CADERNO DO ALUNO

Auditoria Wireless: laboratório com Archer C50 V6

WEP · WPA · WPA2 · WPA3 | Captura controlada e análise de credenciais fictícias

MATERIAL DO ALUNO • 4 horas • TP-Link Archer C50 V6.0 • Parrot Security OS

Curso: Técnico em Segurança Cibernética | Plano de Curso Senac 316 | Professor: Msc Arlindo Batista Xavier Filho

Situação-problema e objetivo

O Centro Horizonte precisa justificar a atualização da segurança wireless. O grupo deverá demonstrar, exclusivamente com o roteador de laboratório, diferenças de configuração, autenticação e resistência a tentativas de descoberta de uma senha fictícia. Não haverá testes em redes reais de terceiros.

Evidências de aprendizagem

- Identificar SSID, BSSID, canal, protocolo, cifra e tipo de autenticação do AP de teste.
- Gerar um dicionário limitado com o Crunch e verificar seu tamanho antes da execução.
- Obter captura passiva somente da WLAN didática e analisar seu conteúdo.
- Distinguir uma demonstração WPA2-PSK bem-sucedida de um resultado não aplicável a WPA3/SAE.
- Documentar conclusões, limitações e recomendações de segurança.

Cronograma de 240 minutos

Momento	Duração
Abertura e limites de autorização	20 min
Montagem da bancada e verificação do C50	30 min
Parrot, reconhecimento e captura	30 min
Experimento WEP ou análise preparada	35 min
Experimento WPA legado ou análise preparada	35 min
Experimento WPA2 com Crunch e Aircrack-ng	50 min
Experimento WPA3/SAE	25 min
Relatório e síntese	15 min

1. Regras para a bancada

- Somente roteador do professor e cliente explicitamente autorizado; não capturar redes próximas.
- WAN desconectada. A ausência de Internet não impede que o Wi-Fi seja recebido fora da sala: reduzir exposição e tempo de uso de protocolos antigos.
- Não usar senhas, MACs ou arquivos de captura pessoais. Desabilitar WEP/WPA legado ao final.
- Não utilizar quadros de desautenticação forçada, ataques de negação de serviço ou injeção de pacotes.
- Não publicar capturas reais, BSSIDs da instituição, senhas ou dados pessoais no portal.

2. Montagem da bancada

Topologia: notebook de administração --cabo LAN--> Archer C50 V6.0 <--Wi-Fi-- cliente de teste. O adaptador USB do Parrot observa somente o BSSID didático; WAN desconectada.

Parâmetro	Ajuste proposto
Equipamento	Archer C50 V6.0, conferir região BR, firmware e menus antes de usar
WAN	Desconectada; não ligar à rede institucional
LAN	192.168.50.1/24 (configuração proposta, não padrão de

	fábrica)
DHCP	192.168.50.100 a 192.168.50.150
Rádio	2,4 GHz; canal 6 se apropriado; largura 20 MHz
WPS/gerenciamento remoto	Desabilitados, se disponíveis no firmware
Cliente	Notebook/celular de teste autorizado
Acesso admin	Somente via cabo Ethernet
SSID	Um dos nomes TSC03-WEP, TSC03-WPA, TSC03-WPA2, TSC03-WPA3 por vez

Anote no caderno: revisão de hardware V6.0 (confirmada); versão de firmware (a verificar); BSSID da banda de 2,4 GHz; canal observado; opções de segurança existentes no menu. O C50 tem múltiplas revisões e os menus podem variar.

3. Preparação do Parrot OS

```
sudo apt update
sudo apt install -y iw aircrack-ng crunch wireshark tshark tcpdump
ip -br link
iw dev
iw list
sudo airmon-ng
```

Localize a interface Wi-Fi USB e confirme “monitor” em Supported interface modes. Se for uma VM, faça o repasse do dispositivo USB; uma interface Ethernet virtual não captura quadros 802.11 nativamente.

```
sudo airmon-ng start wlan1
# Confirme o nome real, geralmente wlan1mon:
iw dev
mkdir -p ~/TSC03-C50/capturas ~/TSC03-C50/dicionarios
cd ~/TSC03-C50
```

Substitua wlan1 pelo nome realmente exibido. Se a alteração interromper a rede do Parrot, use conexão administrativa via outra interface ou opere offline.

4. Reconhecimento controlado do C50

Com um único SSID de teste ativo, confirme canal e BSSID na interface administrativa do TP-Link e filtre a captura por esses valores. Endereços abaixo são ilustrativos.

```
sudo airodump-ng --bssid AA:BB:CC:DD:EE:FF \
  --channel 6 --write capturas/wpa2-lab wlan1mon
```

Mude o nome do arquivo para cada protocolo. Pressione Ctrl+C ao encerrar. O campo BSSID é o identificador do rádio — não é o nome do SSID. Somente reconecte voluntariamente o dispositivo cliente de laboratório.

