P.S

OPERATION CHIMERA

PHYSICAL SECURITY MODULE // SECURITY BLUE TEAM

CONTENTS

This information has been gathered from public sources and combined with my own knowledge and experiences for the purpose of Operation Chimera, an online, live blue-team training operation conducted by myself under the alias Known Divide, for the SecurityBlueTeam community.

Useful Links:

[1]
https://en.wikipedia.org/wiki/Physical_security

[2]
https://www.cpni.gov.uk/physical-security

Anything that we missed? Please let us know, so we can add it in here, and create a useful resource for security professionals worldwide!

If you've enjoyed this event, please consider donating whatever you can spare to buy me pizza, coffee, and help fund future events! (even £5/$5 will make a huge difference, and it only takes a few seconds).

PayPal.Me

https://paypal.me/KDMentoring

OPERATION CHIMERA – PHYSICAL SECURITY

This document is not 100% finished and will be updated throughout Chimera. Thank you for your patience.

This module is designed to give a look into the world of Physical Security. It is aimed at individuals who are moving in to Cyber, so the material is aimed at an entry-level student. We strongly encourage further reading using the provided sources and any that you find yourself. Want to talk to other hackers about this specific module? Join the discussion in the "physical-sec-module" channel within the "Operation Chimera" category in the SBT Discord server. There is also a Chimera mega-thread on Reddit. Please make use of this to ask questions and talk to other participants!

WHAT IS PHYSICAL SECURITY?

Physical security controls are used to prevent unauthorized access to a building, or areas within. These controls help to make intrusion as hard as possible. The three main controls are Deterrents, Monitoring controls, and Access controls. Examples can include locked doors, security guards, CCTV, and barriers. Although this is not usually the responsibility of a cyber team, it is still very important to know, and may come in useful during investigations.

WHY IS IT USEFUL?

Usually if an attacker has physical access to systems, it's game over. This could include terminal access to servers, physical data theft in the form of paper documents or hard drives, or even physical damage to systems causing a denial of service.

By using Access Controls, we can make it hard for unauthorized individuals to gain access to protected areas. An example of this would be turnstiles at a main entrance that require an RFID badge to unlock and pass through. Using this control, only employees that have a badge with the correct digital keys will be able to pass through.

Monitoring Controls such as CCTV are useful for live monitoring and keeping a record of any malicious behavior so that it can be used in the event of prosecution. CCTV can also be classed as a deterrent, because if people know they're being recorded, they may be less likely to commit a crime or malicious act.

Deterrents are designed to deter people; an example would be warning signs telling people that if they go any further, they will be trespassing. This may be enough to prevent some people from continuing.

ASSOCIATED ROLES

Below is a list of roles that need to consider physical security, and why.

- **Incident Responder**
  After an incident, a Responder may need access to physical security logs, such as CCTV, electronic gates, and electronic doors to help aid the investigation.
- **Red Teamer**
  Knowing how physical security controls work, and how to bypass them, are key skills for a Red Team member that is involved in physical penetration tests.

DETERRENTS

Security controls that act as deterrents include warning signs and barbed wire. Their purpose is to deter potential attackers and make them less likely to attempt to gain entry.

- **Warning Signs:** Signs such as "DO NOT ENTER" and "You Are Trespassing" can be enough to make people turn around, as they have been informed that any further activity may be illegal.
- **Fences:** Chain-link metal fences are very common, with barbed or razor wire on top. This creates a barrier that can't be climbed over, and requires more effort for attackers to bypass, slowing them down and giving more time for them to be detected.
- **Guard Dogs:** Security dogs that are trained to bark and cause distress are a strong deterrent. Despite being highly trained, they still appear to be dangerous in the eyes of the attacker. They are also able to help detain any intruders.
- **Security Lighting:** Lighting is used to prevent low visibility areas caused by darkness, which could allow an intruder to bypass security controls such as CCTV and Security Guards. Lighting the areas in conjunction with cameras is a great deterrent and monitoring solution.

P.S

OPERATION CHIMERA

PHYSICAL SECURITY MODULE // SECURITY BLUE TEAM

MONITORING

These controls, such as CCTV cameras and intrusion detection systems are implemented to provide real-time monitoring and give security personnel the ability to

- **CCTV:** Closed-circuit television allows monitoring from multiple interconnected cameras. This gives security teams expanded visibility.
- **Security Guards**: It's all good to have these technical measures in place, but there needs to be a team that is trained in their use and maintenance so they can fully utilize the security controls and respond to incidents.
- **Intrusion Detection Systems**: These systems have several different triggers that can generate alerts or set off alarms, including thermal (heat) detection, sound detection, and movement detection.

ACCESS CONTROL

Access controls are used to prevent unauthorized people from accessing specific areas of a building or area.

- **Mantraps:** These are a slow but effective security control, where an individual wanting to access a protected area must go through an initial door into a small holding room, where they are inspected from a window or camera before the second door is unlocked.
- **Turnstiles/Gates:** This efficient control is very common in office buildings and requires employees to tap their ID pass on a reader, which will unlock the gate and allow them to pass through.
- **Electronic Doors:** These secure doors should be used throughout the facility, to limit the areas that a person can access, based on their role. For example, it is highly unlikely that someone from Human Resources should have access to a Server room. Only allowing certain people in specific areas not only reduces the risk of malicious activity but can also help find the person accountable as the list of potential suspects is much shorter.

OPERATION CHIMERA

PHYSICAL SECURITY MODULE // SECURITY BLUE TEAM

MODULE CHALLENGE

If you think you're ready for the module challenge, head over to the website and click on the 'Challenge Brief' button under the Physical Security module! Good luck.