DCI

Discovery and Counter-Infiltration

Lab Manual

DC3 Cyber Training Academy

The Academy is accredited by the Commission of the Council on Occupational Education (COE).

COE is a national accrediting body dedicated to ensuring quality and integrity in career and technical education.

911 Elkridge Landing Road
Airport Square 11 Building, Suite 200
Linthicum, MD 21090
Tel: 410-981-1165
Fax: 410-850-8936
www.dc3.mil

[v.1803]

CONTENTS

COURSE INTRODUCTION

MODULE 1 DCI Hunt Mission

Module 1 introduces the Cyber Protection Team Discovery and Counter-Infiltration (CPT-DCI) Hunt Mission. Students are introduced to the concepts of incident response and identifying adversary behavior through network and host-sensor deployment.

Lesson 1: Hunt Activities

All DCI activities revolve around a central theme: identifying adversary activity in a mission commander's network and ensuring visibility and rapid deployment of indicators of compromise (IOCs) to detect, defend and ultimately eradicate enemy freedom of action in friendly networks. Lesson 1 introduces the concepts of threat agents, threats, IOCs, sensors and remediation techniques for use in DCI hunt activity.

MODULE 2 Mission Planning Actions

Module 2 introduces common tasks that DCI squads undertake during the planning phase of a mission. Planning phase activities for which the DCI squad is expected to gain proficiency include: receiving the mission, integrating threat intelligence with the mission owner requirements and preparing equipment for the engagement.

Lesson 1: Analyze Threat Intelligence Reporting

CPT actions are executed in the context of a specific threat, are often well known and considered advanced and persistent. This lesson guides students through analyzing open-source threat reporting to identify known IOCs and introduces useful signatures and tactics, techniques and procedures (TTPs) to use later in updating sensor platforms, denying enemy access, and driving host and network analysis to hunt adversaries in friendly networks. Students use analysis capabilities to develop an initial set of indicators for a known threat agent. These indicators are generated and stored in tools such as IOC Editor and other IOC storage methods and tools to be determined based on job-task analysis.

Lesson 2: Integrating Threat Intelligence with the Supported Mission

The mission owner's network is larger than a CPT can conceivably defend. A CPT must work with the mission owner to agree on the Key Terrain-Cyber (KT-C) the mission will defend. In this lesson, students request critical asset lists from the customer, and analyze the critical asset list in conjunction with the specific squad capabilities, to identify additional resources that would be required to support the mission. For example, the supported mission's KT-C may contain non-standard wireless communications capabilities and SCADA systems that the squad members are unfamiliar with. Exercises focus on the ability for DCI squad members to extract information from a critical asset list to identify gaps in skillsets, training or tools and make appropriate recommendations for successful mission execution.

Lesson 3: Preparing Equipment for Operation Execution

Following the recovery from a previous mission, a deployment kit may remain packed until the next deployment. Prior to deployment, a CPT must update the systems in the go-kit to ensure new vulnerabilities and risks are not introduced to the supported mission commander's network. DCI squad members will exercise updating operating systems, software tools, sensor platforms and network gear to meet the current mandatory version per the toolkit documentation or to meet the supported commander's requirements. Students document the steps and actions taken and identify when they must elevate discrepancies or requirements gaps for software updates. Students also install and test threat intelligence signatures on sensor platforms.

MODULE 3 Survey Stage Actions

Module 3 introduces tasks that are common for DCI squads to undertake during the mission survey stage. Activities the DCI squad is expected to have proficiency in for the survey stage include: coordinating with local cyber network defenders, performing network reconnaissance and collection, and performing host reconnaissance and data collection.

Lesson 1: Working with Supported Mission System Administrators

Students use system administrator documentation to identify network topology and subnets with a focus on the previously identified KT-C. Students will take the network topology (network documentation) into account when

developing a sensor strategy that meets key objectives for observing traffic transitioning KT-C and ensuring visibility to high-probability targets based on threat intelligence. Students will work with typical baseline image formats to develop "known good" baseline datasets for integration in analysis and hunt activities.

Lesson 2: Performing Survey Stage Network Reconnaissance

Students will use a variety of host discovery tools to identify active nodes on a network and will be introduced to tools typically used for host discovery at various layers of the Open Systems Interconnection (OSI) model. Students will use command-line and GUI-based tools to monitor network traffic and identify typical traffic for the network they are monitoring.

Lesson 3: Performing Survey Stage Host Reconnaissance

Students will use a variety of host-discovery tools to identify active nodes and their associated ports and services on a network. Students will identify specific services and service versions in use on the hosts and will perform analysis of volatile data and non-volatile data using host-based sensors and scripting tools to identify active threats.

MODULE 4 Secure Stage Actions

Module 4 introduces tasks that are common for DCI squads to undertake during the mission secure stage. The DCI squad is expected to have proficiency in secure stage activities, including: deploying sensor platforms and monitoring the sensors, identifying indicators of compromise within the mission owner network, and reporting findings through Intel Analysts and other CPT elements.

Lesson 1: Deploying Sensors

Students will use IOCs and network sensors to monitor the KT-C for adversary action and activity. Students will use baseline analysis to develop "known good" models for traffic on various network segments and apply sensor-tuning approaches to reduce the total volume of data that must be analyzed.

Lesson 2: Analyzing Compromised Hosts

Students will analyze host systems using host-based sensors and digital forensic techniques to identify files of interest from affected systems. Students will analyze intrusion scenarios to identify new or previously unknown artifacts for integration into the threat agent signatures. Students will update

signatures for deployed sensors and refine signatures for the operating environment. Students will share reporting through the intelligence analyst channels and ensure other CPT elements are informed of updated IOCs.

MODULE 5 Protect Stage Actions

Module 5 introduces tasks that DCI squads commonly undertake during the Mission Protect stage. During the protect stage, the squad is expected to be proficient in developing remediation strategies and mitigation plans to defend the network from cyber threat actors.

Lesson 1: Developing Remediation Strategies and Mitigation Plans

Students will present findings and work through exercises that develop reporting methods and techniques that are effective for different audiences, which include: the supported command, supported command's network defense capabilities, NETOPS command, CPT leadership and other squads. Students will develop courses of action (COAs) for findings that mitigate ongoing risks and threats and provide short term and long term COAs. The DCI student will develop inputs for the supported command's risk analysis.

MODULE 6 Recover Stage Actions

Module 6 introduces tasks that are common for DCI squads to undertake during the mission recovery stage. Activities in which the DCI squad is expected to be proficient in the recovery stage include: providing After Action Reports (AARs), recovering sensors, outbriefing DCI activity results and returning the network to normal, or as near-normal as possible, operational status. This also includes outbriefing deploying sensor platforms and monitoring the sensors, identifying IOCs within the mission owner network, and reporting findings through Intel Analysts and other CPT elements.

Lesson 1: Performing Post-Operation Recovery Activities

Students will demonstrate the removal of host-based and network-based sensors from a network environment and ensure systems remain operational. Students will develop and implement strategies to recover systems when

removal of sensor capabilities causes system failure. Students will develop a final out-brief to include recommendations to enhance the security posture of the network. Students will perform an After Action Report per USCYBERCOM guidelines and provide inputs specific to the DCI areas of responsibility (AORs).

MODULE 1

DCI Hunt Mission

Module 1 introduces the Cyber Protection Team Discovery and Counter-Infiltration (CPT-DCI) Hunt Mission. Students are introduced to the concepts of incident response and identifying adversary behavior through network and host-sensor deployment.

Lesson 1

Hunt Activities

This course introduces the concepts of threat agents, threats, indicators of compromise, sensors and remediation techniques used in Discovery and Counter-Infiltration (DCI) Hunt Missions.

DCI activities involve identifying and communicating pre-existing or active adversary activity in a mission commander's network. Squads are tasked with rapid deployment of indicators of compromise (IOCs) to detect, defend and ultimately eradicate enemy freedom of action in friendly networks.

DCI Hunt Mission Overview

Introduction: What Does DCI do on a Hunt Mission?
All DCI activities revolve around one central theme – identifying adversary activity in a mission commander's network and ensuring visibility and rapid deployment of IOCs to detect, defend and ultimately eradicate enemy freedom of action in friendly networks. This course introduces the concepts of threat agents, threats, IOCs, sensors and remediation techniques for use in DCI hunt activity.

Hunt Capability Achieved Through DCI Activities

- Integrate threat intelligence
- Perform network reconnaissance and collection
- Perform host reconnaissance and collection
- Deploy sensors
- Identify indicators of compromise
- Develop remediation strategy and mitigation plan of action
- Return network to state that supports command's mission

Integrate Threat Intelligence

- Conduct analysis of threat intelligence
- Create threat indicators from intelligence reporting
- Understand mission-critical asset lists
- Identify resources required to support missions
- Apply threat intelligence signatures to sensor platforms

Perform Network Reconnaissance and Collection

- Identify network topology and subnets
  - Perform logical and physical assessments of a network to identify potential witness devices
- Develop sensor strategy
  - Summarize and complete a sensor strategy
  - Perform logical and physical assessments of a network to identify potential witness devices
  - Determine placement of network monitoring workstations on the network
- Obtain network owner's image baseline
  - Generalize host and network baselining
- Scan network to identify endpoints
- Conduct traffic analysis of the following:
  - Network-based evidence
  - Log files
  - Network traffic
  - Web traffic
  - File transfer traffic
  - Network traffic and system artifacts to identify probing/intrusion techniques
  - Network traffic using an intrusion detection system (IDS)

Perform Host Reconnaissance and Collection

- Obtain network owner's image baseline
  - Generalize host and network baselining
- Scan hosts to identify open ports and services
- Conduct host analysis to identify threat attribution
  - Perform the collection of volatile data from systems
  - Generate hash values for collected data

Deploy Sensors

- Monitor sensors for threat attribution
- Tune network sensors to eliminate noise

Identify Indicators of Compromise

- Analyze host system
  - Explain common Windows file systems and identify key artifacts
  - Analyze volatile data
  - Analyze a memory image
  - Analyze the forensic image of a system

- Refine host and network signatures for deployment
- Update Intelligence Analyst on any new threat intelligence findings
- Report findings to CPT team

Develop Remediation Strategy and Mitigation Plan of Action

- Report findings to CPT team; summarize internal and external reporting
- Provide input for courses of action with the Cyber Protection Team (CPT)
    - Explain recommended remediation actions
    - Analyze and prepare remediation strategy and mitigation plan of action
- Provide input for risk analysis to CPT team
    - Explain recommended remediation actions
    - Analyze and prepare remediation strategy and mitigation plan of action

Return Network to State That Supports Command's Mission

- Recover or remove all host and network sensors
- Brief CPT team on results and provide final recommendations to team
    - List DCI inputs to a final report
- Conduct a weekly After Action Report
    - Summarize an after action review of the mission

Daily and Weekly Reporting

These are activities you must complete each day or once a week. Visit the Daily Operator Log page for the appropriate week and submit daily logs Monday through Friday. On each Friday, you will combine the content from that week's daily logs into a weekly After Action Report and submit.

Daily Operator Logs

During this course, you are required to maintain a DAILY operator log. Download the template for the operator log and upload (submit) a new log each day of class. Each week has its own log upload assignment.

While on mission, it is important to track the activities you perform individually. These activity logs are used to:

- Measure performance and identify effectiveness of activities.
- Take corrective actions after a mistake or error.
- Identify challenges faced in the field.
- Inform the situational reports (SITREPs) and other reports/briefs.

This log will help you:

- Identify areas of performance you need to practice during the individual practice time.
- Develop weekly briefings that are graded.
- Quickly recall techniques and processes that will help you perform actions during assessments.
- Inform appropriate network operations (NETOPS) command of results and ongoing actions.

Daily Operator Log Excel Template

*** Download the Daily Operator Log Excel template and upload (submit) a new log each day of class.**

Date/Time	System/IP	Activity	Remarks
1/1/2018 @ 15:00	192.168.4.2	Configured GRR server with correct IP address for home station. Edited configuration /etc/grr/config/files.yaml. IP from previous mission was 12.19.54.7	Used vi to edit files. Need to review basic Linux commands.
15:15	-	Reviewed network diagram for home station to determine network block - 192.168.4.0/24	
15:34	192.168.4.5	Downloaded host sensor (GRR client) to system and installed with Admin privileges	Needed to repackage the executable on the GRR server for the client to work.
15:52	-	Reached END OF EXERCISE	

Example of Daily Operator Log File

Weekly After Action Report (AAR)

Complete a weekly After Action Report (AAR) each week. This should be a summary of all activities you performed this week and follow the template within the assignment.

Throughout engagement with a supported mission, a CPT will produce a variety of briefings and reports that provide situational awareness for the multiple higher headquarters (HHQ) to which the CPT reports.

This exercise gives you an opportunity to practice consolidating daily experiences in a report that is similar to the After Action Reports (AAR) used operationally.

A weekly After Action Report is a reflective document that helps the CPT, squads and individual members contemplate where the CPT was most successful and where the CPT has opportunities for improvement.

Each student will have an opportunity to record in their AAR during the course.

* **Use the given AAR PowerPoint template to record your personal lessons learned and opportunities for improvement over the last week. Rename and submit one review per week.**

  The template format is shown on the following pages.

Weekly After Action Report Template

Slide 1: Title Page

981st CPT DCI Squad
After Action Review (AAR)

Reported by <NAME>

Slide 2

Overview

Week <#>:

- What I learned this week
- What exercises went well
- What exercises did not go well
- What worked but could have worked better

Slide 3

What I learned this week

- Did you perform some action you have never performed before?
- Did you implement an IOC in a unique or especially effective way?
- Did you use a tool that you were unfamiliar with?
- What was your biggest take-away this week?

Slide 4

What exercises went well?

- Exercise 9.1-014 – Provide NETOPS reporting
  - I have gotten used to tracking my activity as I move through exercises which makes the daily operator logs easy to submit
- Exercise 6.2-079– Collect data from network endpoints
  - I used extra time this week to master deployment of host agents and practiced retrieving different types of information (files, hash values, network connections)

Slide 5

What exercises did not go well?

- Exercise 5.3-081 – Integrate new threat intelligence into network sensors
  - When I added new IOCs to the Snort configuration file, I messed up a previous configuration line. I think I need to practice editing files from basic text editing tools like vi
- Exercise 7.2-022 – Use PowerShell to collect data from endpoints
  - I was able to collect data from 1 endpoint, but was unsuccessful at rebuilding the script to grab data from multiple endpoints. I need to use the next practice time to try this exercise again.

Slide 6

What went well, but could have been better?

- Exercise 4.1-021 – Determine traffic routes based on network topology maps
  - I didn't notice the alternate traffic routes that were possible in the scenario. I caught one of them, but the other 2 eluded me. Since traffic can be routed through malicious tools I only considered the managed/designed network routes. In a real-world scenario, I think I could miss enemy C2 and/or data exfiltration if I don't realize all the possible routes.

Introduction to the Exercise Environment

This course consists of a series of exercises that are completed in a Cybersecurity Range environment. This flexible operating environment allows students to execute a wide range of capabilities using virtualized operational platforms and networks.

For ease of use, the general information about the virtualization environment is being provided here.

