Physical Penetration Testing

A Pen-Tester’s Toolkit

▸ Tina Ellis ▸ March 9th, 2022

What is Physical Penetration Testing?

Physical penetration testing is used to identify weaknesses in physical security systems that attackers could exploit to gain access to the facilities.

Physical penetration testers (pentesters) are hired by organizations to test standing security policies for the purpose of exposing unknown vulnerabilities.

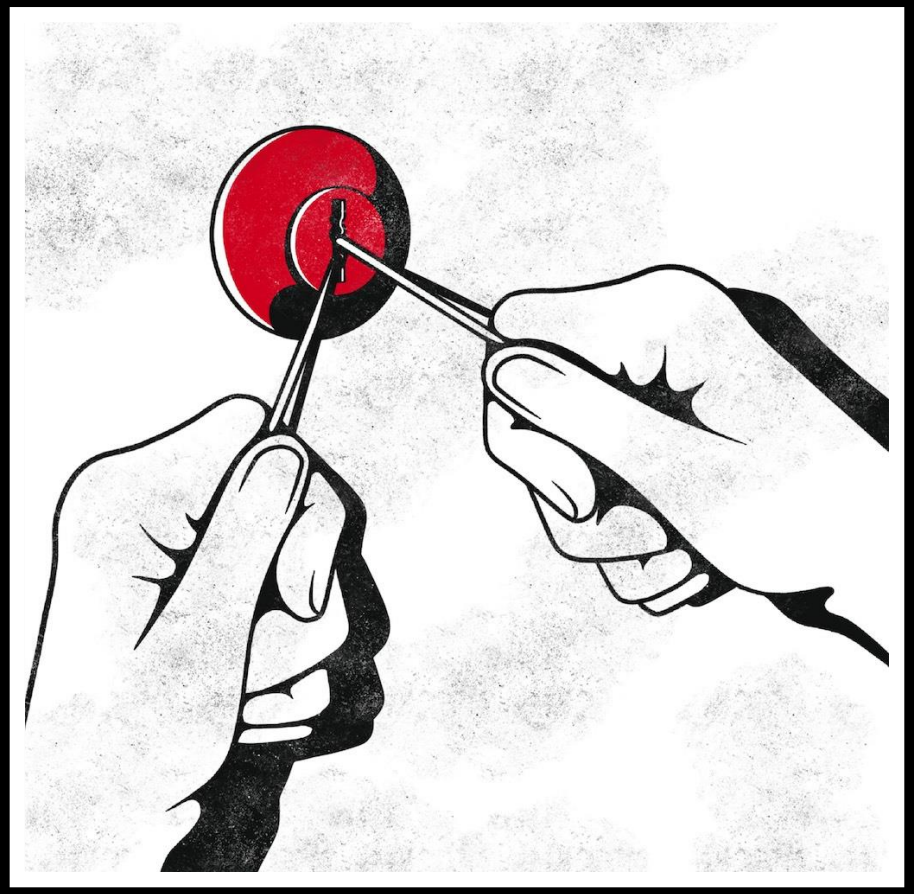
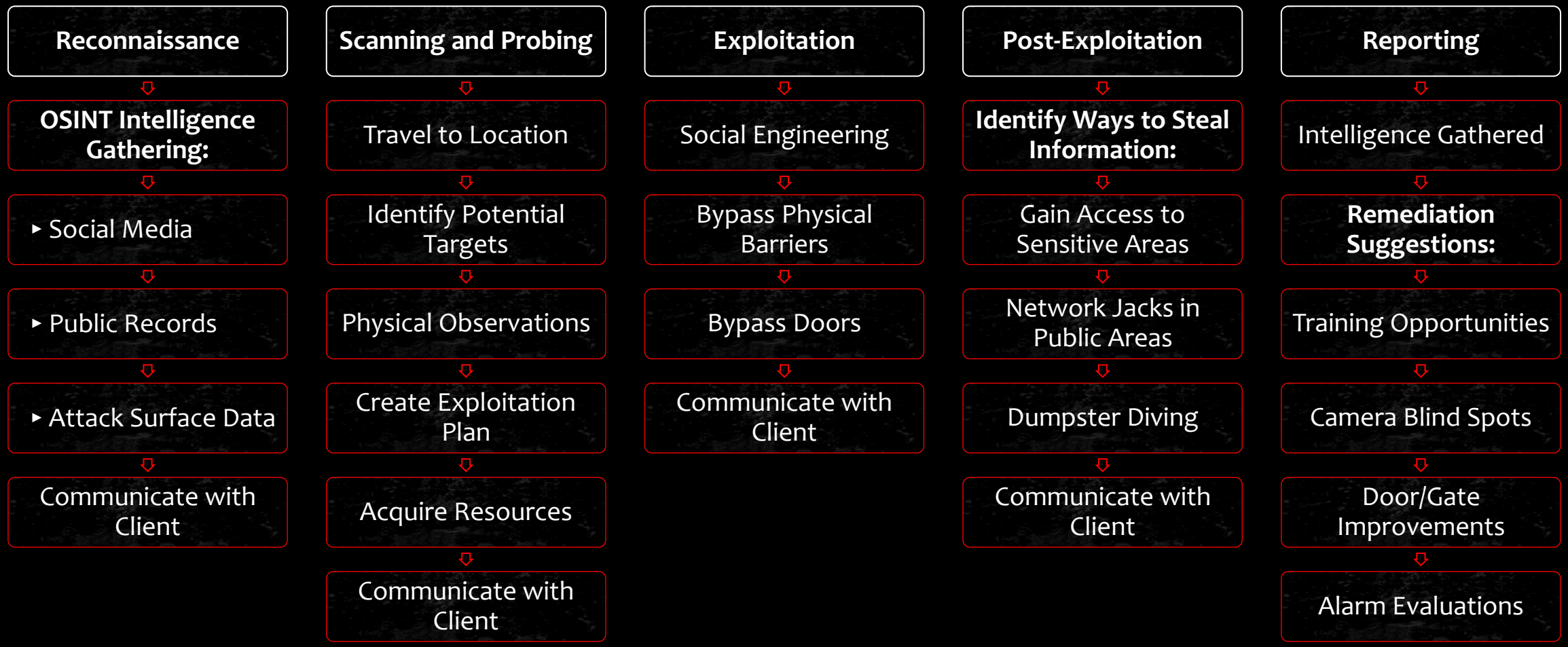


