Weasels e a construção de conhecimento em Segurança Ofensiva

Daniel Dalalana Bertoglio, Henry Cabral Nunes, Pedro Cordeiro Filippi, Avelino Francisco Zorzo
dalalana@gmail.com,henry.nunes@edu.pucrs.br,pedro.filippi@edu.pucrs.br,avelino.zorzo@pucrs.br
Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, Brasil

RESUMO

Atualmente, a preocupação com cibersegurança tem aumentado junto a organizações dado o aumento de ataques cibernéticos - tanto em quantidade como em complexidade. Estes ataques buscam, essencialmente, explorar vulnerabilidades em ativos digitais, i.e. computadores, redes, dispositivos móveis, entre outros. Como forma de mitigação de tais ataques, existem métodos e técnicas para a investigação dessas explorações analisando os vetores de ataque através de práticas que simulam o comportamento dos atacantes. Como forma de disseminar o conhecimento que envolve as simulações de exploração de vulnerabilidades e análise de vetores de ataque, foi criada uma metodologia com o objetivo de formar um espaço de cultura de cibersegurança para auxiliar os participantes a desenvolver seus conhecimentos na área. Esse artigo apresenta o relato de experiência da aplicação desta metodologia para aprendizado de conceitos e técnicas presentes na área de Segurança Ofensiva por meio da utilização de plataformas *online* de treinamento de cibersegurança.

PALAVRAS-CHAVE

Cibersegurança, Segurança Ofensiva, Construção de Conhecimento

1 INTRODUÇÃO

Com o avanço da era da informação, a utilização de tecnologias da informação se torna cada vez mais comum, acessível e transparente. Intrínseco a isso, há também o aumento da necessidade das organizações por ativos digitais para atender a demanda crescente por serviços digitais. Entre os ativos digitais incluem-se aplicações, servidores e equipamentos de redes. Esse tipo de ativo possui a necessidade de ser mantido e gerenciado e, nesse sentido, o gerenciamento inclui a segurança e proteção dos mesmos no âmbito digital.

A tarefa de gerenciar, analisar e avaliar a segurança e proteção dos ativos digitais se torna mais complicada a partir do crescente número dos mesmos. Isso se deve, essencialmente, pois o número de ativos pode impactar no aumento da superfície de ataque [10] - implicando na quantidade de vetores de ataque [9] que podem ser explorados por algum atacante. A negligência na correção, mitigação e prevenção de possíveis vetores de ataque pode gerar expressivos impactos. As organizações que sofrem ataques podem ter perdas financeiras, de danos a marca e a reputação, interrupção de atividades e a possibilidade de enfrentar processos legais.

EduComp'22, Abril 24-29, 2022, Feira de Santana, Bahia, Brasil (On-line)

No geral, a frequência desses ataques tem aumentado consideralmente, conforme as estatísticas que tem se apresentado mundo afora [1]. No Brasil, de forma semelhante, ataques cibernéticos também tem aumentado - atualmente o Brasil é o 5º país do mundo que mais sofre ataques cibernéticos [2]. Os ataques têm como alvo tanto empresas privadas [6], como órgãos públicos [7] e pessoas físicas[5].

Com base nesse cenário notável da cibersegurança foi criado o Weasels[3], um grupo com o objetivo de criar um núcleo de aprendizado na área de cibersegurança e disseminação da cultura de segurança cibernética. Os integrantes do grupo são majoritariamente estudantes da graduação na área de computação da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). O Weasels é administrado e orientado pelo Grupo de Pesquisa de Confiabilidade e Segurança de Sistemas da PUCRS.

Na visão de equipe, os integrantes tem como consequência da participação uma formação em cibersegurança gerando valor através de um diferencial no mercado de trabalho. O conhecimento na área de cibersegurança é útil tanto para profissionais que vão trabalhar diretamente com a área como para outras áreas da computação. Para empresas localizadas na região, a existência do grupo permite acesso a mão de obra com um conhecimento escasso, permitindo indiretamente a uma melhora na proteção de seus ativos digitais. Por fim, as atividades do grupo permitem a produção e desenvolvimento de projetos acadêmicos na universidade, gerando e disseminando conhecimento para a área.

O processo de aprendizado é apoiado pela utilização de laboratórios que simulam um ambiente realista de teste de intrusão [18]. As práticas, então, envolvem a utilização das plataformas *online* de treinamento de cibersegurança existentes, *e.g.* TryHackMe [8] e HackTheBox [4]. A metodologia utilizada inclui reuniões recorrentes em diferentes formatos, orientadas por responsáveis pelo grupo, no qual a natureza e forma foram evoluindo ao longo do tempo baseada no *feedback* proveniente dos participantes. As reuniões disponibilizam um espaço para discussão, troca de ideias e resolução dos problemas nos laboratórios. Além do espaço das reuniões, outras formas de comunicação assíncronas foram estabelecidas para troca de informação entre os integrantes.

Nesse artigo buscamos relatar a experiência de formação do Weasels, desde sua concepção até o momento atual. Neste relato incluímos como o grupo foi sendo concebido e moldado de acordo com objetivos e visão definidos e frequentemente revisitados. Além disso, descrevemos a metodologia criada para o desenvolvimento e construção do conhecimento em Segurança Ofensiva e apresentamos os resultados, processo de avaliação contínua e as lições aprendidas nesta experiência.

O artigo é dividido da seguinte forma: a Seção 3 relata alguns trabalhos relacionados com o ensino de cibersegurança; a Seção 4 descreve a estratégia e planejamento que desenvolvemos para implementação do grupo, e; a Seção 5 relaciona os resultados que

obtivemos com o Weasels até o momento. Por fim, a Seção 6 resume as lições que foram aprendidas durante a execução do projeto e a Seção 7 apresenta as considerações finais e direcionamentos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Segurança Ofensiva

A segurança ofensiva é uma abordagem proativa e antagônica para proteger sistemas de computadores, redes e ambientes. A segurança "tradicional" concentra-se em medidas reativas aos ataques que ocorrem. Em contraste, as medidas de segurança ofensivas se concentram na simulação de ataques com o objetivo de encontrar suas vulnerabilidades e mensurar o impacto na ocorrência de um ataque real [13]. Assim, proteger ambientes corporativos envolve não apenas estratégias padrão (como gerenciamento de patches, uso de firewalls e conscientização de usuários), mas também validação frequente de como o "mundo real" funciona [11].

