Guide to Red Team Operations

Raj   August 5, 2019

In this post you will get to know all about RED TEAM Operation and Practice, idea for this article came from the SANS SEC564 by Joe Vest and James Tubbervile.

Introduction to Red Team

Red Teaming comes under the level of assessment in the information security domain. Red Teamers have to identify the risk to the network infrastructure of an organisation as a measure of pre-evaluation so that the execution of engagement can be carried properly. In order to determine such risks, it is the primary responsibility of Red Team operators to recognise potential threats or vulnerability. Various tools, whether open-source or commercial, can be used by Red Teamers to acknowledge vulnerabilities and to exploit them to their advantage. However, the Red Teaming approach is more in-depth than what most potential attackers follow because they are attempting to find a single vulnerability, whereas security professionals need to find all possible vulnerabilities for a given infrastructure in order to assess the associated risk. Attackers typically only target a single vulnerability for a specific exploit because to do otherwise would increase the possibility for detection. Nevertheless, Red Teaming should test for all types of attacks to provide a complete security assessment. Appropriate situational awareness of security infrastructure is a result of detailed Red Team research. But the process of Red Team will not be sufficient in identifying risk; the organization should continue maintaining the security measures from their end in order to appropriately manage risk and provide security protection.

What is the Red Team?

Red Team is a group of highly skilled pentesters that are summoned by an organization to test their defence and improve its effectiveness. Basically, it is the way of utilizing strategies, systems, and methodology to simulate real-world scenarios so as to prepare and measure the security defences of the organisation. The objective of the Red Team is to simulate the real-world attacks in order to measure the organization's defences and their incident response Team. Red Team follows the Roles of Engagement (RoE).

What are the aspects of the Red Team?

- Threat Emulation
- Operational Impacts
- Comparing Red Team Engagement to other security testing types
- Red Team Operator Traits

Threat Emulation: This is the process of mimicking the TTP's of a specific threat. Emulation can be done of various attacks such as – zero attacks, script kiddie to the advanced adversary or a specific threat like botnets, ransomware, DDOS, etc. No matter what the scenario, the TTP outline by the scenario drive the rules a Red Team must follow to perform an engagement. When creating the threat emulation scenario, that threat's key component should be defined. When in Practice it can be difficult to simulate the real-world scenario in an exact manner. Therefore, the main focus of the Red Team is should be on the key component and then use their own TTP to fill in the gaps. The biggest challenge in threat emulation is simulating the threat to a level where an analyst believes the threat is real, Approaches range from using real malware to developing custom malware that models a real threat, to using tools that generate the indicators of compromise (IOCs) an attack from a real threat leaves behind. In any case, effective planning and determination of the critical components of a threat will lead to better threat emulation design.

Operational Impacts: Operational Impacts are actions or effects performed against a target designed to demonstrate physical, informational or operational weaknesses in security. These effects can be as general as performing a denial of service attack or more specific such as using high jacked ICS equipment to control a city's power grid. It is operational impacts that distinguish Red Teamer from others. Operational Impacts can be very effective in demonstrating realistic impacts against a target. The level of depth and of the impact can be as 'painful' as an organization is willing to explore. These impacts are typically performed against live production systems to have the highest level of fidelity but can be executed on test and development environments if they are representative systems.

Comparing Red Team Engagement to other security testing types

Difference b/w Pentesting and Red Team: Pentesting is used to monitor control and identify vulnerability in order to secure them along with testing the efficiency of the vulnerability management process. It further helps to lay the foundation for security policies. Basically, Pentesting is testing the security environment of infrastructure in order to find and patch vulnerabilities in a limited span of time, so that we can eliminate the false positive scenarios. In comparison to Red Team, Pentesting is the most rigorous and methodical testing of a network, hardware or application. During Pentesting, the pentesters search for vulnerabilities, analysis them and exploit them. Penetration tests are well defined and usually takes up to one to two weeks for the whole process.

Red Team includes tactics, techniques and procedures (TTPs) by adversaries. Red - Team is just like Pentesting in many ways but it is more targeted. A Red-Team overall accesses and evaluates various areas of security through a multi-layered approach. The mission is to present real-world scenarios and hard facts in an attempt to improve the company's response. Every area of security defines how the target will respond or how it is accessed. It follows the concept of defence in depth; therefore, the target must be

tested on each layer. The goal of the Red Team is to not find as many vulnerabilities as possible but to test the detection and response capabilities of infrastructure along with their security environment.

