Serviço Público Federal
Ministério da Educação
Fundação Universidade Federal de Mato Grosso do Sul

Atividade Orientada a Ensino

Acadêmico: Gustavo Lube Machado de Melo
RGA: 2018 1905 0424
Professor: Carlos Alberto da Silva
Atividade: Atividade Orientada a Ensino sobre Segurança computacional (Kali Linux)

Introdução

As atividades orientadas a ensino tiveram foco em segurança computacional. Foram realizados testes de segurança (Pentests) e as ferramentas estudadas estão listadas abaixo, com seus respectivos comandos e vulnerabilidades encontradas.

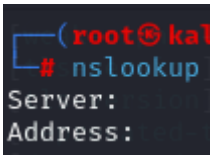
Não será possível demonstrar resultados e sites, pois foi exigido sigilo para realização do estudo.

PENTEST

Footprinting - Coleta de informações

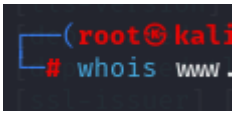
Nslookup:

Ferramenta Unix para saber endereço de respectivo DNS.



Whois:

Utilizado para saber informações básicas dos sites.



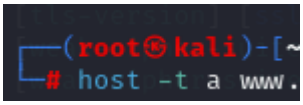
Google Dorking:

Foi utilizado o Google como ferramenta para pesquisa e análises de diretórios, documentos e outras coisas de interesse. Foram encontrados dados possivelmente sensíveis e diretórios mais vulneráveis.

Comandos:
site:
filetype:

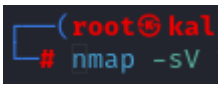
host:

Comando do linux para saber qual o host do site especificado.
comandos:



Nmap:

Ferramenta do KaliLinux para obter mais informações de usuários, além de mapeamento de falhas de segurança. Foram utilizados e estudados várias variações, sendo elas:



Ping:

Comando Linux utilizado para verificar comunicação do servidor e analisar possível bloqueio do mesmo, após detectar os ataques de teste.

Nping:

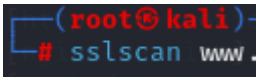
Usado para análise de respostas e tempos de pacotes de dados da rede. Comando utilizado:

Nikto:

Scanner usado para busca de vulnerabilidades de servidores web. Site especificado reconheceu risco do uso e bloqueou sistema atacante.

Sslscan:

Nativo no KaliLinux, utilizado para escanear tipo de criptografia utilizada em site especificado.

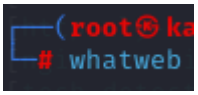


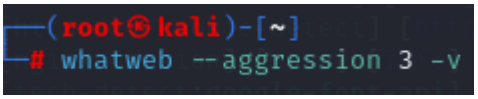
Wpscan:

Ferramenta hacker utilizada para escaneamento de vulnerabilidades web. Site especificado detectou a ferramenta e bloqueou o sistema atacante. Opção utilizada:

Whatweb:

Outro Scanner web que não deu bloqueio do site para o atacante, mas não conseguiu obter informações.



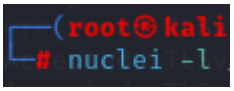


Dirb:

Outro Scanner web que não provocou bloqueio do site para o atacante, mas também não conseguiu obter informações.

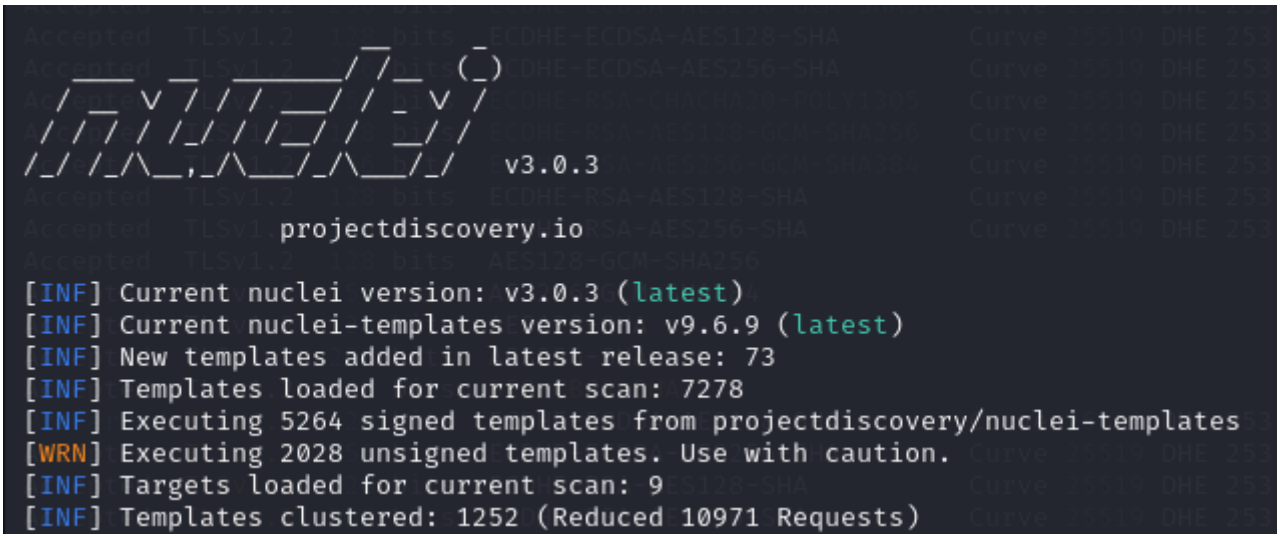
Nuclei:

Scanner web especializado que foi instalado à parte no sistema. Detectou várias vulnerabilidades como método TRACE, sistemas antigos utilizados e falta de headers.
Opções utilizadas:



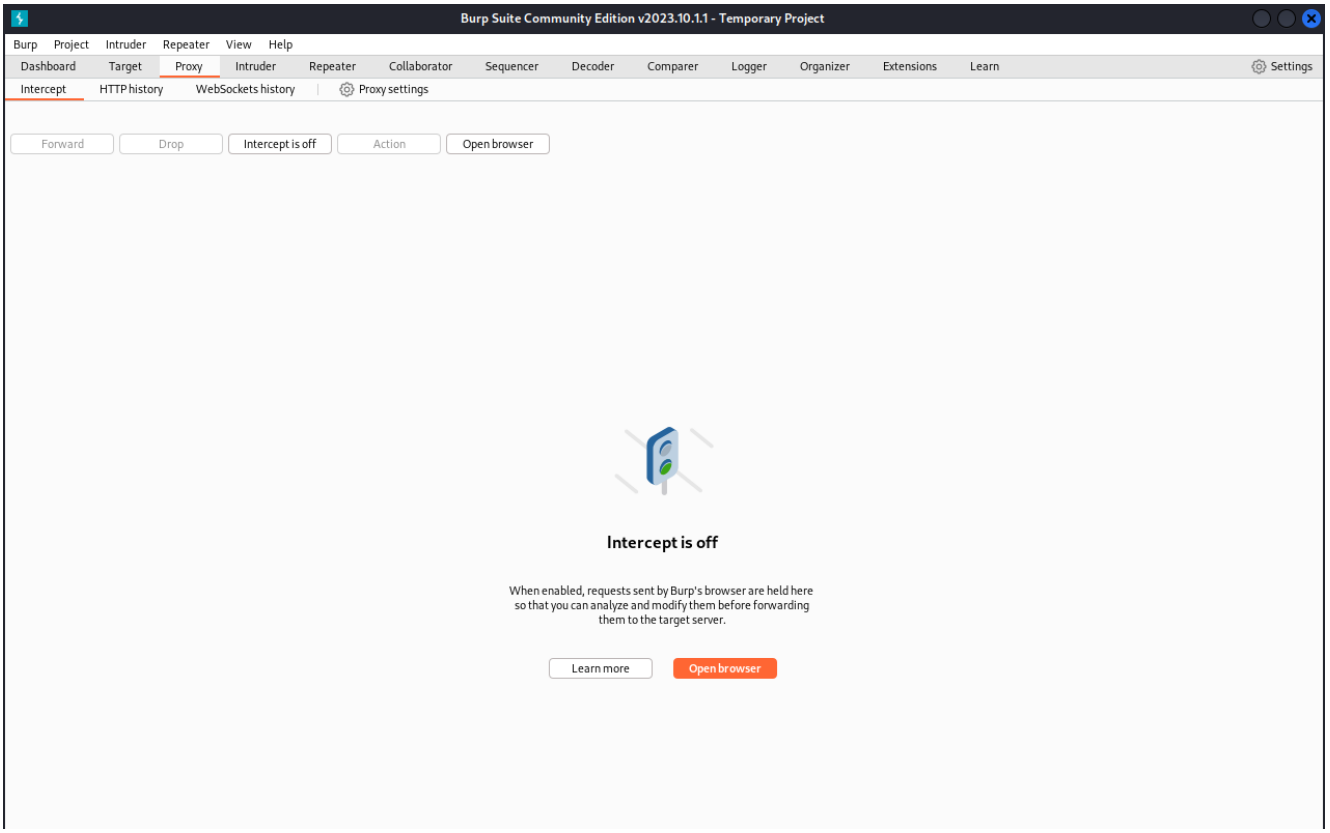
Foi utilizada, também, a opção **-rl num,** sendo **num** um número inteiro que representa a quantidade de testes realizados em um determinado tempo. Foram realizados diferentes números para testes de bloqueio e análises.
Alguns testes tomaram bloqueio, enquanto outros passaram e retornaram as vulnerabilidades.

