Mininet-Sec: plataforma de experimentação para segurança cibernética em redes programáveis

Italo Valcy S. Brito[1], **Leobino N. Sampaio**[1]

[1]Programa de Pós-Graduação em Ciência da Computação (PGCOMP)
Instituto de Computação – Universidade Federal da Bahia (UFBA)
Salvador – BA – Brasil

{italovalcy, leobino}@ufba.br

Abstract. *This paper presents Mininet-Sec, an emulation platform for studying and experimenting with cybersecurity in programmable networks. Mininet-Sec allows rapid prototyping of cybersecurity scenarios, attack simulation, and testing offensive security tools in an isolated and secure environment. The availability of specialized resources, along with support for network programmability, enables fast, effective and skilled development of security solutions. Mininet-Sec will be demonstrated in a variety of scenarios, including secure interdomain routing, DDoS attacks, and network security teaching, revealing how one can leverage Mininet-Sec's resources to provide advanced cybersecurity labs.*

Resumo. *Este artigo apresenta o Mininet-Sec, uma plataforma de experimentação de cibersegurança em redes programáveis, que permite rápida prototipagem de cenários de segurança, simulação de ataques e testes de ferramentas de segurança ofensiva de forma isolada. A disponibilidade de componentes específicos de segurança somado à capacidade de programabilidade da rede permitem o desenvolvimento rápido, eficaz e especializado de soluções de segurança. A ferramenta será demonstrada em cenários diversificados incluindo roteamento inter-domínio seguro, ataques de DDoS e práticas de ensino de segurança de redes, mostrando como os recursos do Mininet-Sec podem ser combinados para realizar laboratórios de cibersegurança avançada.*

1. Introdução

Em resposta à contínua evolução e complexidade das ameaças de cibersegurança, tem se tornado imprescindível o desenvolvimento de novos mecanismos de proteção, construção de soluções inovadoras para os desafios emergentes em segurança, e formação de profissionais para salvaguardar os sistemas, os dados e as pessoas. Ambientes de teste para estudar novos tipos de ataque, para testar vulnerabilidades em sistemas e protocolos ou para validar recursos de defesa, tipicamente são escassos, limitados em termos de escalabilidade ou complexos no que tange a preparação dos cenários de cibersegurança [Rahouti and Xiong 2019]. Pesquisadores e estudantes terminam por lançar mão do uso de *datasets* publicamente disponíveis ou ambientes com restrição de recursos para realizar seus experimentos [Gemmer et al. 2023], impondo desafios à execução de experimentos avançados e realistas de segurança, garantindo aspectos de reprodutibilidade e repetitividade científica.

Diversos ambientes de simulação, emulação e experimentação (e.g., *testbeds*) têm sido utilizados para realizar experimentos e aplicar práticas de ensino em redes

[Gomez et al. 2023]. Variando em termos de escalabilidade, propósito, recursos disponíveis e possibilidades de integração [Gomez et al. 2023], alguns ambientes fornecem suporte a programabilidade da rede, porém eles são de propósito geral e sem recursos nativos de cibersegurança. Por outro lado, ambientes de *testbed* para os chamados *Cyber Ranges* – plataformas de simulação de ataques para capacitação em cibersegurança – oferecem recursos específicos de segurança para experimentação, treinamentos práticos e competições em segurança [Yamin et al. 2020, Chouliaras et al. 2021]. Estes ambientes, no entanto, geralmente não fornecem recursos de programabilidade do plano de controle ou plano de dados da rede.

A programabilidade de rede permite não apenas uma resposta rápida, eficaz e especializada para os eventos de segurança [Gomez et al. 2023], como também, na perspectiva de ensino e aprendizagem, permitem um maior aprofundamento e apropriação tecnológica [Santos et al. 2020]. Dois ambientes bastante populares na criação de cenários de redes programáveis são o Mininet[1][Lantz et al. 2010] e o Containerlab[2]. Ambos os ambientes são altamente personalizáveis e permitem cenários de rede bastante diversos e complexos a partir da composição de serviços, por exemplo através da instanciação de grande diversidade de componentes de *software* através de *containers*. Em ambos os casos, porém, as personalizações específicas de segurança ficam a cargo do experimentador, impactando a complexidade de uso e reduzindo o reuso dos componentes. É importante ressaltar que o Mininet-Sec foi inspirado fortemente no Mininet, portanto eles compartilham muito do estilo de codificação, herança de classes, nomenclatura de componentes e estratégias de execução. Projetos relacionados ao Mininet, como Mininet-Wifi[3] e MiniNDN[4], também serviram de inspiração para o desenvolvimento do Mininet-Sec.