How to Start the Virtual Environment

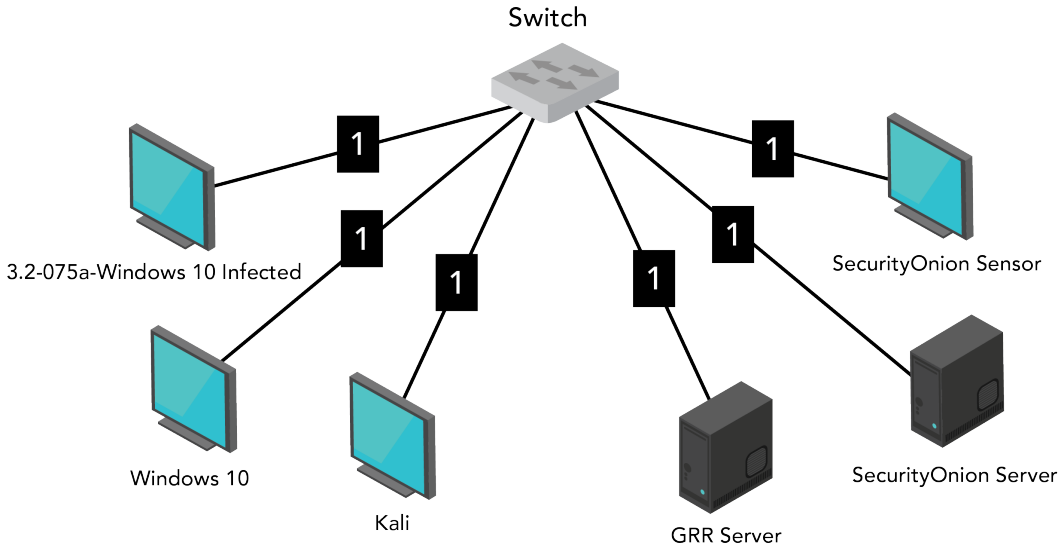
Use the "start the SDI" button in the upper right corner to power on the environment.

Accessing Systems

Any system shown in your environment can be accessed as a user by double-clicking on the system. A new window will open presenting the user interface. Most systems will require you to log on or authenticate with a username and password. The standard usernames and passwords used are:

Username	Password
dcistudent	P@ssw0rd
root	toor

If these username/password combinations do not work, you may not be authorized direct user access on the system.



Module 2 Environment

Tools Available

The course is focused on executing DCI-related actions for any Cyber Protection Team, despite access to specific tools. More important than the specific tools used to perform the various actions are the ideas, concepts and relevance of the information analyzed. A standardized and easily accessible toolset is available on the systems:

Network Sensors

Network sensor capability is provided through the SecurityOnion distribution of Linux. SecurityOnion can be configured to use a variety of signature capabilities (Snort, Bro, etc.), can operate in a production environment with multiple sensors reporting back to a centralized control node, and can provide alerts to the end user through the Sguil and Squert applications.

Host Sensors

Host sensor capability can be leveraged by using the GRR Rapid Response agent-based incident response capability. GRR can be used to remotely retrieve files, memory and registry data from hosts. These retrievals can be highly customized and tailored to your specific desires and are run as "hunts" or "flows." Additionally, PowerShell is leveraged at many points to discover alternative or back-up approaches for collecting host data.

Analysis Platform

The Windows 10 and Kali systems are provided as a standardized analysis platform. With these systems, you will have sufficient tools to perform all manners of analysis based on the scenarios and specific information that will be requested of you.

Exercise Files

The various files and source materials you will need to successfully navigate exercises can be found within the environment. All DCI systems in the environment have a CD attached that contains the resources you will need.

Module Exams

Module exam data sources are also available on the CD-ROM for DCI systems; however, they are password protected. The password for accessing these archives will be provided at the time of testing.

MODULE 2

Mission Planning Activities

Module 2 introduces common tasks that DCI squads undertake during the mission planning phase. Planning phase activities for which the DCI squad is expected to gain proficiency include: receiving the mission, integrating threat intelligence with the mission owner requirements and preparing equipment for the engagement.

Lesson 1

Analyze Threat Intelligence Reporting

CPT actions are executed in the context of a specific threat. These threats are often well known, and are considered advanced and persistent. This lesson guides students through analyzing open-source threat reporting to identify known indicators of compromise and useful signatures. Students will also learn tactics, techniques and procedures (TTPs) to use later while updating sensor platforms, denying enemy access and driving host and network analysis to hunt adversaries in friendly networks. Students will use analysis capabilities to develop an initial set of indicators for a known threat agent. These indicators are generated and stored in tools such as IOC Editor.

Exercise 1.1-001.a - Characterize a Threat Agent 1

Introduction

Objective: Analyze threat intelligence reporting

This exercise will work through performing threat characterization of an Advanced Persistent Threat (APT), specifically, the APT28 threat agent. You will review open-source reporting for the threat agent and consider this information with respect to common cyber threat models.

Scenario

Your team is performing a practice proactive protect mission for the Office of the Florida Secretary of State. Initial threat intelligence identified APT28 as a likely threat to the mission owner.

Background: The presidential election is November 3rd. Florida's Secretary of State has requested USCYBERCOM to provide additional resources to protect the Department of State office from cyberattacks leading up to and during the election. The Office of the Secretary for the Florida Department of State is where all votes are counted and then announced nationally. The office is located at 500 S. Bronough St., Tallahassee, FL 32399. The DCI squad's intelligence analyst has searched through historical data for potential threats to the customer's network.

Action Summary

In this exercise, you will:

1. Read the Diamond Model and the Cyber Kill Chain document to understand how cyber threat actors engage in offensive or exploitive cyber activities.
2. Read the APT28 reports from FireEye, Bitdefender and ESET.
3. Answer the questions for this exercise.

Any additional resources you choose to use are acceptable for this activity.

Why Understanding the Threat Matters

The DCI squad will need to identify what threats to the supported command's mission currently exist. Understanding those threats, tactics, techniques and procedures helps when planning how the DCI squad will conduct its operations. For example, it is critical to the DCI squad detect, defend and eradicate procedures, to understand both how the threat usually compromises a system and what existing IOCs can be found within the network.

Intelligence reports come in many different forms. It is important for members of the DCI squad to scan the intelligence reports and pull out the critical information they need to plan their operations. In this exercise, you will read intelligence reporting, pull out critical pieces of information and explain how that piece of intelligence can help the DCI squad.

Cyber Threat Models

Models are used to represent ideas, objects or a system. Models describe the process through which things happen and are used to explain how certain activities transpire. When we apply cyber threat models to a threat agent, we can better identify methods to locate the adversary or deny an adversary freedom of action.

The Cyber Kill Chain and Diamond Model are two models used in Cyberspace Operations to understand our adversaries and collaborate detailed information about the TTPs that are used. Understanding these models will aid you in characterizing threat actors and improve the effectiveness of response actions.

Resources

Cyber Kill Chain – Threat Actions
http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Diamond Model – Attribution Model
http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

Threat Agent Reporting

Many different vendors track cyber-threat actors and major actor campaigns. Open-source information on these threat actors can be extremely beneficial in developing a characterization of the threat.

Here are reports about APT28 from three different open-source information providers.

FireEye

https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf

Bitdefender

https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28–The_Political_Cyber-Espionage.pdf

ESET

https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf

https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf

https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part3.pdf

Course of Action Matrix

Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Retrieved September 8, 2015, from http://www.lockheedmartin.com/ content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

CREDIT: Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2015)

Closeout

During this exercise, you analyzed threat intelligence reporting and used the Cyber Kill Chain and Diamond Models to align attributes of the threat agent's capabilities and toolkit. Other exercises in this course will integrate this analysis by creating network and host-based sensor signatures as you perform intel-driven hunt operations in friendly networks.

For Further Discussion

Consider the following and discuss as a class:

1. If reports have two different hash values for the same filename and location, do you use both or consider neither to be part of the IOCs?
2. Should you consider any one vendor more authoritative than another?
3. What information was helpful in developing the characterizations? What information was not? Why is this helpful for performing defensive cyber operations?
4. How relevant or helpful is the information if the threat agent is not the actual threat to the mission owner?
5. Would you continue a mission if the threat agent does not line-up?
6. How would you fix the glitch of a mismatch like that?

Exercise 1.1-002.a - Characterize a Threat Agent 2

Introduction

Objective: Analyze threat intelligence reporting

This exercise will work through performing threat characterization of the APT1 threat agent. You will review open-source reporting for the threat agent and consider this information with respect to common cyber threat models.

Action Summary

In this exercise, you will:

1. Read the Diamond Model and the Cyber Kill Chain document to understand how cyber threat actors engage in offensive or exploitative cyber activities.
2. Read the APT1 reports from FireEye/Mandiant and CrowdStrike.
3. Answer the questions for this exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources

APT1 Threat Agent Reports

FireEye/Mandiant

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

CrowdStrike

http://cdn0.vox-cdn.com/assets/4589853/CrowdStrike-intelligence-report-putter-panda.original.pdf

Cyber Threat Actions and Attribution Models

Cyber Kill Chain – Threat Actions

http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Diamond Model – Attribution Model

http://www.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

Closeout

During this exercise, you were asked to review the APT1 reporting and identify information about the technical capabilities of the threat agent that can inform adversary hunt operations, potential cyber effects and artifacts.

For Further Discussion

Consider the following and discuss as a class:

1. Why is intelligence important to the DCI squad member?
2. Why is understanding different names for the same APT important?
3. Why is understanding the TTPs of an adversary important?

Lesson 2

Integrating Threat Intelligence with the Supported Mission

The mission owner's network is larger than a CPT can conceivably defend. A CPT must work with the mission owner to agree on the Key Terrain-Cyber (KT-C) the mission will defend. In this lesson, students request critical asset lists from the customer and analyze the critical asset list in conjunction with the specific squad capabilities, to identify additional resources that would be required to support the mission. For example, the supported mission's KT-C may contain non-standard wireless communications capabilities and SCADA systems with which the squad members are unfamiliar. Exercises focus on the ability for DCI squad members to extract information from a critical asset list to identify gaps in skillsets, training or tools and make appropriate recommendations for successful mission execution.

Exercise 2.1-007.a - Identify Mission Systems in Critical Asset List

Introduction
Objective: Analyze critical asset list from customer

Scenario
The Mission Protection (MP) squad has asked the DCI squad for input in the mission analysis being conducted with the customer. Specifically, the MP squad wants the DCI squad to formulate the customer's Prioritized Defended Asset List (PDAL). The CND Manager has rounded up the squad and has asked for input.

Understand that in a real-life scenario, there are numerous variables and factors that go into figuring out a PDAL. The PDAL may even change as the mission continues, given different circumstances. In real life, there could be multiple answers for each mission and this analysis usually takes one to three weeks to complete. This simulated exercise is looking for the **BEST** answer.

Background: The CPT does not have the time, resources or workforce to secure and defend the entire network. They must focus on mission-critical systems with the highest impact to the customer's mission. Usually, a customer will have already identified mission-critical assets for the CPT. Using their experience and threat-driven approach, the CPT is tasked to re-order critical assets into a PDAL. The PDAL allows the CPT to focus their efforts and resources on the most- to least-critical assets.

Action Summary
This exercise will require you and your team to think critically to understand multiple-infrastructure devices and networking concepts.

In this exercise, you will:
1. Read the resources to understand what the MP squad thinks about when conducting mission analysis.
2. As a team, open the Mission_Analysis_DCI2017_902nd Excel sheet provided by the MP squad and review all the data contained within.
3. Answer the questions in the exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources: Key Terrain-Cyber & Threat Modeling

Key Terrain in Cyberspace: Seeking the High Ground
https://ccdcoe.org/sites/default/files/multimedia/pdf/d2r1s8_raymondcross.pdf

Cyber Mission Assurance: Page 5 to 14, Page 22 to Page 31
http://www.dtic.mil/dtic/tr/fulltext/u2/a563712.pdf

Threat Modeling
https://www.owasp.org/images/a/a6/AdvancedThreatModeling.pdf

Prioritized Defended Asset List

Army Doctrine Reference Publication (ADRP) 3-37 defines the Defended Asset List (DAL) as follows: "The defended asset list is a listing of those assets from the critical asset list prioritized by the joint force commander to be defended with the resources available (JP 3-01). Critical assets that are reinforced with additional protection capabilities or capabilities from other combat power elements become part of the DAL. It represents what can be protected, by priority. The DAL allows commanders to apply finite protection capabilities to the most valuable assets. The combat power applied may be a weapons system, electronic sensor, obstacle, or combination."

Provided

MP Squad Mission Analysis

Closeout

In this exercise, you reviewed a mission analysis of the 902nd MI Wing. The analysis included the supported owner's mission and tasks, the network maps relevant to the supported mission, and the critical assets list. You used this information to develop a Prioritized Defended Assets List based on each mission area and supporting tasks/cyber assets.

For Further Discussion

Consider the following and discuss as a class:

1. Why did the PDAL change when we went from one mission to other mission sets?
2. What are some things that may cause the PDAL to change throughout the mission?

Exercise 2.2-011.a - Identify Missing Go-Kit Equipment

Introduction

Objective: Identify relevant resources (skills, training requirements and tools) to support missions based on unique KT-C and task

Scenario

Your CPT has received a warning order (WARNORD) for a proactive protect mission. The specific supported mission owner location is unknown.

Background: Currently, 14 of your 39 personnel are deployed on another mission. The CPT Team Leader wants to verify CPT readiness to deploy on another mission. The Team Leader is going to go through a list of scenarios for potential deployment locations and requirements. The DCI CND Manager has chosen you to attend this meeting on their behalf with the Team Leader.

Attached is the Unit Readiness spreadsheet. It details various statuses for personnel, equipment and software. Use the readiness spreadsheet to respond to questions about readiness and current squad capabilities.

Action Summary

In this exercise, you will:

1. Download the Unit Readiness Roster.xlsx file.
2. Use the roster as well as the deployment criteria listed below to answer the questions for this exercise.

Deployment Criteria

To participate in the following missions, you should have completed the following:

Combat-zone missions:

- Passport
- Soldier Readiness Processing (SRP)
- Weapon Qualified
- Request for Information (RFI)

Outside Continental United States (OCONUS) travel (non-combat zone):

- Passport
- Government Travel Charge Card (GTCC)
- Defense Travel System (DTS)

Continental United States (CONUS) travel:
- GTCC
- DTS

To go into a CENTCOM area of responsibility, you need a passport and should have completed an SRP, qualified on your weapon and drew out your gear through RFI. Some of these can be waived or agreements can be made, but most likely will involve USCYBERCOM leadership talking to USCENTCOM leadership.

Additionally, you can go on a mission without DTS orders, if your unit signs off on it. You will most likely have orders by the time of your arrival at your destination or by the time you get back off mission. DTS orders sometimes take a while to populate because everyone in your chain must approve the orders. DTS orders can be kicked back multiple times for errors or misunderstanding of information contained within.

Lastly, GTCC's are necessary to book your travel and lodging, and pay for your meals. If you do not have a GTCC or it is not activated in time, the unit can pay for the travel and lodging and then reimburse you for food once you submit your voucher, but this depends on your unit.

Closeout

During this exercise, you analyzed a team readiness roster and go-kit status to meet several potential mission scenarios.

For Further Discussion

Consider the following and discuss as a class:

1. How does the customer's network impact your go-kit?
2. How do the personnel on your team impact the readiness to deploy?

Lesson 3

Preparing Equipment for Operation Execution

Following the recovery from a previous mission, a deployment kit may remain packed until the next deployment. Prior to deployment, a CPT must update the systems in the go-kit to ensure new vulnerabilities and risks are not introduced to the supported mission commander's network. DCI squad members will exercise updating operating systems, software tools, sensor platforms and network gear to meet the current mandatory version per the toolkit documentation or to meet the supported commander's requirements. Students document the steps and actions taken and identify when they must elevate discrepancies or requirements gaps for software updates. Students also install and test threat intelligence signatures on sensor platforms.

Exercise 3.1-015.a - Updating and Wiping in Windows

Introduction

Objective: Update operational platforms

The successful completion of any mission starts with the proper preparation of both the personnel and the equipment they will be using. This includes ensuring that the response systems are up to date and that storage media has been properly prepared. In many cases updating the operating system of your device may be simplified by connecting it to a commercial internet connection. However, in other instances there may be security restrictions preventing systems from being connected to the commercial internet. This lack of a commercial connection does not mean that the device is not updated, it simply means that you must determine a way to download and manually update the system.

Action Summary

In this exercise, you will:

1. Use the updates supplied on the CD-ROM to manually update the Windows 10 x64 operating system.
2. Verify that the updates were correctly installed.
3. Answer questions about this exercise.

Resources

Manually Updating a Windows Operating System
https://support.microsoft.com/en-us/help/973135/how-to-download-a-windows-update-manually

Updating Windows 10 Manually
https://www.windowscentral.com/how-download-and-install-windows-10-cumulative-updates-manually

Microsoft Update Catalog
https://www.catalog.update.microsoft.com/Home.aspx

Update Windows

In preparation for an upcoming mission you will update your systems software and forensically prepare your incident recovery drive. Due to special security parameters, you are unable to connect your system to any commercial internet connection, requiring you to use files available to you

only on the CD-ROM. Update your Windows 10 x64 system and answer the following questions.

