

POLITECHNIKA ŚWIĘTOKRZYSKA		
Cyberbezpieczeństwo – Laboratorium 5		
Kierunek: Informatyka	Rok: 4	Semestr: VII
Student: Krzysztof Siwoń	Data wykonania: 08.12.2018	

Cyberbezpieczeństwo- Lab5_part_1-threats_and_attacks

Cel laboratorium

W tym ćwiczeniu skonfiguruje sieci Wi-Fi dla trzech lokalizacji geograficznych. Ta aktywność będzie korzystać z WEP, WPA2 PSK i WPA2 RADIUS w celu zademonstrowania różnych konfiguracji sieci Wi-Fi i ich względów bezpieczeństwa. Opieka zdrowotna w domu zostanie skonfigurowana za pomocą WEP. Oddział Gotham Healthcare Branch zostanie skonfigurowany z WPA2 PSK, a centrala Metropolis Bank będzie korzystała z promienia WPA2. Adresowanie IP, konfiguracja sieci i konfiguracje usług są już kompletne. Będziesz korzystać z routerów bezprzewodowych i urządzeń klienckich w różnych regionach geograficznych, aby skonfigurować wiele bezpiecznych sieci bezprzewodowych.

Part 1: Configure WEP for Healthcare at Home

Step 1: Setup the Wireless SSID.

What is the IP address for the default gateway?

Default Gateway.....: 10.44.3.1

Step 2: Setup Wireless Security.

WEP and the key 0123456789 are not secure. Why is WEP not recommended for use in securing wireless networks?

WEP (ang. Wired Equivalent Privacy) – standard szyfrowania stosowany w sieciach bezprzewodowych, Do ochrony danych w standardzie WEP wykorzystuje się algorytm RC4, który jest symetrycznym szyfrem strumieniowym z kluczem poufnym.

Według badań przeprowadzonych przez Fluhrera, Mantina i Shamira do złamania jednego bajta klucza niezbędne jest rozkodowanie około 60 pakietów. Wraz ze wzrostem ilości rozkodowanych bajtów wzrasta tempo rozkodowywania. Wydłużenie klucza spowoduje jedynie podwojenie czasu, jaki jest potrzebny na rozszyfrowanie klucza. W praktycznym wykorzystaniu wyników badań przypuszczenia autorów jedynie się potwierdziły. Do złamania całego klucza WEP wystarczyło 256 pakietów. Osoby, które przeprowadziły ten atak opracowały narzędzie AirSnort, które służy do rozszyfrowywania kluczy WEP. Program ten jest dostępny łącznie z kodem źródłowym w internecie.

Jakie hasła stosować:

odpowiednio długie (min. 10 znaków)

odpowiednio skomplikowane

Nie może być używanym wyrazem słownikowym

Musi zawierać znaki specjalne

Musi być zmieniane raz na 1-3 miesiące

Part 3: Configure WPA2 RADIUS for Metropolis Bank HQ

Step 4: Connect the Clients.

When considering a large organization, why is WPA2 RADIUS more beneficial than WPA2 PSK?

RADIUS jest lepszą opcją, pod warunkiem, że używane są bezpieczne (tj. Długie) hasła i istnieje rozsądna polityka blokowania.

Głównym powodem tego jest to, że w przypadku usługi RADIUS należy przeprowadzić interakcję z usługą uwierzytelniania w celu przetestowania hasła, a zatem po zablokowaniu oznacza to koniec próby złamania zabezpieczeń.

W przypadku WPA2 PSK poważnym problemem jest możliwość ataku typu bruteforce

Cisco Packet Tracer - E:\SZKOŁA\SEMESTR VII\IOT\cybersecurity_lab\Cyberbezpieczeństwo- Lab... — □ ×

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 00:44:49

Congratulations Guest! You completed the activity.

Overall Feedback **Assessment Items** Connectivity Tests

Expand/Collapse All Show Incorrect Items

Assessment Items	Status	Points
[-] Security Mode		
✓ Authen Type	Correct	2
✓ Encryption Type	Correct	2
✓ RADIUS Server IP	Correct	2
✓ RADIUS Shared Secret	Correct	2
✓ SSID	Correct	2
✓ SSID BroadCast	Correct	2
[-] Bob		
[-] Wireless		
[-] Security Mode		
✓ Password	Correct	2
✓ User Id	Correct	2
[-] Dave		
[-] Wireless		
[-] Security Mode		
✓ Authen Type	Correct	2
✓ Encryption Type	Correct	2
✓ WEP Key	Correct	1
[-] Mary		
[-] Wireless		
[-] Security Mode		
✓ Authen Type	Correct	2
✓ Encryption Type	Correct	2
✓ WEP Key	Correct	2
[-] Mike		
[-] Wireless		
[-] Security Mode		
✓ Authen Type	Correct	2
✓ Encryption Type	Correct	2
✓ Pass Phrase	Correct	2
[-] NTP/AAA		

Score : 90/90

Item Count : 41/41

Component	Items/Total	Score
Other	41/41	90/90

Cyberbezpieczeństwo-Lab5_part_2

privacy_VPN_transparent_mode

Cel laboratorium

W tym ćwiczeniu zaobserwujemy transfer niezaszyfrowanego ruchu FTP między klientem a witryną zdalną. Następnie skonfigurujemy klienta VPN w celu połączenia się z witryną Gotham Healthcare Branch i wysłania zaszyfrowanego ruchu FTP.

