Process management for red team and threat intelligence activities in an organisation

Theodor Adam, Florin Andrei, Larisa Gabudeanu, Victor Rotaru

Because cyberthreats are continuously escalating, we need to get an authentic picture of our organization's defences. We need to have a clear understanding about how effective our organization's security is, by considering the current threat landscape, in order to continuously improve organization's security effectiveness (people, process, and technology). This challenge can only be addressed with a holistic approach, it is obviously broader than pen-testing, and it should be a continuous process with the following main objectives:

- to prepare the organization for targeted attacks (especially multi-step, multi-vector attacks like Advanced Persistent Threat (APT));
- to assess the effectiveness of the organization's prevention strategy and program;
- to identify and mitigate any kind of vulnerabilities in the organization's infrastructure;
- to minimize the organization's public digital footprint (and consequently, its digital attack surface), and
- to enhance the organization's security team ability to detect and respond to real-world incidents.

The steps an attacker must complete to carry out a successful attack are described by the Lockheed Martin's Cyber Kill Chain model. This model is made up of seven sequential steps including:

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control
- Actions on Objectives

To disrupt an attack, one or more of these steps must be broken for the entire chain to fail. We need to understand adversary behavior in order to apply effective defensive tactics and techniques.

RECONNAISSANCE

The first step of any cybersecurity attack is the collection of information about the victim, also known as reconnaissance. There are two different phases of reconnaissance:

- Passive reconnaissance;
- Active reconnaissance;

During the passive reconnaissance phase, the attacker will use indirect methods to gather information about his target(s) from publicly available sources like:

- Whois
- Google
- Shodan
- Company websites
- Job Listings

A company is a sum of its employees. Today, each employee has his/her own digital footprint. Either in his/her "personal digital life" or "professional digital life", each employee performs some online public digital actions across the public web (uploading a resume to a site, publishing an article on Linkedin or other site, commenting on a blogpost or tweet, etc). All these kind of little seeds of information left by an individual or a company across the public web, we call it "digital footprint". Depending on the individual's age, some of the online public digital actions could have been performed years ago when cyber security awareness was virtually non-existent. Any connections between these digital footprints and the company can be used as an enabler (attack vector) against the company. Having a digital footprint is normal – they are very difficult to avoid. What we can do is to become aware about what it looks like and actively manage it.

SpiderFoot is a reconnaissance tool that your security professionals might consider to use for the assessment of the organization's digital footprint on the public web. It automatically queries over 100 public data sources (OSINT) to gather intelligence on IP addresses, domain names, e-mail addresses, names to build up an understanding of all the entities and how they relate to each other. OSINT (Open Source Intelligence) is data available in the public domain. This includes DNS, Whois, Web pages, passive DNS, spam blacklists, file meta data, threat intelligence lists as well as services like SHODAN, HaveIBeenPwned?.

Regardless what tool you will choose to use, you should be aware that there is a dark side to intelligence gathering: anything that can be found by security professionals can also be found (and used) by threat actors. Having a clear strategy and framework in place for intelligence gathering is essential — simply looking for anything that could be interesting or useful will inevitably lead to burnout. A very careful and responsible attitude is mandatory for intelligence gathering because it can change the risk surface of the assessed environment.

The data returned from an intelligence gathering scan will reveal a lot of information, providing insight into possible data leaks, vulnerabilities or other sensitive information that can be leveraged during a penetration test, red team exercise or for threat intelligence. All this information it is very helpful to create a good understanding of what you might have exposed.

Defending against passive reconnaissance means limiting the level of details we expose. To know where our weak points are, we need to understand our complete digital footprint and view our organization like a hacker would and try to limit the exposure, if possible. For instance, this can start with the websites and web/mobile applications of the organization. So, removing specific error messages from the organization's public servers should be considered. In addition, as mentioned previously, employees are a critical component of your cyber security protection, and are often the weakest link in the chain. There is no replacement for employee cyber security education, which emphasizes various tactics used by adversaries and details consequences of actions exposing data. Limiting the information we put on job

postings and on the company's web sites helps to reduce the organization's digital footprint. It will be also a very good idea to consider also your business partners for the digital footprint assessment.

