Atividade Orientada a Ensino

Acadêmico: Gabriel Neris dos Santos
RGA: 202019070232
Professor: Carlos Alberto da Silva
Atividade: Segurança da informação aplicada a redes Wireless

INTRODUÇÃO

O presente documento delineia o progresso da atividade orientada de ensino, cujo propósito é a investigação dos padrões de segurança em redes sem fio e sua operação, incluindo a realização de testes de intrusão utilizando a vulnerabilidade identificada no padrão WPS. Serão apresentadas as tecnologias e ferramentas analisadas e empregadas ao longo do desenvolvimento desta pesquisa.

REDES SEM FIO (WIRELESS)

O padrão IEEE 802.11, popularmente conhecido como Wi-Fi (Wireless Fidelity) foi publicado em 1999, tornando-se a principal tecnologia para redes locais sem fio desde então. Este é amplamente utilizado em locais de trabalho, instituições de ensino, residências, aeroportos, cafeterias, além de outros locais que necessitam de fornecer acesso à internet via conexão sem fio.

Enquanto no meio cabeado a conexão de um dispositivo requer a utilização de um cabo, pelo qual as informações são exclusivamente transmitidas, nas redes sem fio, devido ao uso de radiodifusão, as informações se propagam por todo o alcance da rede, facilitando a recepção de pacotes de informações não solicitadas por computadores vizinhos.

Devido a isso, ao longo dos anos, em resposta a essa questão, foram desenvolvidos protocolos de segurança específicos para o padrão 802.11, destacando-se entre eles o WEP, WPA e WPA2. Esses protocolos visam garantir a integridade e a confidencialidade das informações transmitidas em ambientes de redes sem fio, proporcionando uma abordagem mais robusta para mitigar potenciais ameaças à segurança.

WEP

Na década de 1990, o WEP (Wired Equivalent Privacy) foi desenvolvido para conferir segurança a redes sem fio, aspirando igualá-las às redes com fio em termos de proteção. Embasado nos princípios de confidencialidade, autenticidade e integridade, o WEP utiliza o algoritmo RC4. Contudo, suas múltiplas vulnerabilidades, incluindo a utilização de apenas 24 bits em um total de 128 bits no vetor de inicialização da chave, tornaram-no obsoleto. O WEP2 foi introduzido para corrigir falhas, mas foi eventualmente substituído pelo mais robusto protocolo WPA, devido às suas limitações e preocupações com a segurança.

WPA

O protocolo WPA foi desenvolvido para corrigir as falhas de segurança presentes no WEP, sem a necessidade de substituição de equipamentos. Uma melhoria significativa foi a implementação do MIC (Message Integrity Check) para verificar a integridade dos dados transmitidos, embora tenha aberto a possibilidade de ataques de negação de serviço. O TKIP (Temporal Key Integrity Protocol) desempenha um papel crucial no WPA para criptografar mensagens, adotando medidas preventivas contra possíveis ataques. Ao contrário do WEP, o TKIP evita o envio não criptografado da chave secreta e utiliza uma abordagem mais sofisticada na gestão dos vetores de inicialização.O WPA baseia-se em uma chave secreta chamada PMK (Pairwise Master Key), que gera uma PTK (Pairwise Transient Key) durante a conexão, fortalecendo a segurança da comunicação sem fio. Além disso, destaca-se a criação de diferentes modos de funcionamento, como o Personal para redes domésticas e o Enterprise para corporações, proporcionando um nível adicional de segurança com um servidor de autenticação centralizado.

WPA2

O WPA, ao implementar apenas uma parte do novo padrão IEEE 802.11i, cedeu lugar ao WPA2, que se tornou o novo protocolo padrão para redes sem fio, por abranger todos os pontos do referido padrão. Este protocolo introduziu melhorias significativas em sua criptografia ao adotar o protocolo CCMP, fundamentado no AES (Advanced Encryption Standard), proporcionando maior robustez e resistência contra ataques. Além disso, incorporou um mecanismo de pré-autenticação dedicado à redução da latência durante a autenticação ao transitar entre diferentes pontos de acesso.

WPS

O protocolo WPS (Wi-Fi Protected Setup) foi desenvolvido para simplificar a configuração de pontos de acesso seguros, especialmente para usuários residenciais comuns. No entanto, uma falha crítica em seu design foi identificada em 2011, tornando-se uma

ameaça significativa à segurança. Essa vulnerabilidade permite que um atacante descubra o PIN utilizado na autenticação do WPS, possibilitando o acesso não autorizado à rede.O ataque por força bruta para descobrir o número PIN, um código numérico de 8 dígitos, envolve a tentativa de todas as combinações possíveis. Devido ao último dígito do código ser um checksum dos anteriores, temos apenas 7 números a serem descobertos. Esses 7 números são divididos em duas partes na etapa de verificação, sendo uma de 4 e outra de 3, totalizando 11.000 possíveis combinações numéricas.

