1st Amazon STEM ACADEMY CONFERENCE ASAC21

Teste de Intrusão Independence

Fernando Araujo Alves Filho[1], Adevan Neves Santos[1], Paulo Eduardo Ribeiro Cativo[1], Áurea Hileia da Silva Melo[1]

[1]Escola Superior de Tecnologia (EST) – Universidade do Estado do Amazonas (UEA)
CEP 69050-020 – Manaus – AM – Brasil

faaf.eng19@uea.edu.br, ans.eng20@uea.edu.br, perc.eng18@uea.edu.br, asmelo@uea.edu.br

1. INTRODUÇÃO

Segurança da informação consiste em um conjunto de práticas que visam garantir a integridade, disponibilidade e confidencialidade das informações. Para isso, existem padrões de segurança e métodos para determinar e reparar vulnerabilidades de um sistema. Em geral, nesta grande área existem dois tipos de profissionais: aqueles que trabalham com segurança defensiva (blue team) e aqueles que trabalham com segurança ofensiva (red team).

Teste de intrusão, também conhecido como teste de penetração, consiste em um método utilizados pelo time de segurança ofensiva para avaliar a segurança de um determinado sistema, simula-se um ataque cibernético para descobrir ou explorar vulnerabilidades e avaliar que tipo de informações ou que nível de acesso não-autorizado um invasor poderia conseguir. Este trabalho consiste em fazer um teste de intrusão numa aplicação web de uma organização real, que será referenciada como Independence.

2. OBJETIVOS

2.1 Objetivos Gerais

O objetivo do trabalho foi testar a segurança de uma aplicação web por meio de segurança ofensiva, que aborda um processo de investigação, ataque e análise dos resultados, indicando melhorias e métodos para tratar possíveis falhas identificadas.

2.2 Objetivos específicos

Os objetivos específicos deste trabalho são: (i) conhecer de forma prática algumas ferramentas do Kali Linux, (ii) identificar e classificar em ordem de criticidade as vulnerabilidades encontradas no teste de segurança, (iii) sugerir um conjunto de ações e práticas para que a organização Independence melhore sua segurança da informação, por exemplo filtrar o acesso às informações da aplicação. Também discutir sobre os problemas com base em normas técnicas e a nova LGPD, vigente no ano de 2020.

3. MATERIAIS E MÉTODOS

O experimento foi conduzido com apoio de ferramentas de exploração que são usadas por invasores em situações reais de ataque, que permite obter a visão de um agente externo. Utilizou-se ferramentas do Kali, uma distribuição Linux empregada em tarefas de auditoria de segurança da informação. Pode-se dividir o processo em 3 etapas, descritas a seguir.

3.1 Preparar o ambiente de trabalho

Esta etapa consistiu em mascarar o proxy, a fim de garantir o anonimato no processo, para isso foi utilizado um Proxy Chain(Cadeia de proxy), usufruiu-se do Dynamic Chain para mascarar o proxy, esta cadeia de proxy funciona da seguinte forma: A informação que o atacante passa para o servidor alvo passa por diversos servidores proxy antes de chegar ao alvo, dificultando a identificação do atacante em caso de investigação policial.

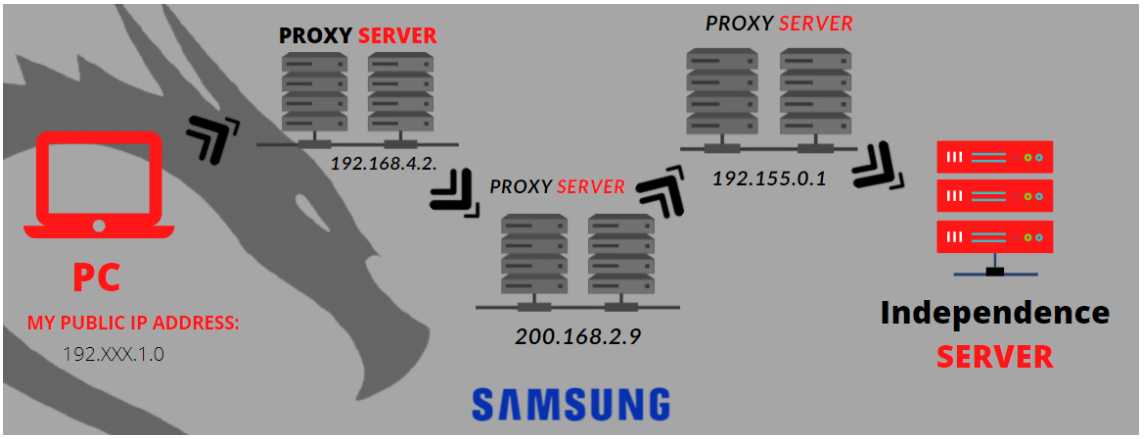

Figura 1. Funcionamento do Dynamic Chain. Todos os endereços de IP mostrados são fictícios. Fonte: Apresentação STEM - Fernando Araujo Alves Filho

3.2 Identificar vulnerabilidades

A segunda etapa consistiu na identificação de vulnerabilidades. Utilizou-se a ferramenta Nmap, presente no próprio sistema operacional, a fim de extrair informações de serviços da rede. Após identificar serviços e protocolos do servidor, foram estudadas informações do domínio na internet, com objetivo de encontrar possíveis vulnerabilidades já exploradas.

3.3 Explorar vulnerabilidades

A última etapa integrou a exploração das vulnerabilidades utilizando outras ferramentas do Kali Linux. Utilizou-se a ferramenta Zed Attack Proxy(ZAP), esta é uma ferramenta de teste de penetração que fornece scanners de um serviço web. Averiguou-se se de fato algo da rede poderia ser acessado remotamente por algum potencial invasor, para esta atividade, recorreu-se à ferramenta Ncat para enviar instruções ao servidor de rede. No Ncat, foi posto

o endereço de IP do servidor, obtido por meio do Nmap. Com o servidor conectado através do Ncat, pode-se forçar respostas e enviar comandos da aplicação.