Este artigo descreve a ferramenta Mininet-Sec, uma plataforma de emulação para cibersegurança em redes programáveis, que consiste em uma derivação do projeto Mininet incorporando recursos específicos de segurança cibernética para facilitar rápida prototipagem, execução de experimentos de segurança de forma isolada e com recursos de programabilidade de redes. O Mininet-Sec possui um conjunto de ferramentas de segurança ofensiva e defensiva pré-instaladas, oferece suporte nativo a emular diversos serviços de rede para testes de segurança (e.g., servidor web, servidor de *e-mail*, DNS, FTP, NTP) e ainda incorpora melhorias na usabilidade do ambiente através de uma interface web enriquecida para gerenciamento da topologia e execução de comandos nos nós. Os requisitos de execução do Mininet-Sec são bastante flexíveis, podendo ser executado servidores *bare metal* e virtuais, *containers*, ambientes de nuvem e ambientes híbridos. Em particular, um dos casos de uso do Mininet-Sec retrata sua execução em ambiente de nuvem Kubernetes[5] integrando múltiplas instâncias através de túneis VXLAN.

Este artigo está organizado da seguinte forma: a Seção 2 apresenta a arquitetura, funcionalidades da ferramenta, casos de uso e disponibilidade de documentação; a Seção 3 descreve o planejamento da demonstração; por fim, a Seção 4 discute as considerações finais e os trabalhos futuros.

[1]`https://mininet.org`
[2]`https://containerlab.dev`
[3]`https://mininet-wifi.github.io`
[4]`https://minindn.memphis.edu`
[5]`https://kubernetes.io`

2. Mininet-Sec

O Mininet-Sec é uma extensão do Mininet incorporando recursos adicionais que tipicamente são utilizados em experimentos de cibersegurança a fim de facilitar a rápida prototipagem de novas estratégias de segurança defensiva, testes de ferramentas de segurança ofensiva ou experimentos de segurança em geral. Nesta seção serão apresentadas sua arquitetura e principais funcionalidades, bem como casos de uso.

2.1. Arquitetura e funcionalidades

A Figura 1 apresenta um diagrama que descreve a arquitetura do Mininet-Sec. Os principais módulos da ferramenta são descritos a seguir:

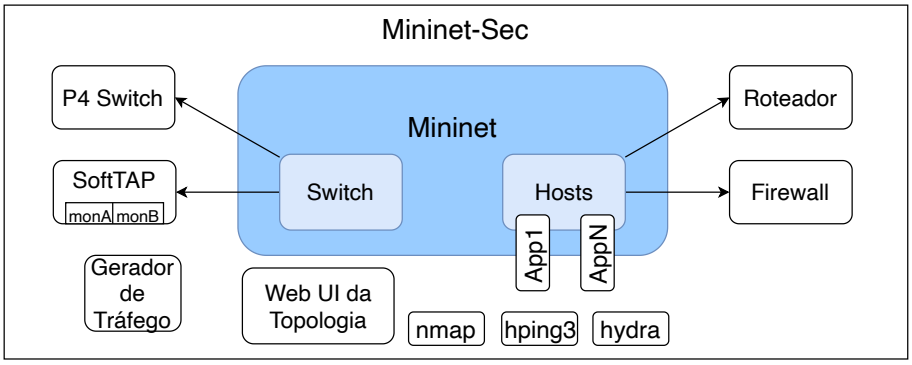

Figura 1. Arquitetura do Mininet-Sec e relação com Mininet.