METODOLOGIA

Escopo

Tive como foco, testar as redes wireless de instituições de ensino, por além de serem ambientes acadêmicos, possuem dados muitos sensíveis trafegando em seu meio e precisam ser devidamente segurados. Em locais como este, é necessário utilizar protocolos de segurança adequados para as redes sem fio, como por exemplo o WPA2 Enterprise, que não permite ataques utilizando a vulnerabilidade do PIN WPS.
Foram escolhidas oito instituições de ensino para a aplicação dos testes, tanto privadas quanto públicas e em diferentes níveis de ensino. O objetivo é verificar se há vulnerabilidade nestas instituições e se as mesmas estão utilizando os padrões ideais de segurança.

Obs: As instituições serão tratadas em anonimato para a segurança das mesmas, visto que vulnerabilidades serão expostas. Dessa maneira, os domínios destas serão ocultados nos resultados dos testes.

Sistemas operacionais focados em segurança

Para execução dos testes e análise de segurança de redes wireless, foi necessário utilizar um sistema operacional focado na área de segurança que pudesse fornecer um ambiente sólido para os testes. Foram elencados alguns SO's:

- Kali Linux: O Kali Linux é uma distribuição de sistema operacional baseada no Debian, projetada para fins avançados de segurança cibernética e testes de penetração. Reconhecido por sua extensa gama de ferramentas especializadas, o Kali Linux oferece aos profissionais de segurança e pesquisadores uma plataforma robusta para avaliar a segurança de sistemas e redes. Sua natureza open-source e foco na comunidade permitem uma constante atualização das ferramentas incluídas, mantendo-se na vanguarda das necessidades em constante evolução no campo da segurança da informação.

- Parrot Security OS: É uma distribuição de sistema operacional baseada no Debian, projetada especificamente para segurança cibernética, testes de penetração e anonimato na internet. Assim como o Kali Linux, o Parrot é uma ferramenta poderosa utilizada por profissionais de segurança e pesquisadores para avaliar a robustez de sistemas e redes. O Parrot Linux diferencia-se por sua abordagem focada em privacidade e anonimato,

fornecendo uma variedade de ferramentas especializadas para testes de segurança, além de uma configuração que suporta a preservação da identidade online.

Black Arch: Projetado para profissionais de segurança, pesquisadores e entusiastas, o BlackArch oferece uma vasta coleção de ferramentas especializadas em testes de penetração, análise de vulnerabilidades e forense digital. Sua estrutura baseada no Arch Linux permite aos usuários personalizar e otimizar o sistema de acordo com suas necessidades específicas.

Dentre as opções apresentadas, o Kali Linux foi escolhido.

Hardware

O hardware utilizado no desenvolvimento foi um notebook comum, além da uma placa wireless usb modelo TP-LINK TL-WN722N Versão 3. O uso desta placa Wi-Fi se deu pelo fato de que para executar testes de intrusão sem fio, é necessário que a interface wireless tenha compatibilidade com os modos monitor e de injeção de pacotes.

O modelo escolhido possui 3 versões, sendo que os modos mencionados acima são encontrados por padrão na versão 01 apenas. Dessa forma foi necessário realizar o Downgrade do driver do dispositivo, instalando o software da primeira versão. Abaixo segue a imagem da placa.

Ataque Pixie-Dust

Visto que o foco da atividade foi utilizar a vulnerabilidade do padrão WPS presentes nas redes sem fio, foi escolhido o método Pixie-Dust, que explora o código PIN, realizando um ataque de força bruta de forma offline. Esse ataque é considerado "offline" porque ele não requer interações ativas entre o atacante e o ponto de acesso Wi-Fi no momento do

ataque. O ataque pode ser descrito das seguintes etapas:

- Captura do Handshake WPS: O atacante captura um handshake WPS entre o dispositivo cliente e o ponto de acesso Wi-Fi durante o processo de autenticação WPS. Esse handshake contém informações cruciais para a geração da chave de criptografia.

- Extração de Informações PixieDust: O PixieDust utiliza as informações contidas no handshake capturado para tentar derivar a chave privada de criptografia utilizada pela rede Wi-Fi. Essa chave é gerada durante o processo WPS e, quando comprometida, pode permitir o atacante descriptografar o tráfego entre o dispositivo e o ponto de acesso.

- Ataque Offline: O atacante realiza a maior parte do processo de quebra de chave offline, sem a necessidade de interagir diretamente com o ponto de acesso ou o dispositivo cliente. Isso significa que o ataque pode ser realizado posteriormente, em um ambiente controlado pelo atacante.