With the GDPR, now the basis for European data protection law, the Right to be Forgotten and the pre-GDPR obligation to delete unnecessary data (for which there is no legal basis of storing), is available to use to remove inaccurate or out of date data. Further, the data minimization principle entailing limitation of data exposure, but also anonymisation or pseudonymisation of data (e.g. in testing environments, in case of data analytics) ensures limitation of unnecessary data exposure. So, don't hesitate to use these. Always ask yourself: does this person need access to this data? And do we really need to keep this data for a specific purpose?

The best advice we can give is this: think before posting – this is one of the easiest ways to keep someone safe online and reduce his/her digital footprint. Don't ever share details you don't want the world to see, and don't ever post something you don't want out in the world forever.

Once an attacker has collected as much public information as possible about his target(s), then he will move on to active reconnaissance. Active reconnaissance involves some level of interaction with your organization.

During this phase, the attacker will actively probe your network looking for open ports and services. The idea is to discover exploitable communication channels and find various ways to intrude the target system. The tools used for active reconnaissance include: nmap, OpenVAS, Nikto, netcat, Metasploit.

Network reconnaissance is a crucial part of any hacking operation. Any information that a hacker can learn about the target environment can help in identification of potential attack vectors and targeting exploits to potential vulnerabilities. Vulnerability scanners are very loud and obvious so attackers will usually limit their scope or slow scan over a period of time to avoid being noticed.

An attacker may choose to obfuscate his scan. A common obfuscation method is to spoof many source IP addresses along with the real source IP for a port scan. The target machine will likely log the scan, but it will be extremely difficult for the network admin to determine from which IP address the port scan actually originated.

During the COVID-19 pandemic crisis, many companies decided to allow remote working through remote services such as VPNs, Citrix, and other access mechanisms that allow users to connect to internal enterprise network resources from external locations. This increases the risks at higher level because adversaries may use remote services to access and/or persist within our network.

For active reconnaissance, our first protection measure is at the network infrastructure level by ensuring that unused ports and services are disabled. A stateful firewall with IPS capabilities placed on a network perimeter is likely one of the best prevention measures for any intrusion. The firewall should be configured to allow only the necessary traffic and should log multiple connection attempts from the same source IP address. This limits the number of entry points an attacker can use to get into our system. Use strong two-factor or multi-factor authentication for remote service accounts to mitigate an adversary's ability to leverage stolen credentials and disable or block remotely available services that may be unnecessary.

The main goal of the reconnaissance phase is to find weaknesses that can be exploited. Once the attacker has found at least one weakness he can move on to the next step. If he couldn't find any weakness, he cannot move forward. This is why it is critical for our security professionals to find and fix all the weaknesses before an attacker can find and exploit them. This is the reasoning behind the defense in depth concept.

WEAPONIZATION

Once an attacker has found a weakness, his next step is to find or create an attack plan to exploit that vulnerability. The weapon of choice will depend on the information collected during the reconnaissance step.

Some commonly used weapons during this phase are tools like Metasploit or Exploit-DB. These are repositories for known exploits. The Veil framework is commonly used to generate metasploit payloads that bypass common anti-virus solutions. TheFratRat is an easy tool to generate backdoors and to post exploitation attacks. The Social-Engineer Toolkit (SET) might be used if the attacker decides to deliver the malware through a social engineering campaign. These are only a few possibilities among many others an attacker has to build his weapon. We need to consider also that the attacker might choose to craft his weapon by using a different pattern than those already available.

What we need to acknowledge is that the vast majority of today's breaches are still because the basics are not fully covered: unpatched servers and computers, outdated antivirus, installed plugins etc. All these are paths for an attacker to exploit. For this reason, patch management along with up to date antivirus program and disabled plugins and macros continues to be the best defensive measures against weaponization phase.

This phase is all about what the attacker can use as a weapon. Reducing the exposure by keeping the operating systems and antivirus up to date are critical because you can't exploit a vulnerability if there is no vulnerability to exploit. We can add an IDS/IPS tuned to look for exploit attempts.

During the weaponization phase, the attacker is selecting which weapon to use, but has not delivered it yet. How the attack is delivered is as critical as what was selected as a weapon. This brings us to the next phase.

