Planejamento

02/07	Retomada / Explicação do Trabalho	
04/07	Defesa avançada de Redes (Raphael)	Estado-da-arte em NIDS
09/07	Tempo para fazer trabalho	
11/07	Tempo para fazer trabalho	
16/07	Revisão SO/SB	
18/07	Vulnerabilidades e ataques em sistemas	BO, ROP, OOB, EoP
23/07	Exploração de vulnerabilidades no kernel Linux	CVE-2023-2008
25/07	Análise de ataques	Tracing
30/07	Defesas para sistemas	Controle de acesso, antivírus, hardening
01/08	PROVA 2	
02/08	Prazo final: solicitação de 2a chamada da P1	
10/08	FIM DO PERÍODO LETIVO	
13/08	EXAME FINAL	
17/08	Último dia para lançar notas e frequências	

Trabalho: Mitnick Attack - LAN

Jorge Correia

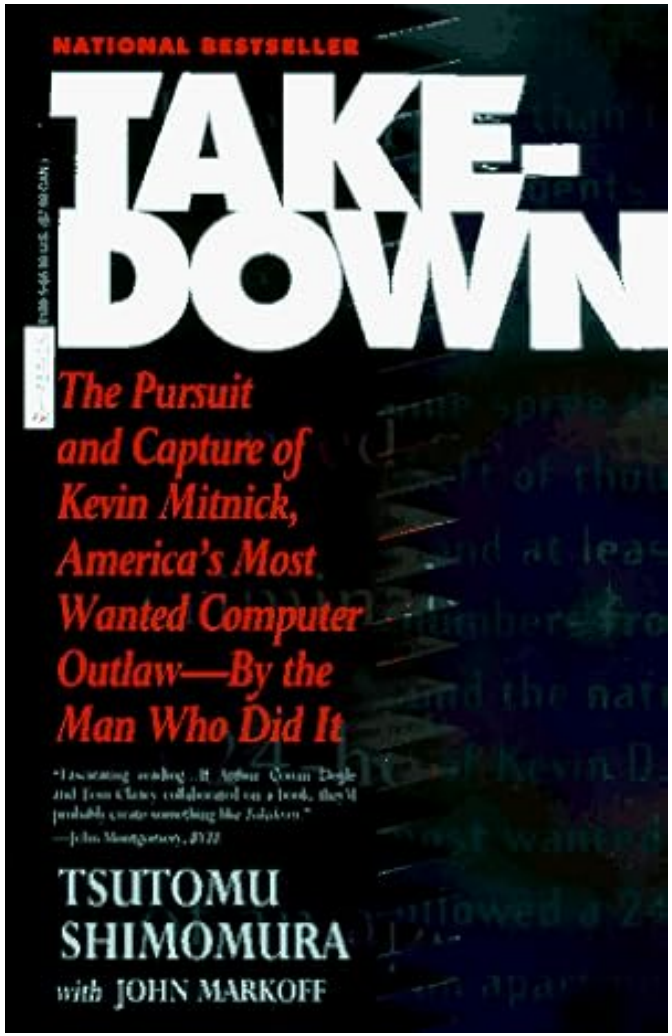
Segurança Computacional
Universidade Federal do Paraná