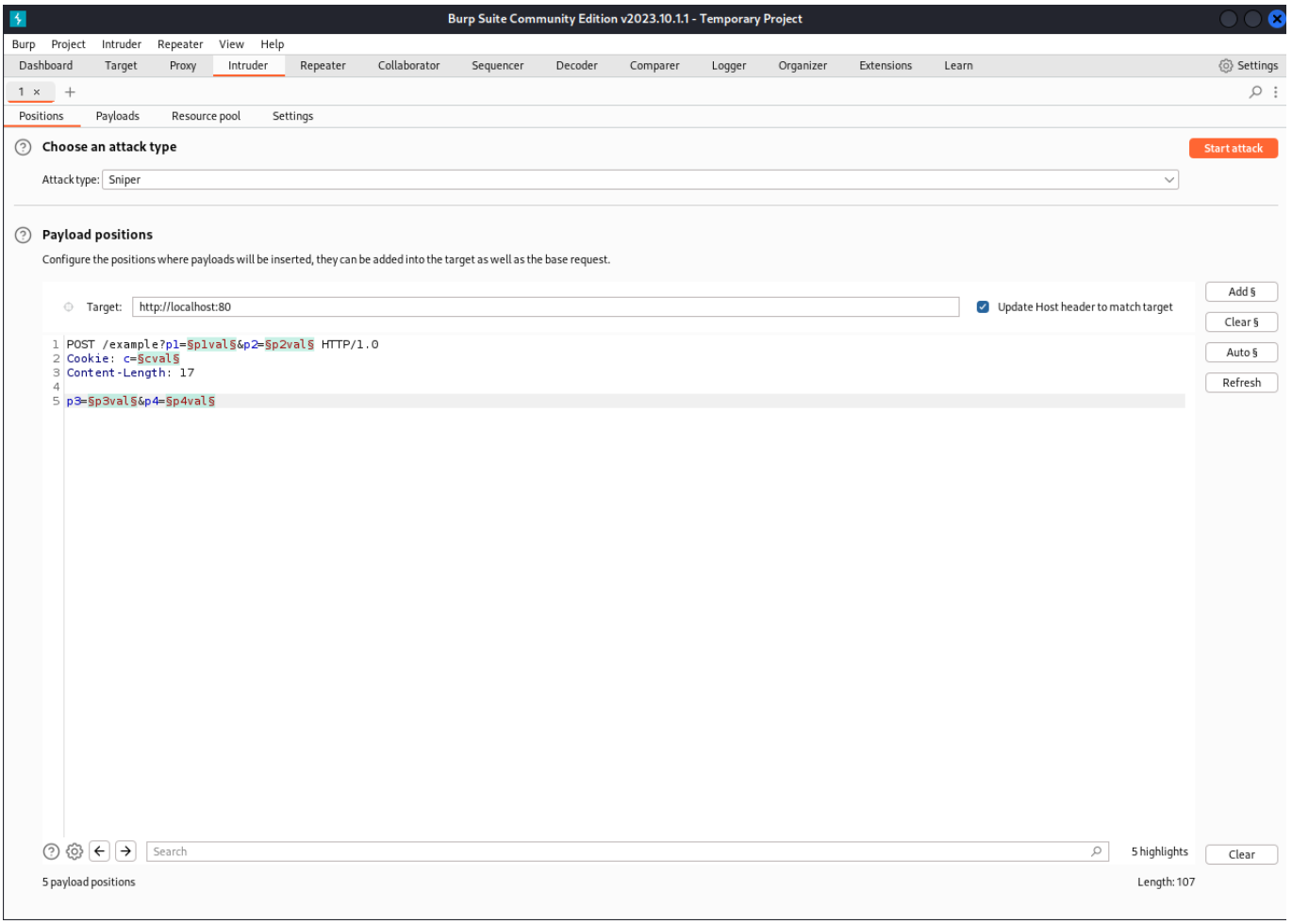
Imagem de iniciação do Nuclei:



Burp Suite:

Multiferramenta para análise, ataque e muito mais para códigos na web. Foi utilizada para validação de vulnerabilidades, testes de injection, obtenções de informações, além de estudos de ataques à força bruta pelo mesmo. Foram obtidas a validação do método TRACE, informações sobre os sistemas utilizados e códigos com possíveis vulnerabilidades. As tentativas de HTML injection foram reconhecidas e não validadas nos testes.





CONCLUSÃO:

Nessas atividades orientadas a ensino foram realizadas vários testes de websites e estudos importantes na análise de segurança de dados e vulnerabilidades existentes. O estudo da gravidade das vulnerabilidades encontradas também foram realizadas, e junto com essa, a análise de consequências foi obtida. Como a gravidade e as consequências encontradas não foram baixas, essa atividade ressalta a importância da cibersegurança no mundo contemporâneo e da constante atualização dos sistemas, pentests e estudos. Dessa forma, é possível manter a estrutura dos servidores afastada de ataques maliciosos.

Assim, o estudo foi essencial para conhecimento pessoal e para a formação acadêmica e profissional.

Campo Grande, 27 de Novembro de 2023.

gov.br
Documento assinado digitalmente
GUSTAVO LUBE MACHADO DE MELO
Data: 30/11/2023 14:47:55-0300
Verifique em https://validar.iti.gov.br

Gustavo Lube Machado de Melo
Acadêmico