Security Updates

The Security Update for Windows 10 for x64-based Systems (KB3172729) has known issues. Review the below information and answer the following questions.

Microsoft KB3172729 Update

https://www.catalog.update.microsoft.com/ScopedViewInline.aspx?updateid=a22a74ea-2c3a-43e7-a6cb-ba01d71fc535

Microsoft Severity Levels

https://technet.microsoft.com/en-us/security/gg309177.aspx

Secure Boot Update

In some instances, there are dependencies that must be satisfied before an update can be installed. While not a true dependency, update KB3172729 does have certain software requirements in the form of services that must be met.

MS16-100: Description of the security update for Secure Boot: August 9, 2016

https://support.microsoft.com/en-us/help/3172729/ms16-100-description-of-the-security-update-for-secure-boot-august-9

Security Bypass Vulnerability

One of the reasons to keep your operating software up to date is to address vulnerabilities. Using the information relevant to the Windows10.0-KB3172729-x64.msu (Windows 10 Version 1511) update, locate any information pertaining to vulnerabilities associated with this update. Review the following link and answer the question.

Microsoft Windows CVE-2016-3320 Local Security Bypass Vulnerability

http://www.securityfocus.com/bid/92304/info

Wiping Media on Windows

1. Use the EnCase Forensic Imager wipe feature listed under Tools to wipe the incident response (IR) 5 GB drive.
2. Verify the drive was wiped with EnCase Forensic Imager.
3. Format and partition the 5 GB drive. Make sure you rename the new volume “IR Drive.”

Additional Resources

EnCase Forensic Imager Data Sheet

https://www.guidancesoftware.com/docs/default-source/document-library/product-brief/encase-forensic-imager.pdf?sfvrsn=12

Media Sanitization Guidelines

- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
- https://www.nsa.gov/resources/everyone/media-destruction/assets/files/storage-device-declassification-manual.pdf
- https://www.us-cert.gov/sites/default/files/publications/DisposeDevicesSafely.pdf

Closeout

In this exercise, you manually updated the Windows 10 x64 operating system, and forensically wiped, partitioned and formatted the storage drives in the standard Windows 10 x64 virtual machine.

For Further Discussion

Consider the following and discuss as a class:

1. What issues are encountered when a system cannot connect to the internet for updates?
2. What are some methods that can be used to address this?
3. Are there issues associated with manually downloading and updating a system from an external drive?
4. Updates are often in response to the discovery of vulnerabilities. Is it possible to know of every vulnerability to your system?
5. Were there any issues with using EnCase?
6. Are there any circumstances where a forensic wipe of a volume instead of a physical drive would be acceptable?

Exercise 3.1-063.a - Forensically Wipe Media for Deployment/Use

Introduction

Objective: Update operational platforms

The successful completion of any mission starts with the proper preparation of the personnel and the equipment they will be using. During the response, there may be opportunities to collect data and store it to digital media. Wiping media prior to an engagement ensures that new data collected is not contaminated or confused with previous engagement data.

Knowing what and how to wipe is only one part of the equation. The other is knowing when to wipe and reuse digital media. As a member of a CPT, you will often move between systems of different classifications, from the unclassified system to a classified system. In each case, the level of classification may dictate whether a drive can be sanitized and reused on one system or another. For example, it may be considered a security risk to use a drive that once held Secret level information on an unclassified system. Knowing the various levels, what can and cannot be used, is valuable information that any member of a CPT should be aware of to safeguard a mission owner's information.

Action Summary

In this exercise, you will:

1. Use software tools to forensically wipe, partition and format media to prepare it for use in data collection efforts.
2. Review relevant documents.
3. Answer questions regarding media sterilization.

Username and Password

System	Username	Password
Kali Server	root	toor

Resources

Media Sanitization Guidelines:

- https://www.nsa.gov/resources/everyone/media-destruction/assets/files/storage-device-declassification-manual.pdf
- https://www.us-cert.gov/sites/default/files/publications/DisposeDevicesSafely.pdf
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

EnCase Forensic Imager Data Sheet

https://www.guidancesoftware.com/docs/default-source/document-library/product-brief/encase-forensic-imager.pdf?sfvrsn=12

About dc3dd for Kali - Linux

http://tools.kali.org/forensics/dc3dd

Linux Man Pages

man <command> e.g., man dc3dd

Scenario 1

You have recently completed a mission at the Defense Red Switch Network. The incident involved several SIPR machines, routers and firewalls were compromised. During the response, you used all your CPT's removable media to store traffic captures and system images for response analysis.

After several long days of analysis, you have finally completed a review of the data. During the analysis of the recovered data, you have determined that the system was compromised, a root kit installed and numerous malicious files were located.

You have now received a task order (TASKORD) to deploy to another site for a protect mission. Joint Force Headquarters – DoD Information Networks (JFHQ-DoDIN) has requested your services to investigate a rogue USB device that was connected to a Joint Worldwide Intelligence Communications System (JWICS) Sensitive Compartmented Information Facility (SCIF) terminal. Upon arrival, it was determined that to ensure a complete and effective response you would need to acquire system images from affected systems within the SCIF. Unfortunately, the SCIF is composed of numerous machines that will once again require the use of all your storage media, which because of the immediate re-deployment you were unable to properly sanitize. The CPT does not have the funding to purchase new hard drives.

Scenario 2

You have just completed a mission at JFHQ-DoDIN. While in route back to your office, your team has received another TASKORD stating that you will deploying immediately for an active incident. The incident is located at the Fort Meade Family and Morale, Welfare and Recreation (MWR) office.

The command has reported that an employee on the Non-Classified Internet Protocol Router (NIPR) had clicked on an attachment contained in an unsolicited email. Shortly after, the Network Administrator noticed a significant degradation in services and identified a beacon that was sending pings to an unknown IP address. The System Administrator believes he has isolated the affected systems. The Mission Commander has requested that you respond to determine how the system was compromised and to what extent. Upon arrival, you determine the most efficient manner to address the request is to obtain images of the affected systems and compare them to previously acquired known base images.

Closeout

In this exercise, you used software tools to forensically wipe, partition and format media to prepare it for use in data collection efforts.

For Further Discussion

Consider the following and discuss as a class:

1. What tools were used to wipe the drive?
2. What other tools available could be used to forensically wipe the storage drive?
3. What are the advantages/disadvantages of using EnCase Forensic Imager versus dc3dd?
4. Are there any special considerations about reuse of media that a CPT may encounter?
5. Are there scenarios that allow for media reuse?
6. What about scenarios that do not allow media reuse?

Exercise 3.2-051.a - Predeployment Configuration and Testing of GRR Rapid Response

Introduction

Objective: Update sensor platforms

Background: Testing and configuring the CPT toolkit prior to deployment is vital. Prior knowledge of the supported command's network is required to understand what tools will need to be updated and/or reconfigured. Deploying to a site with a toolkit that has not been properly tested and configured for that environment will waste time and valuable resources, reducing the CPT's ability to conduct their mission.

Scenario

After returning from a mission, a squad member has reinstalled and tested the GRR Server for a standard CPT baseline. They have asked you to test and verify that the new configuration is correct and works as intended.

In this lesson, you will prepare and test an installed instance of GRR Rapid Response. This testing will include configuring the GRR server, enrolling a client to the GRR server with the help of a GRR agent, and verifying everything is properly prepared prior to deploying to the supported commands network.

Action Summary

In this exercise, you will:

1. Verify the proper configuration of the GRR server.
2. Deploy a GRR agent to the Windows 10 x64 machine.
3. Verify successful deployment by running test flows.
4. Answer questions about this exercise.

Usernames and Passwords

System	Username	Password
GRR Server	root	toor
GRR Web UI	dcistudent	P@ssw0rd
Windows 10 x64	dcistudent	P@ssw0rd

Resources

GRR Rapid Response Documentation

https://grr-doc.readthedocs.io/en/latest/

- GRR Administrator Manual
- Installing GRR Clients
- Troubleshooting Clients
- GRR Flows
- GRR Hunts

Closeout

In this exercise, you updated sensor platforms by preparing an installed instance of GRR Rapid Response, including configuring the GRR server and enrolling a client.

For Further Discussion

Consider the following and discuss as a class:

1. As a CPT, why is it important to understand what environment you will be working in, with respect to the compatibly of your systems to the supported command's systems?

Exercise 3.2-075.a - Use PowerShell to Collect Data

Introduction

Objective: Update sensor platforms

While it is theoretically possible for a DCI team to physically visit and log into each system directly, the speed and action time is dramatically increased when the information collection can be done remotely or even batched together.

PowerShell is a task-based, command-line shell and scripting language designed especially for system administration. It can be used by a DCI team to collect data from a Windows operating system and from applications that run on Windows.

Scenario

One of the hosts you have been tasked to collect information from is not allowing GUI access, however, the PowerShell remote service is active on the system. You have been directed to perform host reconnaissance on the system using PowerShell and to attempt to restore full GUI access to the system.

Background: PowerShell can be used remotely to both gather information and to manipulate data on remote machines. While PowerShell can be used locally as well, sometimes that is not feasible. For example, the machine may be physically far away, or many machines may need the same script executed.

In this exercise, you will use PowerShell to remotely gather information such as users, registry keys and hard drives on the remote machine. PowerShell can also be used to remotely manipulate systems. Therefore, after collecting the necessary data, you will also use remote PowerShell to enable the machine to be used locally by the user.

Action Summary

In this exercise, you will:

1. Review resource documents.
2. Use PowerShell to collect system data from a host machine.
3. Answer questions in this exercise.

Any additional resources you choose to use are acceptable for this activity.

Working with PowerShell

PowerShell includes extensive documentation in the Microsoft Developer Network (MSDN) as well as locally within PowerShell using the cmdlet "Get-Help."

Get-Help can search for information on a cmdlet (such as 'Get-Help Get-Process') or general information about PowerShell topics (such as 'Get-Help about_WMI_cmdlets').

NOTE: If you plan to use Get-Help, be sure to run "Update-Help" while connected to the Internet before departing to a home station.

NOTE: You will have to develop a ping sweep PowerShell Script in order to find the target Windows IP address. Then you will have to remote into that box from your Windows 10 machine using PowerShell. Use Google to figure out how to create a PowerShell script that will ping the subnet. There are multiple ways to do it. If you have trouble, ask the instructor for help!

NOTE: When entering in the Enter-PSSession command ensure you do not use -Credential option (just for this exercise)!

Resources

Click on each of these report links before proceeding.

General PowerShell

https://msdn.microsoft.com/en-us/powershell/scripting/powershell-scripting

Windows PowerShell 5.0

https://msdn.microsoft.com/en-us/powershell/reference/5.1/microsoft.powershell.core/about/about_windows_powershell_5.1

Windows PowerShell PSSession

https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enter-pssession?view=powershell-6

Provided

PowerShell for Responders: Cmdlets and Syntax Resource Guide

Closeout

In this exercise, you used PowerShell to remotely collect reconnaissance information from a Windows host. Using remote PowerShell can quickly provide access to domain-connected systems and speed up host analysis.

For Further Discussion

Consider the following and discuss as a class:

1. What is needed to run a PowerShell script or command remotely?
2. What various types of information can be collected this way?
3. Did you try to run process explorer? Were there any challenges with this? Why?
4. What cannot be performed with a remote PowerShell script?

Exercise 3.2-050.a - Install SecurityOnion and Test Configuration

Introduction

Objective: Update sensor platforms

Testing and configuring the CPT toolkit prior to deployment is vital. Prior knowledge of the supported command's network is required to understand what tools will need to be updated and to what version. Not everything is compatible. Deploying to a site with a toolkit that has not been properly tested and configured for that environment will waste valuable resources and reduce the CPT's ability to conduct their mission.

In this exercise, students will be installing a SecurityOnion sensor on the network to monitor for malicious traffic. After the sensor is installed, students will then test their configurations to ensure that the sensor is working as expected prior to conducting their mission.

Scenario

You have been asked to deploy a remote network sensor and ensure that the collection occurring is sent to a centralized collection server.

Action Summary

In this exercise, you will:

1. Configure a SecurityOnion server.
2. Configure a SecurityOnion sensor.
3. Ensure the sensors are configured to collect traffic and rules can be applied.
4. Answer questions pertaining to this exercise.

Resources

SecurityOnion Installation
https://github.com/Security-Onion-Solutions/security-onion/wiki/Installation

SecurityOnion Cheat Sheet
https://github.com/Security-Onion-Solutions/security-onion/wiki/Cheat-Sheet

SecurityOnion Production Deployment
https://github.com/Security-Onion-Solutions/security-onion/wiki/ProductionDeployment

SecurityOnion Post-installation

https://github.com/Security-Onion-Solutions/security-onion/wiki/PostInstallation

APT1 IOC List

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/comment_crew_indicators_of_compromise.pdf

Closeout

In this exercise, you installed a SecurityOnion sensor on the network, monitored for malicious traffic and tested the configuration to ensure that the sensor is working as expected.

For Further Discussion

Consider the following and discuss as a class:

1. What is the importance of having a server and multiple sensors, as opposed to multiple individual sensors?
2. What are some reasons that an alert would not show on the server?

Exercise 3.3-045.a - Create Filesystem Artifact IOCs for GRR

Introduction
Objective: Apply threat intelligence signatures to sensor platforms

Scenario
Background: The CTE squad has successfully emulated APT1's toolkit. The DCI CND Manager wants you to use GRR to employ the CTE test executable to test IOC artifact identification on your Windows 10 system.

Indicators of compromise are crucial to the hunt mission. IOCs allow the DCI squad to comb through massive amounts of data to identify if there is a pre-existing or active intrusion inside a network. Creating simple IOCs may be an easy task for most but will yield many false positives that will require time and other resources to verify. IOCs created by the DCI squad should be specific and complex enough to reduce false positives and identify the necessary data needed to confirm a malicious activity has taken place.

In this exercise, students will create filesystem artifacts for current IOCs and test them through GRR to ensure proper results before deployment. Students will create flows in GRR to check the filesystem of a suspected compromised machine. After the flow is created, students will test to ensure that they acquire valid results.

Action Summary
In this exercise, you will:
1. Use the File Finder GRR flow to test filesystem-based IOCs.
2. Review the GRR documentation.
3. Answer questions about the exercise.

Resources
GRR Rapid Response Website
https://grr-doc.readthedocs.io/en/latest/
- GRR Flows
- GRR File Finder Syntax
- GRR Registry Finder Syntax
- GRR User Guide

APT1 IOCs

The DCI All Source Intel Analyst has identified the following filenames in APT1 related reporting:

- AdobeARM.exe
- iTunesHelper.exe
- AdobeRe.exe
- rouj.exe
- iexplore.exe
- wuauclt.exe
- adobeup.exe
- AdobeUpdater.exe
- NTLMSVC.DLL
- adobe_sl.lnk
- runinfo.exe

The APT1 report is located in the resources folder. The resources folder should be located on the Desktop and look like a CD-ROM. If you do not see it on the Desktop, it should be added as a Drive (usually the D or E Drive). Use the report to find out exactly where APT1 puts this malware. It will guide you when conducting your searches.

CTE Provided Executable

CTE has provided an executable that exhibits APT1 characteristics. Open the exercise folder on the desktop and run the AdobeUpdater.exe.

Closeout

In this exercise, you used GRR to check a system for different IOCs. You identified malicious files on a system and collected attributes about the file including the hash value, size and date/time stamps.

For Further Discussion

Consider the following and discuss as a class:

1. What are some of the advantages/disadvantages to using a flow instead of a hunt?
2. What are some of the reasons that a File Finder flow would not produce expected results?

