HACK THE BUILDING

2020 | PLAYBOOK

VERSION 1.07

misi

HACK THE BUILDING IS AN UNCLASSIFIED EVENT | HACK THE BUILDING USES REPONSIBLE DISCLOSURE

REVISION HISTORY

Author	Description	Date
MEM	Initial revision, first scenarios and content	23 September 2020
MEM	Devising scenario TTP graphs, discussions with team members	02 October 2020
MEM	Additional content on logistics	14 October 2020
AS	Updates on title, style	15 October 2020
MEM	Continued Adding Scenarios, Hint/Recon Details, Defense section	16 October 2020
MEM	Adding content from MC Dean	23 October 2020

TABLE OF CONTENTS

1 INTRODUCTION

This handbook describes the Maryland Innovation and Security Institute (MISI) Hack the Building (#HTB2020) Event. While this event is socially designed as a showcase inaugural event to take place from November 16 – November 19, 2020, it will be treated as a series of events that can occur on a repeated basis. This playbook is designed to facilitate planning and execution of a HTB2020 event either physical or virtual.

All persons, places and entities used in HTB2020 are fictitious. Any similarity to real-world targets is accidental. Unless otherwise notified, the intellectual property used during any HTB2020 scenario or event is property of MISI

1.1 Goals

HTB2020 is designed to showcase the impact of a cyber-attack on critical infrastructure commercial or government facilities. Commercial and Government facilities are two of the 16 Cybersecurity and Infrastructure Agency critical infrastructure pillars for our nation. The event was inspired by the Department of Defense and their goal of highlighting the attention that needs to be focused on the cyber resilience of commercial and government facilities. There is a hyper focus on cybersecurity inside the buildings that some of the most advanced research and mission sensitive work is conducted in. From manufacturing to innovative medical and scientific research and weapons systems development. If the building and its systems are compromised its systems van be used to pivot to networks inside the facility to exfiltrate controlled unclassified information (CUI) or intellectual property (IP).

HTB2020 seeks to accomplish the following goals:

Number	Description
1	Provide realistic event for qualified United States Government (USG), US Department of Defense (DoD) and military academic or duly authorized teams to attempt offensive cyber and defensive cyber operations against real-life Information Technology, Control System and manufacturing target systems without concern of violating existing legal authority, state, federal or local laws or concern of property damage
2	Provide one or more scenarios to allow authorized parties to exploit building management, digital manufacturing automation or general control systems causing real world physical events which without intervention (of MISI personnel) would result in loss of physical asset or non-volatile electronic information, cause physical damage or destruction or in controlled situations result in physical harm or property destruction.
3	Modeling and Simulation of actual scenarios that affect existing US Defense Industrial Base (DIB) manufacturers and consultants.
4	Realistic evaluation of defensive cyber solutions designed to protect control systems and manufacturing technology.

1.2 Rules

We define the following rules for successful and lawful execution of HTB as described in the next table. Participants are expected to read and understand all these rules before an HTB event beings.

Number	Description
1	No HTB scenario will ever publicize details or source code used in any scenario outcome, finding or successful inject of any vendor (hardware or software) that was not already released to the public (e.g. CVE or vendor produced OVAL report). HTB does NOT disparage vendors or users, HTB is for protection.
2	HTB participants are expected to complete a rules of engagement (ROE) agreement prior to participation and send completed copy to MISI
3	MISI and all participants shall not force any HTB participant into a dangerous or unsafe condition at any time without full disclosure of risks involved. Any situation that includes a potentially unsafe outcome shall be clearly explained in advance and will include countermeasures designed for the safety of the participants sacrificing equipment before the safety of any participant.
4	No HTB scenario shall attack, disable, or target in any fashion any asset that is not under the direct control of MISI or the scenario participants. When available, an offensive team or team member shall complete a request for penetration testing or evaluation if they plan to target a cloud-connected asset.
5	An HTB scenario participant shall participate in official real-time alerting or communication channels (e.g. SMS, Chat, Email) during the entire execution window.
6	An HTB scenario participant shall immediately cease any action when notified by MISI or HTB exercise control (EXCON) personnel.
7	When warranted, an HTB scenario participant acknowledges any device, equipment or software they donate or utilize may be placed into a situation where it can be damaged or destroyed due to an environmental event (water, power surge, heat) as caused by an attacker.
8	Physical or electronic destruction of property within the confines of an HTB scenario ROE notwithstanding, HTB participants agree to abide by all Federal, State and Local regulations and laws that govern the physical location(s) where any scenario may take place.

Participants should take care to consult online HTB information sites to comply with COVID-19 rules to keep participants safe.

1.3 Real-Time Communication

We discuss real-time communication elements of HTB in this section. Not only does MISI run a website for disseminating information on HTB, we intend for an HTB event to be a live event. We are developing a mechanism to broadcast or stream the event live as it occurs with a recording option to review the events later but we also expect participants to either join our live chat or be available via some electronic means during the entire length of the event.

1.3.1 Website

An HTB participant should always check the HTB website if they have questions or to see if any new information is available. The HTB website address is:

https://hackthebuilding.tech

1.3.2 Streaming

This concept is under development. More information will be released as it becomes available.

1.3.3 Chat

We plan to utilize a collaborative chat solution for maintaining real-time communication for participants in any HTB event. MISI currently utilizes Discord for this service and we will issue invitation links to an HTB participant who wishes to join the chat server for an HTB event. A participant can always feel free to request an additional invitation to the chat server if necessary.

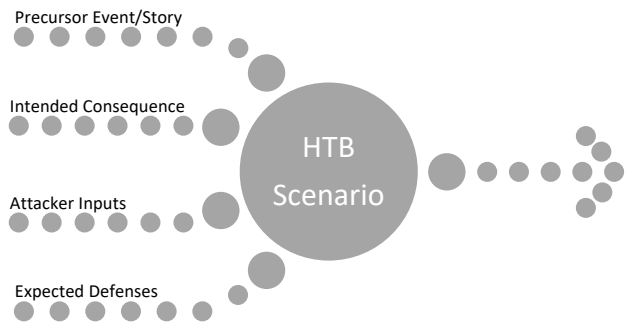
The Discord chat client can be downloaded from:

https://discord.com/download

1.4 What is an HTB Scenario

HTB is designed around specific scenarios that involve the same set of targets. Each HTB outing executes a single story. As HTB evolves, we will define and implement new stories to the HTB playbook to enable future events. Each story scenario is presented in a separate section in this playbook. The high-level stories we describe in this document serve as framing devices for HTB scenarios or events we will conduct. In HTB, one (1) or more teams will participate in a series of scenarios to remotely (or locally) penetrate as attackers or prevent penetration as defenders of the headquarters of a fictious company, organization, or person we have created. While an attacking participant's ultimate job is to cause loss of revenue, reputation and ultimately business for this company, they are expected to stay within the confines of the active scenario.

HTB scenarios are designed to fill an approximate length of two (2) to four (4) hours depending on complexity, expertise and other hints given. They are all designed to be executed from a known starting state and HTB networks are built with the intent of being reset when necessary. It is always intended that a scenario will be started announcing how long it will run for, so participants know it has finished.



Participants should understand that each HTB scenario may include any or all the following story components in the diagram shown on the left. We fully expect participants to read all the required documentation or evidence the scenario story may supply. A participant should also understand that a scenario may expect attackers or defenders to have a specific level of expertise to participate. We attempt to enumerate expected expertise for each scenario in the description we provide. The elements of an HTB scenario are described in the next table.

Element	Explanation
Precursor Event(s)	Each HTB scenario revolves around one or more precursor events. A precursor event is a real-world or simulated real-world action, event,

Element	Explanation
	message, or story that mirrors what a victim may experience, and it sets the stage for any events that follow. In a way, it one of the 'reasons for the scenario'. If the overall HTB story talks about a victim then the precursor events may include a victim employee accidentally exposing information or failing to patch a system which an attacker may be able to exploit and a defender has the responsibility of discovering and ensuring a course of action is executed. Unlike other events, we designed HTB to make vulnerabilities or access vectors more overt. We want participants to focus more on the exploitation of a real-world system and less on the steps that may be required to reach that final exploit
Intended Consequence(s)	An HTB scenario should clearly define the intended consequence or 'what happens if stuff hits the fan'. Many readers will understand the concept that an unpatched vulnerability could be exploited to give someone remote access to a factory but not as many people will understand that through this access, an attacker can modify the state of a control system directing a manufacturing process which could lead to the destruction of the physical system, personal injury to anyone in the vicinity or the undiscovered alteration of a product which will fail immediately on first use. The consequence is what the scenario hopes to achieve given the precursor event(s) defined previously.
Attacker Input(s)	Attacker input(s) are the tools, traffic, communication, or actions we expect an HTB scenario attacker to provide. A successful attacker should bring a functional platform (hardware, software, documentation, and skills) to a scenario and use precursor events to gain access or send traffic at a scenario victim (server or human). If they successfully leverage the precursor events given their skills, they should have an opportunity to exploit the target system and achieve the intended consequence. It may be theft of data, software destruction or one of the 4 D's (discussed later).
Expected Defense(s)	An HTB scenario makes every effort to be as realistic as possible. As such, defenses are common in the real world. First human defenders should be given as many opportunities as possible to train and second advanced defensive platforms need opportunities to study how attackers may think, act, and behave. Attackers should always expect one or more defense countermeasures to be active even if the HTB scenario is explicitly designed for attackers. If an attacker input requires a piece of malware then an expected defense should be an endpoint security product like anti-virus. If an attacker input requires a phishing email than an expected defense would be email security products or anti-spam technologies. Attacker should understand that some defenses will be disabled to allow the scenario to focus on intended consequence. For example, AV may be turned off temporarily.

1.4.1 Participant Roles

In HTB, there are defensive and offensive participants or roles required to play out the scenarios we design. Like a capture the flag or penetration test modeling scenario, HTB uses attackers and defenders and actors as we describe in the next table. In addition, a HTB scenario may require one or more actors to facilitate access vectors (e.g. opening emails or clicking on links).

Team	Description
Attacker (RED)	Attackers are teams of 1 or more people with skills in penetration testing, vulnerability testing, network reconnaissance or even offensive cyber operations. We accept that RED teams will bring varying skill levels to an HTB event, so we define an expected skill level of a RED team for a single scenario. If you do not possess that skill level, you will have trouble during execution. Attackers should be prepared to do all the following: - Web Searching - Social Media Scanning - Website browsing or crawling - 'Throwing Exploits' against websites or servers - Sending phishing emails - Network recon identifying and classifying active hosts - Discovering 'unknown' additional exploit targets (e.g. URLs or in-active hosts)
Defender (BLUE)	A defender is a team of 1 or more people who possess skills in installing and operating network defensive tools either commercial or open source. A BLUE team should be able to operate a suite of tools in a uniform or centralized fashion and have at least 1 person who is able to interpret data based on experience and determine if an attack has taken place and hopefully be able to interpret (or ask for additional data) data to classify the attack. In HTB, a BLUE team is always assumed to have administrative level access to the network(s) they are protecting.
Actor	An actor may be required to provide a human target for a given scenario. This actor will be given a specific set of guidelines they must follow during the scenario which will deliberately override normal human judgement. Without this artificial plot device some scenarios (e.g. those involving phishing) may be impossible to execute.

MISI may conduct RED or BLUE events during a story as demonstrations of specific products or technologies where we must keep tight control over outcomes.

1.4.2 Consequence

As we introduced previously in section 1.3, each HTB scenario is assumed to have one or more intended consequence or outcome. Unless otherwise noted, we expect that more than one (1) team can achieve the intended consequence affecting the scenario victim. A scenario script will clearly define the intended primary consequence and we expect that all participants focus on that intended outcome only and not attempt any other actions that are not directly required to achieve success.

1.4.3 Required Expertise

Each HTB scenario defines expected expertise required to achieve success based on the levels we define later in this playbook in section 0. These expertise levels are not rigid requirements as it is impossible to accurately classify two different people's skill levels on such a wide array of requirements for different scenarios but participants should be forewarned if they cannot easily demonstrate understanding of the target areas or offensive techniques expected they won't have any success in that particular scenario. In other words, 'participate at your own risk'.

1.4.4 Access Vector(s)

An HTB scenario may define an allowed access vector. Unless explicitly noted, we never will expect a RED or BLUE team member to start with nothing for a scenario otherwise it would be impossible to execute in the desired time constraints. If we take the time to define an access vector for a scenario, we expect participants to utilize that vector.