- **Gerenciamento de Aplicações (App1...AppN)**. Uma das características do Mininet-Sec é a emulação de aplicações ou serviços de rede comuns nos *hosts* (App1, AppN na Figura 1). Ao modelar experimentos de segurança, o experimentador tipicamente precisa de serviços de rede comuns para compor os cenários de ataque ou defesa em questão. Servidores *web*, servidores de *e-mail* (SMTP, POP, IMAP), DNS, LDAP, NTP, dentre outros, são alguns exemplos dos mais de 20 serviços que podem ser facilmente instanciados no Mininet-Sec. A partir da rápida prototipagem destes serviços, o experimentador pode focar no seu experimento de segurança, por exemplo um ataque de força bruta contra o sistema de *e-mail*, ataques de negação de serviço contra servidores *web*, análise de consultas DNS benignas e maliciosas para validar uma determinada heurística, etc.
- **Biblioteca de nós**. Além da rápida prototipagem de serviços, outro recurso disponível no Mininet-Sec é a instanciação de alguns serviços e ferramentas específicas de segurança. Alguns exemplos incluem a criação de *Firewalls* (baseado em Netfilter/IPTables), SoftTAPs, IDS (Sistemas de Detecção de Intrusão – baseado no Suricata), WAF (Web Application Firewall – baseado no ModSecurity), entre outros. Além disso, permite também a criação de equipamentos de rede que suportam experimentação em segurança como Switches P4 e Roteadores. O *firewall* é uma solução de segurança que permite a aplicação de controles de porta, protocolo e endereços de rede no acesso aos serviços. Os *SoftTAPs* são dispositivos passivos que permitem o espelhamento de tráfego na camada física, copiando o tráfego de cada direção para uma porta de monitoramento (monA e monB na Figura 1). No Mininet-Sec é possível também instanciar *switches* P4 (baseado

no *software* BMv2[6]), roteadores com suporte a BGPSEC, RPKI e outros recursos de segurança (baseado no NIST BGP-SRx[7]), além de ferramentas específicas de segurança como NMAP[8], HPING3[9], HYDRA[10], Slowloris[11], e mausezahn[12].

- **Gerenciamento de topologia (Web UI)**. Outro recurso disponível é a visualização da topologia que permite verificar a conexão dos componentes, possibilita execução de comandos em equipamentos específicos da topologia, e permite adição/remoção de componentes sobre demanda. O Mininet-Sec provê mecanismo para fácil configuração de parâmetros de monitoramento *sFlow* nos *switches* da topologia. O usuário pode escolher por habilitar ou não a coleta *sFlow*, bem como personalizar o endereço do coletor e taxa de amostragem do tráfego.
- **Gerador de tráfego**. O Mininet inclui por padrão o *iperf*[13] como ferramenta de geração de tráfego, que funciona muito bem para emular as aplicações de grande transferência de dados ou testes de banda. No entanto, para cenários de segurança (para verificação de eficácia dos controles de segurança, medição de falsos positivos, etc), é importante gerar tráfego benigno que se aproxima com perfil de uso da rede típico/realístico (IMIX[14] ou EMIX[15]), seja em termos do tamanho dos pacotes, quantidade de usuários ativos simultaneamente, intervalo entre pacotes, diversidade de aplicações, etc. O Mininet-Sec inclui duas ferramentas de apoio ao experimentador no que tange a geração de tráfego benigno: D-ITG[16] e TRex[17].

A Figura 2 mostra uma captura de tela do Mininet-Sec. A visualização de topologia foi construída com base na biblioteca Dash/Cytoscape[18], o que permite grande interatividade com os elementos, facilitando a organização e entendimento do cenário pelo experimentador. É possível também adicionar *switches*, roteadores, *firewall*, *hosts*, dinamicamente, bem como personalizar algumas configurações como lista de aplicações que executa em cada nó. Deve-se notar também que o usuário tem um terminal virtual disponível para executar comando nos *hosts* da topologia através do navegador web.

