Introdução a Segurança de rede

Segurança em Redes de Comunicações

Mestrado em Cibersegurança

Mestrado em Engenharia de Computadores e Telemática

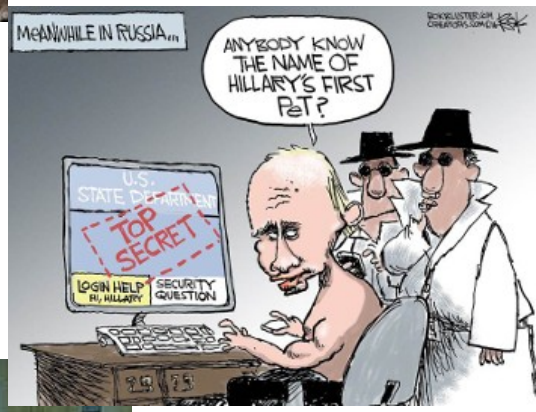
DETI-UA

universidade de aveiro

deti.ua.pt

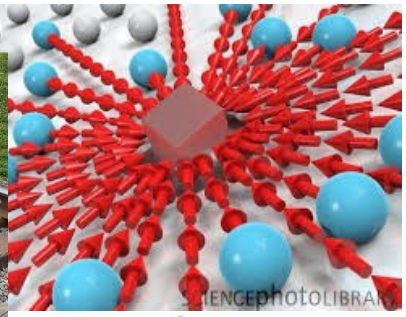
Tipo de ataques (1)

- Objetivos.
  - Diversão e/ou reputação de
  - hacking Fins políticos
  - Fins militares
  - Fins econômicos
  - Outro?
- Objetivos técnicos:
  - Interrupção da operação
  - Para interceptação de dados
  - Ambos
    - Interrupção para interceptar!
    - Interceptar para interromper!

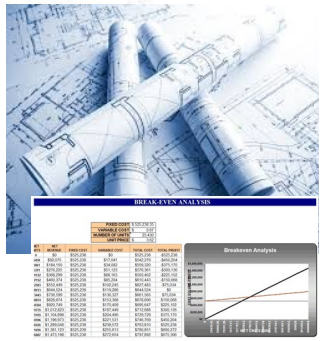


Tipo de ataques (2)

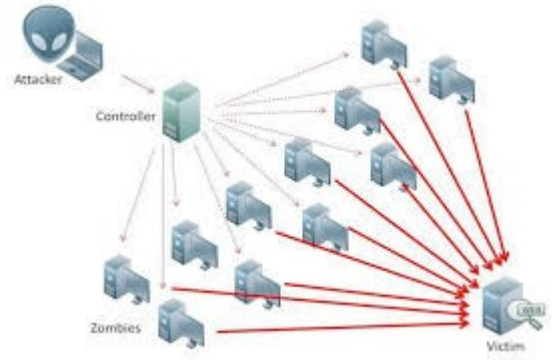
- Objetivos técnicos:
  - Interrupção da operação.
    - (Negação de serviço distribuída.
  - Sequestro de recursos.
    - Spam,
    - Mineração/masternodes em moeda criptografada,
    - plataforma para outros ataques!
  - Interceptação/roubo de dados.
    - Dados pessoais
      - Como objetivo final,
      - Ou como ferramenta para obter mais informações de valor!
    - Dados técnicos,
      - Geralmente usado para obter mais informações de valor!
    - Dados comerciais
      - Objetos digitais, planos financeiros e/ou de engenharia, ...
- A interrupção pode ser usada para conseguir a interceptação!
- A interceptação pode ser usada para causar interrupção (operacional ou comercial)!