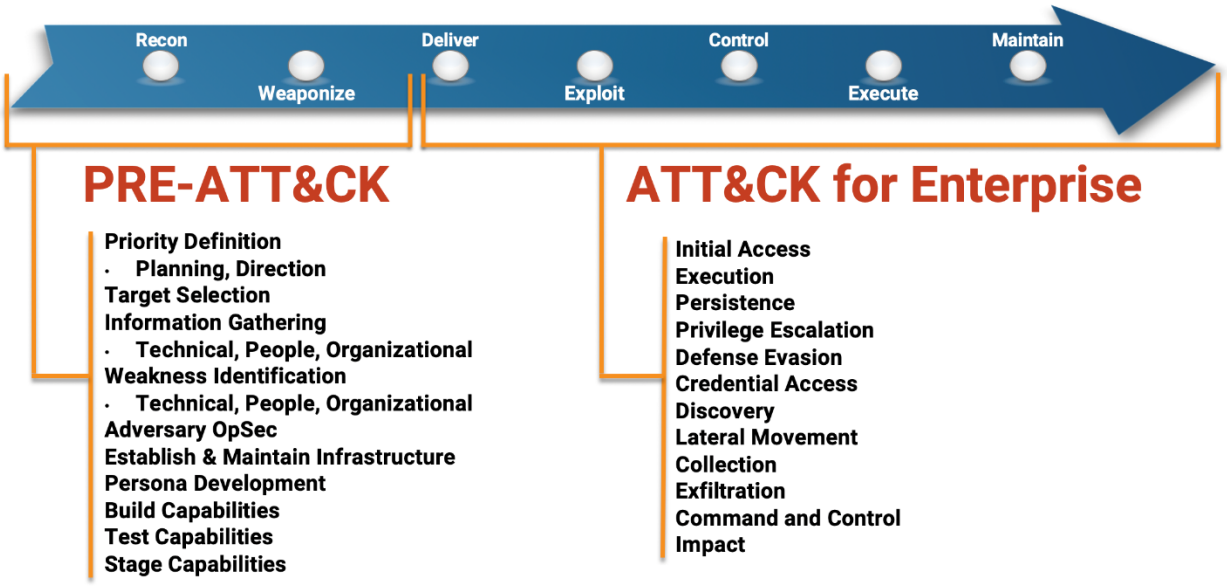
1.4.5 Limitations

A scenario may place limitations on what each side can do. Some scenarios are designed to study or measure an attacker ability not just to gain remote access despite some protections being active but more importantly to incorporate information on the fly (e.g. how to navigate a system they have never seen) while trying to achieve the desired consequence. It is important for defenders to understand this limitation. If they attempt active defensive techniques, they may prevent the scenario execution. If a scenario is designated 'weapons free', both sides should feel free to execute mission to the best of their ability.

1.5 Attack Scenario Modeling

The scenarios defined in this playbook combine attack modeling concepts from a variety of sources. Each scenario provides a TTP graph which builds upon the MITRE ATT&CK framework but includes elements of the United States ODNI cyber threat model. We provide a reference copy of each attack model here in this section. The combination of these models is necessary for HTB because while we want to build each phase of a scenario in repeatable blocks (e.g. the MITRE approach) we keep the ultimate desired consequence in mind to provide real-world understanding of the consequence (ODNI approach) of a cyber-attack.

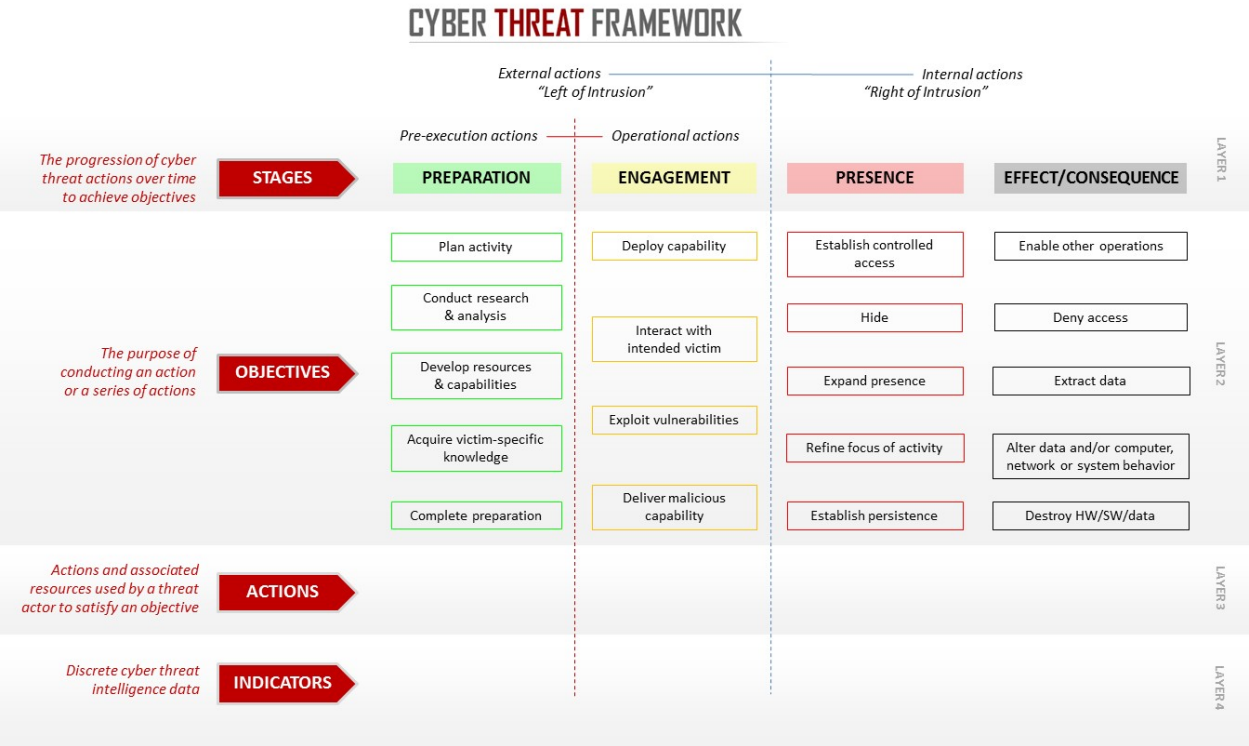
1.5.1 MITRE ATT&CK



MITRE ATT&CK Image Source:

https://attack.mitre.org/theme/images/enterprise-pre-lifecycle.png

1.5.3 ODNI Cyber Threat Framework



ODNI Cyber Threat Framework Image Source:

https://www.dni.gov/index.php/cyber-threat-framework

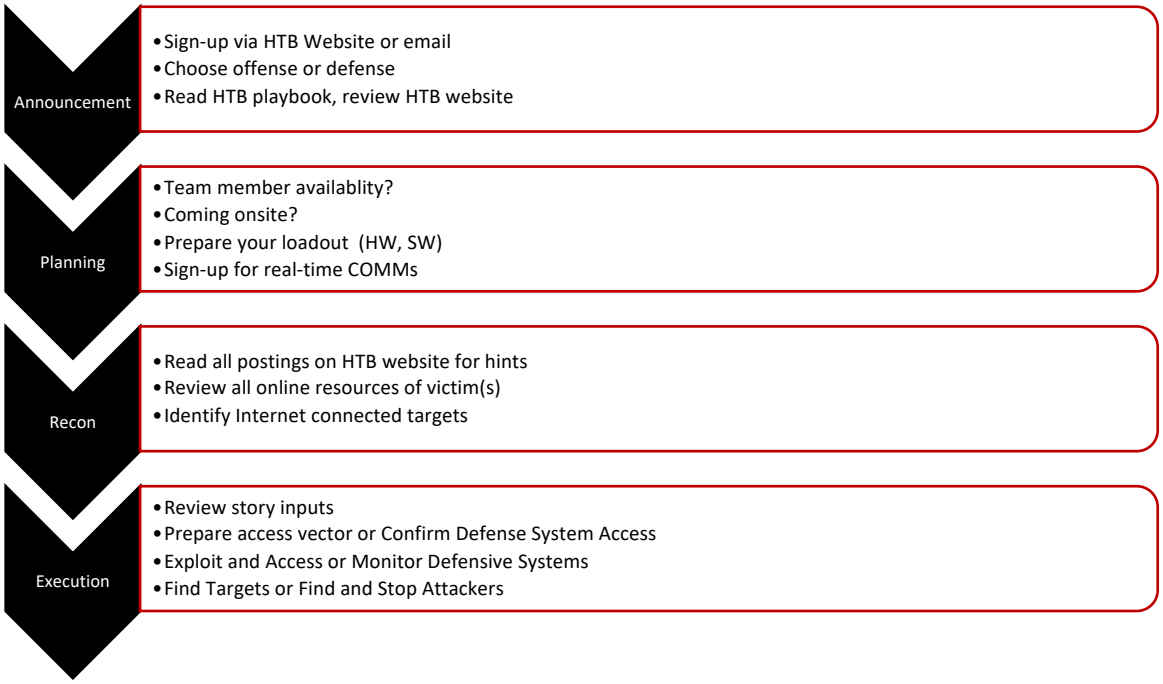
2 PARTICIPANTS

We describe HTB scenario participants in this section. Readers who plan to participate in an HTB event should read this section carefully to understand what is expected of them for the HTB event. We introduce HTB roles earlier in section 1.4.1. In short, you can be either an attacker or defender in an HTB event.

Some HTB events may require actor participants who drive victim systems and ensure access vectors are successful, but we consider this a limited role.

2.1 How Do We Participate?

To start we discuss how someone can participate in an HTB event. The basic flow of events for an HTB event is defined in the next image. All participants are strongly encouraged to read and follow this process.



2.2 How Will We Connect?

A common question we hear from participants for an HTB event is 'how will I connect'? This will be different depending on each event and if you are an attacker or defender. We present information on how attackers and defenders can connect in each subsequent section.

2.3 Rules of Engagement

An HTB participant may be required to sign a Rules of Engagement (ROE) document. If you are not familiar this is a contract between MISI and you ensuring you promise to play be a set of standards or rules. While it is true that an attacker will pull no punches in the real world, ultimately we want to make certain that any participant that discovers a flaw in a system used in an HTB scenario or a new technique for exploitation or operations discloses this information in a responsible manner to not harm the vendor of the software or hardware and most importantly not harm any consumer who utilizes said system. Recent news suggests that an attacker favors publicly available information on vulnerabilities due to the simplicity of exploitation. It is only in effect for the duration of the HTB event and most participants should already be familiar with the concept.

Equally as important, as an HTB defender you may encounter a technique feature or flaw in a product that was donated to the HTB event that the original vendor considers private or proprietary. Completion of the ROE ensures that you agree to treat this information as sensitive and that you will not disclose said information publicly.

If you have a problem with the ROE you can let us know but if we choose to employ the ROE for an HTB event, it is non-negotiable.

2.4 Attackers

We provide background information on offensive participants or attackers for HTB in this section. While any organization can provide an execution of a cyber threat for real-world consumption, without some element of unpredictability, that execution is nothing more than a demonstration. HTB may be meant for normal people to understand the risks posed by cyber threats against buildings and their occupants, we need attackers to make it realistic. HTB attackers can be either remote or local for a particular HTB event. Each scenario should present options for what types of attackers can participate.

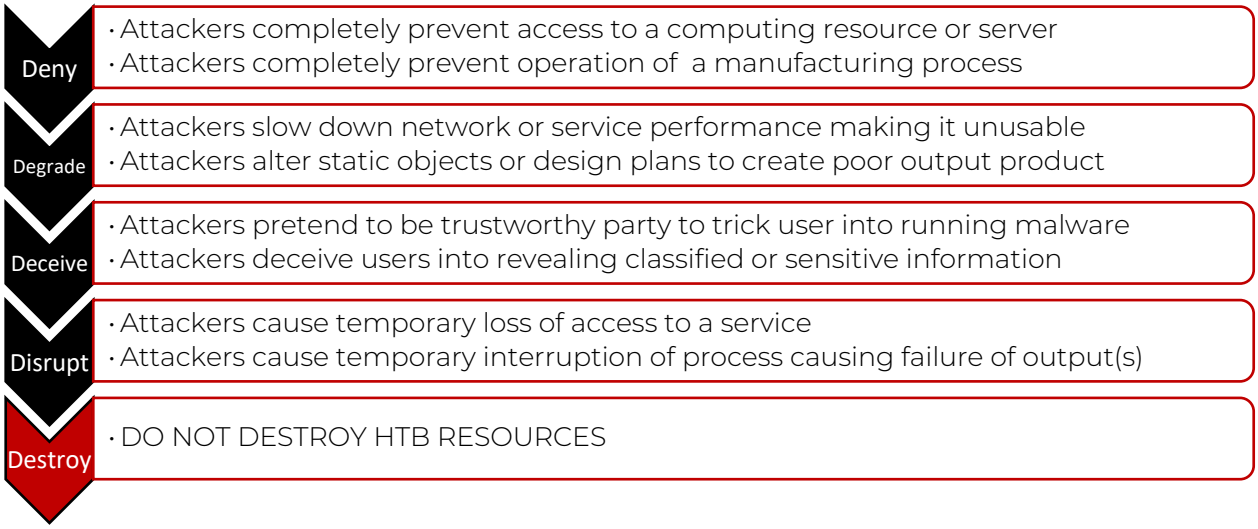
So, you have decided to participant in an HTB event. First, we expect you to be honest of your skill level and your limitations. We define the skill levels we use for HTB scenarios later in this document in section 4, you are strongly advised to understand where your fit on this scale. In addition, while you may wish to work alone, we urge you to work as a team especially since it is a primary goal of HTB to expose attackers to systems they may have never seen previously.