Photo Courtesy of DarknetDiaries.com

90% of network security is removed once a threat actor has physical access

- Wil Allsopp, Unauthorized Access: Physical Penetration Testing For IT Security Teams

Five Phases of Physical Penetration Testing



An Attacker Mindset

Pentesters know precisely how criminals might gain access to both computer systems and buildings and employ a variety of tools and methods to gain access to a facility.

- RedTeamSecure.com

Photo Courtesy of DarknetDiaries.com

Reconnaissance Phase

Pentesters use a variety of Open-Source Intelligence (OSINT) tools to gather information about their target.

OSINT CATEGORY	Social Media Intelligence [SOCMINT]	Digital Network Intelligence [DNINT]	Vehicle and Transportation Intelligence [VATINT]	Mapping and Geo-Spatial Intelligence [GEOINT]
APPLICATION	Hunting ground for company and employee information.	Identify technologies used and vulnerabilities that can be exploited.	Track down company vehicle information. Vehicles can be acquired to blend in.	Identify possible attack vectors (access points).
INTELLIGENCE	▸ Uniforms & Badges ▸ Name & Photo Identification ▸ Coffee & Lunch Hangouts ▸ Network and Systems ▸ Language & Technologies ▸ Possible Attack Vectors	▸ Host, DNS, & Mail Server Info ▸ IoT Device and Open Ports ▸ Public AWS or Azure Buckets ▸ Area Public Wi-Fi AP's ▸ Vendor Vulnerabilities	▸ Vehicle Recognition ▸ VIN Identification ▸ License Plate Lookup	▸ Internet Infrastructure ▸ Satellite Images ▸ Drone Images ▸ Street View Images ▸ Historical Facility Images ▸ CCTV Live Video Feeds
TOOL	Google, OpenPayrolls, GoFindWho, OnePlus OSINT Toolkit, SkyLens, Social-Search, Melissa Lookups, Company & Employee Social Media Pages, and Job Postings	Open Directories CSE, WhoisFreaks, CentralOps, ZoomEye, IntoDNS, Wappalyzer, HackerTarget, Pulsedive, WiGLE, WiFi Map, Shodan, Zoom Eye, Natlas, Public Buckets, CVE Details	CarNetAI, VehicleHistory, FaxVIN	GoogleMaps, Soar Earth, Wayback World Imagery, GeoHack Tools, FreeMapTools, HawkEye360, Satelite.pro, Infrapedia Map, TravelWithDrone, CCTV