Dessa forma, entende-se que as práticas de segurança ofensiva se caracterizam como tentativa controlada de penetrar em um sistema ou rede para identificar vulnerabilidades. Nesse contexto, são aplicadas as mesmas técnicas que são usadas em um ataque regular por um hacker para permitir ações para eliminar vulnerabilidades antes que possam ser exploradas por pessoas não autorizadas. Normalmente, o processo de avaliações e testes de segurança que seguem essa abordagem podem ser divididas nas seguintes atividades: coleta de informações sobre o alvo; escaneamento e varredurado do alvo para identificar os serviços/protocolos; identificação de sistemas e aplicativos existentes que estão sendo executados no alvo; e identificação e exploração das vulnerabilidades conhecidas no sistema e aplicativos [9].

Quando são empregadas as técnicas relacionadas a Segurança Ofensiva, os testadores podem se basear nos seguintes critérios [22]: **base de informações**, que determina o nível de conhecimento que os testadores têm sobre o alvo (geralmente dividido em caixa preta, caixa cinza e caixa branca); **agressividade**, um critério que define o quão agressivo os testadores são durante o teste, ou seja, como são seus comportamentos em relação à exploração de vulnerabilidades; **escopo**, que determina todas as definições sobre os sistemas ou cenários a serem testados; **abordagem**, que trata do método de execução no que diz respeito à geração de ruído no ambiente, dividido em *covert* e *overt*, e que implica nas atividades e comportamento do testador; **estratégia**, que determina quais estratégias podem ser utilizadas no teste, como *external*, *internal*, *applications*, *web-based*, *communications-based*; e, **ponto de partida**, que representa o ponto onde os testadores conectam seus equipamentos para realizar as práticas - que pode estar dentro ou fora do ambiente físico do alvo.

Além disso, as práticas podem ser conduzidos em três etapas: **Pré-Ataque**, **Ataque** e **Pós-Ataque**. O Pré-Ataque compreende a definição do escopo e das regras de engajamento, onde a maioria dos critérios começa a ser estabelecida. Na etapa de Ataque, os vetores de ataque são determinados e são feitas tentativas de executá-los. Por fim, o Pós-Ataque trata de cobrir faixas de teste, preparar relatórios e compreender as descobertas dos testes.

2.2 Comunidades de Prática

A abordagem proposta neste relato de experiência tange características importantes presentes na definição proposta por Wenger[21] sobre Comunidades de Prática (*CoP*). Segundo o autor, comunidades de prática são grupos de pessoas que compartilham uma preocupação ou paixão por algo que fazem e aprendem como fazer melhor conforme interagem regularmente.

As comunidades de prática são consideradas um tipo de comunidade de aprendizagem, sustentadas pelos termos **comunidade** e **comunidade de aprendizagem**. Comunidade descreve grupos de pessoas conectadas por um interesse comum e que definem suas identidades pelos papéis que desempenham e as relações que compartilham na atividade do grupo. Já comunidade de aprendizagem busca desenvolver um alto nível de confiança entre os participantes para se tornar funcional, baseada em uma equalização de papéis entre os agentes em uma comunidade de forma a maximizar a participação de todos [15].

Comunidades de prática, representadas como um tipo de organização de aprendizagem informal, podem ser vistas como um processo de geração, aplicação e reprodução de conhecimento. Hoadley [14] apresenta que as comunidades de prática são grupos nos quais há um processo constante de participação onde os alunos entram em uma comunidade e gradualmente assumem suas práticas. Inicialmente, as pessoas podem participar de formas tangenciais, mas com o tempo, elas assumem cada vez mais a identidade de pertencimento ao grupo e centralidade, e cada vez mais as práticas centrais do grupo.

3 TRABALHOS RELACIONADOS

O desenvolvimento de pessoal capacitado na área de cibersegurança é um desafio para a sociedade. Da mesma forma que as demais áreas da computação, a mão de obra é escassa e a demanda crescente. Essa necessidade traz a atenção da academia[20] para meios de tornar mais eficiente o processo de ensino de cibersegurança, assim permitindo uma maior quantidade e qualidade de pessoas capacitadas na área. Nesta seção relatamos alguns trabalhos com esse foco.

A utilização de laboratórios práticos para o ensino de cibersegurança não é novidade. Esses laboratórios permitem aos estudantes terem um cenário prático muito próximo a um ambiente real para desenvolver suas habilidades. Além disso, esse tipo de prática fornece um desafio motivacional, muitas vezes estando ligados a gamificação. Um exemplo inicial de aplicação desses laboratórios é reportado por Shumba [17]. O relato detalha a utilização desse formato de ensino aplicado em uma disciplina de verão para uma turma do curso de Criminologia. O curso intitulado *"Cybersecurity Basics theories and principles"* utilizou nove diferentes laboratórios com o objetivo de apresentar e familiarizar os estudantes com diferentes ferramentas de cibersegurança. O uso de laboratórios também possui a vantagem de permitir a execução de forma remota e sem a necessidade de um instrutor dedicado. Um dos trabalhos nesse sentido é o de Mirkovic e Benzel [16] onde é apresentado o laboratório DeterLab. Esse laboratório consiste em um *cluster* de computadores disponibilizados *online* para o processo de aprendizado em cibersegurança. Existe a possibilidade de aprendizado de forma autônoma por parte dos alunos, executando exercícios de uma variedade de tópicos de forma independente.

Uma alternativa explorada para o ensino de cibersegurança é a integração de tópicos de cibersegurança em disciplinas obrigatórias do curso de graduação em áreas da computação. A área de cibersegurança é bastante abrangente e pode ser integrada em várias diferentes áreas da computação - isso permite aos estudantes ter uma visão holística da computação, já identificando possíveis vulnerabilidades e ter uma visão defensiva em seus projetos. Essa abordagem é apresentada no relato de Yue [23], onde tópicos de cibersegurança são integrados no currículo de disciplinas obrigatórias do curso de ciência da computação, através de seis aulas em cursos diferentes. De acordo com o autor, essa abordagem complementa a estrutura curricular tradicional e promove uma melhor abordagem em relação a cibersegurança.