It is important to understand, HTB is not capture the flag (CTF). HTB executes several scenarios that include some degree of starting information, reconnaissance, initial access (or leveraging prior access), target selection, exploitation, and consequence. We consider HTB to be a repeated exercise or practice for attackers in the 4 D's (of the normal 5 D's) of computer network attack. The interested reader can learn more about this concept in the following MITRE document:

Characterizing Effects on the Cyber Adversary

https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf

To put this concept in terms of our own picture, during an HTB scenario as an attacker you should be trying to do one of the following:



As fun as it may sound, we do not consider destruction a part of HTB. If you have some experience in penetration testing or offensive cyber operations and wish to be a part of an HTB event, keep reading for more details on what happens. It is also important to repeat clearly for the record, we do not consider HTB scenarios a capture the flag style event. We include elements of CTF competitions, but we want to go further.

2.4.1 How do I Connect?

An attacker should plan on being able to connect both remotely over the Internet and locally (if they choose to attend an event in-person). This means they need to prepare their own hardware and software for the event. We offer the following suggestions on how you may want to connect as an attacker:

- Start with a powerful enough machine to run multiple virtual machines
- Prepare a virtual machine that houses your operational tools
- Make sure you have reliable Internet access, and you are advised NOT to use a public access point
- You may want to secure cloud VPC resources to use for operational events

2.4.2 Assumptions

We define the following assumptions we have made for any HTB attacker participant.

- Attackers participate in the HTB event or scenario(s) at their own expense
- Attackers understand that one or more scenarios during an event may require physical access which can preclude them from participation. We may provide alternate access vectors for remote participants during a physical event, but this will not happen every time. Each scenario will note if physical access is required in advance.
- Attackers provide their own equipment both software and hardware
- Attackers provide contact information for at least 1 team member and will respond to contact requests within 15 minutes or risk losing access during a scenario
- Attackers will cease any action (within 15 minutes) as directed by MISI personnel if it poses physical or technological risk to an HTB actor or participant.
- Attackers understand they are expected to read scenario information prior to the start of an HTB event. This may be distributed via website, email, or social media (or a

combination of sources). If we have published details somewhere you are expected to read them.

- Attackers understand they are may be expected to perform Internet or open source reconnaissance during a scenario. Without this action, required access details will not be available and they will be unable to participate in subsequent scenario stages.
- Attackers understand that scenario descriptions and starting information will be all the information they get. A scenario may describe a control system vendor and platform used to manage a manufacturing process, but it may not reveal the model number, protocol(s) or human interface. They are expected to locate these items during reconnaissance.
- Attackers understand that after starting a new scenario, they may not possess the skills required to move from recon into access. If they find they are unable they must throw in the towel and attempt the next scenario they feel they are able.
- Attackers understand that despite being given hints or starting information during a scenario, they may still not be successful during a scenario. If they are preparing open source malware or exploits, their targets may utilize built-in protections that they should understand in advance and have some techniques for evasion or countermeasures for bypass.

2.4.3 Onsite versus Remote

In HTB we design both remote and local scenarios for execution which break down like the following examples:

In remote scenarios attackers should be ready to	In local scenarios attackers should be ready to
• Conduct online recon • Exploit vulnerabilities in servers • Send phishing emails • Find exposed credentials • Brute-force poor passwords	• Exploit weak WIFI • Connect to unguarded physical interfaces • Distribute malicious USBs • Deploy covert 'leave-behind' • Find the disgruntled employee

2.4.4 What Tools to Bring

We provide a limited set of tools we suggest you bring to an HTB event:

- Laptop with the following features
  - ability to run 2 virtual machines
  - WIFI cards capable of monitor mode
  - Internet Access for searching
- Any offensive distribution of Linux (your choice) that includes:
  - Nmap
  - Metasploit Framework
  - Wireshark/tcpdump
  - Scapy
  - Hydra

In addition, you are advised to have the following resources available:

- Ability to launch VPC resources
- 1 or more DNS domains (under your control)

- Ability to send Email to victim(s) (domains you control)

2.5 Defenders

A defender has the tougher job, we admit. In the wild, the attacker only must win once whereas the defender is constantly under fire. In HTB, defenders will be given access to workstations that have administrative access to all elements of the story victim and their networks. An HTB story will utilize a unique network (per story) but this network is designed to function exactly as a normal entity in the real world. This means that it will have explicit security countermeasures already setup before the defender may arrive. The HTB story victim will always have a network diagram, but this will not be shared until the last minute on purpose. As a defender, you will be granted administrator access to the network and all resources, but you must ensure you do not cause the failure of a scenario.

It is important for a potential HTB defender to understand that some scenarios are designed to focus exclusively on an attacker activity. As such, the defender should consider themselves and their team a part of the background. They will be given access to the HTB network as soon as the event begins but they will not be expected to start spotting attacks until they are explicitly notified.

HTB defenders may have access to commercial products donated to an HTB event for the purposes of computer network defensive or defensive cyber operations. If a donated third-party defensive tool is available for an HTB event, attackers will not have any advance knowledge of this tool. We will ask the third-party organization to have some expertise available to ensure defenders can operate and utilize the tool effectively.

The principal jobs of the defender in HTB are described in the following table.

Task	Description
Detect attacks in progress	The primary job of a defensive team should be to detect attacks in progress or after they have occurred. This amounts to fusing information from all available sources and using experience to either directly interpret tool output or make educated guess(es) based on outputs.
Monitor and search log aggregation	The primary tool for HTB defenders is log aggregation. Log information will flow into a centralized portal from multiple hosts and devices within the HTB network. Defenders may request log aggregation changes which will normally be approved so long as they do not impair scenario execution. At the start of scenario defenders should assume that the log aggregation system does not have any customization installed. Defenders should be prepared to request this installation or configuration change(s).
Monitor host availability	One often overlooked job of a defender is to monitor host availability. Defenders should be prepared to monitor the uptime or availability of a host so they can be alerted when a host has gone down or is behaving erratically. Assume an attacker will get access to a host.
Update firewall(s) to block or allow	During the 'weapons free' scenario a defender is able to update firewall or packet filtering rules of a device to stop a future attack or interrupt an attacker in progress. The only limitation in this case is the defender cannot prevent normal mission functions.

Task	Description
Start/Stop hosts	Similar to updating firewall rules, a defender is able to remotely reboot a host they believe is subject to an attack so long as they do not prohibit normal mission operation.
Find hosts and vulnerabilities proactively	An attacker should attempt to map the network they are defending using active and passive techniques as frequently as possible. They should assume there are elements of the victim network that are not shown on the map. This is always a method to discover potential attack targets as well as the network map usually does not detail the patch level of a remote system.
Execute active defense tactics	Active defense or hunt techniques are permitted so long as they do not prohibit normal operation. This can include the installation of an additional tool on a host or the remote scanning of a host using IoC files to look for common attacker techniques.

2.5.1 How do I Connect?

We describe how we anticipate a defender will connect into an HTB event in this section. In HTB, a defender will be given a virtual private network connection into the HTB network. Using this connection, we will reserve at least one initial access point virtual machine (VM) that they can then use to connect to other remote resources within the HTB network. We will grant additional VM access to other team members if resources allow but a defender should be prepared to utilize a collaborative session such as TeamViewer, VNC or remote desktop to allow multiple members to monitor the single access point.

2.5.2 Assumptions

We describe assumptions we enact for defenders in HTB in this section. It is important for defenders to read and understand all these assumptions:

- A defender will utilize the virtualized platform MISI provides as their initial access point into the HTB event for defense.
- A defender understands they may have to share the initial access point amongst multiple team members as resources may be limited.
- A defender may connect their own platform into the HTB event network if they clear this with MISI in advance.
- A defender may not connect a router into the HTB network without clearing this in advance. If they
- A defender can have access to administrator or root passwords for any scenario asset
- A defender can install software into resources within the HTB scenario (unless asset is a loaner of a third-party HTB participant) for defensive purposes.

2.5.3 What Tools to Bring

An HTB defensive participant should not assume they must bring any tools to an HTB event unless the scenario explicitly requires them. They may however request the installation of a tool in advance but if the tool requires purchase, we may not be able to support due to lack of funds. In general, HTB events will provide the following defensive technologies for an event:

- ELK + FileBeats
- PacketBeat
- Zeek or Snort Intrusion Detection

- Full Packet Capture (for portions of the event network)
- Sysmon (for Windows advanced logging)
- OpenVAS
- OpenSCAP (with SSG)
- Kismet

2.5.3.1 Initial Access Point

We provide a brief description of the HTB defensive initial access point in this section. This platform will be a virtual machine running one of the following possible configurations:

- CentOS 8
    - Desktop
    - SSH Client
    - Wireshark
    - Visual Studio Code
    - GitHub Atom
- Ubuntu 20.04
    - Desktop
    - SSH Client
    - Wireshark
    - Visual Studio Code
    - GitHub Atom

3 STORY: BCR INDUSTRIES

In this story, our victim is named BCR Industries. BCR Industries (BCR) is a fictitious digital manufacturing and engineering company currently headquartered in Annapolis, Maryland and whose chief customer is the United States Government. BCR produces a variety of physical components and software for their customers. In this story, BCR engages in the following types of work:

- Design hardware and software
- 3D Print and modifies enclosures & components
- Design/print/solder circuits
- Test products indoors & outdoors
- Communicate with customers (email, chat, video, voice)
- Writes and stores reports and documentation

There are two (2) primary risks to BCR in this story:

- BCR is housed in a building with outdated building management systems (BMS) that they have not yet identified. These BMS are connected to the Internet and pose 100 percent real physical and virtual dangers to BCR.
- BCR networks and staff do not utilize sufficient operation security and boundary protections. The BCR networks are vulnerable to remote penetration which places all intellectual property at risk from theft or unknown supply chain risk.

This story is designed to take place in an online setting and at the physical location described in section 0.

3.1 Backstory

The principal backstory for this BCR is described as follows:

BCR is the small business set-aside winner of a new (fictitious) contract called ACCORN or the 'Advanced Compact Cyber Operations and Readiness Network'. This contract is a multi-year contract to build mobile devices for cyber defense to combat growing threat from foreign adversaries. During this contract, BCR will design, procure build, test and execute operations and maintenance on multiple devices designed to detect and stop attacks against Internet of

Things (IoT), control systems for digital manufacturing and edge computing across a wide geographic area 24x7.