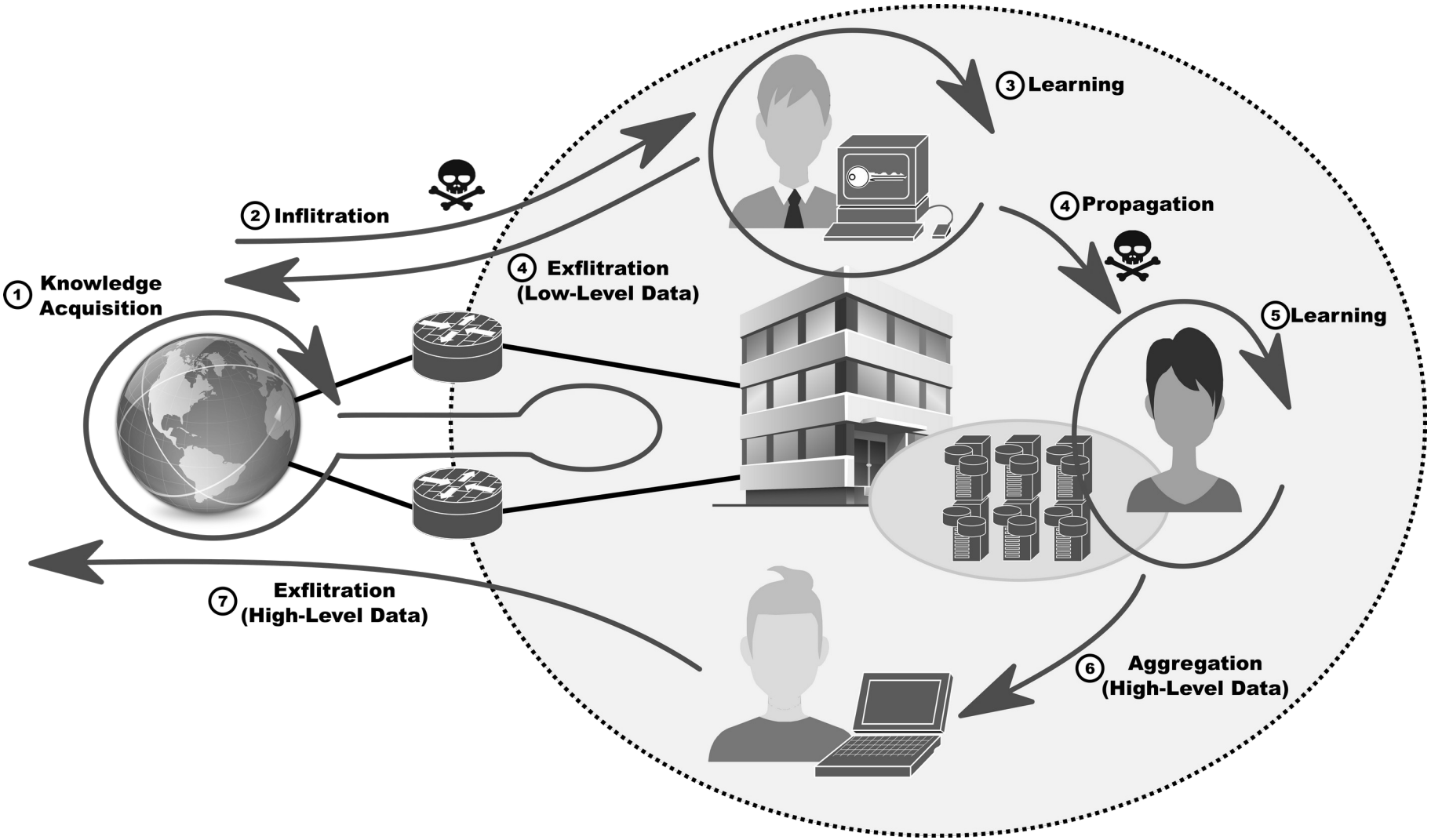


Ataques de interrupção



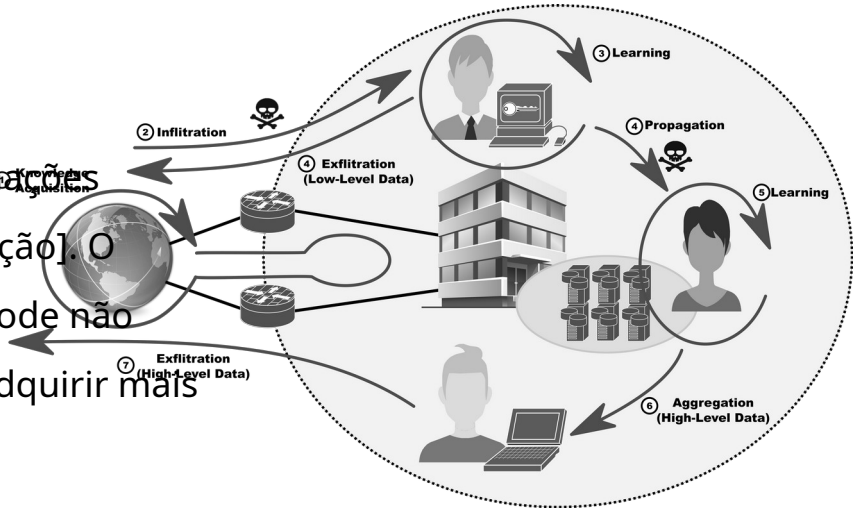
- DoS distribuído
  - Vários dispositivos lentos/pequenos gerando tráfego para um destino
    - TCP x UDP
  - Objetivo da interrupção
    - Por política/econômica/"reputação"
    - Redirecionamento para outro serviço/local?
  - Solução no alvo
    - Balanceadores de carga
    - Para TCP, talvez seja possível sobreviver fazendo redefinições de sessão ativas (com validação de cliente lícita) (servidor/firewalls)
      - Solução de lista branca, para negociação de sessão concluída
    - Para UDP/DNS, bloqueie solicitações para servidores DNS de retransmissão/redirecionamento externos conhecidos (bloqueia amplificação de ataque, falsificação de alvo de IP)
      - Não funciona com botnets grandes e solicitações diretas ao alvo
  - Solução na fonte
    - Detecção de comportamentos anômalos
      - Variações de baixo tráfego difíceis de detectar
      - Mudanças de tempo e periodicidade são mais fáceis de detectar
      - Destinos das mudanças de tráfego
      - Com taxas de dados "realmente baixas" é impossível detectar
- Negação de serviço por interferência de sinal físico
  - Disrupção pura, ou
  - Interrupção para ativar canais secundários (mais facilmente comprometidos).
  - Solução
    - Detecte, localize a fonte e neutralize fisicamente.