Exercise 3.3-048.a - Create Memory and Registry Artifacts IOCs for GRR

Introduction

Objective: Apply threat intelligence signatures to sensor platforms

Indicators of compromise are crucial to the hunt mission. IOCs allow the DCI squad to comb through massive amounts of data to identify if there is a pre-existing or active intrusion inside a network. Creating simple IOCs may be an easy task for most. For some, however, it will yield a lot of false positives that will require time and other resources to verify. IOCs created by the DCI squad should be specific and complex enough to reduce false positives and identify the data necessary to confirm a malicious activity has taken place.

Scenario

The CTE squad has successfully emulated APT1's toolkit. The DCI CND Manager wants you to use GRR to employ the CTE test executable to test IOC artifact identification on your Windows 10 system.

Action Summary

In this exercise, you will:

1. Create memory and registry artifacts for current IOCs and test them through GRR to ensure proper results before deployment.
2. Create a flow in GRR to check the memory and registry of a suspected compromised machine. Test to ensure you acquired the correct results.

Identify Registry IOCs

Use GRR to identify the registry-based IOCs APT1 is known to use.

Registry IOCs

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Acroread"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Adobe Update"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"AdobeCheck"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"AdobeCom"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"IMSCMig"

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"McUpdate"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Register"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"SysTray"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"systemupdate"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"wininstaller"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"APVSVC"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"AdobeUpdate"

RESOURCES

Rekall Plugins

http://www.rekall-forensic.com/documentation-1/rekall-documentation/plugins

APT1 Mutex

https://www.fireeye.com/blog/threat-research/2013/02/threat-actors-mandiant-apt1-report-spear-phishing-nitty.html

GRR Rapid Response Documentation

https://grr-doc.readthedocs.io/en/latest/

- GRR Flows
- GRR Registry Finder

Identify Registry IOCs

Use GRR to identify the registry-based IOCs APT1 is known to use:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Acroread"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Adobe Update"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"AdobeCheck"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"AdobeCom"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"IMSCMig"

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"McUpdate"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"Register"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"SysTray"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"systemupdate"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"wininstaller"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"APVSVC"
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"AdobeUpdate"

Closeout

In this exercise, you executed the CTE-provided executable and performed memory analysis with GRR and Rekall.

For Further Discussion

Consider the following and discuss as a class:

1. What are some reasons that a Registry Finder flow would not produce expected results?
2. What are some reasons that a memory analysis flow would not produce expected results?
3. What are some reasons that you used a certain Rekall plugin argument and why?

Exercise 3.3-046.a - Create Network Traffic IOCs for Snort

Introduction

Objective: Create network traffic IOCs for Snort

Scenario

USCYBERCOM J2 has provided a packet capture (pcap) of APT1 activity recently captured on another mission. The DCI CND Manager has tasked you with creating Snort rules for the network traffic IOCs. The DCI Intel Analyst has compiled a list of network IOCs from threat reports previously provided. Use that list with the pcap capture to identify network IOCs.

Background: Indicators of compromise are pieces of forensic data found in system log entries or files, that can potentially identify malicious activity on a system or network. IOCs aid information security and IT professionals in detecting data breaches, malware infections or other threat activity. By creating and monitoring IOCs, organizations can detect attacks and act quickly to prevent breaches from occurring or limit damages by stopping attacks in the earlier stages. IOCs are an important component in the battle against malware and cyberattacks.

Action Summary

In this exercise, you will:

1. Create Snort rules from the IOC list created by the Intel Analyst.
2. Use the tools available to create Snort rules for the IOCs identified.
3. Use pcap with Tcpreplay and SecurityOnion to validate Snort rules.

Resources

WireShark

https://www.wireshark.org/docs/

Snorpy

http://snorpy.com/

Snort

https://snort.org/documents

TCPREPLAY

http://tcpreplay.synfin.net/tcpreplay.html

Scenario 1: Validate Signatures

A DCI squad member has created two snort rules for one domain name and one IP address. Unfortunately, they have been re-tasked for guard duty. The DCI squad manager has tasked you to use validate the two snort rules created using SecOnion and the pcap provided.

Validate the Snort rules below using SecOnion, Tcpreplay and the pcap that has been provided.

Snort Rules Provided:

alert udp any any -> any any (msg:"Known Good Domain"; content:"google"; sid: 1000117;)

alert ip any any <> 172.27.2.3 any (msg:"Known Good IP"; sid: 10000145;)

NOTE 1: There must be a space between "sid: " and the number. The custom SIDs must start at 1,000,000 (no commas, commas here for clarity).

NOTE 2: You can test these rules by editing the rules file, then performing a rule update and then using Tcpreplay to replay test traffic using options to maximize the speed of the replay and preloading the traffic into memory.

Scenario 2: Develop New Signatures

1. Using the IOC list below, create the rest of the Snort rules in one file.
2. Using SecOnion and Tcpreplay and the pcap provided, validate the Snort rules created are correct.
3. Answer questions on the next page.

Background: There are three malicious domain names and two malicious IP addresses in the pcap. Provided are previously created Snort rules for two of the malicious domain names and one malicious IP addresses:

alert udp any any -> any any (msg:"DNS Request for EPAC"; content:"epac"; sid: 100002;)

alert udp any any -> any any (msg:"DNS Request for drgeorges"; content:"drgeorges"; sid: 1000003;)

alert ip 202.39.61.136 any -> any any (msg:"Known Bad Traffic"; sid: 1000004;)

NOTE 1: There must be a space between "sid: " and the number. The custom SIDs must start at 1,000,000 (no commas, commas here for clarity).

Here is the full list of IOCs from the Intel Analyst.

Provided Documentation
APT1_IOCs_Intel

NOTE 2: Domain names that have a period (.) in front had names removed to protect the victim.

NOTE 3: While conducting WireShark analysis could yield the desired results in this small pcap sample, it is not recommended. Students will have a difficult time conducting WireShark analysis on the test due to time constraints, the size of the IOC list and the pcap size. It is recommended that Snort rules be created for the entire IOC list in order to be successful for the rest of the course.

Closeout

In this exercise, you used traffic from a known malicious APT1 incident to validate signatures you created for Snort using IOCs provided by an Intel Analyst. Developing signature sets like these is a core capability required to identify known malicious activity on a defended network.

For Further Discussion
Consider the following and discuss as a class:

1. What does Tcpreplay do?
2. Why did it play an important part for this activity?
3. You may not be able to obtain network traffic that contains known threat activity. What is another way to validate signatures built for a specific threat agent?

MODULE 3

Survey Stage Actions

Module 3 introduces tasks that are common for DCI squads to undertake during the survey stage of a mission. Activities the DCI squad is expected to have proficiency in for the survey stage include: coordinating with local cyber network defenders, performing network reconnaissance and collection, and performing host reconnaissance and data collection.

Lesson 1

Working with Supported Mission System Administrators

Students use system administrator documentation to identify network topology (network documentation) and subnets with a focus on the previously identified KT-C. Students will take the network topology into account when developing a sensor strategy that meets key objectives for observing traffic transitioning KT-C and ensuring visibility to high-probability targets based on threat intelligence. Students will work with typical baseline image formats to develop "known good" baseline datasets for integration in analysis and hunt activities.

Exercise 4.1-020.a - Document Network Segments/Subnets and Topology Based on Network Maps

Introduction

Objective: Document network segments and topology

CPTs are often provided with network maps by the local CNDs when performing a survey mission. While network maps may be inaccurate, it can be a good baseline to compare to when performing scans to verify the network.

While it is important to verify the network map with your own scans, understanding how the network should be mapped is important. By understanding the current network documentation, you can establish specific differences between the provided documentation and the actual current state of the network.

For example, by performing an Nmap scan, you will find all available devices from your network location. However, if you do not understand that a certain subnet should have been available to you based on current network documentation, then it would not come to your attention to document this. Therefore, it is important to understand the flow and topology of provided network documentation.

Scenario

Your CPT has been provided a network map for your mission. Use this documentation to determine the organization of the network.

Action Summary

In this exercise, you will:

1. Perform network scans with Nmap against the customer network.
2. Compare and contrast the results of the Nmap scan with the provided network map.
3. Answer questions provided in the exercise.

Resources

Nmap Cheat Sheet

https://blogs.sans.org/pen-testing/files/2013/10/NmapCheatSheetv1.1.pdf

Provided Documentation:

Network Map

Closeout

In this exercise, you documented a network based on the provided network map. By understanding the network documentation, you gained understanding of the expected network flow and topology of the network. This understanding is vital to verifying the network using active scanning techniques.

For Further Discussion

Consider the following and discuss as a class:

1. Why is understanding what is on the network important to the success of the mission?
2. What are some other aspects of the mission environment that should be documented?
3. What are some reasons the current state of the network may be different from the network documentation provided?

Exercise 4.1-021.a - Determine Traffic Routes Based on Network Topology Maps

Introduction

Objective: Identify network topology and subnets

After understanding the general topology, organization and devices on the network, the next step is to analyze the network flow that the topology generates. Questions of availability and confidentiality should guide your analysis.

This analysis will be essential to determining the best sensor placement for intrusion detection systems, as well as a baseline to verify against, when performing your own scans of the network. It is also a great tool for troubleshooting network issues and determining threat vectors for attacks.

Scenario

Your CPT has received a network map for your mission. Use this documentation to determine the network flow of the entire system.

Action Summary

In this exercise, you will:

1. Analyze network maps provided to consider potential adversary routes.
2. Answer questions in the exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources

This exercise uses two network diagrams you can find linked below.

Single Site Network
Multi-site Network

Closeout

In this exercise, you determined and analyzed the potential network traffic flow based on provided documentation. This is essential for further steps in the survey mission and is valuable for many other missions such as protect and recovery.

For Further Discussion

Consider the following and discuss as a class:

1. What are some questions to ask when analyzing network flow based on network documentation?
2. What are some device configurations that should be analyzed to verify the network flow is as intended?

Exercise 4.2-023.a - Develop Sensor Strategy - Placement of Sensors

Introduction

Objective: Develop sensor strategy

Background: Any capability that provides insight into the operation of an asset within the defended network can be considered a sensor. More specifically, sensors are typically considered the capabilities that the CPT deploy into the defended network. Sensors provide data feeds that can potentially identify adversary activity. Sensors can also be used in conjunction with IOCs to identify observables consisted with adversary activity.

Within this broad definition of a sensor, the CPT typically considers sensors in "network" and "host" categories. Network sensors could be as simple as configuring log aggregation from a Cisco ASA firewall. They can be as advanced as a 40 Gbps passive fiber optic network tap that allows IDS signatures to be run on every frame and packet traversing the network segment. Host sensors can be as simple as a PowerShell script that collects information for a specific endpoint; they typically include agent-based capabilities that report back to a central authority like GRR or Host Based Security System (HBSS).

Building a sensor strategy starts with understanding how activity on a network takes place. Every network segment, device and endpoint involved in a network-based data flow provides an opportunity to observe adversary activity.

Action Summary

In this exercise, you will:

1. Consider a variety of network configurations and devices that will be found in nearly every network.
2. Consider different elements that go into developing a sensor strategy with the end goal of observing adversary activity.
3. Review external links.

Resources

Basic Network Device Logging

https://www.sans.org/reading-room/whitepapers/logging/logging-monitoring-detect-network-intrusions-compliance-violations-environment-33985

Learn about Netflow from Cisco Documentation

https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html

Network Traffic Logging

https://www.sans.org/reading-room/whitepapers/logging/importance-logging-traffic-monitoring-information-security-1379

IDS and IPS Deployment Strategies

https://www.sans.org/reading-room/whitepapers/detection/network-ids-ips-deployment-strategies-2143

Closeout

In this exercise, you applied your knowledge and understanding of network protocols to identify how traffic is observed in a variety of network conditions/situations.

For Further Discussion

Consider the following and discuss as a class:

1. How does Network Address Translation (NAT) affect IP addressing on a network?
2. How do routers affect Media Access Control (MAC) addresses as identified on a network?
3. What are some challenges you may face in interpreting traffic from multiple points of monitoring on a network?

Exercise 4.2-025.a - Develop Sensor Strategy - Place New Sensors and Re-use Local Resources

Introduction

Objective: Develop sensor strategy

Network intrusion detection systems (NIDSs) can be composed of many sensors which monitor the traffic flowing in the network. Deciding where sensors should be placed and what information they need to detect the desired attacks can be a demanding task for network operators. The development strategy for placing new sensors or reusing local sensors is critical in forming the eyes and ears of any network intrusion detection system.

Scenario

The CPT has multiple missions going on simultaneously:

- Ninety-Two Pines Air Ground Base
- Victorville Naval Air Base

Teams deployed to the other missions need help with their sensor deployment plan. This is their first time on a mission and they do not have the experience nor the knowledge. The CND Manager has tasked you to help the other teams, since you are the most senior DCI member. The other squad members will tell you what they plan to do before they do it. You must choose the best course of action and provide an explanation on why it is the best choice.

Background: In the following three scenarios, students will develop strategies for placing network sensors correctly throughout the networks, which is crucial to successfully implement the intrusion detection system. Before deploying sensors however, they will thoroughly understand the network topology documentation, as well as the critical systems on the network provided by Intelligence Reports that attackers will attempt to compromise (through). Additionally, students will identify where on the network to deploy sensors and how to configure these sensors to maximize their effectiveness toward protecting the network. Students will be able to choose locations where new sensors will be placed as well as choose which existing sensors will need to be reused.

Action Summary

In this exercise, you will:

1. Develop strategies for placing network sensors correctly throughout the network.
2. Identify on the network where to deploy, configure or reuse sensors to maximize their effectiveness toward protecting the network.
3. Review the resources provided.
4. Read the given scenarios and answer questions for this exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources

Sensor Placement - SANS

https://www.sans.org/reading-room/whitepapers/detection/network-ids-ips-deployment-strategies-2143

Sensor Placement

http://www.mecs-press.org/ijisa/ijisa-v6-n2/IJISA-V6-N2-8.pdf

Closeout

In this exercise, you developed strategies for placing network sensors correctly throughout the network and identified where on the network to deploy, configure or reuse sensors to maximize their effectiveness toward protecting the network.

For Further Discussion

Consider the following and discuss as a class:

1. What are some limitations that will impact sensor placement?
2. Assuming the asset is within your area of operation and you are able to meet any limitations on downtime, why would installing new sensors be problematic for the DCI mission?
3. What are the challenges posed by using native capability instead of installing the CPT's sensors in the environment?

Exercise 4.3-026.a - Receive and Process Baseline System Image

Introduction

Objective: Receive and process baseline system images

CPT members must differentiate normal host and network artifacts from ones that are abnormal to determine potential malicious activity. One method of doing so is using a baseline image or data and comparing that data to the current state of the machine.

Scenario

The supported command has given the CPT a host baseline. The CND Manager has tasked you to conduct a comparative analysis against the baseline on the live Windows 10 host machine.

Background: A baseline image is a "known-good" clean system image that is used to deploy new systems. This image can be used to determine differences between the system at the time of installation and its current state. Every change to the system will be revealed by a comparative analysis of the baseline and the current state. Some changes are likely authorized or necessary updates, while other changes may be malicious.

Action Summary

In this exercise, you will:

1. Review the resource documents.
2. Compare the baseline image to the live host machine.
3. Compare the memory given to the CPT against the live host machine's memory.
4. Answer the questions about the above action items.

Any additional resources you choose to use are acceptable for this activity.

Resources

Volatility

https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#

FTK Imager

https://support.accessdata.com/hc/en-us/articles/204056525-FTK-User-Guide

Sysinternals' Handle

https://docs.microsoft.com/en-us/sysinternals/downloads/handle

Closeout

In this exercise, you used FTK Imager and Volatility to process disk and memory baselines. By comparing the current system to a baseline, you can quickly find differences, which can be investigated to determine malicious activity.

For Further Discussion

Consider the following and discuss as a class:

1. What are some artifacts, both on the hard drive and in memory, that are useful to compare from the baseline to the current system?
2. What are some of the limitations of the usefulness of a baseline?

Lesson 2

Performing Survey Stage Network Reconnaissance

Students will use a variety of host discovery tools to identify active nodes on a network and will be introduced to tools typically used for host discovery at various layers of the Open Systems Interconnection (OSI) model. Students will use command-line and GUI-based tools to monitor network traffic and identify typical traffic for the network they are monitoring.