**These are just examples of the OSINT tools available. Actual tools vary.*

Scanning and Probing Phase

Pentesters travel to the location and begin formalizing the exploitation plan.

Physical observations are conducted in person. Night reconnaissance might include locating camera location by using night-vision goggles to see the infrared light emitted by night surveillance cameras. Door, Gate, and Lock Brand information is gathered. SOC location is identified, and any interesting info noted.

Resources are acquired: Pentesters scan and clone badges, put together disguises, rent vehicles, and put together their toolkit.

Exploitation plan is created: After all the intelligence is gathered an exploitation plan is created and shared with the client.

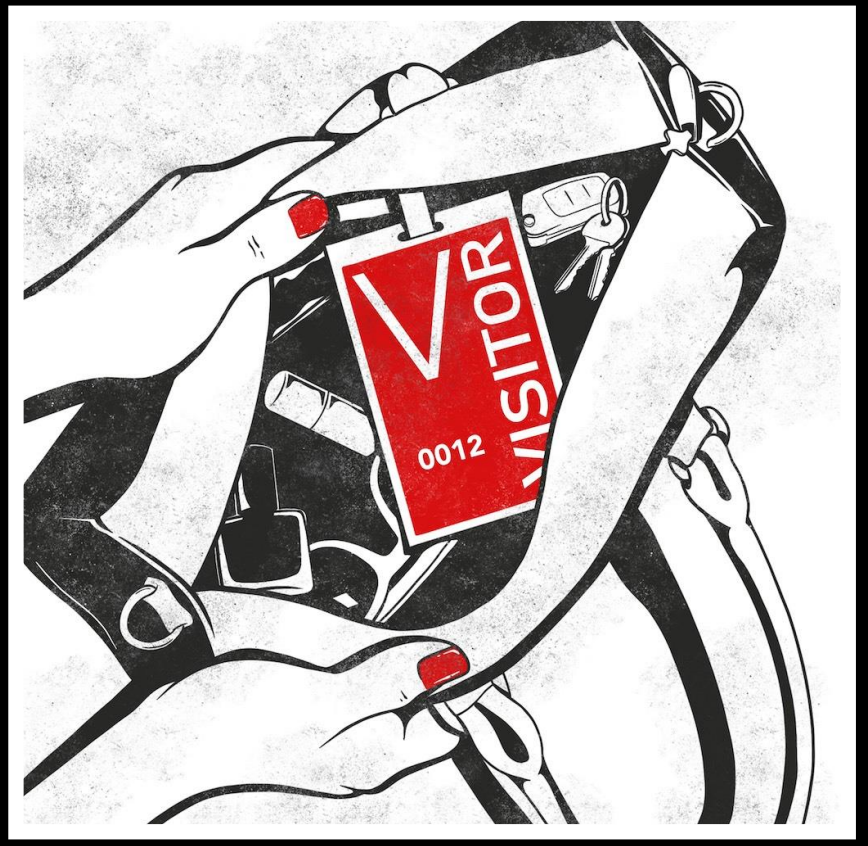


Photo Courtesy of DarknetDiaries.com

A "get-out-of-jail-free" card is acquired that proves their identity if they get caught

Pentesters communicate heavily with the parties. They also notify local authorities of their plan, so that they are not caught off guard. These steps are an important part of maintaining the safety of all parties involved.

Exploitation Phase

This is the phase where pentesters deploy their physical penetration testing plan. To implement this plan, pentesters use a variety of tools and methods, some technical and some not.

Social engineering is one non-technical approach that pentesters may employ to circumvent security controls. Pentesters may use impersonation, disguises, badges, and a sense of urgency to blend in or gain access to sensitive systems and information.

