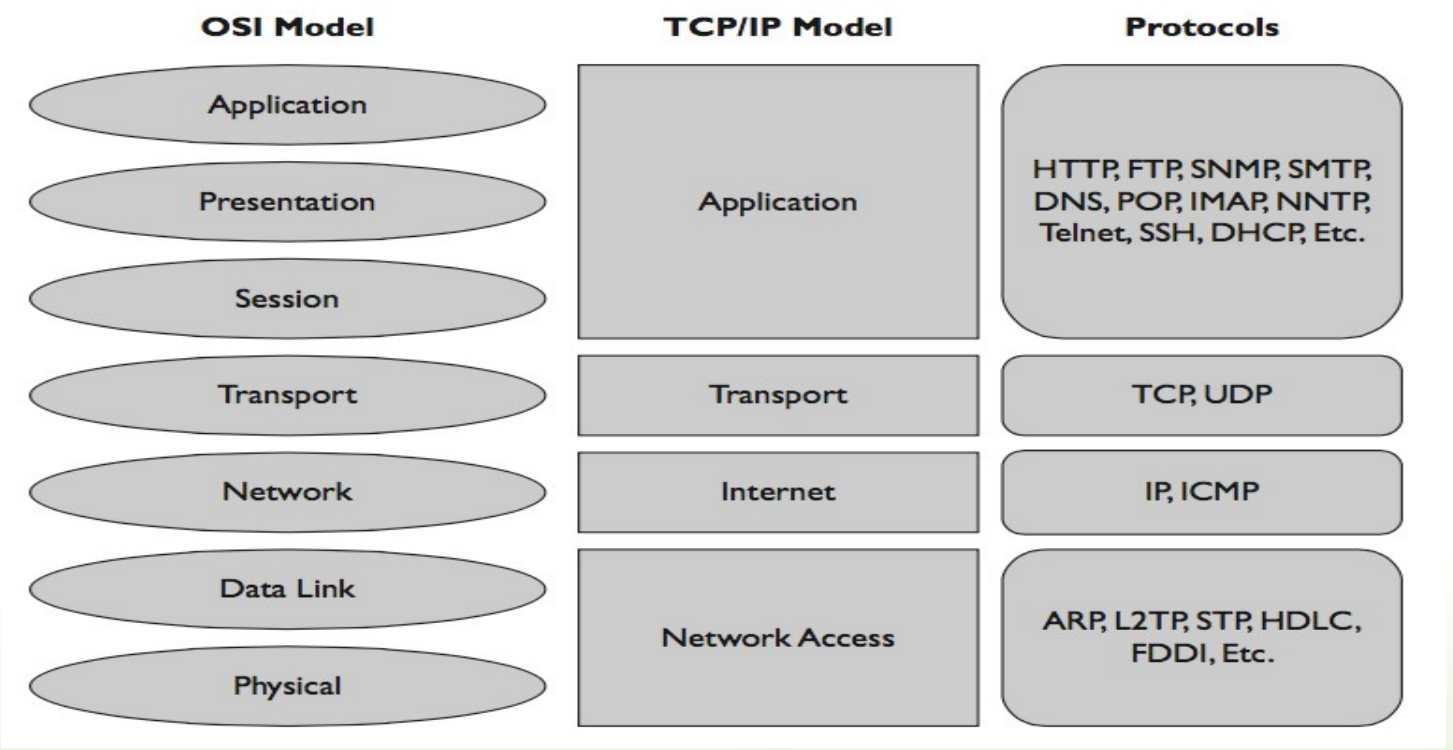
Modelo OSI



[Walker, 2014]