- Believed to have 36 employees
- HQ in Annapolis, MD (described in section 0)
- Offsite Facility (@ DreamPort)

BCR has become the target of well-funded and motivated adversaries whose principal goals are the following:

- Obtain remote access to BCR networks and offices to conduct physical disruption events on-demand designed to slow or stop the manufacture and test of systems and components built for the ACCORN contract.
- Obtain remote access to alter plans, source code or test results of components built for the ACCORN contract without victim knowledge
- Illegally obtain and exfiltrate any and all design plans of components built for the ACCORN contract without victim knowledge

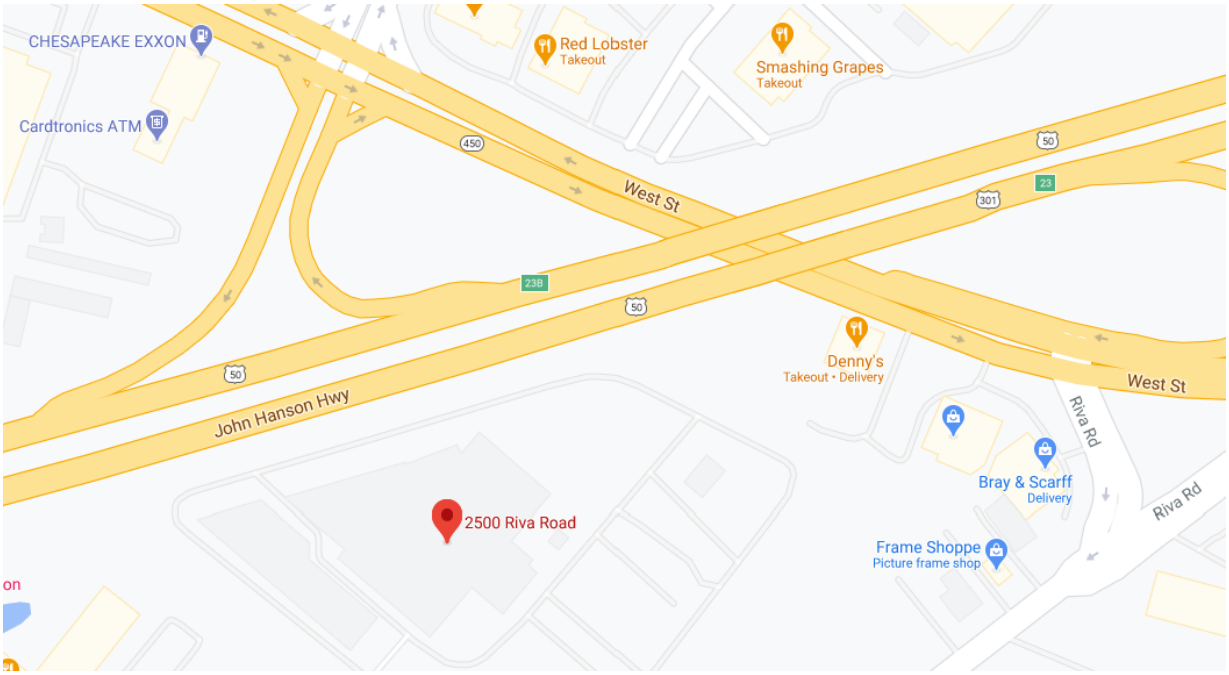
3.1.1 BCR Headquarters

The current physical location of BCR headquarters (HQ) is:

2500 Riva Rd
Annapolis, MD 21041

No HTB participant should ever send or ship any mail or package to a scenario victim.

This location is shown in the Google Maps snapshot shown in the next image.



3.1.2 Physical Facts

We define the following facts for this scenario that facilitates our scenarios:

- BCR HQ includes an onsite coffee house that provide onsite physical stations which facilitate remote access
- The BMS is not connected to actual chiller systems onsite. Success criteria is defined as electronic signals sent to physical controls to adjust temperature or toggle fans

3.1.3 Online Points of Presence

Participants in any event that target BCR are expected to perform standard network and Internet recon tactics to discover specific technologies platforms or services that BCR uses as this constitutes the online attack surface for this target. We provide information on common Internet services used by BCR in this section

Platform	Address
Website	http://www.bcrindustries.com
Email	info@bcrindustries.com

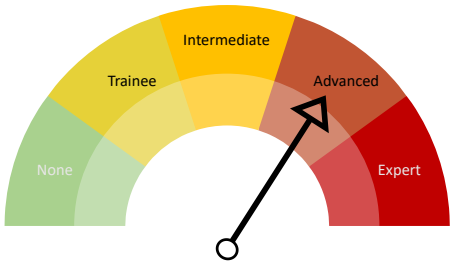
Participants should know that the attack surface for an HTB victim is always changing. They should be prepared to constantly perform reconnaissance and target discovery.

3.1.4 Internal Network Overview

Having grown from a small business to where it is today, BCR acquired many systems over the years to help support its business. From yearly purchases of desktops, varying versions of Microsoft Windows are to be expected consisting of a centralized login infrastructure running on Active Directory (AD) with file shares, Office 365, DNS, and internal and external services. Also, on their manufacturing floor, expect to see industry standard programmable logic controllers (PLC), Human-Machine Interface (HMI), and varying control and monitoring systems aiding in the manufacturing of goods and the safety of the work environment.

3.2 SCENARIO – IT'S GETTING HOT IN HERE

Scenario	It's Getting Hot in Here
Consequence	Loss of System Access
Access Method	Valid Account
CWE	CWE-798
Skill Level	Advanced



In this scenario, we set the stage for remote exploitation of BCR building management systems (BMS) and the unplanned alteration of building environmental controls. This scenario is labeled as advanced difficulty due to combination of the complexity of finding the BMS system interface, researching the weakness and then navigating the system to achieve the designed effect. An improperly secured BMS that offers remote control over temperature or HVAC systems can be used to make rooms hot enough to trip temperature safety monitoring systems or even shutoff computers or servers. We want attackers to conduct online reconnaissance and identify the Internet accessible interfaces to the building management systems that BCR utilizes. If they can gain remote access to these systems without being given the passwords, they should be able to learn about the systems and deliver consequences such as:

- Disabling HVAC fans
- Raising temperature in key areas of BCR headquarters.

Exploitation of this weakness should allow an attacker to be able to raise the temperature gradually or quickly in BCR spaces to a level that makes manufacturing error prone or causes automatic shutoff of IT systems due to the overheating.

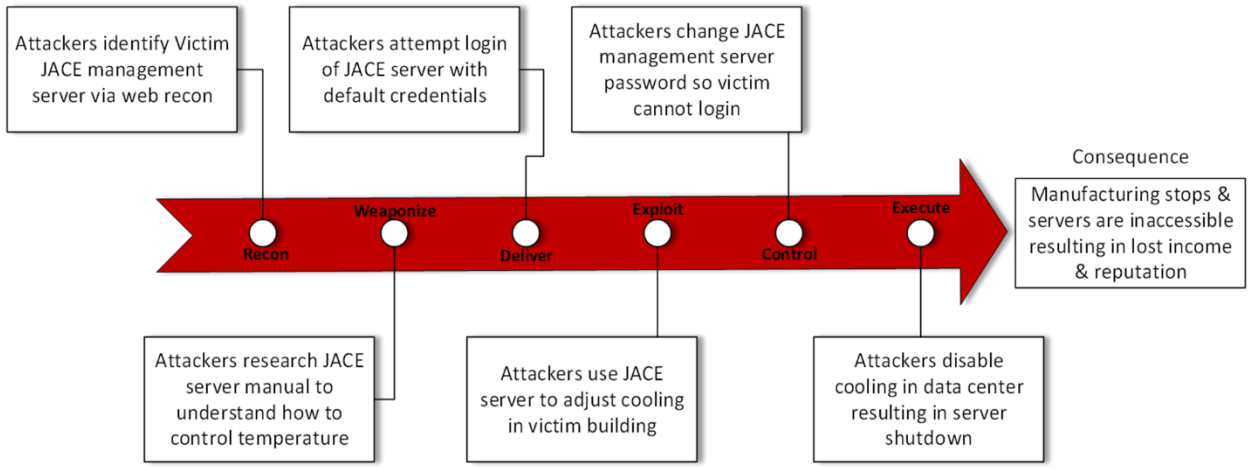
3.2.1 Attacker Actions

In this scenario, attackers must be able to identify target BMS as they will be connected to the Internet but DNS or IP address information for these systems are not immediately obvious. If an attacker can utilize standard reconnaissance techniques, they should successfully locate the BCR BMS servers. This will be a multiple step recon effort.

Once located, they should leverage CWE-798 to attempt to access these systems. This scenario does not give information on what specific BMS software is used or how to manipulate this software to affect HVAC controls. If they can access the BMS they should attempt to adjust temperature or fan controls. If they do so it would achieve the desired effect of changing temperature in an environment where servers would shut down or sensitive electronics under fabrication may fail quality control or be destroyed.

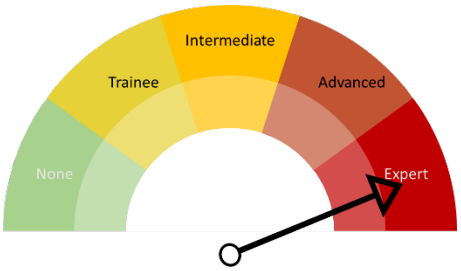
3.2.2 TTP Graph

The following image shows the tactics, techniques, or procedures (TTP) we expect attackers to use in this scenario.



3.3SCENARIO – WHO TOUCHED THE THERMOSTAT?

Scenario	Who Touched the Thermostat?
Consequence	Endangering Human Life
Access Method	Remote/Local
CWE	CWE-787 CWE-119 CWE-416
Skill Level	Expert



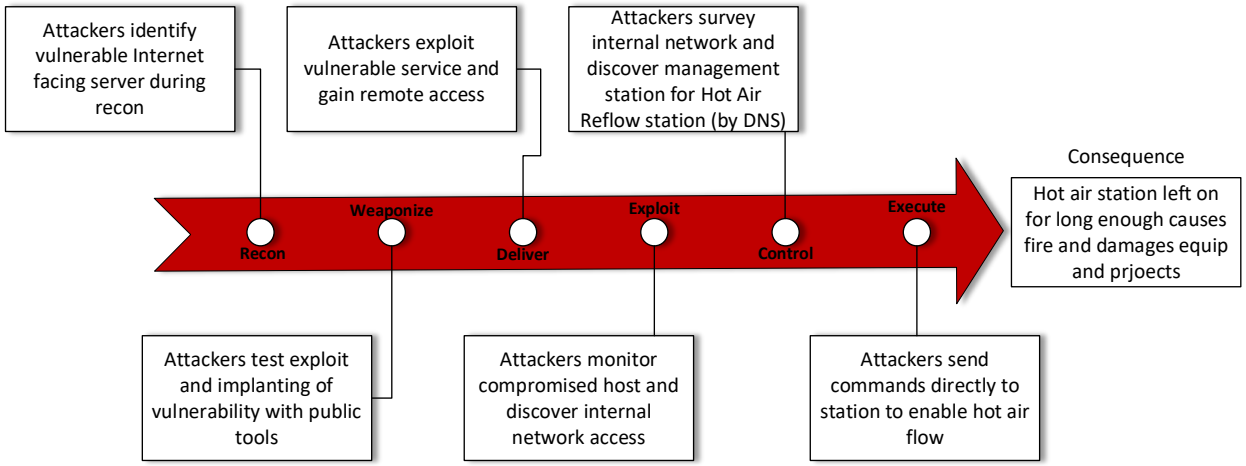
In this scenario, we try to determine if an attacker can gain remote access to the BCR network and then use standard recon techniques to identify a remote-controlled hot air reflow station. This station can be controlled over the network for operation of a hot-air stream used for de-soldering components from a circuit board. If it can be activated remotely, the reflow station could be used cause extreme damage or bodily harm to an on-site operator. We rate this scenario as expert level because an operator needs to understand how to first find the station from across the network and second how to connect to the station and activate the device.

3.3.1 Attacker Actions

In this scenario, an attacker should either utilize a phishing email, stolen VPN credential or remote exploit to gain access to the network. An attacker could also be local and attempt to utilize a WIFI based attack to derive the network key. If they can gain access to the network the need to be able to utilize standard techniques and tools to find the reflow station network connection. If they can find the address of the reflow station controller, they should attempt to remotely activate the reflow station. If they can activate the station they have achieved success.

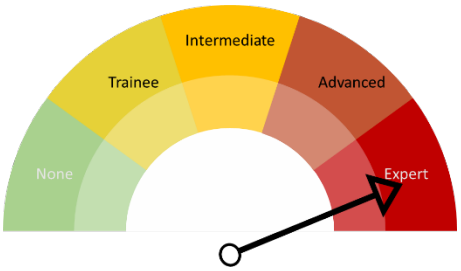
3.3.2 TTP Graph

The following image shows the tactics, techniques, or procedures (TTP) we expect attackers to use in this scenario.