A execução do Mininet-Sec segue os padrões do Mininet, permitindo o uso interativo via linha de comando:

```
mnsec --topo linear,3 --controller=remote,ip=127.0.0.1 \
  --apps h1:ssh:port=22,h1:http:port=80,h3:smtp,h3:imap,h3:pop3
```

Ou ainda a execução de forma programática via API Python, ou via interface web. O Mininet-Sec permite ainda descrever a topologia a partir de um arquivo formato YAML,

[6] https://github.com/p4lang/behavioral-model
[7] https://github.com/usnistgov/NIST-BGP-SRx
[8] https://nmap.org
[9] https://www.kali.org/tools/hping3/
[10] https://github.com/vanhauser-thc/thc-hydra
[11] https://github.com/gkbrk/slowloris
[12] https://github.com/netsniff-ng/netsniff-ng
[13] https://github.com/esnet/iperf
[14] Internet MIX, RFC 6985 (https://www.rfc-editor.org/rfc/rfc6985)
[15] Enterprise Mix, Cisco whitepaper "Network Based Application Recognition Performance Analysis" (https://www.cisco.com/en/US/technologies/tk543/tk759/technologies_white_paper0900aecd8031b712.html)
[16] https://sources.debian.org/src/d-itg/
[17] https://trex-tgn.cisco.com
[18] https://dash.plotly.com/cytoscape

especificando os nós, links, aplicações e demais atributos do experimento.

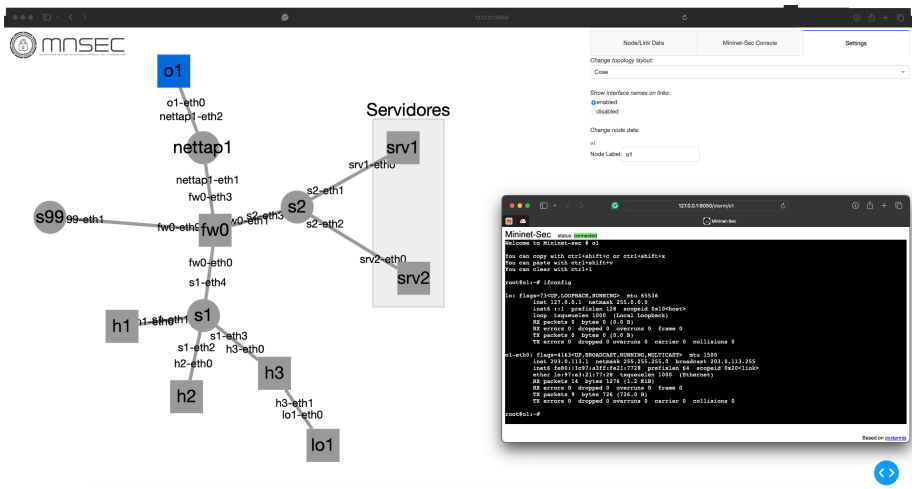

Figura 2. Captura de tela da interface web do Mininet-Sec.

2.2. Casos de uso

O Mininet-Sec pode ser utilizado para experimentos e desenvolvimento/validação de protótipos na área de segurança, assim como também pode servir de apoio para práticas de ensino em redes e segurança. Alguns casos de uso mapeados para a ferramenta são listados a seguir.

Laboratório de roteamento seguro na Internet com validação de origem BGP, validação de caminho BGP e validação de endereçamento IP de origem. Nos últimos anos incidentes, ataques e vulnerabilidades têm afetado protocolos de roteamento como BGP (Border Gateway Protocol) com *hijacking* de prefixo, vazamento de rotas[Sriram and Montgomery 2019], falsificação do IP de origem, entre outros, resultando, em última instância, em negação de serviço, desvios indesejados de roteamento e degradação de desempenho. Este caso de uso permite ao usuário do Mininet-Sec executar cenários similares aos descritos anteriormente, bem como aplicar técnicas consolidadas de segurança no roteamento inter-domínio como RPKI (*Resource Public Key Infrastructure*), validação de caminho com BGPsec, e validação do IP de origem com ACLs e uRPF (unicast Reverse Path Forwarding).

Laboratório de execução, detecção e mitigação de ataques de DDoS. Ataques de negação de serviço distribuídos (DDoS, do inglês *Distributed Denial-of-Service*), se caracterizam pelo volume de tráfego gerado e diversidade de origem visando indisponibilizar um serviço ou seus componentes adjacentes [Aslam et al. 2022]. Detectar e mitigar tais ataques nem sempre é uma tarefa fácil, e o operador precisa lançar mão de práticas de monitoramento eficazes (e.g., telemetria de fluxos de rede via sFlow/Netflow/IPFIX) e técnicas de contenção locais e coordenadas com seus provedores de Internet (e.g., criação de filtros para limitação de banda, BGP Flowspec para mitigação coordenada, RTBH – remotely triggered black hole, ou até mesmo serviços de limpeza de tráfego). Neste caso de uso será demonstrado a execução, detecção e mitigação de ataques de DDoS utilizando recursos disponíveis no Mininet-Sec (i.e., ferramentas de segurança ofensiva como hping3, configuração de monitoramento sFlow, e técnicas de mitigação através da programabilidade da rede).

