Classe de ataques
Dns Spoofing e SEToolkit

Filipe F. Costa[1], Rafael D. Rodrigues[1]

[1]Faculdade de Ciências Exatas e Tecnológicas – Universidade Federal dos Vales Jequitinhonha e Mucuri (UFVJM)
MGT 367, KM 583 – Diamantina, MG – Brasil

{filipe.fernandes, dias.rafael} @ufvjm.edu.br

Abstract. *This project presents the simulation of a DNS Spoofing attack using the SEToolkit and Ettercap tools in a controlled environment. The objective was to demonstrate how DNS requests from a victim machine can be redirected to a cloned malicious website, allowing for the capture of sensitive data. The attack was carried out using three virtual machines: a Kali Linux attacker, a Windows 10 victim, and a third machine for network management through OpenVPN. The steps include cloning a legitimate website, modifying Ettercap's configuration, and performing ARP poisoning to intercept and manipulate network traffic. The results confirmed the effectiveness of DNS Spoofing in redirecting traffic to malicious sites and highlighted potential security risks in poorly configured networks.*
Keywords: DNS Spoofing, SEToolkit, Ettercap, ARP Poisoning, Cybersecurity.

Resumo. *Este projeto apresenta a simulação de um ataque de DNS Spoofing utilizando as ferramentas SEToolkit e Ettercap em um ambiente controlado. O objetivo foi demonstrar como as requisições DNS de uma máquina vítima podem ser redirecionadas para um site malicioso clonado, permitindo a captura de dados sensíveis. O ataque foi realizado utilizando três máquinas virtuais: uma máquina Kali Linux como atacante, uma máquina Windows 10 como vítima e uma terceira máquina para gerenciamento de rede utilizando OpenVPN. Os passos envolveram a clonagem de um site legítimo, a modificação das configurações do Ettercap e a execução de envenenamento ARP para interceptar e manipular o tráfego de rede. Os resultados confirmaram a eficácia do DNS Spoofing em redirecionar o tráfego para sites maliciosos e destacaram os riscos potenciais de segurança em redes mal configuradas.*
Palavras-chave: DNS Spoofing, SEToolkit, Ettercap, Envenenamento ARP, Cibersegurança.

1. Introdução

A segurança da informação é um aspecto crucial na computação moderna, conforme discutido por Andress [Andress 2014]. Neste trabalho, exploramos o DNS Spoofing e a utilização do SEToolkit, ferramentas essenciais em testes de penetração [Moore 2019].

Neste projeto, foi realizada uma simulação de um ataque de DNS Spoofing utilizando as ferramentas SEToolkit e Ettercap [Project 2020] em um ambiente virtualizado. O objetivo do ataque é redirecionar as requisições de DNS de uma vítima para um endereço IP malicioso, permitindo que o atacante capture dados sensíveis ou distribua conteúdos falsificados. Esse tipo de ataque é utilizado para explorar a confiança que os usuários depositam em nomes de domínio legítimos, podendo ser usado em cenários como phishing e distribuição de malware.

O ambiente foi configurado com três máquinas virtuais no Proxmox: uma máquina Kali Linux para executar o ataque, uma máquina com Windows 10 como alvo, e uma máquina intermediária para gerenciamento de rede, conectada através de uma VPN (OpenVPN) para garantir um ambiente controlado e sem interferência das restrições de rede da universidade. Esta configuração permitiu simular o comportamento de uma rede corporativa, reproduzindo as condições reais de um ataque.

A abordagem utilizada no projeto envolveu a clonagem de um site legítimo, configurado para ser servido localmente, e o uso de ferramentas de manipulação de pacotes para direcionar as requisições DNS da máquina alvo ao site clonado. Neste documento, são apresentados o passo a passo de cada configuração e execução, as ferramentas utilizadas, e uma análise dos resultados obtidos.