Difference b/w Read Team and Vulnerability Assessment: Vulnerability assessment is the process of analysing of a system that focuses on finding the vulnerability and prioritizing them by risk. Validation or exploitation of a vulnerability is not performed during while vulnerability assessment. When compared to Red Team engagement vulnerability assessment doesn't take priority. A Red Team may not use any vulnerabilities. They may generate an operational impact that any insider can perform to test the response of an insider attack. Red Teams rarely if ever run common vulnerability assessment tools as they are loud and generate more traffic than a typical Red Team engagement is willing to accept.

Difference b/w Red Team and Blue Team: Red Teams are the attackers whereas Blue Teams are the defenders. Red Team members are adept at all forms of digital attack, as well as social engineering and other methods to find ways to break into the systems of a company – but they are bound by employment agreements or legal contracts to not disclose what they find to anyone but the company that is being tested. While Team almost always works as employees of the company that is undergoing the testing, and are usually members of the IT Security or Data Security divisions of the company's IT group. Blue Teams have two major areas of operations. Their only focus is to find the vulnerability and patch them as it seems fit. They can also keep providing security during the Red Team engagement.

Red Team operator traits

An effective Red Team is comprised of a team of individuals who can contribute 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 multiple areas.

Core Operator Traits :

- Unorthodox Thinking
- Adversarial Mindset
- Experience
- Technical Capability
- Specialization
- Professionalism
- Communication Skills

Red Teams are given opportunities to touch and manipulate target networks in ways typically only done by real threats. Full-scale Red Team operations can allow Red Team operators to really put on their bad guy hats, engagement can be very intellectually stimulating and enjoyable for an operator, but operators must respect target organizations. A great deal of trust is placed on an operator. It is common for a Red Team to position themselves to do serious damage or embarrassment to an organization. And with all this, each Red Team operator should comply the following:

- Executes engagement requirements as directed
- Complies with all laws, regulations, policies, programs, and Rules of Engagement
- Implements the Team's operational methodology and TTPs
- Identifies and has input to target environment deficiencies
- Researches and develops new exploit tools and tests tools for functionality
- Performs Open Source Intelligence as required for the engagement
- Identifies and assesses actions that reveal system vulnerabilities and capabilities
- Assists the Red Team Lead in development of the final engagement report
- Performs Physical Assessment support under the direction of Red Team Lead

Why do we need Red Team?

To challenge the extend of an organisation's defences so that when and if a real attack happens then they stay protected or come up with a counter measure. For example, a group of hackers has a goal of stealing critical data from a target. A targeted phishing attack tests the end user's awareness of the attack. The payload of the attack tests the network and host defences against delivery of malware and ultimately code execution, If the attack does trigger a defence, the response tests the defender's actions in identifying, responding or stopping the attack. In any case, the entire scope of security defence is analysed. A highly skilled Red Teamer can tune their attacks to identify where the failure points are by turning up or down that 'volume' of an attack.

Red Teams are able to execute custom threat as part of their engagement. It can test a subset of security of new threat type or validate the effectiveness of security controls against a new or specific threat types. Threat emulation scenarios are a valuable distinguisher of Red Teaming from other types of security assessments and can be used to understand how an organization stands up to new zero-day attack.

Working of Red Teamers?

Red Team tactics contains a full scope, multi layered diverse attacks to simulate real world attacks to measure the security alignments that are applied. Assessments of Red Team starts with reconnaissance to collect as much information as possible about the target in order to determine the way best way possible to exploit it. This collecting of information also helps to build attacking environment and selection of tools. Most of the working of Red Team is on offensive side rather than defensive. Once the remote access to exploited system is managed and stabilised, the actual attacking takes action.

What is the specialization of Red Teamer?

Red Teamers must understand and be an expert in a diverse set of technologies such as :

- Different operating systems and software packages
- Diverse networking protocols
- Custom applications and protocols
- Physical security defences
- Social interaction
- Custom or specialized technologies
- System Engineering
- Networking
- Software Development
- Physical Attacks