Exercise 5.1-027.a - Perform Nmap Scan for Endpoint Identification

Introduction

Objective: Scan the network to identify endpoints

In this exercise, we will use Nmap to perform host enumeration in different network segments. Nmap is often called the "Swiss Army Knife" of network scanning – you can perform a variety of scans designed to enumerate network devices and even evade certain security capabilities to successfully identify endpoints.

Scenario

Having a variety of methods at your disposal to perform endpoint identification can be important. Network host identification is typically performed passively, however, sometimes more aggressive approaches are necessary.

Action Summary

In this exercise, you will:

1. Use Kali Linux, Nmap and the special network to perform scans against "192.168.13.17" and record the information returned.
2. Use Kali Linux, Nmap and the special network to perform a quick scan with OS detection against "192.168.13.1/24" and record information for endpoints not shown on the network map.
3. Answer the questions within the exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources

Nmap Documentation

www.nmap.org

Nmap Cheat Sheet

https://highon.coffee/blog/nmap-cheat-sheet/

Linux Man Tool for Nmap

man nmap

Closeout

In this exercise, you used Nmap to identify endpoints and identify basic characteristics based on port numbers and expected protocols.

For Further Discussion

Consider the following and discuss as a class:

1. How does Nmap identify the operating system of a host on the network?
2. What are some advantages of using Nmap for host identification?
3. Why would a CPT prefer to use a passive approach to host identification during the survey phase of a mission?

Exercise 5.1-028.a - Develop Rudimentary Ping Scan

Introduction

Objective: Scan the network to identify endpoints

It is important to have multiple methods available to perform endpoint identification since firewalls, intrusion prevention systems (IPS) and other network security devices may limit the full view of the network. One approach to scanning a network is to use Nmap.

In this exercise, students will be developing a script to perform a ping sweep. This will perform endpoint identification if other forms, such as Nmap, are unavailable.

Scenario

Due to deconfliction with the Participative Defensive Evaluation (PDE) being performed by the CTE squad, you are not authorized to use Nmap for endpoint identification, but must continue scanning the network to identify endpoints. DCI will have to quickly develop a ping scanning tool using Windows resources.

Action Summary

In this exercise, you will:

1. Create an alternative method of scanning for host identification using built in capabilities.
2. Answer questions within the exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources

Ping Sweep with PowerShell

https://www.petri.com/building-ping-sweep-tool-powershell

Port Checker with PowerShell

https://www.petri.com/building-a-powershell-ping-sweep-tool-adding-a-port-check

Ping Sweep with Command Line
https://en.wikiversity.org/wiki/Computer_Networks/Ping/Sweep

PowerShell Scripting Cookbook
https://docs.microsoft.com/en-us/powershell/scripting/powershell-scripting?view=powershell-5.1

Writing Scripts with PowerShell
https://docs.microsoft.com/en-us/powershell/scripting/core-powershell/ise/how-to-write-and-run-scripts-in-the-windows-powershell-ise?view=powershell-5.1

Writing Batch Scripts
https://www.howtogeek.com/263177/how-to-write-a-batch-script-on-windows/

Command Line Reference
https://technet.microsoft.com/en-us/library/bb490890.aspx

Closeout

In this exercise, you created scripts to perform host identification based on specific ports.

For Further Discussion

Consider the following and discuss as a class:

1. Could this script be performed or developed in other ways?
2. What are some of the methods that you used to tailor your outputs?
3. What are some other methods or tools that could be used to perform endpoint identification?

Exercise 5.2-031.a - Perform Traffic Analysis using WireShark

Introduction

Objective: Conduct traffic analysis

Analyzing network traffic is a critical skill for any intrusion analyst. In this exercise, you will analyze a short traffic capture to identify some common malware behaviors that are observed on the network.

Scenario

The local CND decided to conduct an audit of an endpoint's network traffic and has provided you with a sample from the endpoint. Use WireShark to analyze the sample traffic for potentially malicious activity.

Action Summary

In this exercise, you will:

1. Analyze network traffic with WireShark to identify signs of malicious activity.
2. Answer questions pertaining to this exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources

WireShark: Display Filters
https://wiki.wireshark.org/DisplayFilters

WireShark User's Manual
https://www.wireshark.org/docs/wsug_html_chunked/

Symantec Security Response: Indicators of Compromise
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/comment_crew_indicators_of_compromise.pdf

Closeout

In this exercise, you analyzed a network traffic capture to identify malicious or potentially malicious network activity.

For Further Discussion

Consider the following and discuss as a class:

1. What is the process of finding interesting or unique network activity?
2. What are some tools or filters in WireShark to help in this process?
3. What would be the advantages and disadvantages of collecting on a switch or network tap?
4. What type of configuration or placement would be necessary to accomplish this?

Exercise 5.2-076.a - Analyze Obfuscated Traffic

Introduction

Objective: Conduct traffic analysis

Malware will frequently use a variety of methods for command and control that appear like typical web traffic but are obfuscated (hidden) to make detection difficult. This exercise will introduce you to several forms of obfuscation and develop your capability in identifying and analyzing more advanced network traffic.

Scenario

Analyzing network traffic is a critical skill for an intrusion analyst. While we have looked at network traffic from aggregate perspectives (netflow, network statistics by host, etc.) we have yet to conduct more in-depth analysis of network traffic. In this exercise, you will have the opportunity to use more advanced searching and extraction capabilities in WireShark to analyze network traffic and the artifacts contained within.

During this exercise, you will gain proficiency analyzing network traffic and web traffic to discover foretelling information and locate prescient artifacts, extract the specific artifact and conduct follow-on analysis of the artifact.

Action Summary

In this exercise, you will:

1. Perform analysis and extraction of artifacts in network traffic using a variety of tools.

Resources

You will likely find the following resources helpful as you perform analysis.

Click on each of these report links before proceeding.

File Signatures

https://www.garykessler.net/library/file_sigs.html

User Agent Strings

https://www.sans.org/reading-room/whitepapers/malicious/user-agent-field-analyzing-detecting-abnormal-malicious-organization-33874

Malware Obfuscation Approaches
https://blog.malwarebytes.com/threat-analysis/2013/03/obfuscation-malwares-best-friend/

Scenario Update

The local cyber defense capability received an intrusion detection system alert identifying an unknown User Agent string leaving the defended network.

Learn more about how User Agent strings can impact network analysis then continue to the next questions.

The User Agent Field: Analyzing and Detecting the Abnormal or Malicious in your Organization
https://www.sans.org/reading-room/whitepapers/malicious/user-agent-field-analyzing-detecting-abnormal-malicious-organization-33874

Scenario Update

The network defenders were able to identify the malware running on the client and have restored the system to a known good. Use what you learned from the command and control to identify other hosts that may be impacted by a similar strain of malware.

NOTE: Malware may morph over time and take on new characteristics of methods of obfuscating information. You may want to learn more about obfuscation techniques commonly used by threat agents.

Malwarebytes - Obfuscation: Malware's best friend
https://blog.malwarebytes.com/threat-analysis/2013/

Closeout

Malware will frequently use a variety of methods for command and control that appear like typical web traffic but are obfuscated to make detection difficult.

For Further Discussion

Consider the following and discuss as a class:

1. How did you identify traffic that contained a JPEG image? How did that differ from identifying the PNG image or the executable?
2. Once you identified the executable, how did you identify the name of the file?

3. What were some of the similarities between the malware command and control features you identified in the last two sequences of communications? How did you approach the challenge of the Base64 encoded data?

Lesson 3

Performing Survey Stage Host Reconnaissance

Students will use a variety of host discovery tools to identify active nodes and their associated ports and services on a network. Students will identify specific services and service versions in use on the hosts and will perform analysis of volatile and non-volatile data using host-based sensors and scripting tools to identify active threats.

Exercise 6.1-034.a - Scan Network Hosts to Identify Ports and Services

Introduction

Objective: Scan the network to identify ports and services

Scenario

It is important to have multiple methods available to scan the network to identify ports and services since Firewalls, intrusion prevention systems and other network security devices may limit the full view of the network. One approach to scanning a network is to use Nmap. The second approach to scanning the network to identify ports and services is using the capabilities of the packet sniffing tool WireShark.

Action Summary

In this exercise, you will:

1. Use Nmap and the special network to perform port scans to include services and operating system information on each machine. When performing these scans, ensure you can see the progress of the scan. Record the information collected for each machine.
2. Use Nmap to perform a banner grabbing scan on each machine. When performing these scans, ensure you can see the progress of the scan. Annotate information that is different than the previous scans completed in the previous action.

Resources

Nmap

https://nmap.org/

Commands in Nmap

https://highon.coffee/blog/nmap-cheat-sheet/

Conducting a Port Scan in Nmap

https://nmap.org/book/man-port-scanning-techniques.html

Conducting a Service Scan in Nmap

https://nmap.org/book/vscan.html

Banner Grabbing in Nmap

https://nmap.org/nsedoc/scripts/banner.html

Closeout

Using Nmap, you scanned network devices to identify their open ports and services. Using the WireShark tool, you confirmed the information gathered in Nmap was correct information.

For Further Discussion

Consider the following and discuss as a class:

1. What are some reasons to use the WireShark tool instead of the Nmap tool?
2. Why would you confirm information collected with more than one tool?

Exercise 6.1-036.a - Scan TCP Ports with Nmap

Introduction

Objective: Scan the network to identify ports and services

It is important to have multiple methods available to scan the network to identify ports and services since firewalls, intrusion prevention systems and other network security devices may limit the full view of the network. One approach to scanning a network is to use Nmap. The second approach to scanning the network to identify ports and services is using WireShark.

Scenario

Background: You have been tasked with verifying the topology of the mission's network. Your CND Manager has provided you with a network map.

Your area of operation consists of the following subnets:

172.29.224.0/19
192.168.13.0/24
10.0.0.0/24

Confirm that the given network map is valid, and document any differences.

Action Summary

In this exercise, you will:

1. Use Nmap to perform a banner grabbing scan on endpoints and open TCP ports identified in the last exercise. When performing these scans, ensure you can see the progress of the scan. Record the information collected for each machine.
2. Answer questions pertaining to this exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources

About Nmap
https://nmap.org/

Technical Reference for commands in Nmap
https://highon.coffee/blog/nmap-cheat-sheet/

Technical Reference for conducting a port scan in Nmap
https://nmap.org/book/man-port-scanning-techniques.html

Technical Reference for conducting a service scan in Nmap
https://nmap.org/book/vscan.html

Technical Reference for banner grabbing in Nmap
https://nmap.org/nsedoc/scripts/banner.html

WireShark Statistics Menu
https://www.wireshark.org/docs/wsug_html_chunkedChUse StatisticsMenuSection.html

Closeout

In this exercise, you used Nmap to scan the AO to determine if the network map was valid.

For Further Discussion

Consider the following and discuss as a class:

1. What differences were found on the network in this exercise? What are some other types of differences you could find on a network?
2. Why is manual verification through banner grabbing an important capability/skill?
3. What are some other tools that can be used to map out the local network?

Exercise 6.2-077.a - Analyze a Security Event Log

Introduction

Objective: Conduct host analysis to identify threat attribution

The Windows Event Logs provide a record of significant events that have taken place on a system and are generated by default. Becoming proficient in processing and analyzing event logs will provide you "first hand" knowledge of events that occur and will help you understand the initial attack vector (delivery and exploitation in the Cyber Kill Chain) as well as post-exploitation actions (installation, lateral network traversal and other actions on objectives per the Cyber Kill Chain).

More importantly still, the specific events logged can inform portions of the Diamond Threat Attribution model and expose the particular tactics, techniques and procedures (TTPs) a threat actor uses in cyber campaigns.

Action Summary

In this exercise, you will:

1. Use built-in Windows utilities to view and analyze event logs
2. Develop the ability to find relevant events through different filtering methods
3. Answer questions about the logged events

Resources

Click on each of these report links before proceeding.

Windows 7 Security Event Log Descriptions

https://support.microsoft.com/en-us/help/977519/description-of-security-events-in-windows-7-and-in-windows-server-2008

SANS Whitepaper on Windows Logon Forensics

https://www.sans.org/reading-room/whitepapers/forensics/windows-logon-forensics-34132

Closeout

The Windows Event Logs are an authoritative repository of events that occur on Windows systems and are readily available in nearly all domain environments. The Security events can be mined for valuable information about accounts, security groups, account management and other events that can reflect an adversaries TTPs.

For Further Discussion

Consider the following and discuss as a class:

1. There are many repositories of information available on the Internet. How do you judge the degree of authority from the various sources?
2. Why is recording date/times as UTC-based values important?
3. What was the most challenging aspect of analyzing the Windows Security Event Log file?

Exercise 6.2-039.a - Analyze Host to Identify Threat Activity

Introduction

Objective: Analyze host to identify threat activity

Scenario

Users have reported that two Windows clients are exhibiting strange behavior. The DCI CND Manager wants you to determine if the behavior on these clients indicates potential malicious activity that may need further analysis.

Background: Knowing how to determine if activity is a threat is crucial to the DCI mission. Analyzing and prioritizing threats based on information gathered allows resources to be allocated appropriately. Minimizing time to determine if a system has been affected by threat activity gives more time to analyze actual threats, and minimize time and resources wasted on false threats. DCI may not always have IOCs to use, or the IOCs of an APT may change. Therefore, it is essential to know how to determine a threat when APT intelligence is not available.

In this exercise, students will use GRR and PowerShell. One machine is accessible by a pre-installed GRR agent. The other machine does not have a GRR agent installed and must be accessed by PowerShell. Students will use these tools to determine the threat on each machine.

Resources

Microsoft: Getting Started with Windows PowerShell
https://docs.microsoft.com/en-us/powershell/scripting/getting-started/getting-started-with-windows-powershell?

Microsoft: Windows PowerShell Programmer's Guide
https://msdn.microsoft.com/en-us/library/ms714674(v=vs.85).aspx

Provided

PowerShell for Responders: Cmdlets and Syntax Resource Guide

Use GRR and PowerShell to perform analysis on the second system

A baseline.txt is provided on the Windows Remote 2 Desktop. This file is a baseline of filenames and SHA-256 hashes for System32. Using this file, write a PowerShell script that determines new, deleted and manipulated files in System32.

Note: If you cannot remote into the box, enable WinRM on the remote machine. If you still cannot remote into the box, run the commands on the remote machine. Yes, we understand this is not realistic. You would not run commands on a compromised box in the real world.

Closeout

In this exercise, you remotely collected data from two Windows hosts and analyzed the information to a known system baseline. You built fundamental comparative analysis tools with PowerShell that aided in identifying threat activity.

For Further Discussion

Consider the following and discuss as a class:

1. What are the advantages of using PowerShell over GRR for collecting host artifacts? What are the disadvantages?
2. Identify several locations where we looked for artifacts of potential malicious activity.
3. What are some additional locations, both network and host, that would contain IOCs?

Exercise 6.2-040.a - Analyze Hosts to Determine IOC Presence

Introduction

Objective: Analyze hosts to determine IOC presence

Cyber threats are enormous and overwhelming. Thousands of attack attempts occur every day. By using indicators of compromise, organizations can efficiently scan through systems and determine if a system has been compromised.

These IOCs are developed by intelligence agencies and provided to your CPT. Cyber security organizations such as Symantec and FireEye compile intelligence reports containing IOCs of specific APTs. These reports can also be used to scan systems for IOCs to determine if they are compromised.

There are potential problems with using IOCs, however. The system may be compromised but not use any of the IOCs in the provided report. Also, the system may have an IOC, but not be comprised. IOCs are just one method to quickly determine APT presence, but they should not be your only indication of threat activity.

Scenario

Background: You have received an IOC list. Using this list and tools you have been given, find all IOCs on a current system. Use WireShark to collect network traffic for five minutes. Analyze the traffic for IOCs from the list received. Look for host-based IOCs using Regedit and the service controller command-line interface (sc.exe). Compile a report of all IOCs found on the system.