2. Material e Métodos

O objetivo deste trabalho é demonstrar o processo de execução de um ataque de DNS Spoofing utilizando as ferramentas SEToolkit [Moore 2019] e Ettercap [Project 2020] em um ambiente virtualizado. A metodologia consiste em configurar um ambiente controlado de rede, simular um ataque *Man-in-the-Middle* (MitM) para interceptação e redirecionamento de tráfego DNS, e validar a eficácia das ferramentas utilizadas, utilizando como alvo o site do **eCampus** da Universidade Federal dos Vales do Jequitinhonha e Mucuri (UFVJM).

2.1. Materiais e Ferramentas

Para a implementação do ataque, foram utilizados os seguintes recursos:

- **Proxmox**: Plataforma de virtualização utilizada para hospedar as máquinas virtuais.
- **Kali Linux**: Sistema operacional especializado em testes de penetração, usado como máquina atacante.
- **Windows 10**: Sistema operacional utilizado como máquina alvo, simulando o comportamento de um usuário típico em uma rede corporativa.
- **OpenVPN**: Protocolo VPN utilizado para conectar a rede local ao ambiente de teste, garantindo uma rede isolada e sem interferências.
- **SEToolkit (Social-Engineer Toolkit)**: Ferramenta para criação de sites falsos e execução de ataques de engenharia social.
- **Ettercap**: Ferramenta para realizar ataques MitM e redirecionamento de tráfego de rede.

2.2. Metodologia

O ataque foi realizado em um ambiente de rede controlado com as seguintes etapas:

2.2.1. Configuração do Clone de Site

Inicialmente, foi utilizado o SEToolkit para criar uma réplica do site legítimo do **eCampus UFVJM** (`https://ecampus.ufvjm.edu.br/`), que serviu como isca para capturar as credenciais da vítima.

1. Iniciou-se a ferramenta SEToolkit com o comando: `setoolkit`.
2. Selecionaram-se as seguintes opções na interface:
    - Opção 1 - **Social-Engineering Attacks**
    - Opção 2 - **Website Attack Vectors**
    - Opção 3 - **Credential Harvester Attack Method**
    - Opção 2 - **Site Cloner**

3. Foi adicionado o IP da máquina Kali Linux, `10.0.0.217`, e o link do site a ser clonado, `https://ecampus.ufvjm.edu.br/`.

A ferramenta então criou uma réplica do site, disponível localmente no endereço `http://10.0.0.217/`, pronta para ser utilizada no ataque.

2.2.2. Configuração do Ettercap

Em seguida, foram realizadas modificações nas configurações do Ettercap para permitir o redirecionamento de tráfego DNS:

1. Foi editado o arquivo `/etc/ettercap/etter.dns` para adicionar a entrada DNS:
   ```
   * A 10.0.0.217
   ```
   Isso direciona qualquer requisição DNS para o IP da máquina atacante.
2. Modificou-se o arquivo `/etc/ettercap/etter.conf` para executar o Ettercap com permissões de root, ajustando as linhas:
   ```
   ec_uid = 0
   ec_gid = 0
   ```

2.2.3. Execução do Ataque DNS Spoofing

Com o Ettercap configurado, o ataque foi iniciado com as seguintes etapas:

1. Iniciou-se o Ettercap com a interface gráfica: `ettercap -G`.
2. Definiu-se a interface de rede (ex.: `eth0`) e aceitou-se a configuração.
3. Executou-se um scan para identificar os dispositivos na rede e adicionou-se a máquina alvo como **Target 1**.
4. Selecionou-se **MitM > ARP poisoning** para envenenar a cache ARP da vítima e redirecionar o tráfego.
5. No menu **Plugins**, ativou-se o plugin **dns_spoof** para redirecionar as requisições DNS.

2.3. Verificação do Ataque

Para validar o ataque, a vítima foi instruída a acessar o site legítimo do **eCampus UFVJM** pelo navegador (`https://ecampus.ufvjm.edu.br/`). Com sucesso, o navegador foi redirecionado para o site clonado hospedado no IP da máquina Kali (`http://10.0.0.217/`), confirmando a eficácia do ataque e a captura de credenciais.