Red Teaming Operations Modules

Methodology of Red Team
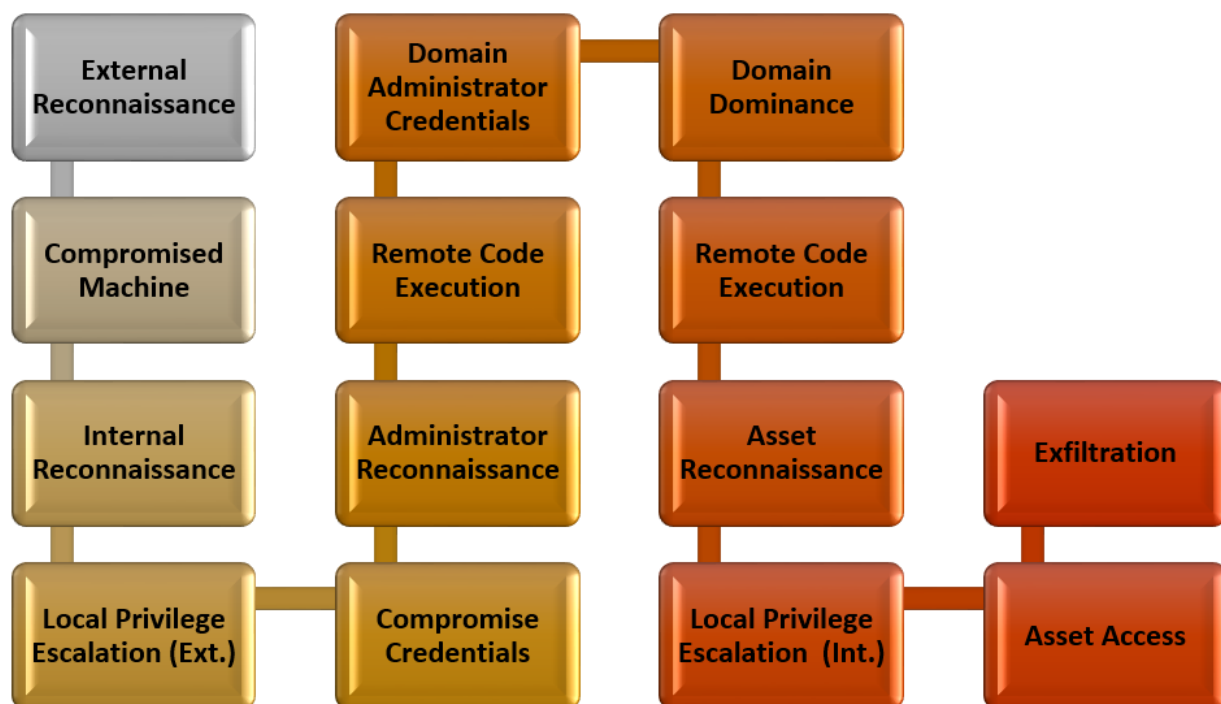
What are the Pre-Engagement Data Requirements?

The pre-engagement data requirements are
:

- Target POC list
- Notification Requirements
- Threat level
- ROE

- OSINT
- Analysis of Potential Attack Vectors and Tools

What is a Red Team Standard Attack Platform?

A standard attack platform is the common set of tools and hardware used by a Red Team to perform an engagement. The term standard is critical. Using a standard platform allows for:

- **Better Logging:** A common platform shares the same base build, directory structure, and built-in data capture capability.
- **Easier Deconfliction:** A common set of tools and payloads, along with standard logging, can help an organization quickly work through the deconfliction process.
- **Common Baseline:** A common base provides a stable, functional environment for a Red Team to operate.

- **Access to Better Toolset :** A shared platform is built from the knowledge of many people. The best tools, references, and guidelines can be contributed from multiple senior Red Team members to include their expertise in the toolbox.
- **Custom Tools Work Across Attack Platforms :** Red Teams often build tools. If these tools are built to work on a standard attack platform, they will work for all Red Team operators.
- **Tool Vetting :** In some cases, a Blue Team or customer requires tools to be vetted as threat faithful. When using a standard attack platform, a tool vetting process is often required before including a tool. This way, all tools are managed and validated before use. Tool validation is often due to a fear the Red Team tools may cause damage to a system.
- **Consistent Processes :** Using a common baseline help enable a common set of processes. A common set of processes can allow the skills and knowledge of senior operators to be used by junior operators. This can greatly enhance an engagement's success and better use limited resources.

What are Red Team engagement roles and responsibility?

White Cell : A white cell basically enforces the rules of the engagement to ensure neither Red Team nor defender activities cause unexpected alerts or problems on the target environment. It helps to co-ordinate activities to ensure engagement goals.

Engagement Control Group : It represents the management of target environment as well as provides required information that is necessary for constructing valid scenarios. Also, it helps to establish blacklist if its needed.