Outra opção é a competição em diferentes modalidades de cibersegurança, oferecendo a oportunidade aos competidores de testarem e melhorarem suas habilidades, além de permitir que os participantes tenham a oportunidade de se preparar para a competição através de estudo de cibersegurança [19]. Existem vários diferentes modelos de competição, e entre um dos mais populares está o *King of the Hill*, onde diferentes equipes tentam, através de testes de intrusão, tomar controle de algum ativo digital. Bock [12] apresenta em seu trabalho a concepção e implementação de umas dessas competição. De acordo com o autor, esse formato ressalta diversas melhorias em relação às competições tradicionalmente implementadas na área, como *Capture the Flag* e *Build-it/Break-it/Fix-it*. Seu trabalho destaca o *King of the Hill* como uma implementação ideal em um ambiente de sala de aula. A participação em tais competições traz outros benefícios como é apontado por Lindsey *et al.* [19]. Nesse estudo de caso é demonstrado que a participação aumenta o nível de interesse, motivação e confiança dos participantes.

4 ESTRATÉGIA E PLANEJAMENTO

4.1 Concepção

O Weasels é uma iniciativa que oportuniza um espaço de cultura de cibersegurança por meio de atividades que promovam a construção de conhecimento através de interações, discussões e práticas organizadas em diferentes formatos. O grupo surgiu com o objetivo de disseminar os temas relacionados a área de Segurança Ofensiva, aumentar o interesse pelas iniciativas existentes e auxiliar a inserção de profissionais na área - que tem se mostrado com inúmeras oportunidades.

A proposição inicial se deu, primordialmente, devido ao interesse expressivo dos alunos pertecentes a nossa instituição em conhecer mais sobre a área de cibersegurança. Aliado a isso, o histórico de estudos e produções do grupo de pesquisa ao qual estamos inseridos potencializou esse interesse por meio de ações, palestras e eventos relacionados ao tema.

Além de fomentar as atividades discentes, os planos de concepção do Weasels estavam também voltados ao envolvimento de empresas parceiras do nosso grupo. Assim, entendia-se que um agrupamento de pessoas interessadas - que não somente em um formato de grupo de estudos - poderia contribuir para a avaliação, análise e solução de problemas de segurança existentes nessas empresas.

A partir dessas motivações, foi necessário estruturar e organizar os planos de ação para que fosse viável iniciar o grupo de forma com que as ideias iniciais fossem validadas em um projeto piloto e que a continuidade pudesse ser um critério avaliado para a consistência do planejamento inicial.

Assim, em 2020, iniciamos as tratativas de formalização do grupo como um projeto para que alunos pertencentes ao Programa de Educação Tutorial (PET) da CAPES[1] pudessem dedicar seu tempo na experimentação de técnicas e métodos aplicados à Segurança Ofensiva. Nesse sentido, acolhemos três alunos do PET para a execução de atividades que haviam sido previamente planejadas. A partir disso, foram conduzidas práticas com esses alunos que permitiram ratificar aspectos determinantes para que uma metodologia pudesse ser criada.

4.2 Experimentação Prévia

Em outubro de 2020, as atividades com os três alunos começaram a ser realizadas a partir de determinações dos gestores do projeto. Este início foi sustentado em oferecer uma base de conhecimentos necessários em Segurança Ofensiva - chamamos este trecho de *nivelamento* já que não tínhamos conhecimento do *background* teórico dos participantes. Contudo, por ser uma área que envolve múltiplos cenários de aplicação, decidimos direcionar os esforços para uma sustentação sobre duas temáticas centrais: *base ferramental* e *comunicação de dados*.

Para esse nivelamento utilizamos a plataforma de ensino de cibersegurança *TryHackMe*, estipulamos objetivos para cada uma dos laboratórios (*rooms*) utilizados e geramos discussões sobre os tópicos cobertos neles.

Após o nivelamento, foram propostos dois tipos diferentes de atividades para que fosse possível aplicar alguns conhecimentos obtidos previamente. O primeiro tipo consistiu em desafios aplicados de segurança ofensiva por meio de laboratórios do *TryHackMe* que necessitassem de maior autonomia para suas resoluções. Nesse sentido, adotamos, por exemplo, os laboratórios *Vulnversity*, *Basic Pentesting*, *Blue* e *Ice*. Já o segundo tipo de atividade objetivou as ações cocriativas e colaborativas dos participantes pois foi necessário que os mesmos atuassem conjuntamente para desenvolver, em um primeiro momento, um *script* em *Bash* que realizasse alguma técnica de Segurança Ofensiva.

Durante quatro meses o conjunto de atividades prosseguiu com essa estrutura e com acompanhamento por meio de encontros semanais com todos os participantes. Para além do emprego de técnicas e desenvolvimento de *hard skills*, a experimentação prévia permitiu a criação de um espaço colaborativo, com um grupo de participantes coeso e exercitando aspectos relacionados a *soft skills*. Adicionalmente, a autonomia de cada participante mostrou-se, juntamente às demais questões, um importante valor para o Weasels.

4.3 Metodologia Criada

O conjunto de atividades realizadas, aliado ao formato das reuniões, a promoção de discussões técnicas e os processos avaliativos permitiram que fosse criada uma metodologia a partir da experimentação prévia. O objetivo de tal proposição é organizar e padronizar o conjunto de práticas de forma a replicar o mesmo para outros grupos de participantes. A Figura 1 apresenta o roteiro de atividades práticas que compõem a primeira versão da metodologia.

[1] http://portal.mec.gov.br/pet/pet

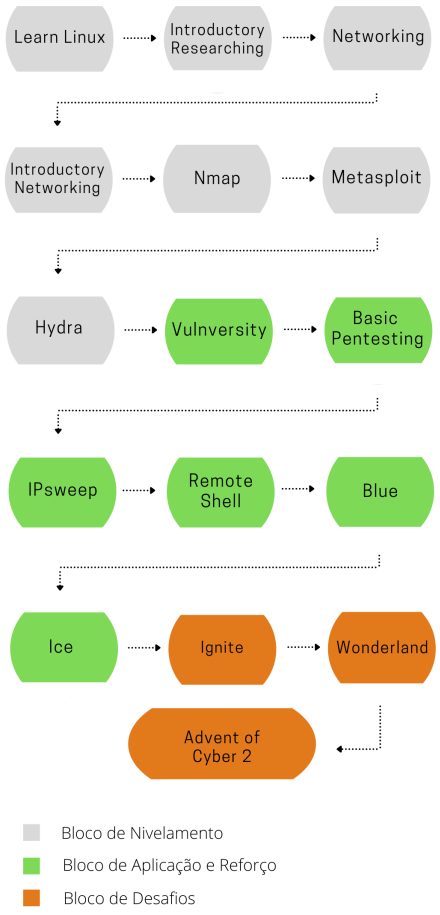

Figura 1: Diagrama das atividades práticas da metodologia.