DELIVERY

At this point, the attacker has selected the weapon based on his earlier reconnaissance. Now, he will try to use one or multiple paths to deliver his weapon(s). The delivery path varies by the kind of attack, but the most common examples are: e-mail, website, social media and USB flash drives. Through e-mail, if the attacker has found during the reconnaissance phase, a partner or a supplier he can use, then he might embed a malware into an attached file and might disguise ("phish") the e-mail to make it look like it's coming from that partner/supplier. In this way, there is very likely that an employee will open it. The attacker might choose as well to infect a frequently used website. To use a social network as vector to targeted attack, this means that the attacker has some level of interaction with this environment. It is not difficult for example, during a conference, an attacker to obtain one or more USB flash drives with the conference materials, to infect them with a rootkit and to return them. Or even worst and less daring, by leaving an infected USB flash drive somewhere in a public area, around employees, hoping that the temptation for them to put it into their computer will be big enough to make it happen.

The single best security measure against the delivery of the attack is user awareness. This includes security training for both employees and security staff about threats and good security practices. If we acknowledge that careless or uninformed staff, for example, are the second most likely cause of a serious security breach, finishing only second to Phishing/Malware (which still requires a human error to activate), we will understand how important is the employee awareness to keep the organization safe.

To limit the delivery paths an attacker can use we can implement the following measures:

SPF, or Sender Policy Framework, is an email validation protocol designed to detect and block email spoofing. SPF is a "proposed standard" that helps protect email users from potential spammers.

DKIM, or DomainKeys Identified Mail, lets an organization (or handler of the message) take responsibility for a message that is in transit.

DMARC, or Domain-Based Message Authentication Reporting and Conformance, is an added authentication method that uses both SPF and DKIM to verify whether or not an email was actually sent by the owner of the "Friendly-From" domain that the user sees.

Installing Web Application Firewall (WAF) or at least web filtering to prevent an user to access known bad websites.

DNS filtering to prevent DNS lookup attempts.

Disabling USB ports on the computers and not giving administrative rights to users prevents on one of delivery paths.

Nevertheless, we need to do SSL inspection for all of our delivery channels. Full SSL Inspection or Deep SSL Inspection is required to do antivirus scanning, web filtering, email filtering, etc. in order to filter out malicious content from our network traffic. New generation of firewalls also support a second type of SSL inspection, called SSL certificate inspection. It's worth noticing that an attacker will almost always use encrypted connections to avoid being caught. If we are not doing full SSL deep packet inspection, we have no chance to detect any communication attempts going through an encrypted communication tunnel.

If the attacker succeeds to deliver the weapon, then he will move to the next phase.

EXPLOITATION

During the Exploitation phase, the attacker has delivered his weapon(s) of choice to the victim(s) and the attack has been executed. This means that we failed with all of our prevention measures to keep the weapon outside of our environment. Now, we wait for the moment when the attacker will pull the trigger and 'detonate' the attack. We should expect also that the attacker will attempt to compromise additional systems and/or accounts by gaining admin-type rights.

Once the attacker has been able to execute the exploit, the protective measures we can rely on are very limited. If we are lucky and the exploit used by attacker is known, then we still have Data Execution Prevention (DEP) and the anti-exploit technology embedded in antivirus.

Data Execution Prevention (DEP) is a security feature within operating system that prevents applications from executing code from a non-executable memory location. It was designed to secure against memory-based code exploits and it is available in Windows, Linux and Mac OS.

An appropriate countermeasure might be to deploy an automatic rights escalation and de-escalation to streamline the process and contain an infection in case of an intrusion.

Although there's no guarantee that sandboxing will stop zero-day threats, it offers an additional security layer by separating the threats from the rest of the network because it runs in a separate system. When threats are quarantined, cybersecurity experts can study them to identify patterns, helping to prevent future attacks and identify other vulnerabilities. It also allows IT to test malicious code in an isolated testing environment to understand how it works within a system as well as more rapidly detect similar malware attacks.

An exploit is not a one hit operation. The goal of the exploit is to gain better access on our resources. This leads us to the next phase.

INSTALLATION

From the attacker's perspective, gaining better level of access allows him to control the victim, even after the system has been patched or restarted. The attempts for gaining better level of access are not limited to one system. The attacker might choose to take his time and restart internally the cyber kill chain by starting a fresh reconnaissance phase after he gets full access to one of our systems.