Physical Access Team : The sole purpose of Physical Access Team in Red Team is to enter gates, buildings, offices, server rooms, etc. along with demonstrate physical access to systems and network in order to gain access to devices or anything desirable.

General Guidelines for Red Teaming :

- All Red Team members are responsible for safeguarding all customers data. This said data includes Personally Identifiable information (PII), Industry BBP.
- Red Teamers should work under Privacy Act Information.
- They should avoid data mining of files containing privacy act, medical, justice, worship or religious pursuit or any other protected or privilege information.
- Red Team is normally authorised to exploit files, e-mail and/or message traffic stored on the network or communications transiting the network including everything else. However, each Red Team member should ensure that all the information exploited is necessary and within the scope of engagement.
- Red Team should not be modifying the data found or conduct DDOS unless it's specifically requested. As it is required of the Red Team to not otherwise intentionally degrade or disrupt normal operations of targeted system being exploited.

How to handle client data?

Client data should be handled with extreme care. The information collected during an engagement can be misused if fallen in wrong hands.

Permission :

The ROE should identify permissions for Authorization :

- Actions
- Data Collection
- Data Leverage
- Target Space
- User Groups

Policy Controls :

It is implemented by the Red Team and it includes :

- A Red Team non-disclosure agreement
- Data training which means identifying and avoiding PII, PA data, etc.
- Ethics training
- Individual Background Checks

Physical Controls :

There should be multi-layer of physical controls applied to protect the engagement tools and operating system from any kind of loss. Therefore, Red Teamers should be accustomed with physical controls that are in place. Such security mechanisms include :

- Tools, computing systems and costumer data be stored inside isolated room secured with cipher lock and controlled only by Red Team.
- Minimize contact between the Team and external entities.

- When not in use, all data and equipment should be removed and placed into lockable cases, safes or storage cabinets.
- During travel, laptops, and hard drives are secured at all times.
- All visitors to Res Team space should be escorted and signed in and out.
- Customer data should only be handled by Red Team personnel with need to know.
- During off-site engagement, data should be encrypted for transmission.

Software Controls :

The following software controls are designed to ensure the confidentiality, anonymity and safety of information should always be employed in whatever context :

- Each host and guest operating system should be encrypted and protected with a strong password.
- Each host and guest operating system should be employed with a host-based firewall specific to the engagement.
- Data and tools utilized during an engagement should be stored in an encrypted container and moved to the working directory only when needed.
- All Red Team tools and software should be removed from the target environment at the end of the engagement.
- All access, movement and use of data and tools should be added to the OPLOG (Operations Logs).
- If a tool is not needed then it should be removed from the environment.

Common repository :

- A common repository should be made available to all the Red Teamers assigned to engagement.
- It should be stored within an encrypted volume
- It should always be encrypted volume lives on centralised server/NAS/file share
- It should be mountable or accessible only after authentication
- Repository layout should be in Hierarchy.

Data Collection

Data collection is the core of every engagement. Data collection is directly proportionate to the success of engagement. in other words, the collection of data drives the value of the engagement. Data collection should be complete with the enabling of replication of activities and results. It should also help you to identify the items of significant interest to the operators. Final Data sets should include :

- Pre-event data
- Execution data
- Operator logs
- Automated data collection and logs
- Screenshots
- Post event data (data archive, closeout brief, final report)

Execution data requirements

Under this, the Team has to make sure that all data that is being handled is safely logged. All activities related to Red Team operations should be logged as the engagement begins and only terminates after all the activity related to the engagement is completed. The events that should be logged are :

- Scanning activities
- Exploiting events
- Stimulation efforts
- Deconfliction discovered
- Target information discovered
- Target acquired and lost
- System events
- Login attempts
- Credentials captured
- Credentials used
- File system notifications
- Modification or disabling of security controls
- Modifications or suppression of security alerts or logs
- Methods of persistence employed
- Methods access
- Methods of access
- Methods of persistence employed
- Command and control channels established
- Request to increase, decrease, pause activity
- ROE conflicts, request and modifications

Operator Logs

As stated earlier, all the activity should be logged accurately and concisely. at the very least, the following information must be collected and logged for each action performed :

- Start Timestamp (UTC Recommended)
- End Timestamp (UTC Recommended)
- Source IP (Attack/Test System IP address)
- Destination IP (Target IP Address)
- Destination Port (Target Port)
- Destination System Name
- Pivot IP (if applicable, list IP of any system used as a pivot, port forwarder, etc.)
- Pivot Port (if applicable, list send and receive ports leveraged in pivot system)
- URL (Note, it is important to capture the FULL URL of the Target instance)
- Tool/Application
- Command (Full command)
- Description (why or for what purpose was the action was performed)
- Output

- Result
- System Modification (Modified file, dropped binary location, enabled functions, etc.)
- Comments
- Screenshot
- Operator Name

Also, when creating log entries, documenting actions, uploading/downloading files, dropping binaries, etc. It is recommended to document this in the YYYYMMDDHHMM_IPDescription format.