Attackers identify vulnerable Internet facing server during recon
Attackers exploit vulnerable service and gain remote access
Attackers survey internal network and discover management station for Hot Air Reflow station (by DNS)
Consequence
Hot air station left on for long enough causes fire and damages equip and prjoects
Recon
Weaponize
Deliver
Exploit
Control
Execute
Attackers test exploit and implanting of vulnerability with public tools
Attackers monitor compromised host and discover internal network access
Attackers send commands directly to station to enable hot air flow

3.4 SCENARIO – LET'S EVACUATE THE BUILDING

Scenario	Let's Evacuate the Building
Consequence	Personnel evacuating the building, suppression of fire alarms
Access Method	Loss of System Access / Network Compromise
CWE	CWE-498 CWE-798
Skill Level	Expert



In this scenario, we set the stage for remote exploitation for the fire alarm system. This scenario is labeled as expert difficulty due to combination of the complexity of finding multiple system interfaces, researching the weakness, and then navigating the system to achieve the designed effect. An improperly secured fire alarm system can be used to trigger alarms to evacuate personnel or disable fire monitoring and interfere with fire agent release mechanisms. We want attackers to conduct online reconnaissance and identify internal Ethernet and PTSN (dial up modem) interfaces to the fire alarm system computers and primary control panel. If they can gain remote access to these components without being given the passwords, they should be able to learn about the systems and deliver consequences such as:

- Sounding alarms
- Disabling alarms
- Disabling notification to fire department (external monitoring)

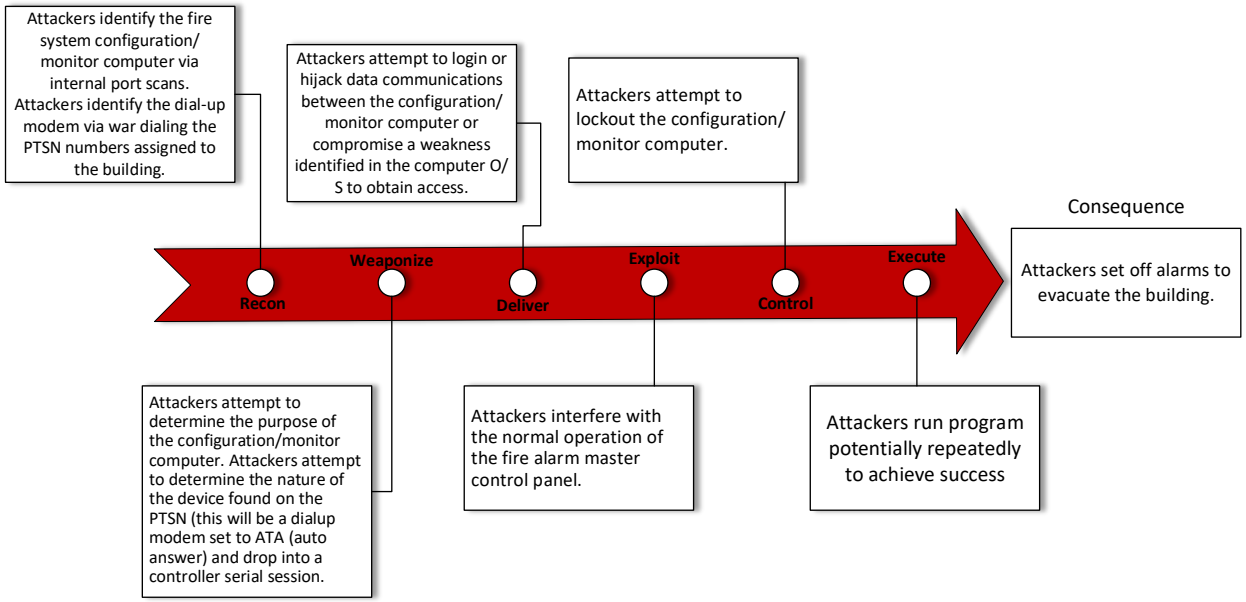
3.4.1 Attacker Actions

In this scenario, attackers must be able to identify target fire alarm control components. There will be a PC connected to the network that has file alarm configuration and monitoring software as well as a serial (dial up modem) connection directly to the master control panel available for exploitation. This will be a multiple step recon effort and required knowledge of industrial grade file alarm systems.

Once located, they should leverage CWE-489 or CWE-798 to attempt to access these systems. This scenario does not give information on what specific file alarm systems are used; however, it is one commonly found in large buildings. If they can access the file alarm system, they should attempt to disable fire alarm monitoring or manually activate alarms in a monitored zone within the building. If they do so it would achieve the desired effect of taking control of fire alarm system, that if compromised, and a fire were to be started (arson or accidental), the potential for servers or catastrophic equipment damage would result. Furthermore, this could result in a major life safety event.

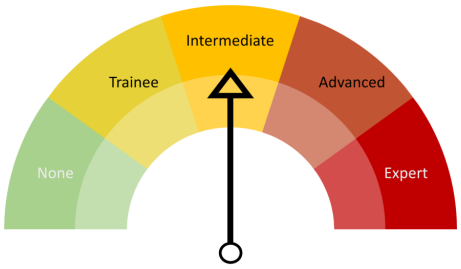
3.4.2 TTP Graph

The following image shows the tactics, techniques, or procedures (TTP) we expect attackers to use in this scenario.



3.5 SCENARIO – LET'S GAIN PHYSICAL #1

Scenario	Let's Gain Physical #1
Consequence	Obtaining unauthorized physical access to the building
Access Method	Physical Access Compromise
CWE	
Skill Level	Intermediate



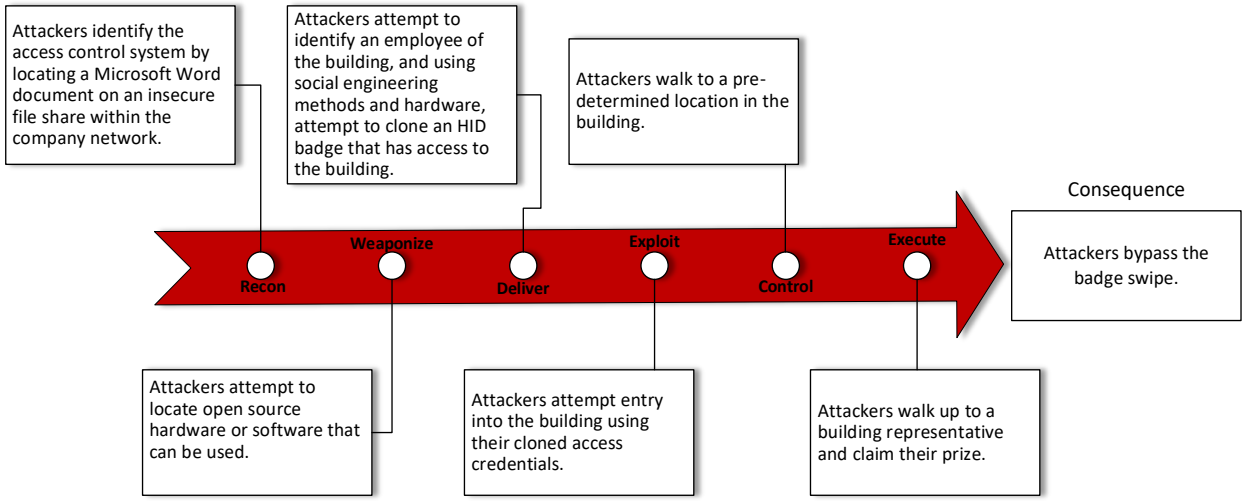
In this scenario, we set the stage for on-site exploitation of an HID-based access control system. This scenario is rated intermediate given the overall complexity, however, widely available open-source software and hardware available that can defeat an HID access control system. In this scenario, attackers can search existing building information derived from a Microsoft Word document that is located on an insecure file share on a server. This documentation will contain information about the access control panels and types of access control cards used. Once this information has been obtained, an attacker by multiple means, can either attempt to generate their own HID access badge, or clone an existing access control badge from an individual exterior to the building.

3.5.1 Attacker Actions

This scenario requires social engineering and knowledge of hardware/software components and is labeled intermediate difficulty. An attacker has to identify what kinds of cards are used by the access control system, determine the method to clone an access card, identify an employee who has a card, duplicate the card, and finally walk in the front door of the building. The intent of this scenario is to highlight the weaknesses of legacy access control systems which are still widely deployed.

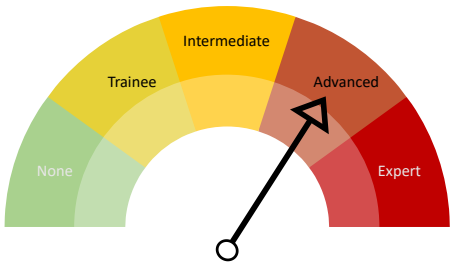
3.5.2 TTP Graph

The following image shows the tactics, techniques, or procedures (TTP) we expect attackers to use in this scenario.



3.6 SCENARIO – LET'S GAIN PHYSICAL #2

Scenario	Let's Gain Physical Access #2
Consequence	Obtaining unauthorized physical access to the building using a blended logical and physical attack vector
Access Method	Physical Access Compromise
CWE	
Skill Level	Advanced



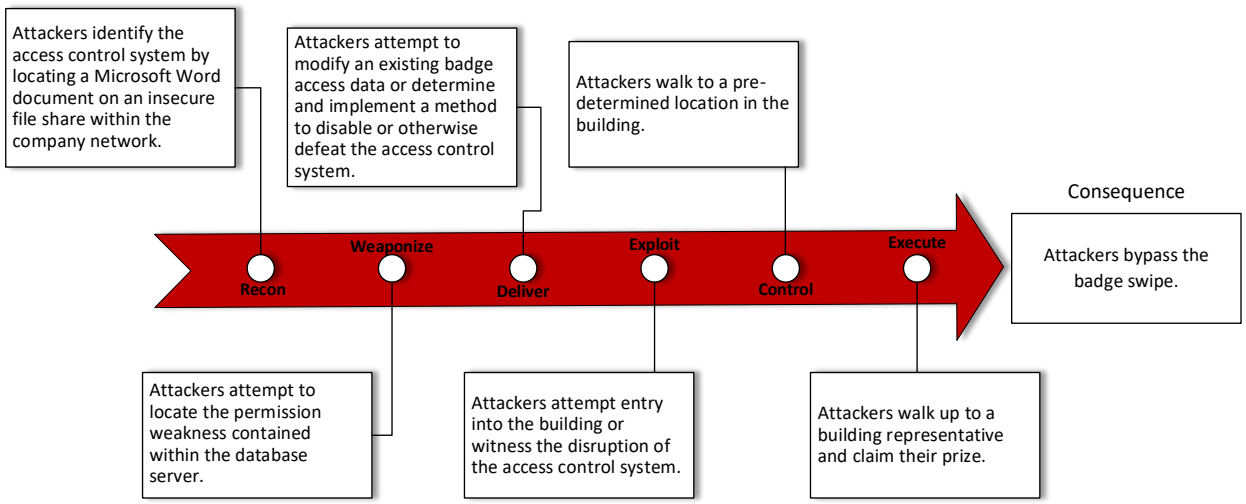
In this scenario, we set the stage for on-site exploitation of an HID based access control system. This scenario is rated advanced given the overall complexity, but widely available open-source software and hardware available that can defeat an HID access control system. In this scenario, attackers can search existing building information derived from Microsoft Word document located on an insecure file share on a server. This documentation will contain information about the design of the access control system. Once this information has been obtained, an attacker can enumerate the access control workstation and database server. The attacker will then find a way to access the database used to maintain card information and exploit.

3.6.1 Attacker Actions

This scenario is based on exploiting a weakness in the database itself (logical attack), and obtaining physical access based on the database change, or a disruption in the access control system itself (physical attack). An attacker must identify what data is accessible in the database and manipulate that data to obtain additional access control of an existing badge or cause a denial of service (disable the access control system). Based on the attack being blended using logical and physical attack vectors, the skill level for this scenario is advanced.

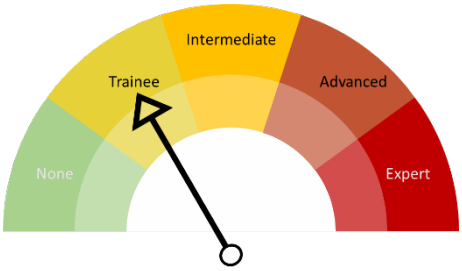
3.6.2 TTP Graph

The following image shows the tactics, techniques, or procedures (TTP) we expect attackers to use in this scenario.