Action Summary

In this exercise, you will:

1. Use the IOC list provided to articulate all IOCs that are present on the system.
2. Answer questions in the exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources

IOC List from Semantic

APT1 IOC List from Symantec

Service Controller Command sc

https://technet.microsoft.com/en-us/library/bb490995.aspx

WireShark - Displaying Filters

https://wiki.wireshark.org/DisplayFilters

Windows Automatic Startup Locations

https://www.ghacks.net/2016/06/04/windows-automatic-startup-locations/

Closeout

In this exercise, you discovered both network and host IOCs to determine IOC presence on a system.

For Further Discussion

Consider the following and discuss as a class:

1. What are the advantages of using IOCs to determine if a system is compromised?
2. What are some disadvantages?
3. Would using a baseline be more efficient in determining a compromised system, or an IOC list? Why?

Exercise 6.2-078.a - Characterize a Suspicious File

Introduction

Objective: Conduct host analysis to identify threat attribution

During analysis of hosts, you will likely encounter a variety of files with unknown or suspicious origins. In these circumstances it is important to be able to characterize the file to understand likely impact and whether the executable is a threat to the system's security.

Action Summary

In this exercise, you will:

1. Be introduced to some static analysis techniques that will aid in characterizing suspicious files.
2. Use open-source resources to ascertain further information.
3. Answer the questions in the exercise.

Resources

Click on each of these report links before proceeding.

Malwarebytes Windows Portable Executable (PE) Analysis Tools
https://blog.malwarebytes.com/threat-analysis/2014/05/five-pe-analysis-tools-worth-looking-at/

Structure of a Portable Executable (Graphic)
https://upload.wikimedia.org/wikipedia/commons/0/09/Portable_Executable_32_bit_Structure.png

Structure of a Portable Executable
https://msdn.microsoft.com/en-us/library/windows/desktop/ms680547(v=vs.85).aspx

Close Out

In this exercise, you performed a basic assessment of an unknown executable using static analysis techniques. Static analysis can provide valuable details about the nature and character of an unknown file.

For Further Discussion

Consider the following and discuss as a class:

1. Describe, in your own words, a portable executable. What are some

characteristics of a portable executable?

2. What is a packer? How does it change the characteristics of an executable?
3. VirusTotal allows submitting samples or hash values - which do you think is the better option for DoD operational security?
4. Which antivirus vendor website did you use to research the sample?

Exercise 6.2-079.a - Become Familiar With Executable Static Analysis

Introduction

Objective: Characterize a suspicious file

During analysis of hosts, you will likely encounter a variety of files with unknown or suspicious origins. In these circumstances it is important to be able to characterize the file to understand likely impact and whether the executable is a threat to the system's security.

Action Summary

In this exercise, you will:

1. Be introduced to some static analysis techniques that will aid in characterizing suspicious files.
2. Use open-source resources to ascertain further information.
3. Answer the questions in the exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources

Click on each of these report links before proceeding.

Kris Kendall's presentation on Practical Malware Analysis
https://www.blackhat.com/presentations/bh-dc-07/Kendall_McMillan/Paper/bh-dc-07-Kendall_McMillan-WP.pdf

Structure of a Portable Executable (Graphic)
https://upload.wikimedia.org/wikipedia/commons/0/09/Portable_Executable_32_bit_Structure.png

Structure of a Portable Executable
https://msdn.microsoft.com/en-us/library/windows/desktop/ms680547(v=vs.85).aspx

Malwarefox.com: Classes/types of Malware
https://www.malwarefox.com/malware-types/

Close Out

In this exercise you used a variety of utilities to perform basic static assessment of two unknown samples. This static assessment introduced hash values, online resources like VirusTotal.com and various utilities that can be used to collect artifacts about unknown executables. You also developed IOCs based off the analysis.

For Further Discussion

Consider the following and discuss as a class:

1. What is the most common packer used for malware? How can it be identified?
2. Describe the Portable Executable format.
3. Characterize the Portable Executable sections.

Exercise 6.2-080.a - Characterize Binaries

Introduction

Objective: Conduct host analysis to identify threat attribution

Exposure to a variety of sample binaries will develop a rote ability to assess the static features of a sample and provide insight to malware features and your ability to hone and develop IOCs based on findings.

Action Summary

In this exercise, you will:

1. Perform static assessments of three different potentially malicious sample binaries.
2. Learn to quickly triage portable executable files to improve your team's ability to clear potential threats on defended systems.
3. Answer questions in this exercise.

Resources

Click on each of these report links before proceeding.

Mandiant: Practical Malware Analysis by Kris Kendall
https://www.blackhat.com/presentations/bh-dc-07/Kendall_McMillan/Paper/bh-dc-07-Kendall_McMillan-WP.pdf

Structure of a Portable Executable (Graphic)
https://upload.wikimedia.org/wikipedia/commons/0/09/Portable_Executable_32_bit_Structure.png

Structure of a Portable Executable
https://msdn.microsoft.com/en-us/library/windows/desktop/ms680547(v=vs.85).aspx

Malwarefox.com: Classes/types of Malware
https://www.malwarefox.com/malware-types/

Close Out

In this exercise, you performed static analysis of three sample executables.

For Further Discussion

Consider the following and discuss as a class:

1. Why wouldn't you implement all the strings within the sample as network and filesystem IOCs for warning about these threats?
2. What are some methods for overcoming challenges with packed samples? What if we do not have an appropriate unpacker?
3. What are some situations that you would want more in-depth analysis performed on a sample?

Exercise 6.2-081.a - Coaxing Network IOCs

Introduction

Objective: Conduct host analysis to identify threat attribution

More advanced malware samples may make IOC identification difficult through static analysis approaches. In many cases you will want or need to execute the sample to observe behavior. When performing dynamic assessment of samples, it is critical to use isolated physical or virtual machines.

Additionally, having the ability to revert the system to a known-good baseline is critical for eliminating cross-contamination between different samples. While rare, some malware will wait until specific conditions (like user activity, date/time events, application execution, etc.) before exhibiting behavior. If you do not return to a known baseline for each dynamic analysis, you may incorrectly attribute IOCs to the wrong sample.

Action Summary

In this exercise, you will:

1. Perform our first dynamic analysis of a sample to explore the network communications that occur upon execution of the sample.
2. Use FakeNet to provide network facilities malware will likely expect.
3. Execute a sample.
4. Record our observations about the network activity.
5. Identify relevant network-based IOCs.
6. Answer questions in the exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources

Click on each of these report links before proceeding.

FakeNet-NG - Next Generation Dynamic Network Analysis Tool
https://github.com/fireeye/flare-fakenet-ng

Closeout

You have reached the end of this exercise. At this time, you must restart your environment to ensure you are back to the known-good baseline!

You performed your first dynamic assessment of a sample to develop network IOCs. Fakenet creates a fast and easy way to emulate these services and dynamically support attempted Malware C2 for a more in-depth assessment of the samples' capability.

For Further Discussion

Consider the following and discuss as a class:

1. What are some advantages to using Fakenet?
2. What are some disadvantages to using Fakenet?
3. Did you restart your environment? What repercussions might you expect to experience if you did not restart the environment?

MODULE 4

Secure Stage Actions

Module 4 introduces tasks that are common for DCI squads to undertake during the secure stage of a mission. Activities the DCI squad is expected to have proficiency in for the secure stage include: deploying sensor platforms and monitoring the sensors, identifying indicators of compromise within the mission owner network, and reporting findings through Intel Analysts and other CPT elements.

Lesson 1

Deploying Sensors

Students will use indicators of compromise and network sensors to monitor the KT-C for adversary action and activity. Students will use baseline analysis to develop "known good" models for traffic on various network segments and apply sensor tuning approaches to reduce total volume of data that must be analyzed.

Exercise 7.1-042.a - Investigate a False Positive

Introduction

Objective: Monitor sensors for threat attribution

An essential element of incident response is to effectively manage the incident so that the damage is limited, and both recovery time and costs are kept at a minimum. This makes it critical to analyze alerts or incidents to determine the cause and whether an emergency response is required.

The analysis of an alert or signature will answer several questions, including the following:

- What are the symptoms of the problem?
- Were other security incidents recently observed?
- What software or hardware components are affected by the incident?
- What theories exist for how the compromise occurred?
- Does the affected system pose any risk to the organization?

Scenario

Background: A user has reported unusual behavior when attempting to open the Google Chrome browser on their Windows machine. The user states that opening their Google Chrome browser opens a different browser. Additionally, the user reports that the browser starts up automatically after rebooting the machine.

Action Summary

In this exercise, you will:

1. Review the Indicators of Compromise List by the Symantec Comment Crew.
2. Answer the questions for this exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources

Indicators of Compromise List by the Symantec Comment Crew

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/comment_crew_indicators_of_compromise.pdf

Closeout

In this exercise, you analyzed a victim's system and attempted to determine the cause and effect of the reported incident.

For Further Discussion

Consider the following and discuss as a class:

1. How would you define a false positive with respect to an incident?
2. What would you consider a benign true positive?
3. What would be the next step to confirm this is not an APT?
4. This might seem like an example of a silly prank. How likely is this to happen inside a work environment?

Exercise 7.1-043.a - Investigate a True Positive

Introduction

Objective: Monitor sensors for threat attribution

An essential element of incident response is to effectively manage the incident so that the damage is limited, and both recovery time and costs are kept at a minimum. This makes it critical to analyze alerts or incidents to determine the cause and whether an emergency response is required.

The analysis of an alert or signature will answer several questions, including the following:

- What are the symptoms of the problem?
- Were other security incidents recently observed?
- What software or hardware components are affected by the incident?
- What theories exist for how the compromise occurred?
- Does the affected system pose any risk to the organization?

Scenario

Within the USER's Downloads directory, there is an executable called ituneshelper.exe that matches a known indicator of compromise.

Investigate the file and determine if any other potential indicators of compromise exist on the system.

Action Summary

In this exercise, you will:

1. Review the Indicators of Compromise List by the Symantec Comment Crew.
2. Analyze a victim's system and attempt to determine the cause and effect of a reported incident.
3. Answer the questions presented in this exercise.

Resources

Indicators of Compromise List by the Symantec Comment Crew
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/comment_crew_indicators_of_compromise.pdf

Closeout

In this exercise, you analyzed a victim's system and attempted to determine the cause and effect of the reported incident.

For Further Discussion

Consider the following and discuss as a class:

1. How would you define a false positive with respect to an incident?
2. What would you consider a benign true positive?
3. What would be the next step to confirm this is not an APT?
4. This might seem like an example of a silly prank. How likely is this to happen inside a work environment?

Exercise 7.1-054.a - Create a PowerShell Script to Collect Data from Multiple Systems

Introduction

Objective: Monitor sensors for threat attribution

Finding artifacts that determine malicious presence is one of the primary tasks of the DCI squad. PowerShell is a Windows tool that allows for quick collection of system and network artifacts. Using PowerShell scripting, this process can be saved and built upon, and can be tailored to specific needs of the mission. Scripts developed for one mission may also be applicable to future missions, saving even more time and resources for the CPT. PowerShell is built for remote access and administration, and is built into Windows, allowing for easier setup and less dependence on third-party software.

Scenario

Your team has been tasked with searching the network for given IOCs for Windows Machines. You have been given a subnet you are authorized to access, and a network map. However, network maps can be outdated, so you will verify for yourself what machines are available on the network.

Create a PowerShell script that determines machines on the network that can be connected to, and then gathers registry keys, files, and network locations based on given IOCs. Your script should then alert the user to what machines have matching IOCs, and what the matching IOCs are. Your area of operations is 10.10.10.0/24.

Action Summary

In this exercise, you will:

1. Develop a basic PowerShell host-sensor capability.
2. Deploy the host-sensor capability to multiple endpoints.

Any additional resources you choose to use are acceptable for this activity.

Resources

Microsoft has extensive documentation about PowerShell that can be found on the docs.microsoft.com website. Arrays and the ability to invoke commands will be particularly important to master for this exercise.

Microsoft PowerShell Invoke-Command
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/invoke-command?view=powershell-5.1

Microsoft PowerShell About Arrays
https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_arrays?view=powershell-5.1

Closeout

In this exercise, you used PowerShell to gather information from multiple Windows machines using a custom script you created. You then compared this to a given IOC list and alerted the user what IOCs were found.

For Further Discussion

Consider the following and discuss as a class:

1. Is your script flexible enough to be used in different scenarios and networks? How could you make it more reusable?
2. What system and network artifacts can be found using PowerShell? What limitations does PowerShell have?

Exercise 7.1-052.a - Deploy GRR Agent

Introduction

Objective: Monitor sensors for threat attribution

Deploying to a site will always come with challenges. There will be times when machines on the client's network will not be physically accessible and/or a remote desktop will not be available. Additional steps will need to be taken to ensure that the CPT is able to monitor those remote systems. Students will need to install the GRR client binary on the remote machine and register it as a client, all without physical access to the machine or a remote desktop session.

Scenario

Having completed collection activities with any datasets and capabilities that are native in the network, it is time to deploy CPT capability onto specific hosts. The threat in question has recently started using the file wdboot.sys for dynamic-link library (DLL) hijacking and you must verify this file has not been affected.

Action Summary

In this exercise, you will:

1. Deploy a GRR client to the Windows Server target using PowerShell.
2. Verify you have deployed the GRR client by collecting information with Flows.
3. Answer questions pertaining to this exercise.

Resources

GRR Rapid Response Documentation

https://grr-doc.readthedocs.io/en/latest/

- Installing GRR Server
- Troubleshooting Clients

Windows Remote Management

https://msdn.microsoft.com/en-us/library/aa384426(v=vs.85).aspx

PsExec

https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

Closeout

In this exercise, you deployed a host sensor using remote execution tools and PowerShell.

For Further Discussion

Consider the following and discuss as a class:

1. What are some other methods we can use to deploy host sensors?
2. What are some advantages of a host sensor versus a network sensor?
3. What are some advantages of a network sensor versus a host sensor?
4. Why would you use native resources for initial collection instead of starting with your CPT capabilities that you trained on?

Exercise 7.1-041.a - Analyze Network Traffic to Identify Beacon

Introduction

Objective: Monitor sensors for threat attribution

Beacons are a common form of malware that reach out to a server. Beacons can have different purposes. Some beacons reach out to verify that the machine still has Internet access. Others reach out to a malicious server that the threat actor controls so they know the box is still owned. Beaconing is used in other types of malware such as botnets and trojans. The beacon reaches out for commands to execute on the infected machine.

Finding beacons can be very difficult. Some beacons have a set time interval, while some are random. This time interval can be from every few seconds, to once a year or longer. Beacons use various protocols and techniques. These variations can make beacons very difficult to find in network traffic.

Scenario

The local defenders have found IOCs of APT1 on their server. They have provided you with a pcap of the network traffic of a specific workstation. Your Intel Analyst has provided APT1 IOCs.

Determine what beacons are evident in the network traffic.

Action Summary

In this exercise, you will:

1. Use WireShark and/or PowerShell to analyze network traffic to identify potential beacons.
2. Answer questions pertaining to this exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources

WireShark: Display Filters
https://wiki.wireshark.org/DisplayFilters

WireShark User's Guide
https://www.wireshark.org/docs/wsug_html_chunked/

Provided
Indexed PR_Mod3 Slides

APT1 IOCs in your Exercise folder

Closeout

In this exercise, you discovered multiple beacons using WireShark and PowerShell. Using filters, time-bases analysis and IOCs, you distinguished normal traffic from beacons.

For Further Discussion
Consider the following and discuss as a class:

1. Beacons were found using various protocols in this exercise. What other protocols could a beacon use? Would some be harder to find than others?
2. Beacons usually take up a very small portion of network traffic. How do you filter out as much as possible without filtering out beacons?
3. What are indicators that a connection is a beacon as opposed to normal network traffic?

Lesson 2

Analyzing Compromised Hosts

Students will analyze host systems using host-based sensors and digital forensic techniques to identify files of interest from affected systems. Students will analyze intrusion scenarios to identify new or previously unknown artifacts for integration into the threat agent signatures. Students will update signatures for deployed sensors and refine signatures for the operating environment. Students will share reporting through intelligence analyst channels and ensure other CPT elements are informed of updated IOCs.