3. Análise e Discussão dos Resultados

O experimento realizado com o ataque de DNS Spoofing utilizando as ferramentas SEToolkit e Ettercap demonstrou a vulnerabilidade de sistemas que não possuem mecanismos de proteção adequados contra ataques de *Man-in-the-Middle* (MitM). Os resultados mostram como é possível redirecionar o tráfego de um usuário desavisado para um site falso e obter suas credenciais sem que ele perceba a manipulação [Moore 2019].

3.1. Validação do Ataque

A replicação do site do **eCampus UFVJM** foi executada com sucesso, criando uma versão idêntica visualmente ao original, o que contribuiu para enganar a vítima. Durante os testes, a vítima, ao acessar o endereço original do eCampus (`https://ecampus.ufvjm.edu.br/`), foi redirecionada para o site falso hospedado no IP do atacante (`http://10.0.0.217/`). Este redirecionamento foi possível graças à manipulação das requisições DNS, que fizeram o navegador apontar para o endereço IP da máquina Kali Linux em vez do servidor legítimo.

A ferramenta Ettercap se mostrou eficaz ao realizar o ataque de envenenamento de cache ARP (ARP Poisoning) e ao gerenciar as regras de redirecionamento DNS definidas no arquivo `etter.dns` [Project 2020]. A combinação das técnicas utilizadas permitiu que o tráfego da vítima fosse interceptado e redirecionado sem gerar alertas visuais no navegador, uma vez que o site falso utilizava o mesmo layout do original, mantendo a aparência legítima.

3.2. Captura de Credenciais

Uma das principais validações do sucesso do ataque foi a captura das credenciais de login no site clonado. Ao tentar acessar o eCampus, a vítima inseriu suas credenciais, acreditando estar no site verdadeiro. Essas informações foram registradas no *Credential Harvester* do SEToolkit, demonstrando que é possível obter dados sensíveis de maneira relativamente simples quando o ambiente de rede é vulnerável [Andress 2014].

Durante o ataque, a vítima não percebeu nenhuma diferença visual ou de desempenho, o que comprova a eficácia de ataques MitM bem executados em redes sem segurança adequada. A ausência de alertas HTTPS também foi um fator relevante, já que o site falso não possuía um certificado de segurança válido, mas o navegador não exibiu advertências significativas [Stallings and Brown 2012].

3.3. Limitações e Desafios

Embora o ataque tenha sido bem-sucedido no ambiente controlado, alguns desafios e limitações foram identificados:

- **Detectabilidade em Redes Seguras**: Em redes reais, com soluções como DNSSEC ou com protocolos de detecção de MitM, o ataque poderia ser rapidamente identificado e bloqueado [Kurose and Ross 2017].

- **Certificados SSL/TLS**: A ausência de um certificado SSL/TLS válido no site clonado poderia levantar suspeitas em um usuário mais atento. No entanto, muitos usuários tendem a ignorar tais advertências, o que ainda torna esse tipo de ataque relevante.
- **Monitoramento de Rede**: Em ambientes corporativos, ferramentas de monitoramento de rede podem detectar alterações nas tabelas ARP e a presença de pacotes com destinos modificados, o que indicaria a presença de um ataque [Scarfone and Mell 2008].

3.4. Impacto na Segurança de Redes

O experimento reforça a importância de implementar medidas de segurança adequadas em redes corporativas e acadêmicas. A manipulação de requisições DNS pode ser prevenida com a adoção de técnicas como:

- **Uso de DNSSEC**: Protocolo que adiciona autenticação de origem aos dados DNS, prevenindo alterações maliciosas [Stallings and Brown 2012].
- **Monitoramento de Atividade de Rede**: Ferramentas de detecção de intrusões (IDS) para identificar padrões anômalos de tráfego.
- **Habilitação de HTTPS Obrigatório**: Implementar certificados válidos e forçar a navegação segura, educando os usuários a verificar a legitimidade dos sites [Erickson 2008].