Com base na Figura 1, as subseções a seguir descrevem os conteúdos e objetivos abordados nas atividades práticas que compõem cada um dos blocos: **Bloco de Nivelamento**, **Bloco de Aplicação e Reforço** e **Bloco de Desafios**.

4.3.1 Learn Linux. O **Bloco de Nivelamento** traz, no seu primeiro momento das atividades, a utilização do laboratório *Learn Linux* para tratar os conceitos substanciais a respeito do sistema operacional Linux e seus recursos intrínsecos. Como conteúdo principal, as atividades trataram a execução de comandos via terminal, operadores e comandos básicos. Adicionalmente, este laboratório do *TryHackMe* apresenta noções de permissões, diretórios comuns, acesso remoto com SSH e a introdução a *shell scripts*.

4.3.2 Introductory Researching. O segundo momento idealizado para o bloco consiste em um laboratório que demonstra formas de pesquisar soluções para enventuais problemas relacionados ao contexto de Segurança Ofensiva. Além da demonstração de uso de pesquisas direcionadas no Google, também apresenta o ExploitDB - um repositório onde é possível encontrar vulnerabilidades comuns de diversos softwares, muitas vezes relacionando com o seu identificador de vulnerabilidade em consonância com as *Common Vulnerabilities and Exposures* (CVEs)[2] existentes. Por fim, discute ainda a utilização do manual do Linux pelo terminal através do comando *man*, o qual fornece informações sobre a maioria das ferramentas e funcionalidades pertencentes ao sistema operacional Linux.

4.3.3 Networking. Como início da base de comunicação de dados e redes de computadores, o laboratório relaciona os diversos tipos de Protocolo de Internet versão 4 (IPv4) e suas classificações. Além disso, sumariamente, também faz uma introdução aos números binários e as conversões entre binário e decimal.

4.3.4 Introductory Networking. Como forma complementar do momento anterior, este laboratório trata das características fundamentais e diferenças dos modelos OSI e TCP/IP, bem como apresenta os protocolos de comunicação entre sistemas mais utilizados. Adicionalmente, demonstra a utilização e objetivos do uso dos comandos *ping*, *traceroute* e *dig*, que permitem obter informações diversas sobre o alvo avaliado.

4.3.5 Nmap. A partir do entendimento dos processos de comunicação de dados e alguns protocolos, o início do contato com ferramentas se dá neste momento da metodologia com a utilização deste laboratório. As práticas nele contidas consistem em introduzir a feramenta de mapeamento de redes Nmap, utilizada na etapa de reconhecimento de um teste de intrusão. Nesse sentido, as atividades envolvem os diferentes tipos de varreduras como: *UDP Scan*, *TCP Scan*, *SYN Scan*, e também os *scripts* disponíveis para detecção de vulnerabilidades e opções específicas para evasão de mecanismos de defesa.

4.3.6 Metasploit. Entendendo que era necessário dispor de uma atividade que envolvesse termos e práticas essenciais da Segurança Ofensiva, a adoção do laboratório Metasploit nesse momento foi primordial. As tarefas apresentam a ferramenta e seus diversos módulos de *exploits*, recursos auxiliares e *payloads* disponíveis. A proposição de colocá-lo após o uso do *Nmap* se deu também pois o Metasploit permite a utilização do *Nmap* de forma integrada - o que permite a criação de base de dados de informações das varreduras realizadas e demais vulnerabilidades identificadas.

4.3.7 Hydra. Ao final do Bloco de Nivelamento, adicionamos as práticas com a ferramenta *Hydra* tendo em vista a necessidade do entendimento dos ataques de força bruta envolvendo diferentes serviços e protocolos. A partir disso, entendemos que os aspectos essenciais para a realização de outras atividades do bloco seguinte são devidamente subsidiadas para as discussões de resolução de problemas em grupo.

4.3.8 Vulnversity. Dando início ao **Bloco de Aplicação e Reforço**, começamos a abordagem de vulnerabilidades no contexto *web* com a utilização deste laboratório em específico. Ele possibilita o contato com as técnicas de enumeração e busca de diretorios não listados, uso da ferramenta *BurpSuite* e explicações sobre *reverse shell* com a ferramenta *Netcat* para exploração e obtenção de acesso. Como parte da etapa de pós-exploração, a prática apresenta a escalação de privilégios por meio de uso do SUID (*Set owner User ID up on*

[2]https://cve.mitre.org

execution) que permite, durante a execução de um binário, conseguir o nível de permissão do criador do arquivo.

4.3.9 Basic Pentesting. Nesta prática propusemos a discussão e aplicação de fatores previamente vistos no bloco de nivelamento - isso se deve ao fato de que o laboratório Basic Pentesting propõe o uso do *Nmap* e do *Hydra*, além de processos de enumeração com a utilização da ferramenta *LinPEAS* - um *script* para identificar possíveis falhas que podem levar a escalação de privilégios. Nas atividades finais do laboratório há a abordagem com *hash cracking* com o uso da ferramenta *John the Ripper*.

4.3.10 IPsweep. Uma das propostas que não utilizou a plataforma *TryHackMe* foi a proposição, por parte dos responsáveis do Weasels, de um desafio que consistia em desenvolver, em grupo, um *script* em *Bash* para criar um IPSweep - técnica que consiste em identificar e mapear *hosts* vivos em uma rede por meio do uso do protocolo *ICMP*. Para tal, a ideia é criar um *script* operado por linha de comando que recebe como parâmetro um endereço IP de uma rede e um intervalo de endereço IPs a serem escaneados. Adicionalmente a tarefa também exige que, de forma opcional, seja possível configurar como parâmetro um intervalo de tempo entre os *pings* dos diferentes IPs.

4.3.11 Shell Remota. Ainda no conjunto de tarefas em grupo, o desafio proposto é o estudo, análise e criação de *remote shell* - que permite realizar uma conexão de forma remota em outro computador, o qual conseguimos acessar como se estivéssemos em um terminal local. Na resolução desse desafio são necessárias duas aplicações, ambas desenvolvidas em *Python* representando um servidor e um cliente. Uma vez que ambas aplicações estão desenvolvidas, a execução do *remote shell* é possível.