Fases de Ataques



Os ataques são feitos de forma incremental

- Escalada de metas e privilégios.
  - O conhecimento público abre portas para informações privadas e acesso a domínios protegidos [Infiltração]. O primeiro acesso ilícito a um domínio protegido pode não fornecer uma saída relevante. O atacante deve adquirir mais conhecimento [Aprendizado].
  - O conhecimento adicional permite acessar outras zonas/dispositivos/ dados de domínio seguros com relevância crescente [Propagação].
    - Em qualquer fase, o invasor pode exigir conhecimento adicional [Aprendizado].
  - Quando um resultado relevante é adquirido, ele deve ser transferido para fora do domínio protegido [Exfiltração].
  - A exfiltração direta pode denunciar os pontos relevantes dentro do domínio seguro.
    - O resultado relevante deve primeiro ser transferido dentro do domínio protegido para um ponto menos importante [Agregação].
    - O atacante escolhe um ponto que pode ser detectado e perdido sem causar danos.



Vulnerabilidades técnicas de rede

- Programas
  - Formulários
  - Estruturas/API
  - Protocolos
  - Sistemas operacionais
    - Kernel, módulos do kernel, drivers e aplicativos básicos.
    - Configurações!
  - Código de baixo nível
    - Microcódigo da CPU, firmware e BIOS/UEFI.
- Hardware
  - Temperamento físico
  - Emissões físicas
    - Emissões eletromagnéticas, som, ...
  - Instabilidade de energia, pulsos eletromagnéticos (EMP), etc...
- Conhecido versus desconhecido
  - CVE
  - Bancos de dados de IDS/IPS e antivírus

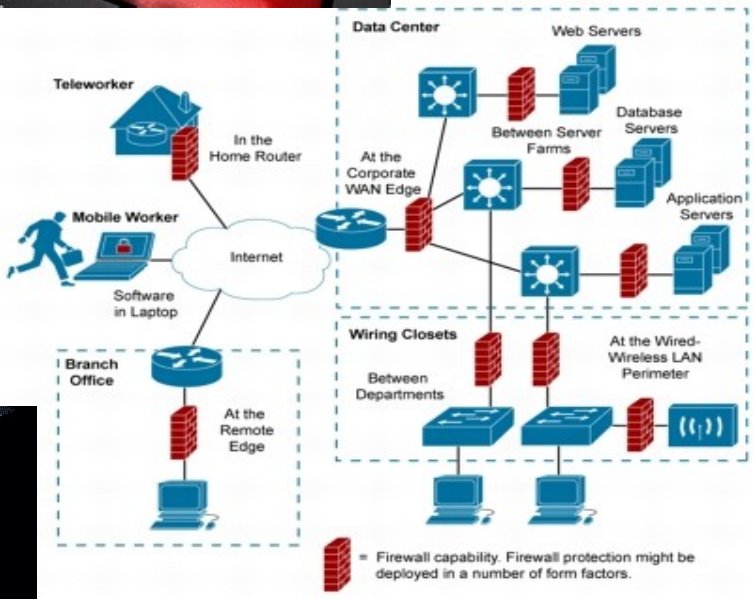
CVE

Common Vulnerabilities and Exposures

universidade de aveiro

Defesas Tradicionais

- Correção de vulnerabilidade.
- Firewalls
  - Centralizado.
  - Distribuído.
- Prevenção de intrusões e Sistemas de Detecção (IDS/IPS).
- Antivírus.