5. Crunch: criando um dicionário pequeno

Para ilustrar previsibilidade, utilizaremos o padrão fictício Aula%%2026. No Crunch, % representa um algarismo de 0 a 9. O padrão produz 100 combinações com dez caracteres.

```
crunch 10 10 -t 'Aula%%2026' -o dicionarios/c50-100.txt
wc -l dicionarios/c50-100.txt
wc -c dicionarios/c50-100.txt
grep -Fx 'Aula422026' dicionarios/c50-100.txt
```

A senha exclusivamente didática da WLAN WPA2 será Aula422026. Nunca reutilize esse padrão em uma rede efetiva. O comando não gera uma senha “segura”; gera candidatos previsíveis para avaliação didática.

6. Quatro estações experimentais

Protocolo e SSID	Atividade	Resultado que deve ser registrado
WEP: TSC03-WEP	Se a opção existir, configurar WEP com	WEP apresenta problemas próprios de

	chave fictícia AB123 (5 ASCII, 40 bits efetivos); capturar IVs do tráfego legítimo; analisar com Aircrack-ng.	projeto. Se não houver IVs suficientes ou o modo for inexistente, registrar limitação.
WPA: TSC03-WPA	Somente se WPA-Personal legado estiver disponível; conectar cliente consentido, capturar associação e testar dicionário local.	Confirmar se é realmente WPA/TKIP, e não modo misto WPA2.
WPA2: TSC03-WPA2	WPA2-Personal/AES; senha Aula422026; capturar handshake por reconexão voluntária; testar wordlist de 100 entradas.	A captura deve conter handshake válido e a palavra do dicionário deve coincidir.
WPA3: TSC03-WPA3	WPA3-Personal/SAE puro se disponível; cliente compatível; observar RSN/SAE e PMF; comparar com WPA2.	Não pressupor recuperação offline da senha por captura passiva SAE.

7. Experimentos e comandos de análise

Para WEP, use os arquivos produzidos na própria bancada; o resultado depende da quantidade e qualidade dos IVs. Não empregue injeção para acelerar tráfego.

```
# Somente se existir uma captura WEP legítima suficiente:
aircrack-ng -b AA:BB:CC:DD:EE:FF capturas/wep-lab-01.cap
```

Em WPA ou WPA2-Personal, confirme o handshake no airodump-ng ou examine EAPOL no Wireshark. Só depois execute o teste com candidatos fictícios:

```
# Só depois de capturar handshake WPA2-PSK válido:
aircrack-ng -w dicionarios/c50-100.txt \
  -b AA:BB:CC:DD:EE:FF capturas/wpa2-lab-01.cap
```

A mensagem “No valid WPA handshakes found” indica ausência de material suficiente para o teste; “KEY NOT FOUND” significa que os candidatos testados não recuperaram a senha. Nenhum desses resultados prova segurança absoluta. WPA3/SAE usa outra negociação e não deve ser avaliado pela mesma hipótese de dicionário offline.

8. Evidências e reflexão final

Protocolo	Opção no C50?	Captura válida?	Resultado/limitação
WEP			
WPA			
WPA2			
WPA3			

- Por que uma senha previsível compromete WPA2-Personal mesmo quando usa AES?
- Por que o teste offline realizado em WPA2 não representa quebra de WPA3/SAE?
- Que medidas recomendaria ao Centro Horizonte: WPA3, WPA2/AES, WPS, senhas, segmentação e atualizações?

Entrega: um parecer de até uma página, acompanhado de evidências sanitizadas (sem senhas reais), configuração do laboratório e declaração das limitações observadas.

Referências técnicas consultadas

TP-Link - Download Archer C50 V6: https://www.tp-link.com/br/support/download/archer-c50/v6/

TP-Link - Especificações Archer C50: https://www.tp-link.com/br/home-networking/wifi-router/archer-c50/

Aircrack-ng - Airodump-ng: https://aircrack-ng.org/doku.php?id=airodump-ng

Aircrack-ng - WPA/WPA2 (referência técnica): https://aircrack-ng.org/doku.php?id=pt-br:cracking_wpa

Debian - Crunch manual: https://manpages.debian.org/trixie/crunch/crunch.1.en.html

NIST SP 800-153 - WLANs: https://csrc.nist.gov/pubs/sp/800/153/final

Folha de registro final da equipe

Equipe: _____ Data: _____ Código da bancada: _____

Firmware do C50 observado: _____ Canal: _____ BSSID anonimizado: _____

Teste executado	Evidência verificada	Conclusão/limitação
WEP (se disponível)		
WPA legado (se disponível)		
WPA2-PSK/AES		
WPA3-Personal/SAE		

Recomendação para uma WLAN real: _____

_____

Assinatura do relator: _____ Confirmação de desligamento WEP/WPA: _____