Automated Data Collection

Where ever the chance, the Team should use tools and scripts available to capture and consolidate engagement data. Data collected by automated tools will never be enough for Red Team. However, if employed properly, complements the Red Team workflow and enables the operator to continue operations with the manual capture of data pertinent to the activity performed.

Terminal logs

All Red Teams engagement systems should have automated collection of raw terminal data. Each command should be prefixed with operator's IP and UTC timestamp. It is more important that data is accurately captured rather than being captured in a novel way.

Commercial tools

Most tools used for Red Team have some level of logging the activities, but the location of logs that will be maintained is different depending on the tool and many of them requires for the operator to trigger log generation. In any case it is quite handy to use commercial tools.

Consolidation

Daily transfer of these logs to the engagement repository is recommended. Preference should be to create a backup script that copies each set of logs to the repository when executed at the end of the day.

Screenshots

Details concerning Red Team actions are often met with disbelief. Even when the Team has undeniable evidence of access to a highly restrictive network or physical area, target personnel sometimes have issues conceding access was obtained. And so, provide the proof whenever required.

What is Red Team Engagement flow?

The Red Team engagement flow is a dynamic process but can be managed through distinct steps. the flow of Red Team includes
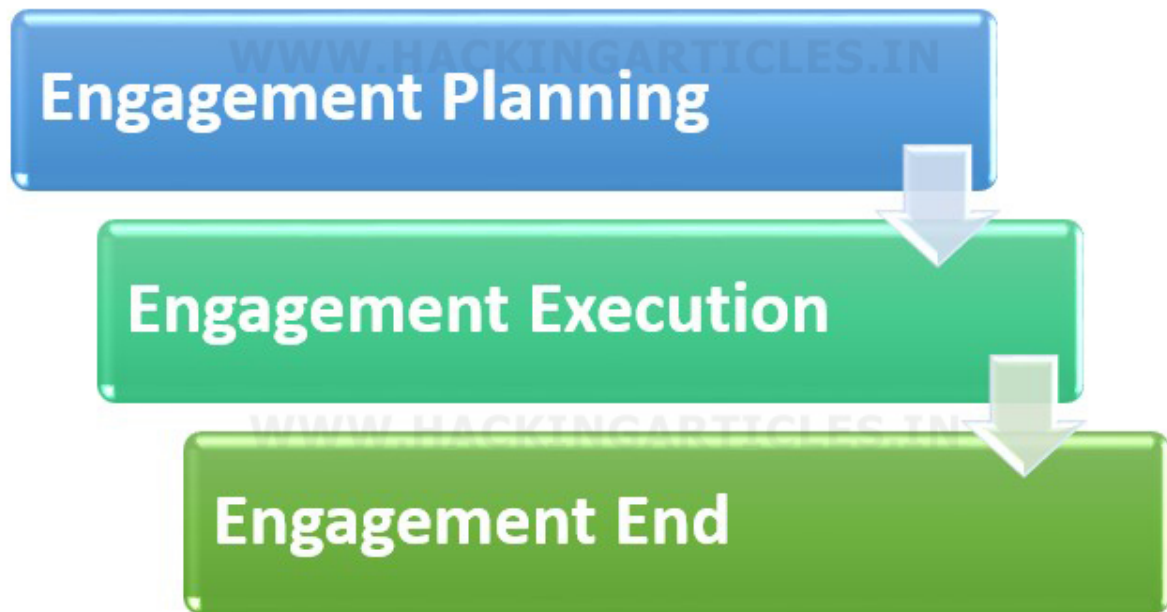
Engagement planning starts when first contacted by the customer and realistically doesn't end until the day of execution. Engagement determines the objectives of the working of the Team. Engagement planning includes :

- Rules of engagement
- Management risk
- Threat Planning
- Deconfliction Process
- Costs and Funding