The goals of the installation phase are to create persistence and to get better level of access to accomplish the mission. Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials and other interruptions that could cut off their access.

Traditional detection sensors based on traffic analysis and comparisons with known attack signatures, are not particularly effective when it comes to detecting subtle attacks like APTs, or unknown threats like 0-day.

Endpoint Detection and Response (EDR) focuses on detecting attackers that evaded the prevention layer of an Endpoint Protection Platform (EPP) solution and are now active in the target environment. EDR can detect an attack has taken place, take immediate action on the endpoint to prevent the attack from spreading, and provide real-time forensic information to help investigate and respond to the attack. EDR is today considered an essential part of EPP.

Once we determine that a system was infected we can start the process to restore that system to a known stable state.

COMMAND AND CONTROL

At this stage, the system is compromised and under attacker's control. If he completed the previous steps correctly, his access is persistent even after we patch the vulnerability or restart the system. The infected system can be used either to carry out the attack mission or it can wait for future instructions from its command-and-control server.

Our defending tactics should be around detecting unusual activity and limiting what the attacker can control. Network segmentation and application segmentation will make it harder for the attacker to perform lateral movement and it will be easier to detect his presence. Detection tools can seek for changed patterns of network usage, such as increased amount of information sent or downloaded to/from an external server, or changed behaviours on the internal servers, like an unusual spike in CPU or memory utiliation, or at unusual hours.

Lateral movement is the set of steps that an attacker who gained a foothold in a trusted environment take to expand his level of access, move to additional trusted assets, and further advance in the direction of his ultimate target.

With the help of Breach and Attack Simulation (BAS) tool we can simulate real attacks against our data center so we can review the results and take action. This is the wisest advice we can follow in order to stay ahead of the attacker.

ACTIONS ON OBJECTIVES

The system is now infected and the attacker is in full control. Now he can execute the actions to achieve his objectives. The actions the attacker will execute, are predicated by his motivation. He might be motivated by financial reasons, political, or simple wants to move laterally and target a more important system in the network.

Lateral movement is a common step for an attacker to take once he gained the access into a system. At this point he might begin a newer reconnaissance phase to gain information about the internal network.

The pandemic crisis we all faced has obliged many companies to suddenly move some or even all of employees outside their “traditional” network. Apart from the raised risks of unauthorized access to assets, this bring us closer to a zero trust security model as a transformation need to improve the organization’s security facing continuous threats.

Zero trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are located within or outside of the network perimeter. Zero trust security means that no one is trusted by default from inside or outside the network, and verification is required from everyone trying to gain access to resources on the network.

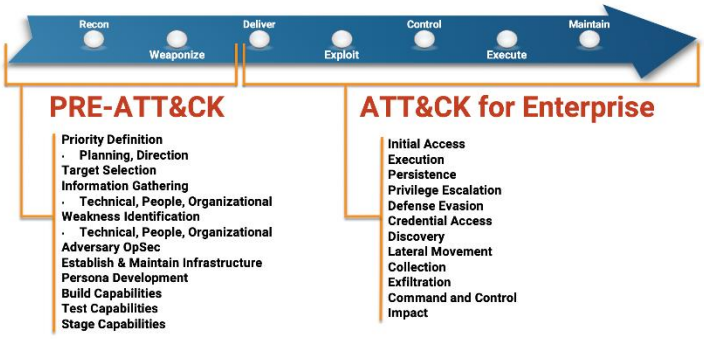
The philosophy behind a zero trust network assumes that there are attackers both within and outside of the network, so no users or machines should be automatically trusted.