4.3.12 Blue. Para que fosse possível discutir sobre vulnerabilidades conhecidas, definimos neste momento da metodologia a utilização de uma prática de exploração da vulnerabilidade *ms17-010/Eternal Blue*. Dessa forma, possibilitamos a aplicação dos conhecimentos envolvendo os laboratórios *Introductory Researching*, *Nmap* e *Metasploit* para resolução dos desafios presentes. Além disso, também são introduzidos conceitos de quebra de criptografia de senha e exploração dos arquivos padrões do Windows.

4.3.13 Ice. Como forma de reforço do momento anterior, as práticas desse momento envolvem falhas em um serviço conhecido como *Icecast*, também em um sistema operacional *Windows*. A principal diferença está no vetor de ataque que se utiliza de uma vulnerabilidade de (*buffer overflow*) para conceder acesso à máquina. Para a etapa de pós-exploração, utilizamos a ferramenta o *Exploit Suggester* de forma conseguir um nível de permissão de acesso maior.

4.3.14 Ignite. No bloco final das atividades, o **Bloco de Desafios** é composto por três momentos de maior complexidade em relação aos anteriores. Nesse sentido, a proposta deste bloco é promover um contato diversificado com tópicos presentes na área de Segurança Ofensiva em um formato de desafio.

Complementando as práticas no contexto web, o laboratório *Ignite* trata uma aplicação com o serviço *FUEL CMS* sendo executado em um servidor *Apache*. Essa identificação do serviço, assim como em momentos anteriores, propõe uma repetição de investigações e pesquisas de vulnerabilidades ao utilizar, por exemplo, o *ExploitDB* para procurar por falhas já conhecidas de tal serviço. Como forma de exploração, é utilizado um *script* em *Python* para obtenção de acesso e execução de comandos remotos. Uma vez com o acesso com o usuário *www-data*, a escalação de privilégios ocorre com uma busca por credenciais disponíveis no alvo - neste caso, credenciais de *root* estão presentes no diretório *config*.

4.3.15 Wonderland. O laboratório *Wonderland* traz, nas suas práticas, o uso de esteganografia na resolução do desafio. A partir da identificação de uma porta 80 aberta e da enumeração de diretórios via força bruta, o caminho da tarefa envolve o diretório */img* contendo três imagens. A indicação das imagens dá conta de que é necessário "seguir o coelho", uma analogia a história de Alice no País das Maravilhas. Nesse sentido, investigando os diretórios com as opções *"/r/a/b/b/i/t"*, é possível descobrir credenciais válidas para a conexão via *SSH*. Após a conexão estabelecida, a escalação de privilégios requer, inicialmente, a modificação de um módulo em uma biblioteca presente no *script Python* e, posteriormente, a manipulação de uma variável em um arquivo *ELF* com *SUID bit*. Por fim, a técnica de escalação consiste na utilização de *capabilities* de um arquivo *Perl* - similar na questão da funcionalidade do *SUID bit*.

4.3.16 Advent of Cyber 2. A finalização do bloco de desafios e também do roteiro utilizado na metodologia foi através do laboratório *Advent of Cyber 2*[3]. Esse tipo de desafio é composto por um agrupamento de atividades dividido em cinco módulos: Explorações *Web*, Desafios de Redes, Desafios de *Scripts*, Engenharia Reversa e Desafios de *Blue Team*. Na ocasião da primeira execução dessas atividades, os participantes do Weasels realizavam uma tarefa por dia, em um total de 24 ao final.

4.4 Expansão

Ainda no final do ano de 2020 foram traçados planos para que o grupo recebesse novos participantes no início de 2021. Para tal, foi necessário criar um material e um meio de divulgação que pudesse atingir as pessoas interessadas. Inicialmente, adotamos como critério que apenas alunos e colaboradores da universidade pudessem integrar o grupo - e, considerando isso, a forma de divulgação definida contou com a ajuda dos coordenadores e professores dos cursos da área de computação.

No primeiro semestre de 2021 contamos com 18 novos participantes, e isto permitiu que fosse aplicada a metodologia que criamos para os novos ingressantes - entendendo que auxiliaríamos na construção de conhecimento base a partir da experiência prévia obtida. Ao mesmo tempo, o número expressivo de novos participantes também exigiu que organizássemos de forma diferente o grupo e também os encontros. Assim, iniciamos nossas atividades de 2021 com uma divisão de subgrupos de três pessoas e com três diferentes tipos de reuniões:

- Reunião Semanal: cada subgrupo definiu um representante para participar da reunião semanal cujo objetivo era, exclusivamente, a troca de ideias e dúvidas provenientes das atividades baseadas na metodologia criada. Assim, exercitamos a comunicação entre todos os participantes através da explanação das questões envolvendo técnicas e métodos da Segurança Ofensiva.

[3] https://tryhackme.com/room/adventofcyber2

- Reunião Mensal: todos os participantes do Weasels se reuniram para assistir a apresentação feita por um integrante do grupo mostrando a resolução de algum desafio. Esse tipo de reunião proporcionou uma experiência de contato com técnicas mais avançadas ou desconhecidas pelos participantes e a discussão sobre as mesmas com aqueles que eram mais experientes ou já haviam tido contato prévio.
- Reunião de Mentoria: cada subgrupo, ao concluir trechos da metodologia criada, se reunia com os responsáveis pelo Weasels para uma discussão com mais proximidade, em formato de mentoria. Com isso, asseguramos que novos ingressantes realizem as atividades seguindo a metodologia criada. Assim, foi possível direcionar os esforços para resolução de dúvidas e problemas mais pontuais, ao passo que também permitiu avaliar o andamento e entendimento de cada subgrupo.

Essa expansão do grupo possibilitou a replicação da metodologia criada previamente, bem como o surgimento de novas ideias e rumos para o grupo. Ainda no primeiro semestre de 2021 participamos do CTF da SANS [4] de forma colaborativa, discutindo os desafios e experimentando o emprego de novas técnicas não antes vistas. Além disso, expandimos as resoluções de desafios para a plataforma de ensino e aprendizagem de cibersegurança *HackTheBox*, cuja proposição difere em complexidade e formato em relação aos laboratórios do *TryHackMe*.