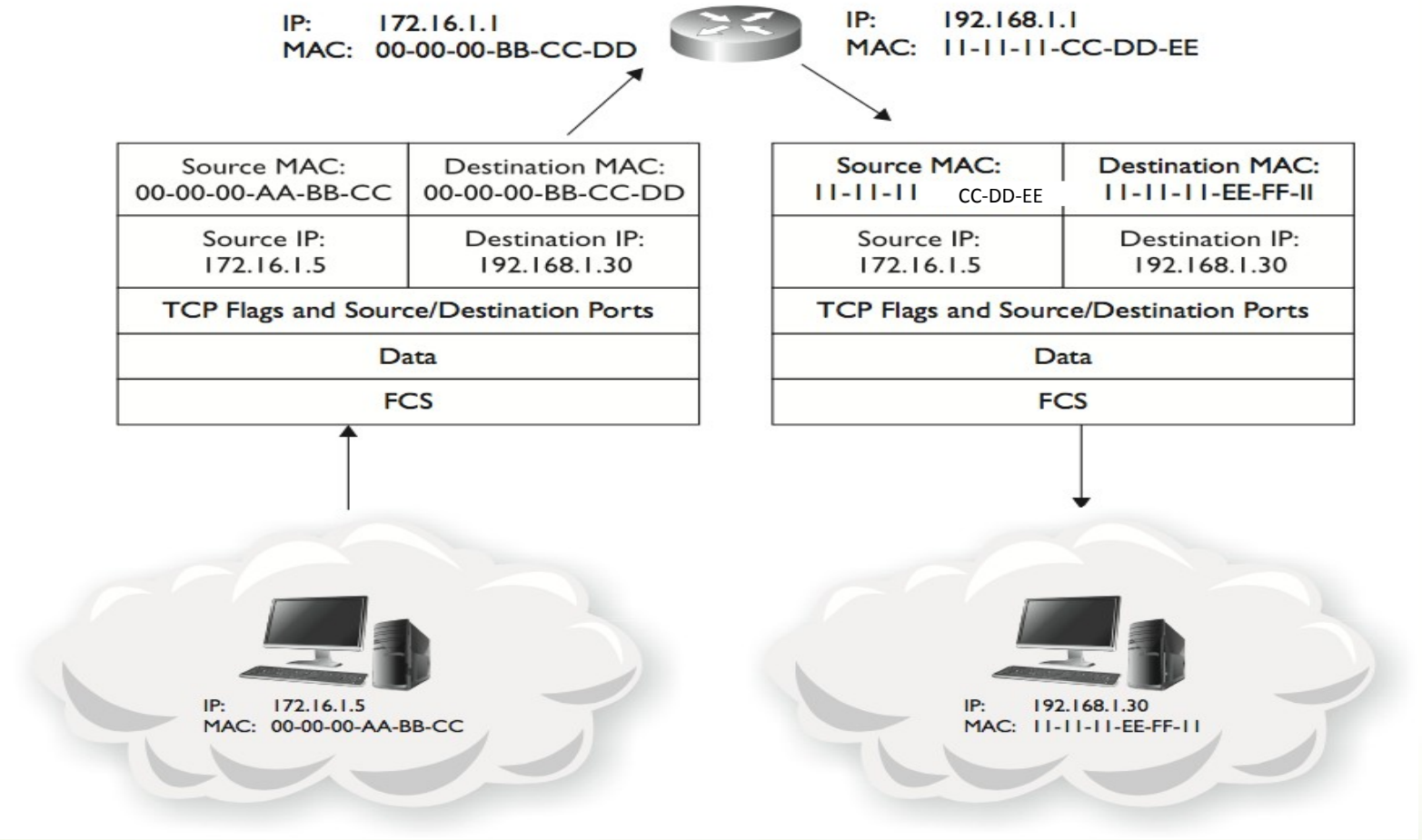
TCP/IP

- Conjunto de protocolos de comunicação que permite que hosts em uma rede se comuniquem uns com os outros



[Walker, 2014]

Exemplo de um acesso web



[Walker, 2014]

Exemplo de um acesso web

- Navegador – url
- Protocolo http faz uma requisição para a camada de transporte – UDP – DNS - ARP
- Com o IP, o http faz outra requisição para a camada de transporte – TCP
- 3 handshake – SYN, SYN/ACK, ACK
- Conteúdo é baixado
- Término da conexão

- O endereço mac origem e destino mudam a cada salto; o IP nunca muda (a não ser com NAT)!