2024

Kevin Mitnick

Tsutomu Shimomura

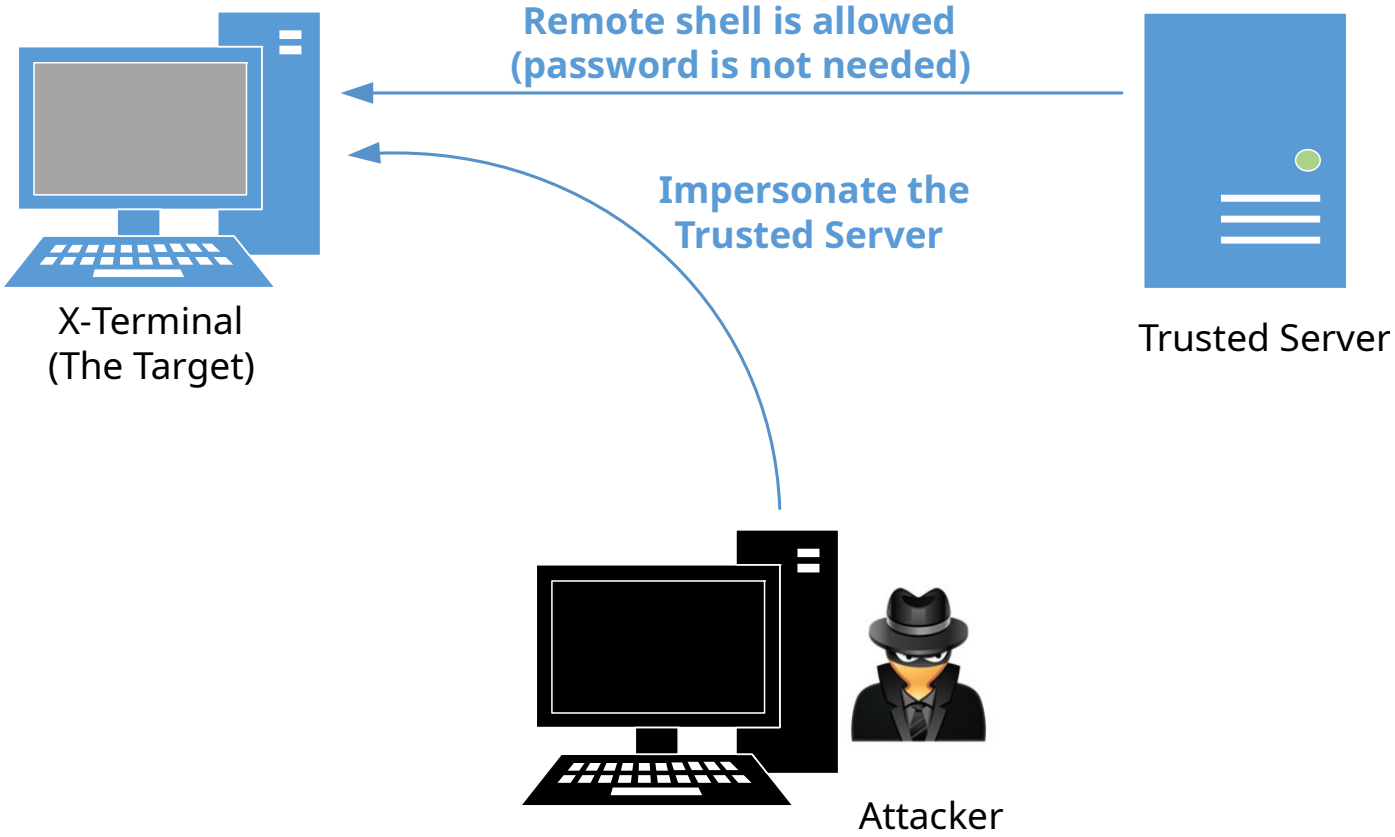
Tsutomu Shimomura



Mitnick Attack

- 1994
- Duas vulnerabilidades no protocolo TCP
- Relação de confiança entre duas máquinas do Shimomura
- TCP session hijack

Arquitetura



Número de Sequência Inicial TCP

- Na criação da uma conexão TCP, cada lado escolhe um número de sequência inicial

Número de Sequência Inicial TCP

- Na criação da uma conexão TCP, cada lado escolhe um número de sequência inicial
- Na época do ataque, o número de sequência inicial (ISQ) seguia um padrão

Número de Sequência Inicial TCP

- Na criação da uma conexão TCP, cada lado escolhe um número de sequência inicial
- Na época do ataque, o número de sequência inicial (ISQ) seguia um padrão
- Mitnick enviou um pacote SYN, seguido de um pacote RST para verificar o ISQ utilizado

Número de Sequência Inicial TCP

- Na criação da uma conexão TCP, cada lado escolhe um número de sequência inicial
- Na época do ataque, o número de sequência inicial (ISQ) seguia um padrão
- Mitnick enviou um pacote SYN, seguido de um pacote RST para verificar o ISQ utilizado
- Existia um padrão entre duas conexões sucessivas.

Derrubar o Trusted Server

- As respostas do X-terminal chegariam no Trusted Server, e este responderia com RST

Derrubar o Trusted Server

- As respostas do X-terminal chegariam no Trusted Server, e este responderia com RST
- Para resolver o problema, Mitnick realizou um DoS através de um SYN flood

TCP/RSH Spoof

- Com o ISQ previsível e o Trusted Server derrubado, Mitnick conseguiu forjar uma conexão TCP da sua máquina como se fosse o Trusted Server

TCP/RSH Spoof

- Com o ISQ previsível e o Trusted Server derrubado, Mitnick conseguiu forjar uma conexão TCP da sua máquina como se fosse o Trusted Server
- Ele não recebia as respostas de fato