Durante a execução das atividades e encontros realizados, os responsáveis pelo grupo frequentemente avaliaram a organização geral, objetivos e formatos adotados. Essa avaliação se deu por meio de encontros semanais de discussão, permitindo que as práticas se mantivessem em sinergia com a proposição do Weasels.

Para o segundo semestre de 2021 foram abertas novas oportunidades de ingresso de participantes no grupo. Nessa nova entrada, 25 pessoas demonstraram interesse e participaram de uma reunião inicial de apresentação do grupo. Entendendo que essa expansão do grupo ocorre de forma natural e gradativa, notou-se a importância da metodologia criada para auxiliar a organização das atividades.

Como principal mudança de melhoria para as ações do segundo semestre de 2021, decidimos aumentar o tempo da reunião semanal, encerrar a divisão em subgrupos e, principalmente, adotar a resolução de desafios de Segurança Ofensiva de forma conjunta e colaborativa - tendo em vista os *feedbacks* obtidos pelos participantes que estavam no primeiro semestre de 2021. Atualmente o Weasels conta com 44 participantes e realiza, nos encontros semanais, análises de vetores de ataque, vulnerabilidades, técnicas e ferramentas utilizadas na Segurança Ofensiva de forma aplicada em desafios de diferentes dificuldades.

5 RESULTADOS

5.1 Documentos e Artefatos

Durante a existência do Weasels, uma série de artefatos foram criados recorrentemente como parte das atividades executadas. Estes artefatos foram gerados em dois formatos diferentes: o primeiro é a documentação escrita da solução dos laboratórios propostos e outras atividades, como por exemplo a participação da equipe em

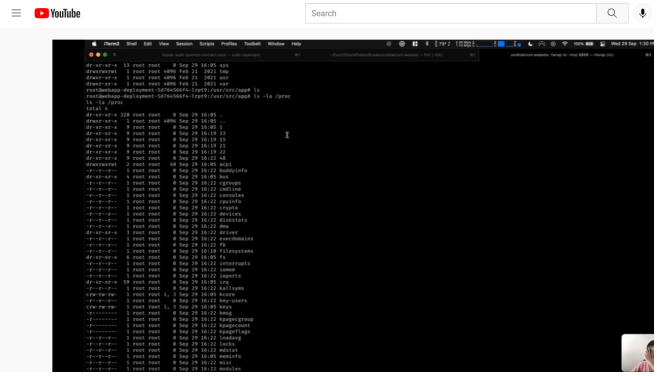

Figura 2: Gravação de Reunião disponibilizado no YouTube

provas de *Capture The Flag*. Esse registro foi feito em ocasiões diferentes tanto pelos membros responsáveis como por outros membros do grupo. Resumidamente, além de descrever um passo a passo para resolver os laboratórios específicos, essa documentação também inclui relatos de situações como as dificuldades encontradas durante a resolução. Já a segunda forma é o registro das reuniões via gravação de vídeo. Esses vídeos são disponibilizados no YouTube conforme Figura 2. Nesse tipo de artefato temos o registro das discussões pontuais que acontecem recorrentemente sobre ferramentas, métodos e a área de cibersegurança de forma geral.

A documentação gerada tem o intuito de atender três pontos:

- Ter uma biblioteca própria e em português da solução de laboratórios para consulta e auxílio no processo de aprendizado.
- Ter um registro das atividades do grupo para fim de refinamento e utilização no processo de avaliação continuada.
- Ter uma base de conhecimento para produção e geração de conteúdo científico.

5.2 Participação em eventos

O Weasels apesar de ser um grupo recente, já tem a participação em eventos tanto de cunho acadêmicos quanto científicos. Na parte acadêmica o grupo já apresentou um *workshop* com objetivo de introduzir estudantes ao teste de intrusão. Essa apresentação fazia parte de um evento dedicado ao curso de Engenharia de Software, mas que estudantes de outros cursos da universidade podiam participar abertamente. Devido a pandemia a apresentação foi feita em modelo remoto utilizando-se laboratórios práticos para o aprendizado. Ao final, obteve-se um *feedback* positivo pelos participantes a partir de discussões e dúvidas - alguns dos participantes inclusive passaram a fazer parte do Weasels posteriormente.

O funcionamento geral do grupo Weasels também foi apresentado no Salão de Iniciação Científica da universidade por um dos participantes. Após a apresentação foram levantadas considerações sobre o futuro do grupo e apontamentos para uma possível escalabilidade onde abrangeria empresas, pessoas não atreladas a universidade e até mesmo parcerias com o governo regional.

[4] https://www.sans.org

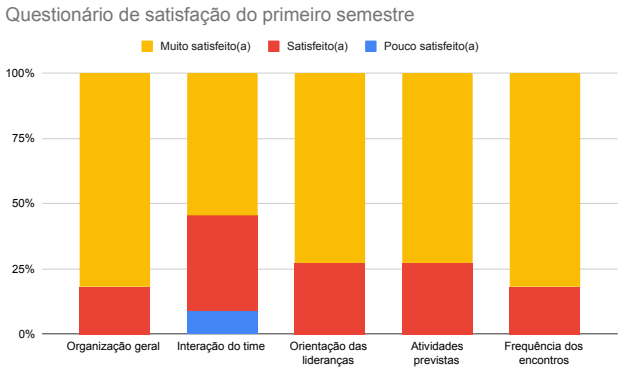

Figura 3: Questionário de satisfação

5.3 Avaliação Contínua

Como já anteriormente mencionado, os responsáveis pela organização do Weasels mantém uma avaliação contínua para o processo de execução das atividades do grupo. Além das reuniões de discussão semanais, foram adotados ainda dois instrumentos de avaliação quantitativa e qualitativa para análise dos objetivos, contribuições e produções do grupo.

5.3.1 Questionário Semestral. Ao final do primeiro semestre de 2021 foi aplicado, como primeiro instrumento de avaliação, um questionário com o objetivo de entender sobre a participação dos integrantes (sua frequência nas reuniões e realização das atividades), sobre o aprendizado em Segurança Ofensiva durante o período de 6 meses, sobre a estrutura e organização do grupo e sobre os tópicos específicos cobertos pelas atividades.