4. RESULTADOS

A partir de análises da terceira etapa, encontrou-se os seguintes alertas de vulnerabilidades:

1. "x-frame-options header is not included in the http response". Esta falha indica que o navegador não tem a informação se deve ou não acessar determinada página na web, este tipo de falha, caso corrigida pode evitar ataques do tipo clickjacking(roubo de clique), esta falha consiste em desviar cliques de uma determinada página para uma página possivelmente fraudulenta.
2. "Remove the private IP address from the HTTP response body". Esta falha indica que há informações que podem ser acessadas sobre o IP privado do servidor a partir de usuários remotos, este tipo de falha pode acarretar em intrusões, roubo de informações e outros danos à organização.

Com base nos resultados dos experimentos, nota-se que o serviço web em questão possui vulnerabilidades que podem ser exploradas por possíveis atacantes.

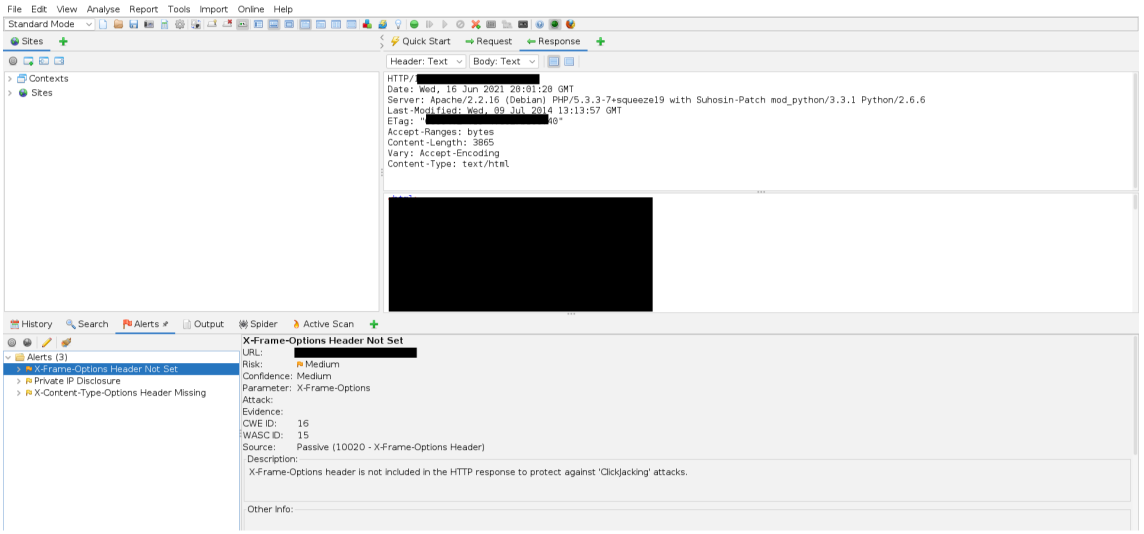

Figura 2. apresentação da vulnerabilidade encontrada. Falha: "x-frame-option header is not included in the http response"

Figura 3. apresentação da vulnerabilidade encontrada. Falha: “Remove the private IP address from the HTTP response body”.

5. CONCLUSÃO

A investigação resultou na identificação de duas falhas importantes. Além de enfatizar aspectos de segurança sob o olhar da Lei Geral de Proteção de Dados vigente desde 2020 no Brasil. A primeira falha, relacionada com o cabeçalho não incluso na resposta HTTP, possibilita a falta de integridade da informação acessada, expondo a página a ataques de clickjacking, pois o usuário pode não ser capaz de identificar a veracidade daquele conteúdo. A situação apresentada não atende ao princípio VII da lei 13.789, que suporta a informação do usuário contra a manipulação ilícita e/ou acidental de seus dados. A segunda, que diz respeito à obtenção de informações do servidor de maneira remota, tem potencial de prejudicar a confidencialidade das informações e, dependendo da criticidade do conteúdo, pode gerar vazamento de dados. Neste cenário, o artigo 52 parágrafo 7 determina que o controlador dos dados está sujeito a aplicação de penalidades, que podem ser multas e/ou sanções.

Para a defesa contra “Clickjacking”, a maioria dos navegadores Web oferece suporte ao cabeçalho “HTTP X-Frame-Options”, recomenda-se certificar que o cabeçalho está definido em todas as páginas web retornadas pelo site alvo. já para defesa contra “Remove the private IP address from the HTTP response body” pode ser solucionado configurando o servidor para filtrar as respostas entregues à requisições de usuários, bloqueando o acesso em informações que possam ser usadas contra a organização e monitorar preventivamente comportamentos incomuns de usuários.

Diante da situação descrita, a organização Independence pode rever sua Gestão de Risco, considerar que as falhas representam um risco elevado e aplicar boas práticas na segurança e configuração correta de ferramentas de rede com a intenção de prevenir incidentes posteriores.

REFERÊNCIAS BIBLIOGRÁFICAS

KALI LINUX TOOLS. **Nmap Usage**. Disponível em: www.kali.org/tools/nmap. Acesso em: 26 ago.2021.

GITLAB. **ncat-W32**. Disponível em: gitlab.com/kalilinux/packages/ncat-W32. Acesso em: 27 ago. 2021.

OWASP-ZAP. **Getting Started**. Disponível em: https://www.zaproxy.org/getting-started/. Acesso em: 27 ago. 2021.