Exercise 8.1-060.a - Identify Data Exfiltration Artifacts on a Windows System

Introduction

Objective: Analyze a host file system

One of the primary goals of intrusions is to acquire valuable data from the victim and collect, or exfiltrate, it. This data can include, but is not limited to, Personally Identifiable Information (PII), credit card numbers, financial data, intellectual property or classified information.

The ability to find and determine potential artifacts used in data exfiltration will facilitate the process of detecting intrusions and assessing the type of information accessible by intruders.

In this exercise, you will use Windows PowerShell to search for files that may have been exfiltrated by an intruder. Utilizing PowerShell will prove useful since most environments heavily utilize Windows Operating Systems.

Concepts that should be familiar to students include the following:

- Basic PowerShell cmdlets such as Get-Process, Get-Service, etc.
- Basic PowerShell scripting functionality such as loops, variables, script and module files.

Scenario

Background: You are tracking down a series of indicators that may relate to data exfiltration. There are no additional tools authorized for deployment, however, the system you are analyzing has PowerShell.

Action Summary

In this exercise, you will:

1. Use documentation from the resources section as needed.
2. Collect information from a system using PowerShell and analyze the data in search of potential exfil data.
3. Answer questions about this exercise.

Resources

List of File Signatures

https://en.wikipedia.org/wiki/List_of_file_signatures

Alternate Data Streams in NTFS (PowerShell)

https://blogs.technet.microsoft.com/askcore/2013/03/24/alternate-data-streams-in-ntfs/

PowerShell Check File Headers

http://learningpcs.blogspot.com/2012/07/powershell-v3-check-file-headers.html

PowerShell Get-Content Documentation

https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-content?view=powershell-5.1

Get Hex Dump of Files in PowerShell

http://windowsitpro.com/powershell/get-hex-dumps-files-powershell

Closeout

In this exercise, you used Windows PowerShell to search for files that may have been exfiltrated by an intruder, also known as an exfil. You used PowerShell since most environments utilize Windows Operating Systems.

For Further Discussion

Consider the following and discuss as a class:

1. Besides changing the extension, what other ways could the exfil have been hidden?
2. Would the file signature technique have worked if the file was encrypted?
3. Does finding the file equate to successful data exfiltration?
4. What artifacts would indicate that the file was transferred?
5. What are some analysis limitations when working with RAR and ZIP files?
6. What if they are password protected?
7. What are some common file formats for an exfil?
8. What other file formats could contain exfil data (video, audio, etc.)?
9. What could you learn about the threat agent through exfil, for example, what they care about, their level of access and sophistication, etc.?

Exercise 8.1-059.a - Identify Keylogger Artifacts on a Windows System

Introduction

Objective: Analyze host file system

One of the primary goals of intrusions is to acquire valuable data from the victim and collect it. This data can include, but is not limited to, Personally Identifiable Information (PII), credit card numbers, financial data, intellectual property or classified information. One method that a malicious actor will use is a keylogger to collect keystrokes by end users.

The ability to find and determine potential artifacts used in keyloggers will facilitate the process of detecting intrusions and assessing the type of information intruders accessed.

Scenario

In this exercise, you will use Windows PowerShell to search for files that may have been created by a keylogger. Utilizing PowerShell will prove useful since most environments utilize Windows Operating Systems heavily. Students will also be using GRR to search for other log files that have been created by the suspected keylogger.

Action Summary

In this exercise, you will:

1. Create a PowerShell script to search windows systems for the keylogger tool used by APT1.
2. Modify the PowerShell script to collect the log data associated with the keylogger.
3. Use GRR to find files created around the time of the keylogger's creation date/time.
4. Use GRR to collect registry keys created around the time of the keylogger's creation date/time.
5. Record your findings.
6. Answer questions within the exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources

PowerShell Get-Content Documentation

https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-content?view=powershell-5.1

APT1 Documentation

https://malware.lu/assets/files/articles/RAP002_APT1_Technical_backstage.1.0.pdf

GRR Rapid Response Documentation

https://grr-doc.readthedocs.io/en/latest/

- GRR Flows
- GRR File Finder Syntax
- GRR User Guide

Closeout

In this exercise, you used Windows PowerShell to search for files that may have been created by a keylogger and used GRR to search for other log files that have been created by the suspected keylogger.

For Further Discussion

Consider the following and discuss as a class:

1. Was it easier to use PowerShell or GRR? Why?
2. Explain the process used in this exercise to expand analysis criteria beyond the initial IOC?

Exercise 8.1-082 - Assess a Potentially Compromised Host 1

Introduction

Objective: Analyze host systems

In this exercise you will assess a system that has likely been compromised. You will identify actions on objectives (the last stage of the Cyber Kill Chain) the adversary has performed and provide a summary of the likely impact caused by the threat.

This is an unguided exercise. The scenario provided will require extensive use of all skills and capabilities you have exercised and demonstrated throughout the course.

Action Summary

In this exercise, you will:

1. Use host and network sensor capabilities to assess the state of a system
2. Identify actions performed post-compromise
3. Identify indicators of compromise and the threat agent likely responsible

Scenario

The potentially compromised host you are investigating in this scenario is 172.16.12.7.

Rules of Engagement: Your analysis is isolated to the specific host. Do not access other hosts as part of your analysis of this scenario.

Questions in this exercise ask about the following areas of attacker activity:

1. Data collected by the attacker
2. Command and Control IP addresses and domain names
3. Unauthorized access to credentials
4. Attempted and/or successful privilege escalation
5. Attempts by the adversary to evade discovery and remediation
6. Activities performed to discover other potential targets on the network
7. Any executables the adversary ran during their operation
8. Successful or actual lateral movements performed by the adversary
9. Methods of persistence used
10. A full accounting of any malware left on the system

Closeout

The scenario you assessed contains a combination of FiN-4 TTPs and other common attacker methodologies.

Find open-source reporting related to this threat and review your findings. Spend the remainder of the available time reviewing the assessed host to identify activities you may have missed.

Exercise 8.1-083 - Assess a Potentially Compromised Host 2

Introduction

Objective: Analyze host systems

In this exercise you will assess a system that has likely been compromised. You will identify actions on objectives (the last stage of the Cyber Kill Chain) the adversary has performed and provide a summary of the likely impact caused by the threat.

This is an unguided exercise. The scenario provided will require extensive use of all skills and capabilities you have exercised and demonstrated throughout the course.

Action Summary

In this exercise, you will:

1. Use host and network sensor capabilities to assess the state of a system
2. Identify actions performed post-compromise
3. Identify indicators of compromise and the threat agent likely responsible

Scenario

The potentially compromised host you are investigating in this scenario is 172.16.12.8.

Rules of Engagement: Your analysis is isolated to the specific host. Do not access other hosts as part of your analysis of this scenario.

Questions in this exercise ask about the following areas of attacker activity:

1. Data collected by the attacker
2. Command and Control IP addresses and domain names
3. Unauthorized access to credentials
4. Attempted and/or successful privilege escalation
5. Attempts by the adversary to evade discovery and remediation
6. Activities performed to discover other potential targets on the network
7. Any executables the adversary ran during their operation
8. Successful or actual lateral movements performed by the adversary
9. Methods of persistence used
10. A full accounting of any malware left on the system

Closeout

The scenario you assessed contains a combination of PLATINUM TTPs and other common attacker methodologies.

Find open-source reporting related to this threat and review your findings. Spend the remainder of the available time reviewing the assessed host to identify activities you may have missed.

Exercise 8.1-084 - Assess a Potentially Compromised Host 3

Introduction

Objective: Analyze host systems

In this exercise you will assess a system that has likely been compromised. You will identify actions on objectives (the last stage of the Cyber Kill Chain) the adversary has performed and provide a summary of the likely impact caused by the threat.

This is an unguided exercise. The scenario provided will require extensive use of all skills and capabilities you have exercised and demonstrated throughout the course.

Action Summary

In this exercise, you will:

1. Use host and network sensor capabilities to assess the state of a system
2. Identify actions performed post-compromise
3. Identify indicators of compromise and the threat agent likely responsible

Scenario

The potentially compromised host you are investigating in this scenario is 172.16.12.9.

Rules of Engagement: Your analysis is isolated to the specific host. Do not access other hosts as part of your analysis of this scenario.

Questions in this exercise ask about the following areas of attacker activity:

1. Data collected by the attacker
2. Command and Control IP addresses and domain names
3. Unauthorized access to credentials
4. Attempted and/or successful privilege escalation
5. Attempts by the adversary to evade discovery and remediation
6. Activities performed to discover other potential targets on the network
7. Any executables the adversary ran during their operation
8. Successful or actual lateral movements performed by the adversary
9. Methods of persistence used
10. A full accounting of any malware left on the system

Closeout

The scenario you assessed contains a combination of APT2 TTPs and other common attacker methodologies.

Find open-source reporting related to this threat and review your findings. Spend the remainder of the available time reviewing the assessed host to identify activities you may have missed.

Exercise 8.1-085 - Assess a Potentially Compromised Host 4

Introduction

Objective: Analyze host systems

In this exercise you will assess a system that has likely been compromised. You will identify actions on objectives (the last stage of the Cyber Kill Chain) the adversary has performed and provide a summary of the likely impact caused by the threat.

This is an unguided exercise. The scenario provided will require extensive use of all skills and capabilities you have exercised and demonstrated throughout the course.

Action Summary

In this exercise, you will:

1. Use host and network sensor capabilities to assess the state of a system
2. Identify actions performed post-compromise
3. Identify indicators of compromise and the threat agent likely responsible

Scenario

The potentially compromised host you are investigating in this scenario is 172.16.12.10.

Rules of Engagement: Your analysis is isolated to the specific host. Do not access other hosts as part of your analysis of this scenario.

Questions in this exercise ask about the following areas of attacker activity:

1. Data collected by the attacker
2. Command and Control IP addresses and domain names
3. Unauthorized access to credentials
4. Attempted and/or successful privilege escalation
5. Attempts by the adversary to evade discovery and remediation
6. Activities performed to discover other potential targets on the network
7. Any executables the adversary ran during their operation
8. Successful or actual lateral movements performed by the adversary
9. Methods of persistence used
10. A full accounting of any malware left on the system

Closeout

The scenario you assessed contains a combination of APT26 TTPs and other common attacker methodologies.

Find open-source reporting related to this threat and review your findings. Spend the remainder of the available time reviewing the assessed host to identify activities you may have missed.

Exercise 8.1-086 - Assess a Potentially Compromised Host 5

Introduction

Objective: Analyze host systems

In this exercise you will assess a system that has likely been compromised. You will identify actions on objectives (the last stage of the Cyber Kill Chain) the adversary has performed and provide a summary of the likely impact caused by the threat.

This is an unguided exercise. The scenario provided will require extensive use of all skills and capabilities you have exercised and demonstrated throughout the course.

Action Summary

In this exercise, you will:

1. Use host and network sensor capabilities to assess the state of a system
2. Identify actions performed post-compromise
3. Identify indicators of compromise and the threat agent likely responsible

Scenario

The potentially compromised host you are investigating in this scenario is 172.16.12.11.

Rules of Engagement: Your analysis is isolated to the specific host. Do not access other hosts as part of your analysis of this scenario.

Questions in this exercise ask about the following areas of attacker activity:

1. Data collected by the attacker
2. Command and Control IP addresses and domain names
3. Unauthorized access to credentials
4. Attempted and/or successful privilege escalation
5. Attempts by the adversary to evade discovery and remediation
6. Activities performed to discover other potential targets on the network
7. Any executables the adversary ran during their operation
8. Successful or actual lateral movements performed by the adversary
9. Methods of persistence used
10. A full accounting of any malware left on the system

Closeout

The scenario you assessed contains a combination of MOLERATS TTPs and other common attacker methodologies.

Find open-source reporting related to this threat and review your findings. Spend the remainder of the available time reviewing the assessed host to identify activities you may have missed.

Exercise 8.1-087 - Assess a Potentially Compromised Host 6

Introduction

Objective: Analyze host systems

In this exercise you will assess a system that has likely been compromised. You will identify actions on objectives (the last stage of the Cyber Kill Chain) the adversary has performed and provide a summary of the likely impact caused by the threat.

This is an unguided exercise. The scenario provided will require extensive use of all skills and capabilities you have exercised and demonstrated throughout the course.

Action Summary

In this exercise, you will:

1. Use host and network sensor capabilities to assess the state of a system
2. Identify actions performed post-compromise
3. Identify indicators of compromise and the threat agent likely responsible

Scenario

The potentially compromised host you are investigating in this scenario is 172.16.12.12.

Rules of Engagement: Your analysis is isolated to the specific host. Do not access other hosts as part of your analysis of this scenario.

Questions in this exercise ask about the following areas of attacker activity:

1. Data collected by the attacker
2. Command and Control IP addresses and domain names
3. Unauthorized access to credentials
4. Attempted and/or successful privilege escalation
5. Attempts by the adversary to evade discovery and remediation
6. Activities performed to discover other potential targets on the network
7. Any executables the adversary ran during their operation
8. Successful or actual lateral movements performed by the adversary
9. Methods of persistence used
10. A full accounting of any malware left on the system

Closeout

The scenario you assessed contains a combination of DRAGONFLY TTPs and other common attacker methodologies.

Find open-source reporting related to this threat and review your findings. Spend the remainder of the available time reviewing the assessed host to identify activities you may have missed.

Exercise 8.1-088 - Assess a Potentially Compromised Host 7

Introduction

Objective: Analyze host systems

In this exercise you will assess a system that has likely been compromised. You will identify actions on objectives (the last stage of the Cyber Kill Chain) the adversary has performed and provide a summary of the likely impact caused by the threat.

This is an unguided exercise. The scenario provided will require extensive use of all skills and capabilities you have exercised and demonstrated throughout the course.

Action Summary

In this exercise, you will:

1. Use host and network sensor capabilities to assess the state of a system
2. Identify actions performed post-compromise
3. Identify indicators of compromise and the threat agent likely responsible

Scenario

The potentially compromised host you are investigating in this scenario is 172.16.12.13.

Rules of Engagement: Your analysis is isolated to the specific host. Do not access other hosts as part of your analysis of this scenario.

Questions in this exercise ask about the following areas of attacker activity:

1. Data collected by the attacker
2. Command and Control IP addresses and domain names
3. Unauthorized access to credentials
4. Attempted and/or successful privilege escalation
5. Attempts by the adversary to evade discovery and remediation
6. Activities performed to discover other potential targets on the network
7. Any executables the adversary ran during their operation
8. Successful or actual lateral movements performed by the adversary
9. Methods of persistence used
10. A full accounting of any malware left on the system

Closeout

The scenario you assessed contains a combination of HIDDENCOBRA TTPs and other common attacker methodologies.

Find open-source reporting related to this threat and review your findings. Spend the remainder of the available time reviewing the assessed host to identify activities you may have missed.

MODULE 5

Protect Stage Actions

Module 5 introduces tasks that DCI squads commonly undertake during the protect stage of a mission. The squad is expected to be proficient in the following activities during the protect stage: developing remediation strategies and mitigation plans to defend the network from cyber threat actors.

Lesson 1

Developing Remediation Strategies and Mitigation Plans

Students will present findings and work through exercises that develop reporting methods and techniques that are effective for different audiences, which include: the supported command, supported command's network defense capabilities, NETOPS command, CPT leadership and other squads. Students will develop courses of action (COAs) for findings that mitigate ongoing risks and threats and provide short term and long term COAs. The DCI student will develop inputs for the supported command's risk analysis.

Exercise 9.1-065.a - Provide Situation Report, Timeline and Operator Log of Activity

Introduction

Objective: Present most current findings of ongoing DCI operation to supported command

Scenario

The USCYBERCOM Commander is on-site. They have requested a brief be made to them and the supported command that explains what has happened so far. Due to the limited time, the CND Manager is going to ask you questions in order to understand the full picture before the briefing. Your previous exercise operator logs will be used to complete the situation report (SITREP), timeline and this brief.

Background: During a mission, it is vital to keep communicating activity through the chain of command. These reports that are created by the CPT allow for deconfliction and gives decision-makers a way to adjust plans, capabilities and resources accordingly.