Ensino de Segurança de Redes. O Mininet-Sec pode ser utilizado como ambiente de suporte a práticas de ensino de redes e segurança, tanto pelos recursos específicos que disponibiliza, quanto pela flexibilidade e facilidade de personalização dos cenários, além claro do isolamento do experimento que permite realizar testes disruptivos sem impactar no ambiente de produção. Em particular, o Mininet-Sec tem sido usado como base para execução de experimentos no projeto HackInSDN[19] – grupo de trabalho do projeto Hackers do Bem – que visa fornecer insumos para capacitação avançada de times de segurança defensiva e ofensiva incluindo temáticas como recursos de programabilidade de rede para detecção e mitigação de ataques, Inteligência de Ameaças, detecção de anomalias com aprendizagem de máquina, dentre outros.

2.3. Manuais e documentação

O código-fonte do Mininet-Sec, manuais de uso e instalação, além de alguns alguns vídeos explicativos sobre sua funcionalidades podem ser encontrados no site do projeto, disponível em `https://mininet-sec.github.io`.

3. Planejamento de Demonstração

A demonstração da ferramenta dar-se-á com o suporte de um computador e uma televisão. Nesta oportunidade, será criada uma topologia executada no próprio computador disponibilizado, conforme descrito na Figura 3. A topologia é composta por cinco sistemas autônomos, sendo que alguns deles possuem máquinas clientes e servidores nas redes internas, incluindo componentes como *firewalls*, roteadores, *switches* tradicionais e SDN, servidor Web e sistemas de IDS. Através de tal estrutura, a demonstração visa ilustrar algumas das características do Mininet-Sec.

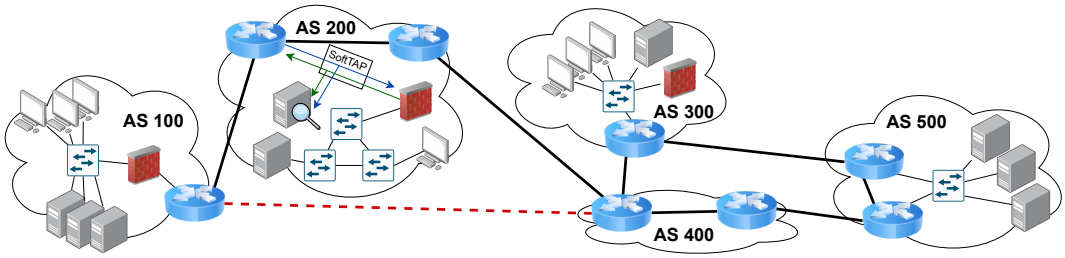

Figura 3. Cenário de uso/experimentação do Mininet-Sec.

A topologia descrita permite a demonstração dos três exemplos apresentados na Seção 2.2. No cenário 1, será simulado uma topologia composta por 5 sistemas autônomos com roteamento BGP e recursos de numeração específicos de cada um deles. Utilizando os recursos do Mininet-Sec, serão executados testes mostrando ataques de sequestro de prefixos IP, desvio de roteamento e falsificação de endereços IPs de origem. Após a execução de cada um dos ataques, será demonstrado possíveis impactos ao usuário, como alteração inadvertida de conteúdo, monitoramento não autorizado de tráfego e negação de serviço. Em seguida, serão demonstrados também o uso de protocolos/técnicas como RPKI, BGPSec e uRPF para prevenção de tais ataques.