Physical access may also be obtained by observing the physical layout of the premises and identifying weak areas of security that do not require any special tools. Unlocked doors and unmonitored entryways provide an opportunity for access.

Bypassing security controls may also be an option by employing bypass tools such as plug spinners, hinge pin tools, door and gate tools, generic keys, and SEARAT tools.

Photo Courtesy of DarknetDiaries.com

The Physical Penetration Tools

Long range RFID readers and a Proxmark III for cloning cards

Disguises: Safety vests, uniforms, company cars, hard hats, lanyards

Multimeter, for equipment testing and failure issues.

Camera, flashlight, GoPro, Binoculars

Ladders of various heights

LANstar, LAN Cables, Small Wireless Router, for Network System Access

Raspberry Pi's – Plug into Network Connection for Network Access

Shortwave radios for communication

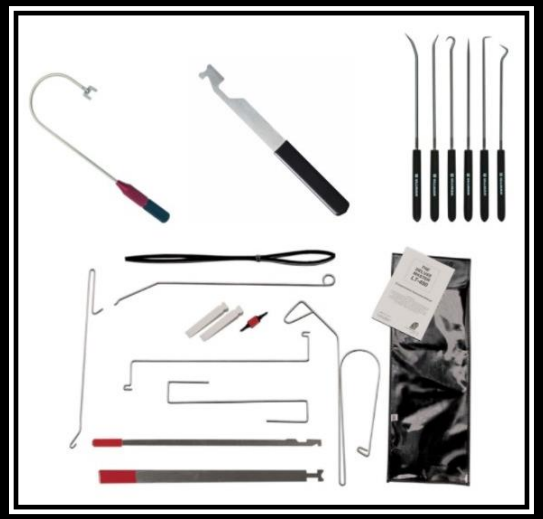
The Physical Penetration Tools

Borescope to see under doors or around corners

Night Vision Goggles: See at night and locate night vision cameras

Fence keys: Linear & Door King have generic keys available on Amazon

Wool blanket to protect your body from barbed-wire fences



Door Tools: Double Door Tools, Under the Door Tools, Shove-It Tool, Lockpicks

Plug Spinner: Prevents pins from reengaging after lockpick, and re-locks

Hinge Pin Tool: Spring-loaded tool used to pop hinges off doors

SEARAT: all-in-one entry tool includes key blade, Window-Breaker, Gas Shut-off

Photo Courtesy of DarknetDiaries.com

Post-Exploitation Phase

During the Post-Exploitation phase, the pentesters identify the opportunities where information could be stolen. They do not actually steal anything but take pictures or leave evidence (like a business card), to prove that they could have stolen information.

- Gain Access to Sensitive Areas
- Network Jacks in Public Areas
- Dumpster Diving

Reporting Phase

After the exploitation plan has been executed, pentesters compile their findings and create a report. The report includes any intelligence that was gathered during the reconnaissance and probing phases; a list of detailed steps and methods that were taken during the exploitation phase, as well as remediation suggestions that will improve an organization's overall security program.

Physical pentesters “undertake wildly ambitious and incredibly complex activities intended to reveal opportunities for a potential real-life showdown between good and evil - a heavily defended company against a would-be attacker"