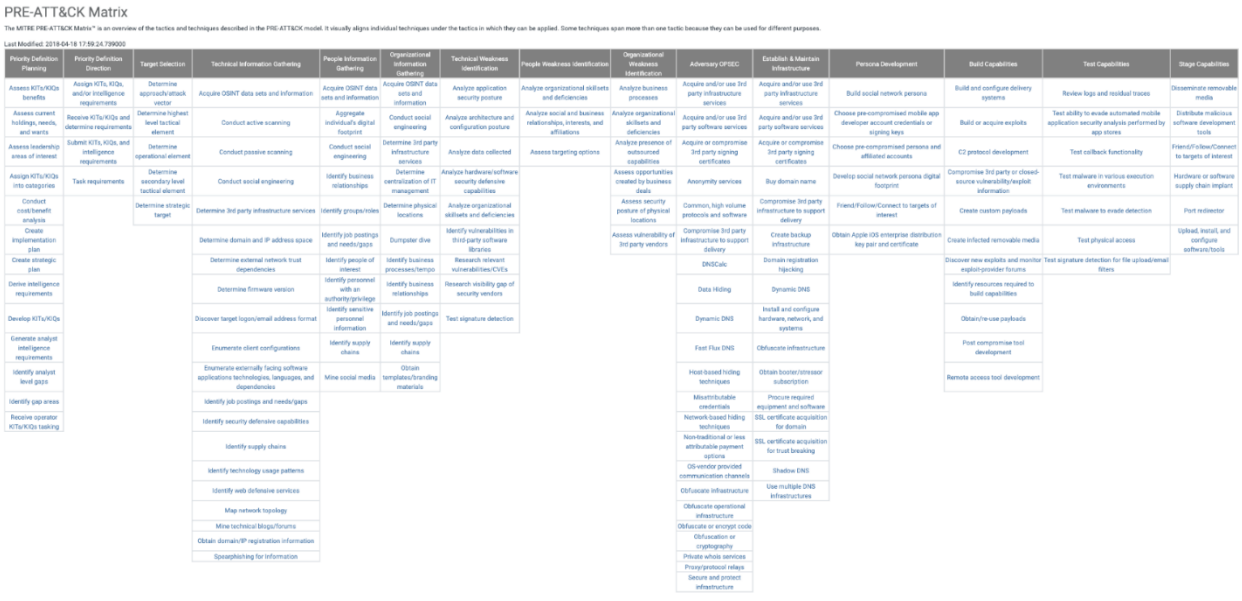
Another principle of zero trust security is least-privilege access. This means giving users only as much access as they need. This minimizes each user’s exposure to sensitive parts of the network and can prevent privilege escalation, which is a vital part of the cyber kill chain.

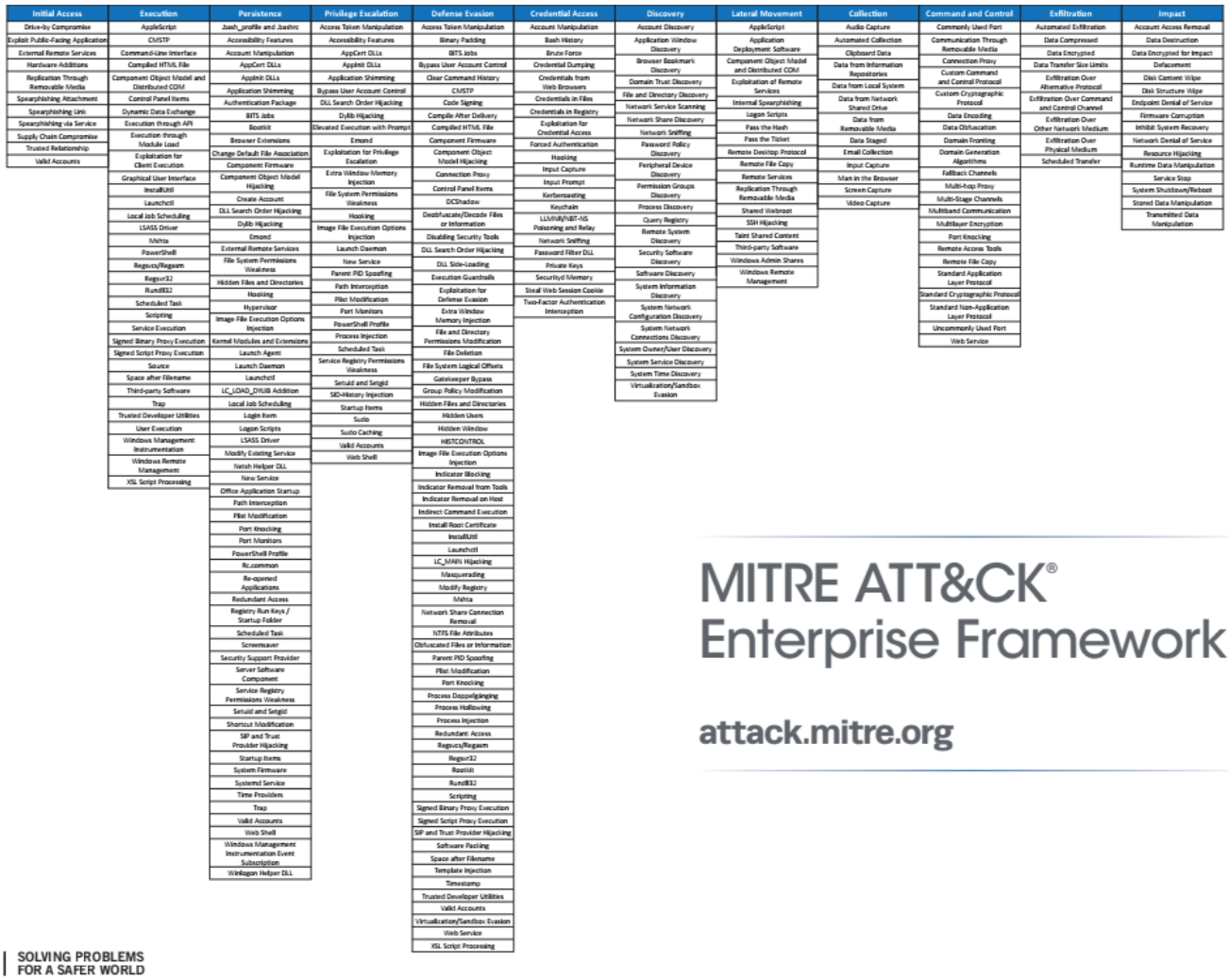
Zero trust networks also utilize micro-segmentation. Micro-segmentation is the practice of breaking up security perimeters into small zones to maintain separate access for separate parts of the network. This principle of micro-segmentation, included within the design of an application, ensures implementation of the privacy by default principle.