Protocolo TCP

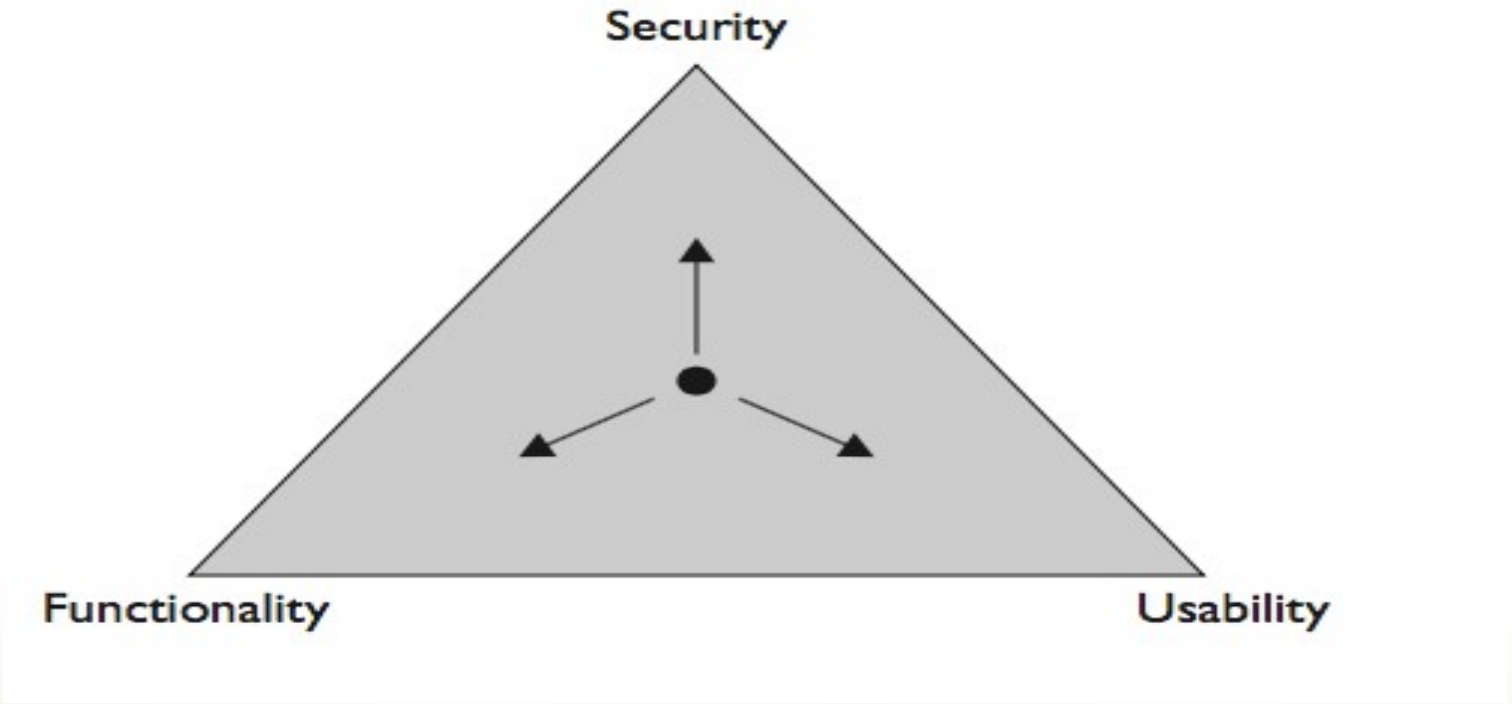
- Multiplexação de portas
- Recuperação de erros – confiabilidade (seq, ack)
- Controle de fluxo
- Segmentação
- Estabelecimento e término de conexão

3 way handshake

1474	148.997704000	192.168.1.112	66.235.153.36	TCP	78 50930→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=735805143 TSecr=0 SACK_PERM=1
1485	149.217115000	66.235.153.36	192.168.1.112	TCP	74 80→50930 [SYN, ACK] Seq=0 Ack=1 Win=4320 Len=0 MSS=1440 TSval=3572585060 TSecr=735805143 SACK_PERM=1
1486	149.217227000	192.168.1.112	66.235.153.36	TCP	66 50930→80 [ACK] Seq=1 Ack=1 Win=65535 Len=0 TSval=735805360 TSecr=3572585060