Rules of Engagement : The rule of Engagement establishes the responsibility, relationship and guidelines between the Red Team, the customer and the system owner. This Rules of Engagement drives the whole process of execution. Rules of Engagement includes :

- Authorised Actions
- Explicitly Restricted Actions
- Authorised Targets and Target Space
- Restricted Items
- Engagement Objectives

The Rule of Engagement document consist of Red Team methodology with detailed description of activities and execution process along specification of the hardware and software to be employed. It also includes deconfliction process with the mention of threats available and their comparison. It also must include identification and references to appropriate legal requirements along with the legal responsibility disclaimer. Task of each Red Teamer must also be documented along with the whole information of the target. This information of the target has organization name, address, specific groups or divisions, organizational identifiers, senior management contact info.

Pre-coordination is the base of successful engagement. To construct an effective plan, the Red Team must understand the target environment, all stakeholders, and any addition legal and contractual requirements of the target environment.

Management Risk : It is a process of identifying, accessing and controlling that risk that comes from the engagement factors. The main aim of managing risk to remove unnecessary risks instead of eliminating all of them, along with implementing efforts that are outlined in ROE without causing any irreversible damage to target environment. It is the responsibility of Red Team to implement risk management and accepting all the risks at an initial stage. Risk Management is important to Red Team engagement as it helps to conserve resources, avoid unwarranted risk, making alternative decision when required and taking effective control measures. The Risk management process includes :

- Identify potential issues
- Assess each risk to determine the direct impact to the target environment
- Develop controls designed to mitigate risks
- Make a risk decision
- Identify Residual risk
- Continually assess

Risk Evaluation under Management Risk

Evaluation is often visualized by constructing a Risk Assessment Matrix. This matrix is commonly used to estimate the degree of severity and probability for each potential vulnerability.

Standard 3×3 Vulnerability Risk Matrix Example:

Probability: The likeliness that an event will occur

- Low — Unlikely
- Medium — May result in
- High – Likely

Impact: is the expected result of an event (degree of injury, property damage or other mission impairing factors) measure as:

- Low — Restricted Impact on Operations
- Medium — Measurable impact on Operations
- High — Important Impact on Operations

Standard 5×4 Vulnerability Risk Matrix Example:

Probability: The possibility of occurrence of an event

- Frequent – Occurs often
- Likely – Occurs several times in x period
- Occasional – Occurs sporadically

- Seldom – Unlikely, but could occur
- Unlikely – Probably will not occur

Severity: is the expected result of an event (degree of injury, property damage or other mission impairing factors) measure as:

- Catastrophic Direct impact, Rustically long duration if not permanent
- Critical —Significant Impact, Stops or Halts operation
- Moderate — Noticeable loss, Reduces/Slows Operation/Production
- Marginal — Limited loss, noticed but does not halt operation
- Negligible — Some loss, Unnoticed if not monitored closely

The key in the above matrix construct is vulnerability; however, Red Teaming is not vulnerability focused. Given that thought process, the Red Team's alternative risk matrix should be constructed to determine the risk of potential threat actions.

Threat Planning

It is a major factor in Red Teaming engagement. In this stage following information is obtained from the customer and OSINT:

- Threat Information (Landscape TTPs)
- Threat to the Target Environment (OSINT)
- Threat to the Target Environment (Customer Issues, Previous Grievances)
- Real world example of threat
- Threat in Engagement condition
- Level of Threat
- Target Data

The realism of threat must be taken under consideration by the Red Team. It is the job of Red Team to select attack types and strategies to simulate realistic threats even if the organization decide not to unleash the full capabilities of the threat. Defining threat-based attacks will provide a viable mechanism for training the target audience and strengthening the target environment. In order to outline the initial list of attacks the Red Team to carefully weigh the different options in regard to the engagement.

The end goal of threat planning is to portray the threat as real as possible in order to protect the organization from the real attack.

De-confliction process

De-confliction allows Red Team to clearly identify which activity is to be and not be generated by them. The said activity includes both network and physical activities. In this stage of engagement is to be able to distinguish between Red Team activity and real-world attack as quickly and as correctly as possible. deconfliction process includes :

- Ensuring trusted agents understand the actions and impacts of activities as they occur.

- All OPLOGS are accurately and thoroughly completed.
- Providing OPLOGS and activity list to the ECG as requested
- Exchanging periodic situation reports with the white cell.