- RedTeamSecure.com

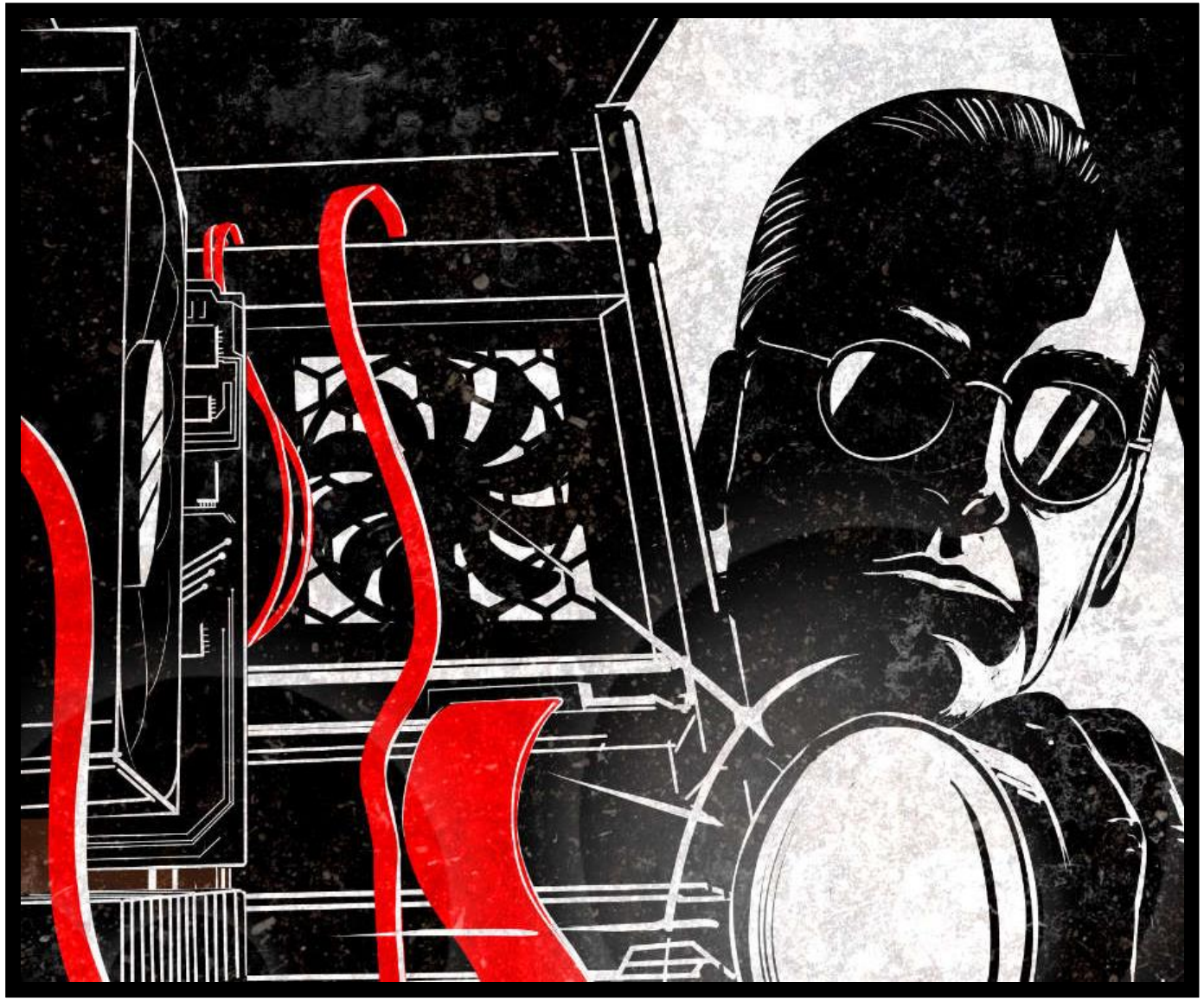


Photo Courtesy of DarknetDiaries.com

References

Darknet Diaries. (2021, June 22). Retrieved from https://darknetdiaries.com/

Deane, A. J., & Kraus, A. (2021). *The official (ISC)2 CCSP Cbk Reference*. Sybex.

Halton, W., & Weaver, B. (2017). *Penetration Testing: A Survival Guide.* Packt Publishing.

Mike Sheward. (2020). *Security Operations in Practice.* BCS, The Chartered Institute for IT.

Rhysider, J. (Host). (2021, June 22). *Jon and Brian's Big Adventure [Audio podcast].* Retrieved from https://darknetdiaries.com/transcript/95/

RedTeam Security, R. (n.d.). *Physical penetration testing services: RedTeam Security. RedTeam Security* - 5200 Willson Rd. Suite 150, Edina, MN 55424. Retrieved March 4, 2022, from https://www.redteamsecure.com/penetration-testing/physical-penetration-testing

Sillanpää, M., & Hautamäki, J. (2020, July). Social Engineering Intrusion: A Case Study. *In Proceedings of the 11th International Conference on Advances in Information Technology* (pp. 1-5).

Young, J. A. (2020). The Development of a Red Teaming Service-Learning Course. *Journal of Information Systems Education, 31*(3), 157–178.