Em especial, este primeiro instrumento sinalizou que os participantes identificaram uma evolução no seu aprendizado em Segurança Ofensiva comparado à antes de sua entrada ao Weasels. Os resultados mostram que 73,7% dos participantes concordam plenamente que seu conhecimento de técnicas em Segurança Ofensiva evoluiu durante sua participação no grupo.

No que diz respeito à organização geral (veja Figura 3), 81% dos participantes mostraram-se muito satisfeitos e os outros 19% satisfeitos com a estrutura. Nesse sentido ainda, os participantes puderam avaliar a interação do grupo (54% muito satisfeitos, 37% satisfeitos e 9% pouco satisfeitos), a orientação das lideranças (73% muito satisfeitos e 27% satisfeitos), as atividades previstas na metodologia (73% muito satisfeitos e 27% satisfeitos) e a frequência dos encontros (81% muito satisfeitos e 19% satisfeitos).

Já no que tange os cenários de aplicação das técnicas, os participantes destacaram maior aprendizado no contexto web - justificado pelo fato de que os desafios, em sua maioria, possuem algum tipo de aplicação de técnica desse cenário. Em um aspecto ordinário, temos o uso de técnicas relacionadas com protocolos, seguido da parte de sistemas operacionais e, após, de redes de computadores.

5.3.2 Entrevistas Individuais. O segundo instrumento utilizado para a avaliação foi a aplicação de entrevistas individuais com os participantes do grupo. O objetivo geral da entrevista foi avaliar a percepção dos participantes em relação a **conhecimentos da área de Segurança Ofensiva**, **posicionamento sobre a área de Segurança Ofensiva** e **ambiente para o aprendizado em Segurança Ofensiva**.

Perguntamos, inicialmente, como cada participante define a área de Segurança Ofensiva hoje em dia. A proposição da questão teve o intuito de identificar como que cada participante caracteriza a área, de forma a confrontar com a questão posterior onde questionamos se o participante via alguma diferença em relação à definição do que é a Segurança Ofensiva após os 6 primeiros meses de participação no grupo. As respostas apontaram, principalmente, que sem conhecer a área os participantes associavam as práticas com um massivo uso de ferramentas como solução para os problemas de segurança identificados. Após estarem devidamente contextualizados com o grupo, os participantes ressaltaram a importância e responsabilidade das práticas da segurança no decorrer dos novos conhecimentos obtidos.

Em relação ao posicionamento sobre a área, procuramos observar quais os conhecimentos que cada participante julga necessário para atuar com Segurança Ofensiva. As respostas obtidas evidenciaram um diferente conjunto de possibilidades que envolvem desde programação e desenvolvimento de soluções até aspectos de sistemas operacionais, redes e comunicação de dados.

Por fim, ao abordar perguntas sobre o ambiente para o aprendizado em Segurança Ofensiva proposto pelo Weasels, termos como colaboração, interação, autonomia e flexibilidade se destacam nas respostas obtidas. Embora alguns dos participantes tenham trazido frases que denotem uma comparação de conhecimento com os demais, a organização do grupo em relação ao processo de aprendizagem autônomo e, ao mesmo tempo, colaborativo, foi um ponto de destaque. Especificamente neste bloco de questões conseguimos compreender que a unificação dos subgrupos, o espaço de troca expositiva e prática e a resolução de dúvidas e problemas de forma colaborativa foram aspectos que impactaram nas mudanças realizadas pelos responsáveis do Weasels desde a criação do grupo. A ideia de aplicar esses instrumentos permite que façamos uma avaliação contínua de toda a organização e funcionamento do grupo.

6 LIÇÕES APRENDIDAS

Considerando as diversas atividades e métodos de funcionamento, algumas das lições aprendidas foram:

- **Coesão do Grupo**. Todas as proposições só fazem sentido quando há uma coesão entre os participantes do grupo. Durante a experimentação prévia das atividades, exercitamos ao longo dos encontros o desenvolvimento de *soft skills* para atingir os objetivos de forma compartilhada, colaborativa, comunicativa e em um espaço de cocriação. A partir disso, notamos que, para as pessoas que ingressaram nas duas entradas que tivemos ao longo do ano, o exercício dessas práticas auxiliou expressivamente a condução das tarefas.
- **Autonomia como motivação**. Com a complexidade dos temas envolvidos na Segurança Ofensiva, adotamos a autonomia como um dos valores do grupo. Foi necessário articular com o grupo a forma de resolução das atividades para oferecer um espaço que potencializasse a autonomia de forma equilibrada a responsabilidade que a área exige, bem como as exigências estabelecidas para o andamento das reuniões.

Ao mesmo tempo, procuramos flexibilizar ao máximo as participações das pessoas de acordo com a janela de tempo a qual cada um poderia dedicar na execução das práticas - entendemos que isso também implicou para que a autonomia fosse um fator motivacional.

- **Resolução de atividades de forma guiada**. Com tantas atividades dispostas na nossa metodologia, conseguimos experimentar diversos formatos de apresentação e discussão dos conhecimentos envolvidos na resolução dos problemas. Nesse sentido, dois formatos se destacaram: as práticas *hands-on* guiadas por algum dos participantes com os demais, replicando o emprego das técnicas enquanto ocorriam discussões teóricas sobre as mesmas; e as práticas *hands-on* em caráter de observação - nesse formato, um dos participantes compartilha o momento da resolução dos desafios enquanto os demais observam, tomam notas e contribuem para tal resolução.

7 CONSIDERAÇÕES FINAIS

Neste trabalho apresentamos a estrutura, metodologia e funcionamento de um espaço de aprendizado e troca de conhecimentos que promove a cultura de cibersegurança, tema que tem se mostrado altamente relevante nos anos recentes. Construímos este relato em uma narrativa que descreve, inicialmente, a concepção e ideias primordiais do grupo dentro da nossa universidade. A proposição de potencializar os conhecimentos de Segurança Ofensiva norteou nossas ações para que fosse possível realizar a experimentação prévia - o "piloto" do nosso grupo. Para além disso, estabecelemos os componentes que compuseram as atividades da nossa metodologia durante o período da experimentação - o que nos permitiu validar a organização dos aspectos presentes na concepção.

A partir da expansão do grupo, a entrada de novos participantes e a organização dos diferentes tipos de encontros do grupo possibilitaram o desenvolvimento de novas ideias e motivaram iniciativas como a participação em competições que envolvessem a aplicação de conhecimentos aprendidos. Da mesma forma, esses aspectos permitiram novas investigações e práticas envolvendo outras plataformas de treinamento de cibersegurança e *wargames*.