SITREPs are usually reported every 24-72 hours to higher headquarters (HHQ). These reports give insight to what has happened in the last 24, 48 or 72 hours and what is planned for the next 24, 48 or 72 hours.

Timelines help everyone understand what activity was recorded during an incident response, detailing the malicious activity from first seen to current findings. It is used to continue campaign analysis against an adversary and help future operations stop the malicious activity at the initial compromise stage of a kill chain.

The operator log is a wealth of information. It can be used for deconfliction between the CPT and supported command. It also allows a greater understanding between the CPT members who are working shifts, because the log details every action taken on any machine. Operator logs also provide training to junior members with little or no experience. It allows those members to understand the flow of a mission and what commands or tools were used to accomplish each task.

Action Summary

In this exercise, you will:

1. Collect your previously saved operator logs for exercises.
2. Answer questions in this exercise.

Resources

Ensure you have your weekly exercise operator logs. If you do not, try accessing your daily operator logs and AARs from the submission pages or contact an instructor!

Closeout

In this exercise, you used documentation from previous mission activities to provide SITREPs and inputs for reporting.

For Further Discussion

Consider the following and discuss as a class:

1. Why is it important to document actions and findings when they occur?
2. What type of information may you expect to be requested later in a mission?

Exercise 9.2-066.a - Provide SITREP and IOCs Identified for NETOPS

Introduction

Objective: Inform appropriate NETOPS command of results and ongoing actions

Scenario

The USCYBERCOM commander is on-site. You have been requested to develop a timeline of DCI Squad activity and provide a SITREP to NETOPS.

Your operator logs from previously completed exercises will be used to complete the SITREP and timeline.

Background: During a mission, it is vital to keep communicating activity through the chain of command. Reports that are created by the CPT allow for deconfliction and give decision-makers opportunities to adjust plans, capabilities and resources.

SITREPs are usually reported every 24-72 hours to higher headquarters. These reports give insight to what has happened in the last 24, 48 or 72 hours and what is planned for the next 24, 48 or 72 hours.

Timelines help all stakeholders understand activities that occurred during an incident response; detailing the malicious activity from first sight up to current findings and actions. Timelines are used to perform campaign analysis about an adversary and help future operations stop this malicious activity at earlier stages of the Cyber Kill Chain.

The operator log is a wealth of information. It can be used for deconfliction between the CPT and supported command. It also allows a greater understanding between the CPT members who are working shifts because the log details every action taken on any machine. Operator logs also provide training to junior members with no experience. It allows those members to understand the flow of a mission and what commands or tools were used to accomplish each task.

Action Summary

In this exercise, you will:

1. Collect your previously saved operator logs for exercises.
2. A SITREP example is included.

NOTE: You will be graded on the content not the layout of your SITREP.

Closeout

In this exercise, you developed content for typical operational products: SITREPs and timelines.

For Further Discussion

Consider the following and discuss as a class:

1. Was it difficult to locate the information required for development of SITREPs?
2. Why are accurate and complete operator logs important?
3. How well were you able to recall events that happened over the last 72 hours.

SITREP Template

A situation report (SITREP) is used by all units to give an executive summary to higher headquarters elements. It is used to describe what the unit has been doing throughout the designated time period (usually 24-72 hours). The SITREP is usually due at the close of business each day.

LAST 24

This portion of the SITREP documents significant events that happened in the last 24 hours. Broad descriptions of what is going on. In the planning phase of operations, the staff element creates a notional timeline of the mission. This is to make sure the CPT is staying on that timeline.

Examples:

- CPT members arrived on-site at 1700 EST and have begun doing X, Y, Z.
- The CPT Mission Commander along with senior members of the CPT has conducted the interview with the mission and network owners.
- The Mission Protection Squad has started their mission analysis.
- The Cyber Support squad has started their network validation, host discovery and design assessment.
- The Discovery and Counter Infiltration Squad has started reviewing the networks organic sensor capabilities to determine network visibility.
- The Cyber Readiness squad has started their compliance and policy assessments.
- The Cyber Threat Emulation squad is working with the All-Source Intelligence Analyst to develop threat intelligence and Indication and Warnings (I&Ws).
- The Cyber Threat Emulation Squad will work with the Cyber Readiness squad to develop and prepare for the Participated Defensive Evaluation of the network.
- The CPT Staff element is working with external organizations to provide support as needed to the CPT on-site.
- CPT on-site has identified suspicious activity. They created SPOTREP 01 and created a Request for Analysis (RFA) which was sent to the Cyber National Mission Force (CNMF) Battle Bridge for additional malware triage and forensics.

NEXT 24

This portion of the SITREP documents what the CPT is doing in the next 24 hours and includes broad descriptions of what is going on. In the planning phase of operations, the staff element creates a notional timeline of the mission. This is to make sure the CPT is staying on that timeline.

Examples:

- The Mission Protection Squad will have completed their mission analysis.
- The Cyber Support Squad will continue their network validation, host discovery and design assessment.
- The Discovery and Counter Infiltration Squad will develop a sensor emplacement plan, with the local cyber defenders' assistance, to provide proper network visibility.
- The Cyber Readiness Squad will continue their compliance and policy assessments.
- The Threat Intelligence Report will be disseminated to the CPT on-site. The All Source Intelligence Analysts (ASIAs) will continue to use internal and external resources to continue to develop I&Ws.
- The Cyber Threat Emulation Squad will continue to work with the Cyber Readiness squad to develop and prepare for the Participated Defensive Evaluation of the network.
- Lines of communication will be established between the CPT on-site and all supporting organizations.
- CPT Mission Commander will work with the supported command to identify, contain and eradicate procedures based on suspicious malware and analysis.

Below this line, the information will be filled out by the DCI CND Manager

==========

PRIORITIES OF WORK

This portion of the SITREP documents at a high-level what the priority is for the mission now for the next 24 to 72 hours.

Examples:

1. Mission Analysis (Staff and MP)
2. Identify and Validate C-KT (CS and MP)
3. Network and Host Enumeration (CS and DCI)
4. Compliance, Policy, Design and Vulnerability Assessments (CR and CS)
5. Network and Host Baselining (DCI and CS)
6. Cyber Dependency Model (MP)
7. Request for Information / Request for Analysis

ISSUES

This portion of the SITREP documents any issues that cannot be handled by the CPT Team Lead or Mission Commander. These issues will affect the overall mission if not taken care of within a reasonable amount of time. These issues may even need higher headquarters to intervene to accomplish the mission.

Examples:

- The deployed CPT does not have enough members to conduct the mission. Requesting additional support. Will need X, Y, Z (by name request or position request) to continue mission on time.
- The deployed CPT does not have the correct tool kit to continue mission. Will need X, Y, and Z (additional capabilities, tools, forensics support, etc.).
- The deployed CPT is still trying to gain access to the supported network. The Network Owner has yet to provide username and passwords for X number of CPT members.
- The deployed CPT do not have enough space to employ all members of the CPT. Will need to work in three shifts to accommodate spacing issues. Still working with the supported command to obtain more X, Y, and Z.
- The deployed CPT has waited for X amount of time for malware analysis. Must receive malware analysis no later than X time to continue the mission.

Exercise 9.3-064.a - Select Appropriate Courses of Action to Mitigate Threats

Introduction

Objective: Provide COAs to CPT leadership and supported commander

Understanding how to isolate, contain and eradicate malware is a critical skill for any DCI member. As subject matter experts on "hunting the adversary" in the network, the team will be relying on your expertise to lead the effort to apply the appropriate mitigation strategies to any cyber incident. There are a lot of variables to be taken into consideration to choose the best mitigation strategy for the supported command. You will encounter times where you will be required to make numerous COAs to address different constraints or limitations. Understand these are just recommendations. The supported command has the final say on which COA will be used to isolate, contain and eradicate the malware.

Scenario

Currently the malicious activity has been isolated. The DCI squad must lead the effort to determine the best course of action to contain and eradicate the malicious activity. The DCI CND Manager wants the whole DCI squad to work together to develop the best course of actions to properly contain and eradicate the malicious activity. The DCI CND Manager warns you to be prepared to make more than one COA, or adjust certain portions of a COA. The supported commander must approve the full COA before it can be implemented.

Action Summary

In this exercise, you will:

1. In teams of three, research each malware to gain an understanding of how it works.
2. The same team of three should review the Australian Signals Directorate (ASD) Strategies to Mitigate Cyber Security Incidents documents in the Resources section.
3. Answer the questions contained in this exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources

Poison Ivy: Assessing Damage and Extracting Intelligence
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf

Mimikatz Overview, Defenses and Detection
https://www.sans.org/reading-room/whitepapers/detection/mimikatz-overview-defenses-detection-36780

Pass-the-Hash Attacks: Tools and Mitigation
https://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283

ASD – Mitigation Details
https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-details.htm

ASD – Mitigation Table
https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-table.htm

ASD – Mitigation Strategies
https://www.asd.gov.au/infosec/mitigationstrategies.htm

Closeout

In this exercise, you imposed mitigation techniques to stop the delivery, exploitation and installation of several incidences of malware.

For Further Discussion

Consider the following and discuss as a class:

1. How difficult was it as a team to come up with the **BEST** mitigation technique?
2. Who on your team took the lead point? Was that person the highest ranking or did they have the most experience? Why did they take point?
3. Did you encounter any difference of opinion?
4. If you did, how did you come to select the **BEST** technique to implement?

Exercise 9.4-070.a - Provide Risk Analysis Based on an RMP

Introduction

Objective: Provide input to supported commander's risk analysis

When applying mitigations to address risk, there is a chance that there is still leftover risk. That risk must be either accepted as leftover risk by the supported command, thus making it acceptable risk, or addressed by more mitigation strategies. The CPT identifies this leftover risk by continuously monitoring and validating each risk through a defensive evaluation conducted by the CTE squad. DCI has expertise on how to defend against an APT. This makes them uniquely qualified to provide guidance to the MP squad on the final risk analysis.

Scenario

Background: The supported command has accepted and implemented the CPT's COAs. The CPT has monitored the network and host machines to ensure the COAs implemented are successful. The CPT could not address every single risk identified throughout the mission due to numerous variables. The DCI CND Manager has tasked you to work with the MP squad to determine if there is any risk left over from implementing the mitigation strategies. These will need to be briefed to the supported command.

Action Summary

In this exercise, you will:

1. Understand how to apply mitigation strategies to leftover risk.
2. Monitor and evaluate leftover risk through a defensive evaluation.
3. Answer questions in the exercise.

Any additional resources you choose to use are acceptable for this activity.

Resources

APT1

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

NIST 800-30: Risk Analysis Process

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

ASD – Mitigation Details

https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-details.htm

ASD- Mitigation Table

https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-table.htm

ASD- Mitigation Strategies

https://www.asd.gov.au/infosec/mitigationstrategies.htm

Closeout

In this exercise, you learned how to apply mitigation strategies to leftover risk.

For Further Discussion

Consider the following and discuss as a class:

1. How can an adversary use the lack of web content filtering to deliver its malware?
2. Is there leftover risk from Block Spoofed Emails mitigation strategy? If so, what is it?
3. Will whitelisting and blacklisting of applications and devices stop the execution of malicious applications on machines?
4. How can an adversary use Facebook or Twitter platforms to deliver a malicious payload?

MODULE 6

Recover Stage Actions

Module 6 introduces tasks that are common for DCI squads to undertake during the mission recovery stage. Activities the DCI squad is expected to have proficiency for the recovery stage include: providing after-action reports, recovering sensors, outbriefing DCI activity results and returning the network to normal operational status, or as near-normal as possible. Outbriefing deploying sensor platforms and monitoring the sensors, identifying indicators of compromise within the mission owner network, and reporting findings through intel analysts and other CPT elements.

Lesson 1

Performing Post-Operation Recovery Activities

Students will demonstrate the removal of host-based and network-based sensors from a network environment and ensure systems remain operational. Students will develop strategies and implement strategies to recover systems when removal of sensor capabilities causes system failure. Students will develop a final out-brief to include recommendations to enhance the security posture of the network. Students will perform an after-action AAR per USCYBERCOM guidelines and provide inputs specific to the DCI areas of responsibility (AORs).

Exercise 10.1-067.a - Remove All Sensors Placed on the Network

Introduction

Objective: Remove all sensors from the network

Once the mission is complete, it is important to remove all sensors, both hardware and software, from the network. Every piece of software or hardware that is not in use is another potential vulnerability for which threat actors may take advantage. By leaving hardware, you are negatively impacting the future mission capability of the CPT.

Scenario

Your team is finalizing all the reporting, and briefing the local command on a successful operation. You have been tasked to remove the host-based sensors deployed for the mission.

Action Summary

In this exercise, you will:

1. Fully uninstall the GRR client on a remote host with PowerShell.
2. Answer a question confirming that GRR has been removed from the machine.

Any additional resources you choose to use are acceptable for this activity.

Resources

GRR Rapid Response Documentation

https://grr-doc.readthedocs.io/en/latest/

- GRR User Manual

Closeout

In this exercise, you removed sensors you had placed on a defended network.

For Further Discussion

Consider the following and discuss as a class:

1. What are some types of sensors that you may need to remove from a network?
2. Why is it important to remove any sensors from the network?

Acronyms

A	
AAR	After Action Report
ADRP	Army Doctrine Reference Publication
ADS	Alternate Data Streams
AO	Area of Operation
AOR	Area of Responsibility
APT	Advanced Persistent Threat
ASD	Australian Signals Directorate
C	
CENTCOM	United States Central Command
CI	Counterintelligence
CND	Computer Network Defense
CNMF	Cyber National Mission Forces
COA	Course of Action
COM	Component Object Model
CONUS	Contiguous United States
CPT	Cyber Protection Team
CSS	Com Structured Storage
CTE	Cyber Threat Emulation
CVE	Common Vulnerability and Exposure
D	
DAL	Defended Asset List
DCI	Discovery and Counter-Infiltration
DHCP	Dynamic Host Control Protocol
DISA	Defense Information Systems Agency
DLL	Dynamic-link library
DNS	Domain Name Servers
DTS	Defense Travel System

G	
GPO	Group Policy Object
GRR	GRR Rapid Response
GTCC	Government Travel Charge Card
H	
HBSS	Host Based Security System
I	
I&W	Indications and Warnings
ICMP	Internet Control Message Protocol
IDS	Intrusion-detection System
IOC	Indicator of Compromise
IOCe	Indicator of Compromise Editor
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IR	Incident Response
J	
JFHQ-DODIN	Joint Force Headquarters –DOD Information Networks
JWICS	Joint Worldwide Intelligence Communications System
K	
KT-C	Key Terrain-Cyber
M	
MAC	Media Access Control
MP	Mission Protection
MSDN	Microsoft Developer Network
MSRC	Microsoft Security Response Center
MWR	Family and Morale, Welfare and Recreation
N	
NAT	Network Address Translation
NETOPS	Network Operations
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NIPR	Non-Classified Internet Protocol Router
Nmap	Network Mapper
NTFS	New Technology File System
O	
OCONUS	Outside the Contiguous United States
OSI	Open Systems Interconnection

P	
PAT	Port Address Translation
PCAP	Packet Capture
PDAL	Prioritized Defended Asset List
PDE	Participative Defensive Evaluation
PE	Portable Executable
PII	Personally Identifiable Information
R	
RFA	Request for Analysis
RFI	Request for Information
RMS	Rights Management Service
S	
SCADA	Supervisory Control and Data acquisition
SCIF	Sensitive Compartmented Information Facility
SEC	Sensor Emplacement Plan
SIGINT	Signals Intelligence
SIPR	Secret Internet Protocol Router
SITREP	Situation Report
SMM	Session Manager Subsystem
SNMP	Simple Network Management Protocol
SRP	Soldier Readiness Processing
SSDT	System Service Descriptor Table
SSU	Servicing Stack Update
T	
TASKORD	Task Order
TTPs	Tactics, Techniques and Procedures
U	
USCYBERCOM	United States Cyber Command
V	
VM	Virtual Machine
VPN	Virtual Private Network
W	
WARNORD	Warning Order