TCP/RSH Spoof

- Com o ISQ previsível e o Trusted Server derrubado, Mitnick conseguiu forjar uma conexão TCP da sua máquina como se fosse o Trusted Server
- Ele não recebia as respostas de fato
- Após a finalização do three-way-handshake, era necessário iniciar uma conexão RSH

TCP/RSH Spoof

- Com o ISQ previsível e o Trusted Server derrubado, Mitnick conseguiu forjar uma conexão TCP da sua máquina como se fosse o Trusted Server
- Ele não recebia as respostas de fato
- Após a finalização do three-way-handshake, era necessário iniciar uma conexão RSH
- O arquivo de configuração .rhosts define quais são os IPs que podem acessar a máquina sem autenticação

TCP/RSH Spoof

- Com o ISQ previsível e o Trusted Server derrubado, Mitnick conseguiu forjar uma conexão TCP da sua máquina como se fosse o Trusted Server
- Ele não recebia as respostas de fato
- Após a finalização do three-way-handshake, era necessário iniciar uma conexão RSH
- O arquivo de configuração .rhosts define quais são os IPs que podem acessar a máquina sem autenticação
- Adicionar a string "+ +" no arquivo .rhosts permite o acesso sem autenticação por qualquer máquina

Adaptando o ataque para os dias atuais

- Não é possível derrubar uma máquina com SYN flood

Adaptando o ataque para os dias atuais

- Não é possível derrubar uma máquina com SYN flood
- O ISQ é randômico

Adaptando o ataque para os dias atuais

- Não é possível derrubar uma máquina com SYN flood
- O ISQ é randômico
- E se considerarmos um cenário em LAN?

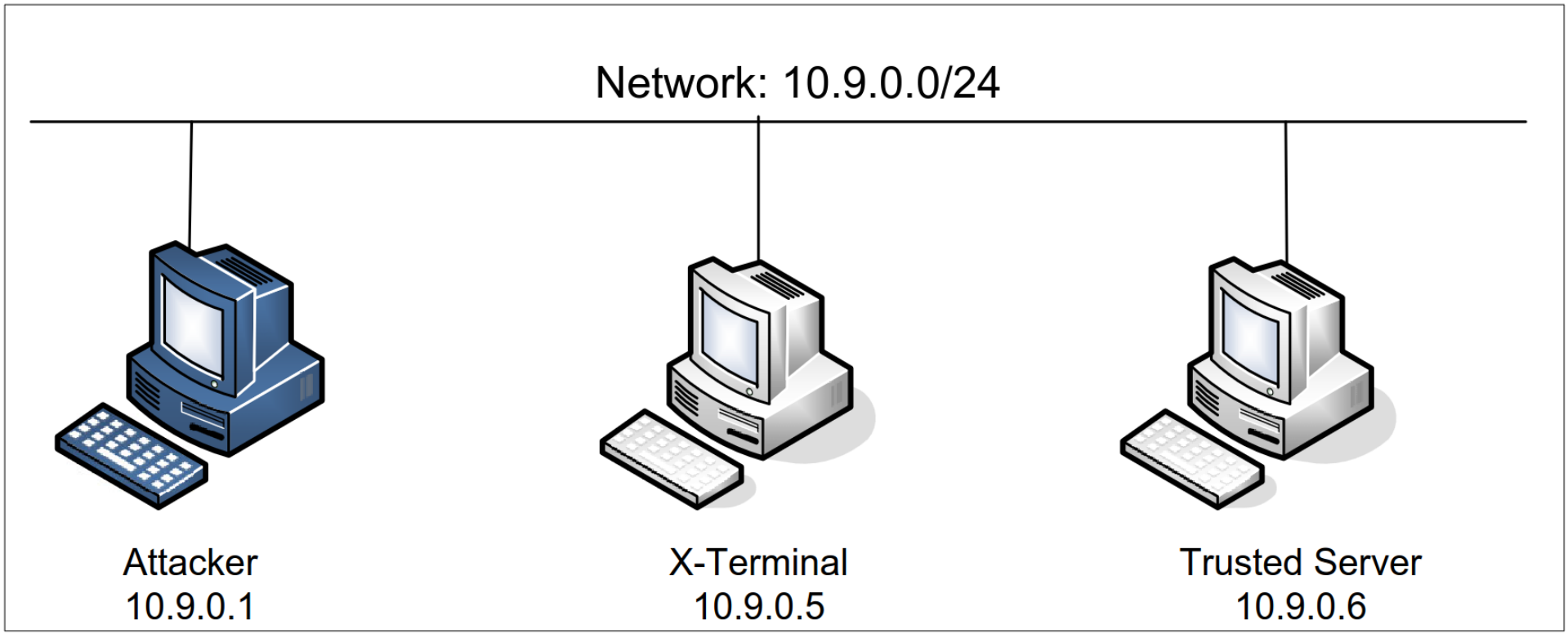
Objetivo do trabalho

- Realizar o Mitnick Attack, sem as vulnerabilidades do TCP citadas anteriormente
- Considerar um cenário em LAN