Nossas percepções após um ano de experiência com o Weasels revelam que valores como autonomia e flexibilidade proporcionam aos participantes do grupo melhores possibilidades no desenvolvimento de seus conhecimentos em Segurança Ofensiva, especialmente por se tratar de um tema que engloba diversas outras áreas da computação. O fato de não obrigar nenhum participante a apresentar ou discutir as atividades nas reuniões e, ao invés disso, promover a resolução de forma colaborativa e a partir de escolhas conjuntas, auxilia para que o Weasels seja um espaço diferenciado de aprendizado. Adicionalmente, compreendemos também que nosso funcionamento precisa ser dinâmico e mutável, moldando nossas atividades a partir dos diferentes tipos de experiências vividas ao longo dos encontros e atividades extras.

Como trabalhos futuros e evolução do grupo pretendemos promover a aproximação com as empresas, instigar o desenvolvimento de soluções e ferramentas relacionadas à Segurança Ofensiva e expandir nossas relações com outras universidades para a aplicação da nossa metodologia. Consideramos que a nossa experiência com o Weasels possibilita a abertura de discussões e novos desafios para a construção do conhecimento em Segurança Ofensiva (e Segurança da Informação de maneira geral), entendendo a necessidade de estabelecer métodos, ordenação de conteúdos e saberes pedagógicos que embasem as práticas e experimentações.

8 AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001. Avelino F. Zorzo possui bolsa de produtividade em desenvolvimento tecnológico do CNPq/Brasil.

REFERÊNCIAS

[1] [n.d.]. Alarming Cybersecurity Stats: What You Need To Know For 2021. https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=6ae7f87158d3 Accessed: 2021-10-18.
[2] [n.d.]. Brasil já é o 5º maior alvo global de ataques de hackers a empresas. https://economia.uol.com.br/noticias/estadao-conteudo/2021/09/12/brasil-e-5-maior-alvo-de-cibercrimes.htm Accessed: 2021-10-18.
[3] [n.d.]. Discord Weasels. https://discord.gg/gzRhets5jR Accessed: 2021-10-25.
[4] [n.d.]. Hackthebox. https://www.hackthebox.eu/ Accessed: 2021-10-25.
[5] [n.d.]. Número de aplicativos falsos cresce 225,1% no Brasil; tecnologia permite até abrir câmera do celular da vítima. https://extra.globo.com/economia/financas/numero-de-aplicativos-falsos-cresce-2251-no-brasil-tecnologia-permite-ate-abrir-camera-do-celular-da-vitima-25159369.html Accessed: 2021-10-18.
[6] [n.d.]. Site das Lojas Renner sai do ar após ataque hacker. https://g1.globo.com/economia/tecnologia/noticia/2021/08/19/site-das-lojas-renner-sai-do-ar-apos-ataque-hacker.ghtml Accessed: 2021-10-18.
[7] [n.d.]. STJ é alvo de ataque de hacker e Polícia Federal investiga o sistema. https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/stj-e-alvo-de-ataque-de-hacker-e-policia-federal-investiga-o-sistema Accessed: 2021-10-18.
[8] [n.d.]. Tryhackme. https://tryhackme.com/ Accessed: 2021-10-25.
[9] Daniel Dalalana Bertoglio and Avelino Francisco Zorzo. 2017. Overview and open issues on penetration test. *Journal of the Brazilian Computer Society* 23, 1, 1–16.
[10] Matt Bishop. 2003. What is computer security? *IEEE Security & Privacy* 1, 1, 67–69.
[11] Matt Bishop. 2007. About Penetration Testing. *IEEE Security & Privacy* 5, 6, 84–87.
[12] Kevin Bock, George Hughey, and Dave Levin. 2018. King of the Hill: A Novel Cybersecurity Competition for Teaching Penetration Testing. In *2018 USENIX Workshop on Advances in Security Education (ASE 18)*. USENIX Association, Baltimore, MD. https://www.usenix.org/conference/ase18/presentation/bock
[13] D. Geer and J. Harthorne. 2002. Penetration testing: a duet. In *Computer Security Applications Conference, 2002. Proceedings. 18th Annual.* 185–195.
[14] Christopher Hoadley. 2012. 12 What is a community of practice and how can we support it? *Theoretical foundations of learning environments* 286.
[15] Linda C Li, Jeremy M Grimshaw, Camilla Nielsen, Maria Judd, Peter C Coyte, and Ian D Graham. 2009. Evolution of Wenger's concept of community of practice. *Implementation science* 4, 1, 1–8.
[16] Jelena Mirkovic and Terry Benzel. 2012. Teaching Cybersecurity with DeterLab. *IEEE Security Privacy* 10, 1, 73–76.
[17] Rose Shumba. 2004. Towards a More Effective Way of Teaching a Cybersecurity Basics Course. In *Working Group Reports from ITiCSE on Innovation and Technology in Computer Science Education* (Leeds, United Kingdom) *(ITiCSE-WGR '04)*. Association for Computing Machinery, New York, NY, USA, 108–111.
[18] Matthew Swann, Joseph Rose, Gueltoum Bendiab, Stavros Shiaeles, and Fudong Li. 2021. Open Source and Commercial Capture The Flag Cyber Security Learning Platforms-A Case Study. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE, 198–205.
[19] Lindsey J Thomas, Moises Balders, Zach Countney, Chen Zhong, Jun Yao, and Chunxia Xu. 2019. Cybersecurity Education: From Beginners to Advanced Players in Cybersecurity Competitions. In *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*. 149–151.
[20] Luke Topham, Kashif Kifayat, Younis A Younis, Qi Shi, and Bob Askwith. 2016. Cyber security teaching and learning laboratories: A survey. *Information & Security* 35, 1, 51.
[21] Etienne Wenger. 1998. *Communities of Practice: Learning, Meaning, and Identity*. Cambridge University Press.
[22] Andrew Whitaker and Daniel Newman. 2005. *Penetration Testing and Cisco Network Defense*. Cisco Press, Indianapolis, USA.

[23] Chuan Yue. 2016. Teaching Computer Science With Cybersecurity Education Built-in. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)*. USENIX Association, Austin, TX. https://www.usenix.org/conference/ase16/workshop-program/presentation/yue