[19] `https://hackinsdn.ufba.br`

Com objetivo de demonstrar o uso de ferramentas específicas de segurança, capacidade de ativação e configuração de monitoramento de telemetria de fluxos de rede via *sFlow* e vantagens do uso de equipamentos de rede programáveis, no cenário 2 será simulado o processo de execução, detecção e mitigação de ataques de DDoS. Para isso, considera-se que algumas máquinas infectadas com vírus e funcionando como *bots* no AS 100 e do AS 300 atacando um servidor web do AS 500. Este cenário permite ainda demonstrar o uso do *SoftTAP* para habilitar inspeção de pacotes (AS 200), e uso da programabilidade da rede para conter máquinas possivelmente infectadas e identificadas pela inspeção de segurança. O ataque ao servidor web no AS 500 será identificado a partir do monitoramento *sFlow* e regras de bloqueio serão criadas no *switch* programável para conter o ataque.

Por fim, o terceiro cenário demonstrado se refere ao uso do Mininet-Sec como parte do projeto HackInSDN para facilitar práticas de ensino em segurança da informação. Serão apresentados os ambientes em que o Mininet-Sec está sendo utilizado, integração com os componentes da arquitetura do HackInSDN e exemplos de cenários de uso.

4. Considerações finais e Trabalhos Futuros

Este artigo apresentou o Mininet-Sec, uma plataforma de experimentação em cibersegurança com recursos de redes programáveis, que permite rápida prototipagem de cenários de segurança, execução de experimentos de forma isolada e integrada, e com suporte a recursos de programabilidade de rede que ao serem combinados com os controles de segurança podem oferecer soluções mais rápidas, eficazes e especializadas. Conforme apresentado nos casos de uso, o Mininet-Sec pode ser aplicado em cenários de diversas naturezas, incluindo ambientes de ensino e aprendizagem em segurança avançada. O Mininet-Sec pode ser executado localmente ou ambientes de nuvem, possibilitando inclusive experimentos de múltiplos domínios através da integração de instâncias híbridas do Mininet-Sec com túneis VXLAN. Por fim, tal como o Mininet possui alto grau de extensibilidade – de tal modo inclusive que possibilitou o desenvolvimento deste trabalho, o Mininet-Sec também permite extensibilidade em seus múltiplos componentes. A título de exemplo, o módulo de gerenciamento de aplicações inclui padrões de projeto de engenharia de software para facilitar desenvolvimento futuro.

Como trabalhos futuros, espera-se investigar a implantação de novas ferramentas de segurança e recursos de experimentação, por exemplo, adicionando suporte a execução de traces de forma personalizada (i.e., taxa de comutação, cabeçalhos de rede, etc) e coleta de telemetria de redes por pacote com protocolos como INT (do inglês *In-band Network Telemetry*).

Agradecimentos

Os autores agradecem o apoio da Rede Nacional de Ensino e Pesquisa (RNP), do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e da Fundação de Amparo à Pesquisa do Estado da Bahia (FAPESB).

Referências

Aslam, N., Srivastava, S., and Gore, M. M. (2022). ONOS Flood Defender: An Intelligent Approach to Mitigate DDoS Attack in SDN.

Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., and Ferrag, M. A. (2021). Cyber ranges and testbeds for education, training, and research. *Applied Sciences*, 11(4):1809.

Gemmer, D. D., Meyer, B. H., Mello, E. R. d., Schwarz, M., Wangham, M. S., and Nogueira, M. (2023). A Scalable Cyber Security Framework for the Experimentation of DDoS Attacks of Things. In *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, pages 1–7.

Gomez, J., Kfoury, E. F., Crichigno, J., and Srivastava, G. (2023). A survey on network simulators, emulators, and testbeds used for research and education. *Computer Networks*, 237:110054.

Lantz, B., Heller, B., and McKeown, N. (2010). A network in a laptop: rapid prototyping for software-defined networks. In *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, pages 1–6.

Rahouti, M. and Xiong, K. (2019). A Customized Educational Booster for Online Students in Cybersecurity Education. In *CSEDU (2)*, pages 535–541.

Santos, J. B., Ribeiro, A. V., Brito, I. V. S., de Souza, M. C. S., de Souza Matos, E., and Sampaio, L. N. (2020). Uma experiência de avaliação multidimensional de cursos de redes de computadores em ambientes de testbeds. In *Anais do XXXI Simpósio Brasileiro de Informática na Educação*, pages 1703–1712. SBC.

Sriram, K. and Montgomery, D. (2019). Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation. Technical report, National Institute of Standards and Technology.

Yamin, M. M., Katt, B., and Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, 88:101636.