3.5. Considerações Finais

Os resultados indicam que, sem medidas de proteção adequadas, mesmo redes aparentemente seguras estão vulneráveis a ataques MitM e redirecionamento de tráfego. A execução do experimento destaca como a engenharia social e a ausência de proteção DNS robusta podem facilitar a obtenção de credenciais e outras informações sensíveis, representando um risco significativo para organizações e instituições que não possuem uma política de segurança rigorosa [Andress 2014].

4. Conclusão

O presente trabalho demonstrou como é possível realizar um ataque de DNS Spoofing, que pertence à classe de ataques de *Man-in-the-Middle* (MitM). Esse tipo de ataque envolve a interceptação e manipulação de tráfego de rede para redirecionar vítimas para destinos falsificados, possibilitando a captura de credenciais e outros dados sensíveis. Ferramentas de código aberto, como SEToolkit e Ettercap, foram utilizadas para capturar credenciais e redirecionar tráfego em um ambiente controlado, ilustrando a vulnerabilidade de redes que não implementam mecanismos de segurança avançados, como DNSSEC [Stallings and Brown 2012], e evidenciando como a ausência de protocolos de proteção pode levar a graves compromissos de segurança.

Durante o experimento, a clonagem do site do **eCampus UFVJM** e a manipulação das requisições DNS foram realizadas com sucesso, resultando na captura das credenciais de um usuário desavisado. Os resultados reforçam a importância de educar usuários sobre os riscos de ataques MitM [Mirkovic and Reiher 2003] e de implementar medidas de segurança robustas em redes corporativas e acadêmicas.

Além disso, o estudo destacou a necessidade de soluções de monitoramento e defesa ativa para identificar atividades anômalas na rede e proteger os dados dos usuários. A detecção precoce de manipulações ARP e a adoção de certificados SSL/TLS válidos são medidas fundamentais para mitigar esse tipo de ataque [Scarfone and Mell 2008].

4.1. Formas de Prevenção

Para prevenir ataques de DNS Spoofing e outros ataques MitM, as seguintes abordagens técnicas e medidas de conscientização humana são recomendadas:

- **Implementação de DNSSEC:** Adotar o protocolo DNSSEC para autenticar a origem das respostas DNS e garantir que os dados não sejam manipulados.
- **Uso de HTTPS e Certificados TLS Válidos:** Implementar certificados SSL/TLS válidos e forçar a navegação segura por HTTPS para dificultar a interceptação de dados.
- **Monitoramento de Atividade de Rede:** Utilizar ferramentas de detecção de intrusões (IDS) para identificar padrões anômalos de tráfego e manipulações ARP.
- **Segmentação de Redes:** Segmentar redes corporativas para limitar a propagação de ataques MitM e garantir que dispositivos vulneráveis estejam isolados.
- **Educação e Treinamento dos Usuários:** Capacitar os usuários a reconhecer sinais de sites falsificados, como a ausência de certificados de segurança e mudanças suspeitas nos endereços de URLs.

Por fim, conclui-se que, embora este ataque tenha sido realizado em um ambiente simulado, a facilidade de sua execução em redes vulneráveis ressalta a urgência de se adotar práticas de segurança cibernética e monitoramento constante, especialmente em contextos educacionais

e corporativos, para garantir a integridade e a confidencialidade das informações trafegadas [Erickson 2008].

Referências

Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Syngress Publishing.

Erickson, J. (2008). *Hacking: The Art of Exploitation*. No Starch Press, 2nd edition.

Kurose, J. and Ross, K. (2017). *Computer Networking: A Top-Down Approach*. Pearson, 7th edition.

Mirkovic, M. and Reiher, P. (2003). A taxonomy of ddos attack and ddos defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2):40–53.

Moore, D. (2019). Social-engineer toolkit (set). `https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/`.

Project, E. (2020). Ettercap: Comprehensive suite for man-in-the-middle attacks. `https://www.ettercap-project.org/`.

Scarfone, K. and Mell, P. (2008). Guide to intrusion detection and prevention systems (idps). Technical Report Special Publication 800-94, NIST.

Stallings, W. and Brown, L. (2012). *Computer Security: Principles and Practice*. Prentice Hall, 3rd edition.