- Acesso a chave: Utilizando técnicas de quebra de chave, o PixieDust tenta derivar a chave criptográfica a partir das informações obtidas. Se bem-sucedido, o atacante terá acesso à chave privada necessária para descriptografar o tráfego entre o dispositivo e o ponto de acesso Wi-Fi.

A execução offline é mais efetiva devido ao fato de que com a divulgação da vulnerabilidade do PIN WPS, os fabricantes e desenvolvedores de software realizaram a limitação das tentativas de conexão por dispositivo, além de outras técnicas de prevenção. Essa abordagem evita a necessidade de realizar múltiplas tentativas de inserção do PIN.

Wifite2

O Wifite2 é uma ferramenta de código aberto projetada para auditoria de segurança em redes sem fio. Essa ferramenta é uma versão aprimorada da primeira versão do Wifite e é utilizada para automatizar ataques e testes de penetração em redes sem fio. O objetivo principal do Wifite2 é simplificar e agilizar o processo de auditoria de segurança, tornando mais fácil para os profissionais de segurança e pesquisadores identificarem vulnerabilidades em redes sem fio. Possui capacidade de realizar ataques de força bruta, capturar handshakes WPA, realizar ataques de desautenticação e explorar outras vulnerabilidades de segurança em redes Wi-Fi. Todos estes ataques são feitos utilizando outras ferramentas incluídas no Wifite2, como por exemplo o aircrack-ng.

O Wifite2 possui em sua composição a ferramenta Pixiewps, que implementa o ataque Pixie-Dust.

Para executar o wifite2, basta executar o comando abaixo:

sudo wifite

Obs: O comando deve ser executado como administrador do sistema, caso contrário não será executado.

A partir do comando, a ferramenta irá inicializar, solicitando senha de administrador e permitindo a escolha da interface que executará os testes.

Após a escolha do adaptador, a ferramenta começa a escanear as redes em seu alcance, apresentando uma lista com suas informações. Abaixo podemos ver uma varredura realizada em uma região do campus da UFMS, a fim de exemplificar a listagem das redes, ressaltando que não foi realizado teste de intrusão neste ambiente.

A partir da varredura das redes no alcance da placa Wireless, é possível então iniciar um ataque a partir do ID do alvo. A partir disso, o Wifite2, executa uma bateria de ataques, incluindo o Pixie-Dust. Porém também é possível executar o Pixie-Dust individualmente através do comando:

-sudo wifite –pixie

Abaixo podemos conferir um teste realizado em uma das instituições, onde a vulnerabilidade foi explorada com êxito.

Como é possível visualizar na figura, o código numérico PIN foi obtido com êxito, possibilitando o acesso à senha da rede sem fio e concluindo o Pixie-Dust em poucos minutos.

Foi realizado o mesmo procedimento nas oito instituições, sendo que foram obtidos resultados abaixo. Obs: As instituições de ensino foram identificadas com letras devido ao anonimato necessário descrito no início do relatório:

Instituição	Redes WPA-P Encontradas	Redes WPS Ativo	Ataques Bem Sucedidos
A	4	1	1
B	5	1	0
C	2	2	2
D	1	1	0
E	2	1	0
F	2	2	2
G	1	1	0
H	2	1	1

Como é possível visualizar, houve êxito em quatro das oito instituições de ensino, ou seja, em 50% dos casos a vulnerabilidade foi explorada com sucesso.

CONCLUSÃO

Nas atividades orientadas a ensino aqui descritas, foram estudados os padrões de segurança em redes wireless e seu funcionamento, além de realizados testes de vulnerabilidade em redes reais, nas instituições de ensino. Tais testes puderam apontar que a vulnerabilidade do WPS pode representar uma ameaça, afinal como visto nos resultados, alguns dos alvos testados apresentam vulnerabilidades relacionadas ao WPS em suas redes, o que pode resultar em sérias repercussões para a organização. Uma vez que um invasor não autorizado obtém acesso à rede da instituição, ele pode desencadear uma série de ataques, incluindo a interceptação de pacotes, exposição de dados de usuários, ataques a outras instituições por meio da rede comprometida e, dependendo da configuração da rede, realizar varreduras em dispositivos conectados usando softwares específicos.Assim, a investigação em segurança de redes sem fio revelou-se de suma importância, enriquecendo significativamente meu entendimento na área por meio da combinação de teoria e prática. Além disso, evidenciou uma situação crítica que frequentemente encontramos em nosso cotidiano, proporcionando um valor acrescido ainda mais significativo

Campo Grande, 01 de dezembro de 2023.

gov.br Documento assinado digitalmente
GABRIEL NERIS DOS SANTOS
Data: 02/12/2023 17:43:12-0300
Verifique em https://validar.iti.gov.br

Gabriel Neris dos Santos
Acadêmico