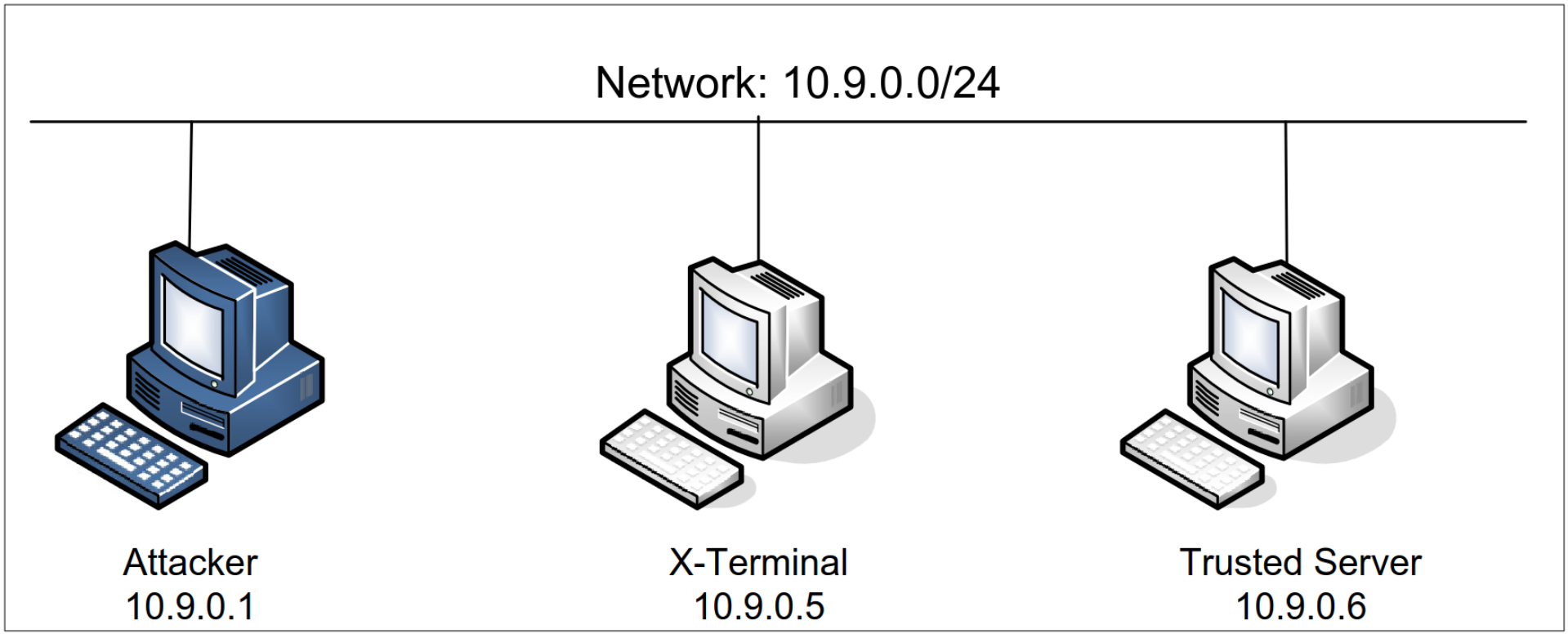
Objetivo do trabalho

- Realizar o Mitnick Attack, sem as vulnerabilidades do TCP citadas anteriormente
- Considerar um cenário em LAN
- Será disponibilizado um ambiente Docker

Rede


Network: 10.9.0.0/24
Attacker
10.9.0.1
X-Terminal
10.9.0.5
Trusted Server
10.9.0.6

Rede



- Diretório volumes

Requisitos obrigatórios

- Utilizar ARP spoofing para derrubar o Trusted Server e capturar o ISN
- Forjar pacotes do three-way-handshake, conexão RSH, e execução de comandos via RSH
- Conseguir acesso à máquina X-terminal via máquina atacante

Entrega

- Scripts utilizados para realizar o ataque
- Documentação dos scripts e descrição de reprodução
- Prazo: 12/07