When the De-confliction is requested it is the duty of the Red Team lead to assess the information and isolate the information from Red Team activity. This includes:

- Halting all activities in the area of the incident
- Reviewing the ROE for limitations, objectives and dc-confliction instructions
- Reviewing OPLOGS to determine activities the Team was conducting at the time indicated
- Confirming or Denying Red Team activities for each deconfliction incident
- Confirm findings with the ECG, White Cell, and TA.
- Ensure findings are relayed by e-mail as well as by telephone
- Maintaining records of de-confliction information, actions, assessment and findings
- If assessment indicates the Red Team is the originator:
- Determine and isolate the specific activities and scripts employed
- Determine and isolate the specific logs supporting the timeframe of the incident
- Notify the Engagement Control Group

The engagement planning process should include the estimate amount of time required to properly execute the De confliction process and when to use it.

Free play is an excellent concept to greatly enhance the results of A Red Team engagement. This concept allows the time to deviate from plan in order to explore for interesting operations. A Red Team lead can always provide guidance to freely explore as time allows them to.

Engagement Execution

Halting an engagement simply means pausing current actions for a certain span of time. It is important to decide and plan the conditions where a pause is required. In following conditions, a HALT is required:

- Deconfliction request are received
- Real-world issues impact the target environment
- Key personnel suddenly become unavailable

A SITREP (Situation Report) is generally performed by Red Team lead. It is to be maintained at all times. And it should contain the following information:

- Current location of operation (systems/networks for network Teams or buildings/offices for physical Teams)
- Information pertinent to the objectives of the Team
- Information key to the success of engagement impacts
- Updates or modifications to the ROE
- Recent actions of each Team member

- Current action of each Team member
- Intended future actions of each Team member

Detailed methodology of Red Team

- Reconnaissance
- Perform Open Source intelligence (OSINT) against the target
- Search using open unauthenticated sources
- Target websites
- Social Media
- Search engines
- Public Code repositories
- Alternate target sites
- 8 External Enumeration
- Identify external assets
- Perform reverse DNS scan to identify registered hosts
- Identify URLs and other external touch points from scan and OSINT
- Web presence evaluation
- Browse as a normal user through a web proxy to capture intelligence and understanding
- 8 Identify known vulnerabilities and vulnerable conditions
- Do not send attack code at this time
- Execution and 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
- Post-Exploitation
- Continue internal and Domain enumeration
- Identify domain user/groups/memberships
- Identify IP space
- Identify file shares
- Establish persistence
- Use persistence plan to place agents on target systems
- Move Laterally
- Operational Impact
- Perform realistic stimulation against target systems
- Does not need to be highly complex
- Does not need to leverage known or traditional vulnerabilities
- Does not always require administrative (local/domain) privileges
- Does require actual impact to the target environment
- Does require input from the ECG and TA (during planning)
- Do notify the ECG and TA when the operational impact is executed to avoid unwanted (possibly
- catastrophic) defensive actions

- Does need to exercise the target's detection, incident response, continuity, and recovery plans and procedures at a minimum.

How to End the Red Team Engagement?

After the execution of engagement is done, it is very important to systematically end the Red Team Engagement. Some of the important things to remember when ending the Red Team engagement are reverting modifications, executive out brief and tech on tech sessions.

Once the execution of Red Team is done with, all the tools, artefacts, exploits and persistence mechanisms should be auto destroyed by a self-destruct code written as both time-based and target-based; for it to be able to prevent execution outside the engagement window or to prevent exploitation outside the target environment. And for all the things that could be self-destroyed, it is the responsibility of Red Team to essentially remove it from the environment.

In the event that target system security controls were disabled:

- Restore the controls as soon as possible
- Test the control to ensure restoration
- Notify the TA of any security control that does not effectively restore

In the event that target system modifications were made:

- Revert file system modifications
- Remove access mechanisms and/or backdoors
- Remove C2 and persistence mechanisms
- Terminate C2 Channels

For all restoration actions:

- Ensure file artefacts generated by the mechanism are removed
- Examine entire system to confirm the mechanism was not inadvertently copied or moved
- Remove or restore registry keys if used
- Restore modified files
- Remove or replace launch files with original
- Examine start-up scripts if used.
- Remove execution mechanisms
- Remove installation mechanism
- Copy log files generated by the mechanism to the Red Team repository and remove them from target system
- Continue connection monitoring for stray or missed mechanisms
- Repeat process for strays
- Provide a list of all artefacts, names, hashes, locations, and clean-up status to TA

Executive out brief is a meeting dedicated towards impact of Red Team engagement on the organization and how to protect it. In this meeting, Red Team lead has to highlight critical observations made during the engagement along with additional information security or technical staff. Legal staff and critical system information's can also be included with the observation of 'where the organization is vulnerable'.