3.7 SCENARIO – STEALING THE FAMILY JEWELS

Scenario	Stealing the Family Jewels
Consequence	Exfiltration/Theft of CUI
Access Method	Phishing
CWE	CWE-451
Skill Level	Trainee



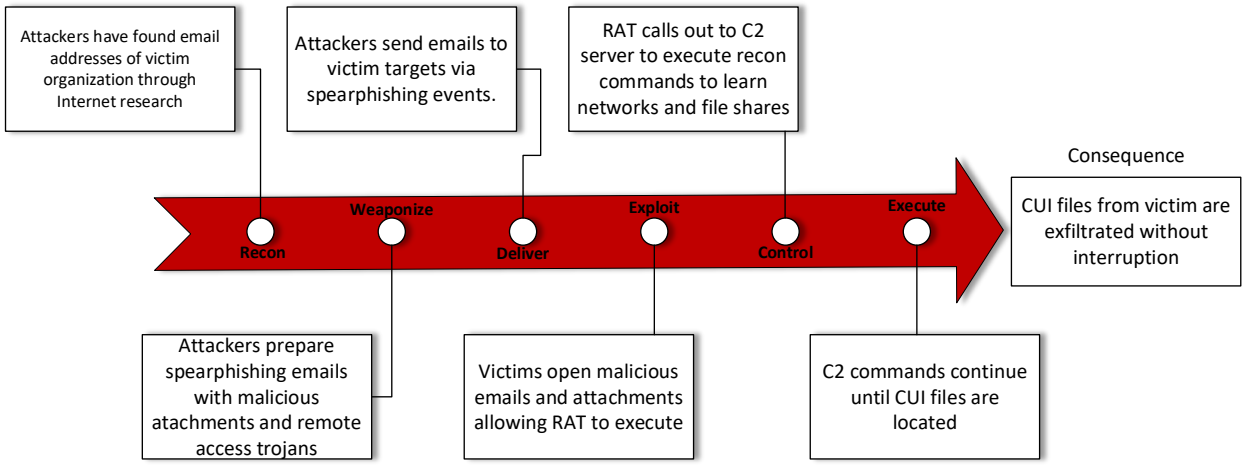
In this scenario, an attacker leverages basic network access to discover controlled unclassified information (CUI) and exfiltrate from the network. This scenario is considered a trainee level of difficulty because after using delivering a phishing message to a BCR employee all the attacker needs to do is leverage the remote access to perform basic recon of network shares for documents which contain CUI markers or classification banners that read UNCLASSIFIED or similar level of classification. This scenario is predicated around the risk that phishing poses to a network and employees and that even basic remote access can be leveraged to cause significant damage to a victim. Sometimes an attacker is just trying to find useful information, and this is easier than exploiting control systems that most attackers may not understand.

3.7.1 Attacker Actions

In this scenario, attackers must prepare a malicious email for a BCR employee. There will be multiple email addresses available for attackers to send messages if they perform advance recon, but they must account for email security countermeasures. If they can guarantee their message is received by the target the BCR actors will open any message they receive for the duration of this scenario.

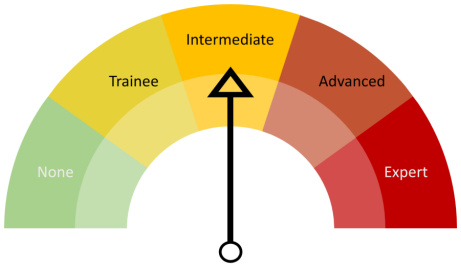
3.7.2 TTP Graph

The following image shows the tactics, techniques, or procedures (TTP) we expect attackers to use in this scenario.



3.8 SCENARIO – PULLED THE RUG OUT FROM UNDER YOU

Scenario	Pulled the Rug Out from Under You
Consequence	Loss of System Access
Access Method	Valid Account
CWE	CWE-798
Skill Level	Advanced



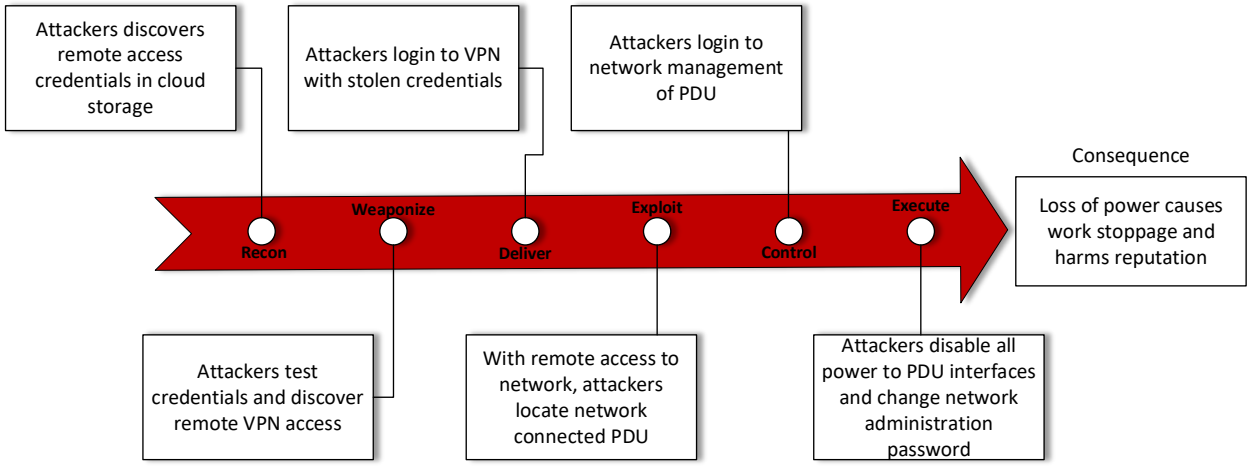
In this scenario, we set the stage for remote control over BCR power distribution units (PDU) giving an attacker the ability to remove power to critical systems at random. This scenario requires attackers to have internal network access. Once inside of the BCR network, they must be able to perform network recon to identify network connected PDU systems and gain access to the PDU web management sites. If they are able to gain access to the management site of the PDU, they will have the ability to disable power to individual outlets cycling power for BCR systems. We rate this scenario as Intermediate difficulty because a PDU is a more common asset for attackers to encounter then targets defined in previous scenarios. It is a simple action to power cycle an outlet using a managed PDU but there is still some degree of difficulty in the brute-force guessing of the passwords to a network connected PDU management website. In addition, the attackers must be able to locate the VPN credentials using standard web recon tactics before they can even access the network.

3.8.1 Attacker Actions

In this scenario, attackers must be able to gain access to the BCR network VPN before they can begin recon for any PDU systems. The access credentials for the BCR VPN will be available only for the window of execution and the must find the credentials and then connect to the VPN. Once connected to the VPN they are expected to locate the PDU and attempt to gain access to the web management interface. If they can gain access to the web interface of the PDU they should shutdown outlets to be considered successful.

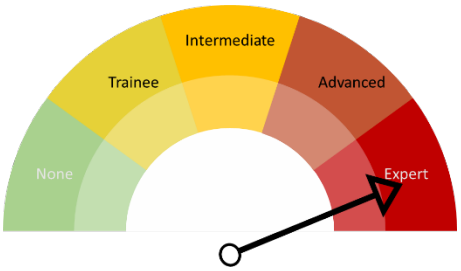
3.8.2 TTP Graph

The following image shows the tactics, techniques, or procedures (TTP) we expect attackers to use in this scenario.



3.9 SCENARIO – NOW YOU SEE ME

Scenario	Now You See Me
Consequence	Enable Other Operations
Access Method	Remote
CWE	CWE-787 CWE-119 CWE-416
Skill Level	Expert



In this scenario, we try to determine if attackers are able to interrupt the primary or secondary surveillance systems of BCR as a companion step to enabling a physical attacker to execute breaking and entering (B&E) on the BCR facility. Like most modern or recent facilities, BCR uses internet protocol (IP) cameras connected to a local area network to send traffic back to a centralized digital video recording (DVR) and reviewing platform. If this surveillance system is not properly secured, an attacker might be able to interrupt the operation of the cameras or even as shown in television and film, loop video to cover up a person being recorded performing an unauthorized entry or access attempt. Unfortunately, an improperly secured surveillance system might allow someone to access the central server and delete past recordings. We consider this scenario as requiring expert level skills because first an attacker has to leverage an access vector and gain internal network access, then the must be able to identify the IP cameras and central collection server. Once done they must craft or inject traffic that either severs the connection between the camera and server, causes the camera to act in an undesirable manner or using a second remote access vector, connect to the central server and delete recordings or turn off the cameras.

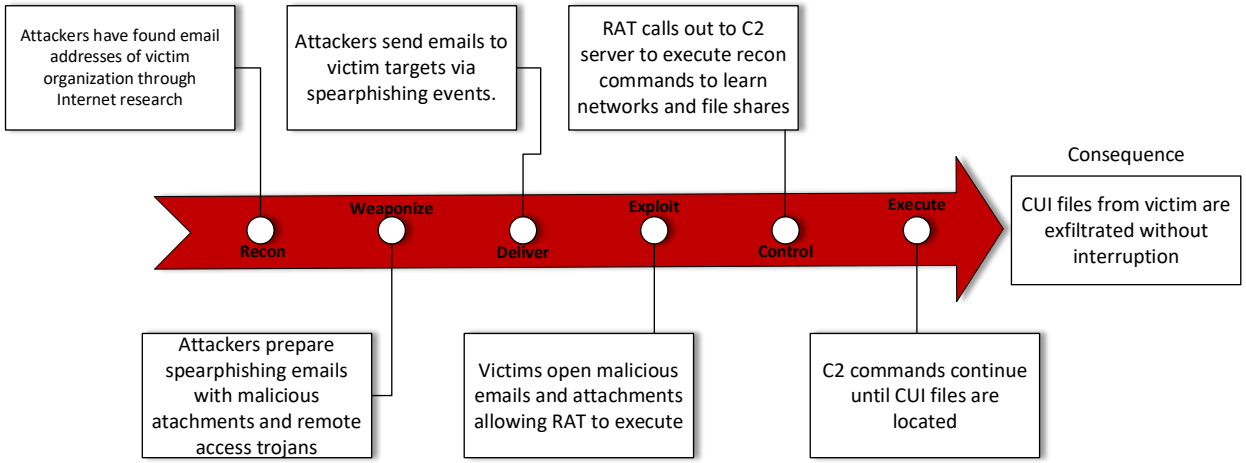
We do not require attackers to have a companion team member to actually step in front of cameras to demonstrate success, simply to prove the camera functions have been altered.

3.9.1 Attacker Actions

In this scenario,

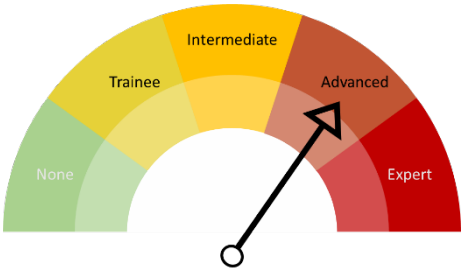
3.9.2 TTP Graph

The following image shows the tactics, techniques, or procedures (TTP) we expect attackers to use in this scenario.



3.10 SCENARIO – DON'T YOU LOSE YOUR HEAD

Scenario	Don't lose your head
Consequence	Endangering Human Life
Access Method	Attackers Already Inside Network
CWE	CWE-522
Skill Level	Advanced



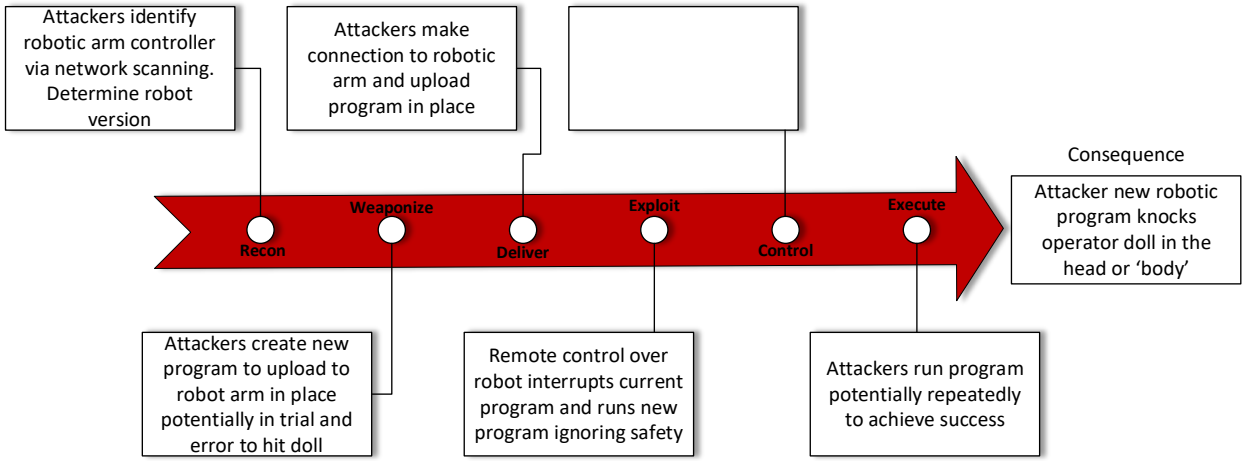
In this scenario, we attempt to determine if our attackers can exploit a robotic arm operating within the network to literally cause bodily harm to a human operator. BCR has decided to increase their market presence and automation by introducing robotic automation into their arsenal of manufacturing. This cooperative robotic (COBOT) arm provides precise control for delicate operations, as well as continuous, repeatable motions providing 24/7 manufacturing assisting in higher volume throughput operations. But, to ensure the safe operation of this robotic arm, safety sensor is installed and added to the current process used by BCR. Safety is paramount in reducing accidents, saving human life, and complying with local, state, and federal guidelines to prevent lawsuits and ensure continuous productivity to enable cashflow. We rate this scenario requires Advanced skill to identify the components of the robotic systems and using the identified protocols/systems, find a method to infiltrate or override the control bypassing the safety mechanisms set in place.