Segurança (questões essenciais)

- Segurança, Funcionalidade e Usabilidade



[Walker, 2014]

Segurança (questões essenciais)

- Gráfico representa uma preocupação dos profissionais de segurança da informação

- Quanto mais seguro algo é, menos usável e funcional se torna

Medidas de segurança

- Medidas preventivas para minimizar ao máximo os riscos existentes
- Dividido em 3 categorias: preventiva, corretiva e investigativa (*detective*)
  - Preventiva: exemplo de autenticação
  - Investigativa: identificação de incidentes (alarmes, alertas, auditorias, etc)
  - Corretiva: backup, *restore*

Confidencialidade, integridade e disponibilidade

- Confidencialidade
  - Baseia-se na privacidade e segredo da informação – acesso a dados por pessoas não autorizadas
  - Maior exemplo de ataque é contra *passwords*.
  - Autenticação de 2 fatores
- Integridade
  - Métodos e ações para proteger os dados de acesso não autorizado – garante que um dado não sofreu alteração
  - Uso de hash (MD-5, SHA-1, SHA-256)

Confidencialidade, integridade e disponibilidade

- Disponibilidade
  - Comunicação de sistemas e dados disponíveis quando solicitados
  - Principal ataque: DoS – denial of service. Previnir usuário legítimos de acessarem os recursos computacionais
  - Ataque de ransonware

Introdução ao hacker ético

- O que difere do hacker ético para um que não é, são os objetivos finais! (motivação)

- A arte de hackear e o uso das tecnologias permanecem as mesmas

Classificação

- Inúmeras formas de classificá-los
- Em geral são divididos em 3 categorias: bons, maus e indecisos
- No mundo da segurança da TI, é atribuído um *hat color*

Classificação

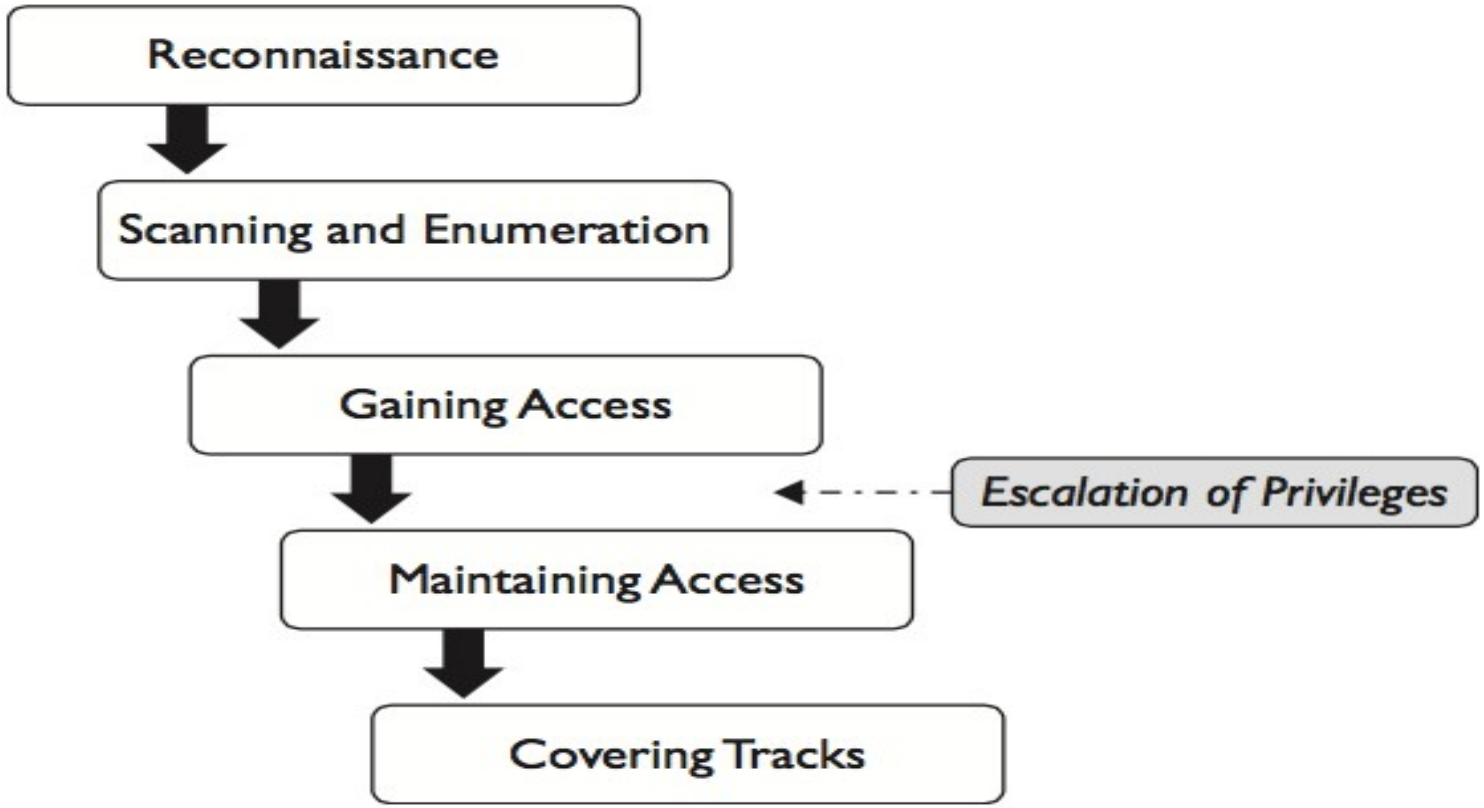
- White hats: Hacker éticos, analistas de segurança
- Black hats: Usam suas habilidades para intenções maliciosas (roubam ou destróem dados)
- Gray hats: Não são bons e nem maus! - curiosos