Part 1: Sending Unencrypted FTP Traffic

Step 3: View the traffic on the Cyber Criminals Sniffer.

Click the **FTP** messages displayed on the sniffer and scroll to the bottom of each one.

What information is displayed in clear text?

Informacje zawarte w pakietach są niezaszyfrowane możemy tam znaleźć login hasło i przesyłany plik które nie są zaszyfrowane.

Part 2: Configuring the VPN Client on Phil's Computer

What is the Client IP for the client-to-site VPN connection?

10.44.2.200

What extra IP address is now shown that was not shown before in Part 1 Step 2c?

Tunnel Interface IP Address.....: 10.44.2.200

Part 3: Sending Encrypted FTP Traffic

Are there any FTP messages displaying the password of internal or the file upload of PrivateInfo.txt? Explain

Nie nie ma ponieważ używamy dane został zaszyfrowane protokołem ESP, udostępniającym możliwość szyfrowania pakietów.

Cisco Packet Tracer - E:\SZKOŁA\SEMESTR VII\IOT\cybersecurity_lab\Cyberbezpieczeństwo- Lab5_part_2-pr...

File Edit Options View Tools Extensions Help

Activity Results Time Elapsed: 00:37:53

Congratulations Guest! You completed the activity.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All Show Incorrect Items

Assessment Items	Status	Points	Component(s)
Network			
Private_FTP		0	Other
FTP Server		0	Other
Server Files		0	Ip
PrivateInfo.txt	Correct	20	Ip
Public_FTP		0	Other
FTP Server		0	Other
Server Files		0	Ip
PublicInfo.txt	Correct	20	Ip

Component	Items/Total	Score
Ip	2/2	40/40

Score : 40/40
Item Count : 2/2

Cyberbezpieczeństwo- Lab5_part_3-privacy_VPN_tunnel_mode

Cel laboratorium

W tym działaniu zaobserwujemy transfer niezaszyfrowanego ruchu FTP między dwiema lokalizacjami geograficznymi. Następnie skonfigurujemy tunel VPN między dwiema lokalizacjami geograficznymi i wyślemy zaszyfrowany ruch FTP.

Part 1: Sending Unencrypted FTP Traffic

Step 3: View the traffic on the Cyber Criminals Sniffer.

Click the **FTP** messages displayed on the sniffer and scroll to the bottom of each one.

What information is displayed in clear text?

Informacje zawarte w pakietach są niezaszyfrowane możemy tam znaleźć login hasło które nie są zaszyfrowane.

Part 3: Sending Encrypted FTP Traffic

Are there any FTP messages sourced from the IP of **Sally's** computer? Explain.

Nie nie ma, ESP (ipsec) zaszyfrowuje pakiet i nie widać z jakiego protokołu korzysta sesja.

The screenshot shows the 'Assessment Results' window in Cisco Packet Tracer. It displays a tree view of assessment items and a summary table on the right.

Assessment Items Table:

Assessment Items	Status	Points	Component(s)	Feedback
Network				
File Backup		0	Other	
FTP Server		0	Other	
Server Files		0	Ip	
FTPupload.txt	Correct	15	Ip	
HQ_Router				
ACL		0	Other	
110	Correct	3	ACL	
IKE				
Crypto IpSec Transform Sets				
Set VPN-SET				
ESP Authentication Transform	Correct	3	Ip	
ESP Encryption Transform	Correct	3	Ip	
Name	Correct	3	Ip	
Crypto ISAKMP Key Address Pairs		0	Ip	
vpnpass	Correct	3	Ip	
Crypto ISAKMP Policy				
Policy 10				
Authentication type	Correct	2	Ip	
Encryption	Correct	2	Ip	
Group	Correct	2	Ip	
Hash algorithm	Correct	2	Ip	
Lifetime	Correct	2	Ip	
Number 10	Correct	2	Ip	
Crypto Map Sets				
Set				
Name	Correct	2	Ip	
Ports		0	Ip	
Port	Correct	2	Io	

Summary Table:

Component	Items/Total	Score
ACL	1/1	3/3
Ip	13/13	43/43
Other	1/1	4/4

Overall Feedback: Congratulations Guest! You completed the activity.

Score: 50/50
Item Count: 15/15

Buttons: Expand/Collapse All, Show Incorrect Items, Close