3.10.1 Attackers Actions

As we stated, an attacker will be given internal access for this scenario. the attacker's goal is to find and identify the system(s) controlling the robotic arm and cause it to bypass the safety checks/mechanism(s) in place and cause harm to the robotic operator actor in place. BCR will use a mannequin doll placed in front of the robotic arm. The attacker will need to be able to modify the robotic programming and potentially ignore the safety sensor to cause the robotic arm to knock into the operator doll.

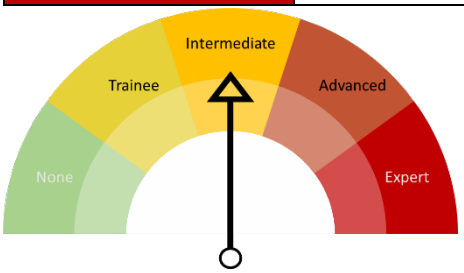
3.10.2 TTP Graph

The following image shows the tactics, techniques, or procedures (TTP) we expect attackers to use in this scenario.



3.11 SCENARIO - SOMETHING DOESN'T SMELL RIGHT

Scenario	Something doesn't smell right
Consequence	Alter System Behavior
Access Method	Already Inside Network
CWE	CWE-807
Skill Level	Intermediate



This scenario looks at the air quality of the BCR manufacturing floor/space. It is vital that safety monitoring of the air is in place to ensure the safety and wellbeing of the workers and the regulated temperatures of the equipment. In this scenario BCR employs an array of sensors to monitor volatile organic compounds, and multiple temperatures at varying points within the production space. These sensors will trigger at certain gas thresholds and when certain temperatures are reached providing advanced warming to ensure the safety of the employees and denotes potential hardware issues due to increased operating temperatures (due to over use/unexplained failure, failing cooling mechanisms, fire/environmental, etc.). Safety is paramount and saving human life, equipment, and infrastructure ensure continued operations while also complying with established local, state, and federal guidelines.

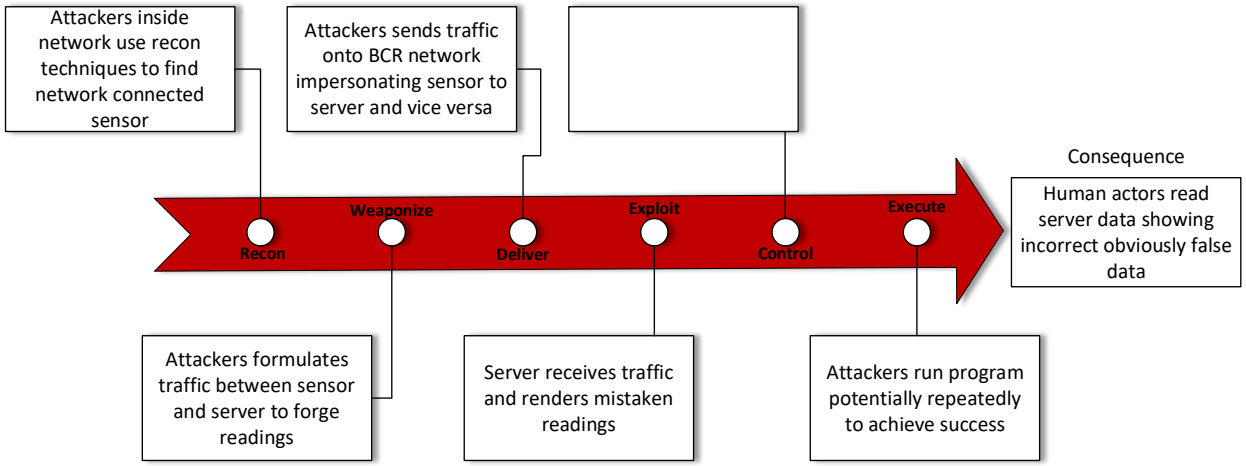
This scenario requires Beginner/Intermediate skill to identify the components of the sensing systems and determine the protocols used and reporting mechanisms. A successful breach denotes the reporting of false information.

3.11.1 Attackers Actions

Assuming one already has internal access, an attacker will probe/identify the systems used to track/control/manage the deployed sensors. Attackers will also successfully identify the sensors and their purpose. With the successful mapping of said systems, a successful scenario completion results in providing false (to include lack of) information compromising the safety of people's environment and equipment with false positive/negative readings potentially putting people in harm's way, causing equipment failure, or premature production stoppages.

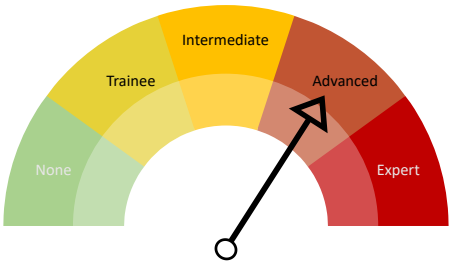
3.11.2 TTP Graph

The following image shows the tactics, techniques, or procedures (TTP) we expect attackers to use in this scenario.



3.12 SCENARIO – THE TICKING TIME BOMB

Scenario	The Ticking Time Bomb
Consequence	Explosion, Fire, Loss of Life, Loss of Property
Access Method	Wi-Fi/Network Compromise
CWE	CWE-327 CWE-521
Skill Level	Advanced



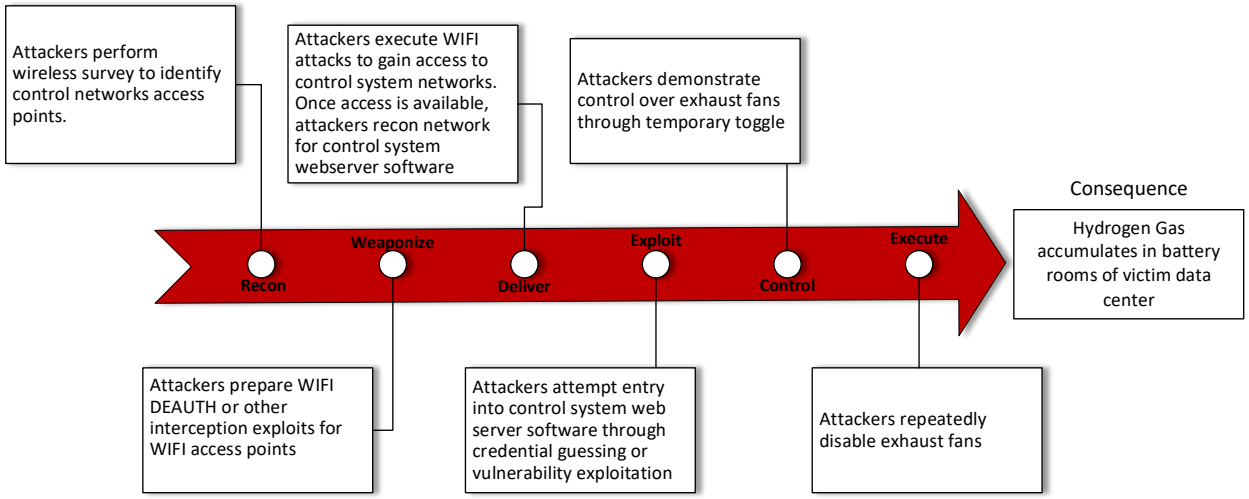
In this scenario, we set the stage for exploitation of the exhaust fan management system in the data center of the victim. The victim operates a large data center for current operations which relies on an automated exhaust fan control system to ensure that the battery backup for the data center does not allow excess hydrogen gas to accumulate. A lead-acid battery backup system is vulnerable to the accumulation of hydrogen gas when the batteries are large enough and are charged in an enclosed space like the victim headquarters. Hydrogen Sulfide gas becomes explosive at a concentration level of 4%. If the exhaust fans are remotely disabled, this can allow the gas to accumulate. Due to the dangerous nature of this scenario, it will only be executed by attackers with on-site access.

3.12.1 Attacker Actions

In this scenario, attackers must be able to gain unauthorized access to the level 2 (PERA) area of the BCR networks that house the exhaust fan control system through exploitation of the wireless access points (CWE-327). Once they have access to the network, they must perform recon activities to identify the controllers that directly interface with the exhaust fans. If they are able to identify these controllers, they should be able to leverage weak passwords to access the control functions and disable the fans. We will have personnel monitoring the fans to detect the control and re-enable if required.

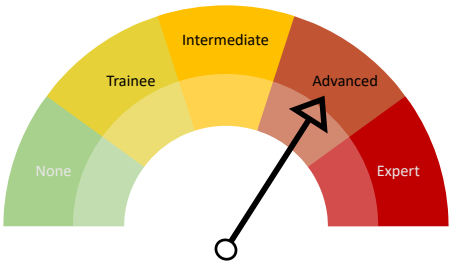
3.12.2 TTP Graph

The following image shows the tactics, techniques, or procedures (TTP) we expect attackers to use in this scenario.



3.13 BUILDING AUTOMATION SYSTEM (BAS) SCENARIO

Scenario	3.14 Building Automation System (BAS) Scenario
Consequence	Unstable environmental conditions
Access Method	Determined by Attacker
CWE	CWE Not Applicable
Skill Level	Advanced



In this scenario, we set the stage for a secondary method for attacker alteration of building environmental controls. Any improperly implemented OT system can be leveraged by an attacker to negatively impact the automated environmental controls of a victim building.

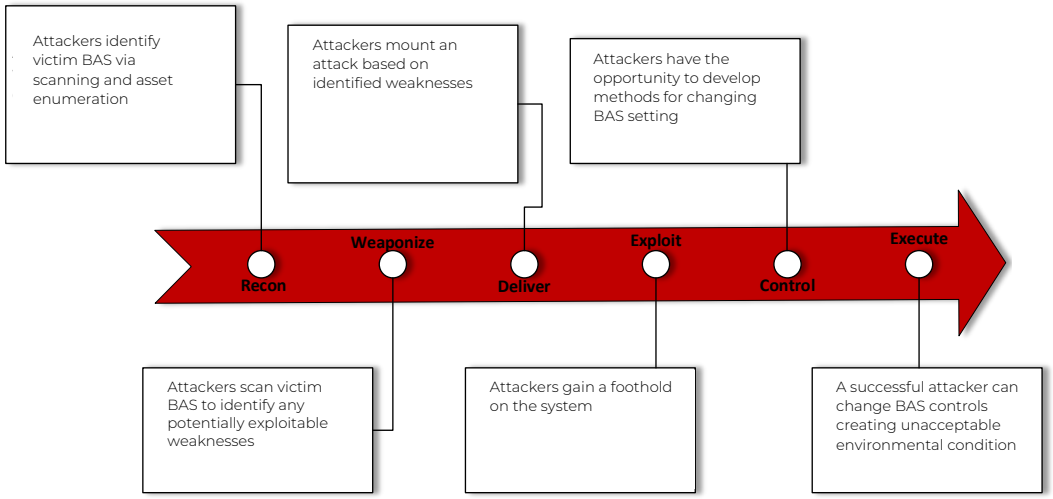
Once perimeter security has been breached and attackers access the building automation network, attackers will have the opportunity to conduct network reconnaissance and identify the devices on the OT network. If they can gain access to a Building Automation System (BAS), they may be able to learn about the systems and deliver consequences, such as:

- Changing occupancy from “Occupied” to “Unoccupied”
- Changing temperature setpoints
- Disabling the hot water plant (shuts down heat to the building)

3.13..1 Attacker Actions

In this scenario, attackers who have breached perimeter security and gained a foothold on the internal company network may be able to identify other building management systems using standard network reconnaissance tools. Attackers could attempt to gain access to the BAS resulting in range of environmental impacts depending on attacker’s choices.