E para testar a segurança da sua empresa?

- **Pentesting**: testar e identificar falhas – mais rápido

- **Red Team**: Testar a capacidade de detecção e resposta – mais eleborado – demorado – para empresas mais maduras!
- https://github.com/infosecn1nja/Red-Teaming-Toolkit

Hackear - fases



Reconhecimento

- Cuidado para não confundir com a fase de scanning
- Nada mais é do que procurar evidências e informações do seu alvo
- Pode ser reconhecimento ativo ou passivo
  - Passivo: Envolve pegar informações sem o conhecimento do alvo
  - Ativo: Usa ferramentas e técnicas que pode ou não ser descoberta pelo alvo (risco maior em relação ao passivo)
- Engenharia social

Scanning

- Envolve a utilização de ferramentas e técnicas para aprofundar as informações coletadas

- Por exemplo: Se na fase de reconhecimento, você obteve a informação de que existe 500 PCs no alvo, nesta fase você conseguiria obter qual SO estaria rodando neles

Ganho de acesso

- Ataques reais são realizados – redes wireless, sql injection, passwords, etc

- Explorar vulnerabilidades

Mantendo o acesso

- Garantir o acesso após o ataque
- Back doors
- Trojans, rootkis são utilizados para manter o acesso

INSTITUTO FEDERAL
São Paulo

Mantendo o acesso

- Quanto tempo (dias) você acha que a empresa demora para identificar que foi invadida???
  - Sem ser por ransomware!!!!

- https://content.fireeye.com/m-trends/ig-m-trends-2021

INSTITUTO FEDERAL
São Paulo

Cobrindo rastros

- Tentativa de ocultar a invasão e evitar que os profissionais de segurança da TI descubram ou detectem a invasão

- Remoção ou alteração de log, arquivos ocultos, etc

Laboratórios Aula 1

1-Instale o wireshark e através de print de tela aponte os pacotes listados abaixo acessando um página web:

a- consulta ao DNS

b-conexão de 3 vias

c-término da conexão

d- resposta do protocolo ARP

Dica: procure na internet por filtros específicos para facilitar a busca!

2. Prepare o ambiente virtual de testes para serem usados nas próximas aulas. Você pode instalar uma vm usando o Kali ou parrot.