- **Todos confiam no conhecimento prévio da ameaça e/ou problema!**

Defesas “inteligentes”

- Detecção de ameaças e/ou problemas desconhecidos.
  - A tempo de implementar contra-medidas.
- Aplicação de técnicas de Big Data e Data Science para dados de monitoramento de redes e sistemas.
- Algumas soluções tradicionais passam a incorporar IA em seus equipamentos
  - Por exemplo, firewalls de rede de Palo Alto, dispositivos Cisco,...
- Ainda limitado a soluções baseadas no fabricante e dados localizados. Ainda
- limitado em escopo.
  - Ameaças óbvias versus ameaças furtivas.
- A implantação ideal requer um conhecimento geral da rede e dos sistemas.
  - Consciência situacional de redes e sistemas (cibernéticos).

Fase de infiltração

- As máquinas lícitas devem ser comprometidas para implementar as diferentes fases dos ataques.
  - Idealmente numa “zona” privilegiada da rede, e/ou
  - Com credenciais de acesso, e/ou
    - Credenciais de usuário, endereço(s), chave de hardware, etc...
  - Com software “especial” e/ou
  - dados de destino.
- Pode incluir a instalação de software ou o uso de software vulnerável lícito.
- Pode ser controlado remotamente (constantemente ou não).
  - Comando e controle (C&C).
- Pode ter bots autônomos (IA) instalados para realizar ações ilícitas.
  - Quando o C&C remoto não é possível ou está sujeito a fácil detecção.

Fase de propagação

- Feito usando uma mistura de metodologias:
  - Exploração de credenciais.
    - Uso direto ou usando aplicativos permitidos.
  - Representando usuários e sistemas.
    - Semelhante à exploração de credenciais, mas mais avançada com base no conhecimento adquirido (comportamento lícito).
    - Requer tempo para aprender e imitar o comportamento lícito.
      - Padrões de tempo, padrões de tráfego, padrões de aplicativos, etc...
  - Exploração de vulnerabilidades.
    - Dentro de um domínio protegido, os sistemas são muitas vezes considerados uma zona segura.
    - Sistemas operacionais/aplicativos menos mantidos e legados podem ser necessários para execução (sem aplicação de patches).
    - Gama mais ampla de vulnerabilidades

Fase de agregação e exfiltração

- Dados transferidos de máquina para máquina.
- Internamente [Agregação] isso pode ser feito usando canais existentes.
- Externamente [Exfiltração]
  - Isso pode ser feito diretamente usando os canais existentes.
    - Cópia de arquivo, e-mail, compartilhamento de arquivos,
    - etc... Podem ser detectados.
  - Isso pode ser feito ocultando informações em canais existentes/permitidos e comunicações lícitas.
    - Transferência de dados mais lenta, mais difícil (impossível?) de
    - detectar. Exemplos:
      - Uso de esteganografia em fotos (via redes sociais).
      - Uso de dados incorporados em mensagens de texto e voz.
      - . . .

Métricas/KPI de segurança

- Gerenciamento de acesso
  - Quantos usuários têm acesso administrativo e com que frequência é usado.
  - Senhas compartilhadas entre funcionários.
- Preparação
  - Porcentagem de dispositivos totalmente corrigidos e atualizados.
- Dias para corrigir
  - Tempo médio entre a disponibilidade do patch e a implantação.
- Dispositivos não identificados
  - Dispositivos implantados ilicitamente.
  - Política BYOD, dispositivos legados, dispositivos não listados, dispositivos IoT, etc...
- Carga média/máxima dos dispositivos de segurança por período de tempo.
- Tentativas de intrusão
  - Quantidade de tentativas detectadas e não detectadas (em tempo real ou após auditoria off-line).
- Custo por incidente
  - Inclui horas extras da equipe, suporte externo, custos de investigação, perda de produtividade dos funcionários, perda de comunicação, falha no serviço, etc.
- Tempo Médio entre Falhas (MTBF)
  - Tempo médio entre falhas (hardware e/ou software).
  - Geral ou por dispositivo/serviço.
- Tempo Médio de Recuperação (MTTR)
  - Tempo médio entre falha e recuperação (hardware e/ou software).
- Tempo Médio para Detecção (MTTD)
  - Tempo médio entre intrusão e detecção.
- Tempo Médio para Reconhecimento (MTTA)
  - Tempo médio entre a detecção e o início da implantação de contramedidas.
- Tempo médio de contenção (MTTC)
  - Tempo médio entre o início da implantação de contramedidas e a mitigação completa.
- Tempo Médio para Resolução (MTTR)
  - MTTA+MTTR