3.13..2 TTP Graph Data :



SCENARIO 3.14

LIGHTS OUT ATTACK CHAIN SCENARIOS

3.14.1 External to Corporate

- Skill level: **ADVANCED**
- Scenario Background
    - Roger Smithson posts on LinkedIN that BCR is accepting applications for multiple corporate postings. He mentions that interested applicants should email their latest resumes to his work email address, rsmithson@BCR.com. Typically, phishing campaigns leverage file attachments, such as malicious *Office Macros,* or *PDFs*, but in this scenario, the attackers are going to leverage a recently expired domain name to promote their *personal (malicious) blog*, hoping Roger will "click" their blog reviewing their *portfolio*. The "click" will not only open a Chrome window, connecting Roger to the blog, it will also execute a reverse shell, connecting back to the attacking team's cloud command and control (C2) infrastructure. They will use Roger's corporate workstation as a pivot point into the target environment.
- Attacker Information
    - Command and Control (C2) with DNS Redirectors
    - Customized Graphic Design Blog
    - Resume (malicious blog URL)
    - Access Achieved
        - rsmithson low-integrity access
- Victim Information
    - Corporation
        - BCR
    - Corporate Target
        - Name: Roger Smithson (rsmithson)
        - Role: HR Recruiter
        - Hostname: ITHRDT7FJ29FA
        - Email: rsmithson@BCR.com
        - LinkedIN: https://www.linkedin.com/rsmithson (not real)
        - Open Position: Graphic Designer
- MITRE ATT&CK TTPS/Mitigations
    - Phishing: Spearphishing Link (https://attack.mitre.org/techniques/T1566/002/)
    - Restrict Web-Based Content (https://attack.mitre.org/mitigations/M1021/)
    - User Training (https://attack.mitre.org/mitigations/M1017/)
- APT References
    - Leviathan (https://attack.mitre.org/groups/G0065)
    - Mofang (https://attack.mitre.org/groups/G0103)
    - Molerats (https://attack.mitre.org/groups/G0021)

3.14.2 CORPORATE FOOTHOLD PRIVILEGE ESCALATION

- Skill level: INTERMEDIATE
- Scenario Background
    - After gaining a foothold to Smithson's corporate workstation, an attackers first task is to migrate to a local service, then attempt to elevate their privileges to obtain local hashes. The local hashes give the attacker a handful of lateral movement options, one being to pass-the-hash (strong passwords), the other to obtain clear text credentials (weak passwords). As part of the corporate "assume breach" scenarios, these steps have already been completed by the adversary.
- Attacker Notes
    - Foothold on the corporate workstation ITHRDT7FJ29FA
- MITRE ATT&CK TTPs/Mitigations
    - Boot or Logon Autostart Execution: Winlogon Helper DLL (https://attack.mitre.org/techniques/T1547/004/)
    - Execution Prevention (https://attack.mitre.org/mitigations/M1038)
    - User Account Management (https://attack.mitre.org/mitigations/M1018)
- APT References
    - Cannon (https://attack.mitre.org/software/S0351)
    - KeyBoy (https://attack.mitre.org/software/S0387)
    - Remexi (https://attack.mitre.org/software/S0375)

3.14.3 CORPORATE LATERAL MOVEMENT

- Skill level: INTERMEDIATE
- Scenario Background
    - The attacker will leverage Roger's hash or cleartext credentials to laterally move to the IT File Server using the PTH technique. Once pivoted, the attacker will enumerate local permissions, including groups. While Roger will not be a local administrator on the new target asset, he does have group permissions to a local "file-sharing" group. This group also contains accounts that extend down in the OT environment, specifically the DMZ. When enumerating files on file shares, the attacker downloads an OT KeePass database, which is configured with a handful of credentials.
- Attacker Information
    - Enumerate corporate assets for open TCP/445
- MITRE ATT&CK TTPs/Mitigations
    - Use Alternate Authentication Material: Pass the Hash (https://attack.mitre.org/techniques/T1550/002/)
    - Unsecured Credentials: Credentials In Files (https://attack.mitre.org/techniques/T1552/001/)
    - Brute Force: Password Cracking (https://attack.mitre.org/techniques/T1110/002/)
    - Privileged Account Management (https://attack.mitre.org/mitigations/M1026/)
    - Restrict File and Directory Permissions (https://attack.mitre.org/mitigations/M1022/)
    - Password Policies (https://attack.mitre.org/mitigations/M1027)
- APT References
    - Night Dragon (https://attack.mitre.org/groups/G0014)
    - Soft Cell (https://attack.mitre.org/groups/G0093)
    - Dragonfly 2.0 (https://attack.mitre.org/groups/G0074)

3.14.4 BREACHING THE IT/OT PERIMETER (LEVEL 4 TO LEVEL 3.5)

- Skill level: INTERMEDIATE
- Scenario Background
    - Once the adversary cracks the KeePass database and documents OT accounts, they will continue their attack, this time attempting to breach the IT/OT perimeter. A simple and common misconfiguration, mapping OT credentials to an IT file share, allows corporate users to copy files to and from the OT environment. The adversary will leverage Denis Savard's credentials to gain a session on the DMZ file server, breaching the IT/OT perimeter. Using the administrator credentials found in the KeePass database, the adversary will attain local administrator, allowing them to dump hashes and continue their attack chain.
- MITRE ATT&CK TTPs/Mitigations
    - Use Alternate Authentication Material: Pass the Hash (https://attack.mitre.org/techniques/T1550/002/)
    - Privileged Account Management (https://attack.mitre.org/mitigations/M1026/)
- APT References
    - Night Dragon (https://attack.mitre.org/groups/G0014)
    - Soft Cell (https://attack.mitre.org/groups/G0093)
    - Sandworm (https://collaborate.mitre.org/attackics/index.php/Group/G0007)
    - Xenotime (https://collaborate.mitre.org/attackics/index.php/Group/G0001)

3.14.5 DMZ LATERAL MOVEMENT

- Skill level: BEGINNER
- Scenario Background
    - After landing on the DMZ file-server, the adversary seems to be isolated to the DMZ environment, being unable to identify any IP addresses outside the current network range. They laterally move within the DMZ, to attempt to identify a path down into the PCN. Using the same admini credentials as the file-server, the adversary was able to laterally move over to the DMZ network monitoring system server. This asset is typically a high-valued target as it often has hooks into the PCN to collect asset information from workstations and servers.
- MITRE ATT&CK TTPs/Mitigations
    - Valid Accounts: Local Accounts (https://attack.mitre.org/techniques/T1078/003/)
    - Use Alternate Authentication Material: Pass the Hash (https://attack.mitre.org/techniques/T1550/002/)
    - Password Policies (https://attack.mitre.org/mitigations/M1027/)
    - Privileged Account Management (https://attack.mitre.org/mitigations/M1026/)
- APT References
    - Night Dragon (https://attack.mitre.org/groups/G0014)
    - Soft Cell (https://attack.mitre.org/groups/G0093)
    - Sandworm (https://collaborate.mitre.org/attackics/index.php/Group/G0007)
    - Xenotime (https://collaborate.mitre.org/attackics/index.php/Group/G0001)

3.14.6 BREACHING THE PCN (LEVEL 3.5 TO LEVEL 3 AND LEVEL 2)

- Skill level: BEGINNER

- Scenario Background
  - Once the adversary gains administrative access to the DMZ network monitoring server, they're able to identify another local administrator account, one that intrigues all adversaries, a privileged service account. As previously mentioned, service accounts are typically configured (or misconfigured) as domain administrator or local administrator on all assets that relay data back to the centralized server. Examples of these applications include SIEMS, AntiVirus solutions, WSUS servers. These configurations are designed to use a service account to pull data from endpoints, but they often don't need to be configured as domain administrator or local administrator. In this scenario, the target organization (BCR) configured their OT service accounts as local administrators. This misconfiguration allows the adversary to laterally move to any machine with this service account as full SYSTEM access.
- MITRE ATT&CK TTPs/ Mitigations
  - Valid Accounts: Local Accounts (https://attack.mitre.org/techniques/T1078/003/)
  - Use Alternate Authentication Material: Pass the Hash (https://attack.mitre.org/techniques/T1550/002/)
  - Password Policies (https://attack.mitre.org/mitigations/M1027/)
  - Privileged Account Management (https://attack.mitre.org/mitigations/M1026/)
- APT References
  - Night Dragon (https://attack.mitre.org/groups/G0014)
  - Soft Cell (https://attack.mitre.org/groups/G0093)
  - APT32 (https://attack.mitre.org/groups/G0050)
  - Sandworm (https://collaborate.mitre.org/attackics/index.php/Group/G0007)
  - Xenotime (https://collaborate.mitre.org/attackics/index.php/Group/G0001)

3.14.7 ENUMERATING & COMPROMISE BAS WORKSTATION

- Skill level: EXPERT
- Scenario Background
  - The final step in this scenario the attackers will gain access access to the Engineeering Workstation (EWS) and interact with the first floor building lights. The EWS will have all of the necessary information and access to the PLC that you can use. This scenario will be the first time that you will be interacting with BAS assets to create a cyber physical effect.
- MITRE ATT&CK TTPs/ Mitigations
  - Remote System Discovery (https://collaborate.mitre.org/attackics/index.php/Technique/T0846)
  - Default Credentials (https://collaborate.mitre.org/attackics/index.php/Technique/T0812)
  - Static Network Configuration (https://collaborate.mitre.org/attackics/index.php/Mitigation/M0814)
- APT References
  - Stuxnet (https://collaborate.mitre.org/attackics/index.php/Software/S0010)
    - Enumerate controllers, not specifically Siemens PLCs

4 SKILL LEVELS

In this section we define the skill levels that each participant should have to be successful in an HTB scenario. Each skill level is considered cumulative of the levels defined prior.

Level	Description
BEGINNER	A beginner is considered either a self-starter or someone who has passed entry level training in penetration testing, vulnerability scanning or ethical hacking. It is possible to be successful in a beginner scenario having only conducted experimentation and research on your own using Internet Searches, YouTube or online videos and trial and error. A BEGINNER scenario contains additional starting information that you will not find in other more difficult scenarios. A BEGINNER scenario may also offer hints if participants are having trouble advancing from start to finish. To be more specific, a BEGINNER should be able discover Internet accessible domains, hosts, email addresses and once inside of a network, they should be able to identify all IPv4 and Ethernet hosts on a single network.
INTERMEDIATE	An INTERMEDIATE team is considered to have 1-3 years of additional experience beyond a BEGINNER. An alternative method of comparison is to consider that an INTERMEDIATE team has participated in 3-5 separate engagements, competitions, or projects more than a BEGINNER. These additional events should have taken place on different starting dates, in different networks and contain a mixture of technologies that were not observed previously. An intermediate team should be able to discover related hosts, domains and addresses based on starting information. They should be able to run vulnerability discovery tools on targets both inside and outside of a network. They should be able to run so called 'low-interaction' exploit tools on vulnerable targets throwing simple exploits or using well-known techniques like password guessing using default options.
ADVANCED	An ADVANCED team should have a minimum of two additional years over an INTERMEDIATE team. An ADVANCED team should have multiple engagements of experience using offensive or exploitation tools. An ADVANCED team should also have experience using network attack tools beyond denial of service. An ADVANCED team should be able to run advanced host discovery, vulnerability discovery and exploit tools on a target network. ADVANCED teams should understand network security tools such as firewalls and intrusion detection and anti-virus even if they do not

Level	Description
	necessarily understand how to evade these systems. ADVANCED teams should be comfortable with non-standard protocols like MODBUS, S7, PROFINET. An ADVANCED team should be capable of compiling their own versions of well-known tools and customizing or building their own operational workstations or platforms. They should also be able to run low-interaction exploit tools that require customization of options.
EXPERT	An EXPERT team should have a minimum of 2-4 years of additional experience over ADVANCED teams. They should be cable of running high-interaction exploitation tools that require user interaction or multi-stage events such as phishing emails combined with watering-hole exploit servers. ADVANCED teams should be able to customize well-known community tools and even construct their own tools using popular libraries (e.g. libPCAP) EXPERT teams should be able to modify tools to reduce or eliminate countermeasure system alerting on tool execution. EXPERT teams should be able to combine multiple intelligence sources into a single plan or campaign of attack techniques to gain remote access to a target network. EXPERT teams should have expertise to modify initial access exploits, shellcode or web payloads for gaining access to target systems.

HACK THE BUILDING

2020 | PLAYBOOK

HACKTHEBUILDING.TECH | MISI.TECH

HACK THE BUILDING IS AN UNCLASSIFIED EVENT | HACK THE BUILDING USES REPONSIBLE DISCLOSURE