A tech on tech briefing can be extremely valuable to the organization as it provides bi-directional exchange of information between Red Team and blue Team. During this exchange, both the Red and defensive elements provide a highly detailed step-by-step technical review of the actions and results (including all associated detail) of the engagement.

The role of Red Team during tech-on-tech:

- Explains Red TTPs and intended IOCs
- Their initial thought process for meeting engagement objectives
- Steps through Red actions and associated activity/commands (This occurs simultaneously to defender walk through)
- Describes why those actions were executed (What lead the RT to that specific action)
- Provides the results of each action and how that action enabled the next
- Provides recommendations or techniques that would limit each threat action

The role of Defensive Team tech-on-tech:

- Has the opportunity to ask the how and why
- Explain the process for securing and defending their environment
- Identify any alerts, triggers, or anomalies within the environment during engagement
- Step through blue actions in response to Red Team activity (this occurs simultaneously to Red Team walk through)
- Identifies how Red Team activity could have been detected, prevented or leveraged
- Provides feedback to Red Team actions and recommendations
- Uses tech-on-tech information to perform post engagement analysis prior to receipt of official report

Report Writing

Reporting is a critical aspect of Red Team Engagement. Reports are major form of evidence that can be analysed and used to provide a base for improving security. Reports are important as they confirm the existence of engagement. Reports not only document the activity that occurred during a specific engagement, but provide an excellent reference that can be used to plan and design other engagements. Many engagements can share similar approaches and goals. Reports can provide a roadmap to design and plan future engagements. Reporting a Red Team engagement can be quite different than reports generated in penetration tests or vulnerability assessments. Red Team engagements are highly scenario focused. This leads to a report that is story driven. Penetration testing or vulnerability assessment reports focus on findings. security tests.

Rather than discover that an out-of-date patch can cause successful exploitation of a workstation, a Red Team may use the exploit to deploy a command and control agent. This agent can be used to explore an organization and ultimately steal proprietary organizational data. The Red Team is driven by goals intended to stimulate or measure not only technical flaws but security operations as a whole. This includes people, processes, and technology. A Red Team report will use a story-based format where observations instead of findings are listed.

Report includes various perspectives such as attack narrative. The Attack Narrative section of the report contains the observations made during a Red Team engagement. These are typically written in a chronological format. Key observations that a Red Team uses to achieve goals must be documented. This includes any step Red Team takes to achieve a goal. Threat profiles or other IOCs that Blue can use during post analysis should be included. The end of a Red Team engagement is can be the beginning of post forensic analysis. Blue Teams who take advantage Red Team IOCs by performing post analysis can use this information to find blind spots or tune security tools to better protect against threats.

Report Outline

```
┌─────────────────────────────────────┐
│            Title Page               │
└─────────────────────────────────────┘

┌─────────────────────────────────────┐
│         Executive Summary           │
└─────────────────────────────────────┘

┌─────────────────────────────────────┐
│       Methodology and Goals         │
└─────────────────────────────────────┘

┌─────────────────────────────────────┐
│         Scenario and Scope          │
└─────────────────────────────────────┘

┌─────────────────────────────────────┐
│          Attack Narrative           │
└─────────────────────────────────────┘

┌─────────────────────────────────────┐
│   Observations and recommendations  │
└─────────────────────────────────────┘
```

Types of observation that should be documented:

Key actions that led from initial access to the final goal

- Initial access
- Lateral movement
- Privilege escalation
- Command and Control (C2) description
- Include network information (IP addresses, Domain name, Ports, Protocols, etc.)
- Include agent information (Binaries, Scripts, Locations, Registry Changes)
- Include persistence methods
- Reconnaissance actions and results
- Other interesting observations that assisted the Red Team during the Engagement
- Other interesting observations that may be of concern but not directly related to the engagement

An observation should include the following elements

- Narrative description
- Technical details
- Source/Destination I P addresses
- Tools or techniques
- Results
- Screenshots

Author: **Yashika Dhir** is a passionate Researcher and Technical Writer at Hacking Articles. She is a hacking enthusiast. contact **here**