Multi-factor authentication (MFA) is another principle of zero trust security. MFA simply means requiring more than one piece of evidence to authenticate an user; just entering a password (i.e. only one authentication factor) is not enough to gain access.

A very helpful knowledge base of adversary tactics and techniques is MITRE ATT&CK. This knowledge base can be used as a foundation for the development of specific threat models and methodologies. It provides recommendations for detection and mitigation for the known threats. You can find it by accessing https://attack.mitre.org/







As we could see until now, preventive measures alone are not enough to deal with adversaries. An organization needs to create a consistent prevention, detection, and response program. Establishing an offensive security program can help improve the security posture of our organization and identify weaknesses in prevention, detection, and response to security incidents. We need to make sure that our security is effective and also that our security staff has appropriate skills and deals effectively with incident responding. Such a broader approach goes beyond penetration testing. Penetration testing is valuable, but it is limited in scope and cannot cover the protection needs of the organization. Being focused on compliance and penetration testing it only creates a false sense of security. Nevertheless, this holistic approach brings challenges from several perspectives.

One of the challenges we will face with when setting up an offensive security program is to get buy-in from the top management. A possible solution might be to propose a lightweight offensive penetration test on the applications/parts of the network chosen after a risk assessment prioritizing exercise. This is useful to explore if more investments would be useful for the organization. If we start out from scratch it might seem rather intimidating, but it's also a great opportunity. The results of this initial

assessment provide the building blocks to improve the security of the organization and can lead to an initial proposal for improvement for the 'quick wins' preferably of high risk items, depending on the company's budget for initial security investment. The most likely scenario in this case is that we will have a one-person show initially (with specific external providers used for very specific tasks), and by demonstrating its value and business impact, the team will start growing organically. Without demonstrating to the top management the added value and the business impact of our work in security there are only theoretical chances that you will transform it in a success story.

Our main goal is to continuously protect our organization. The only proactive pre-compromise tool available is Red Teaming. Red Teaming as a whole is a goal-based adversarial testing process. A red team assessment is ultimately a simulated attack effort that targets a defined set of goals. They use the same tools, techniques, and methods that a real hacker would. In addition, by reference to penetration testing, Red Teaming is interactive, as it entails identification of attacks and back-and-forth interaction with the attackers, similar to real life scenarios. We want to find out whether the organization can prevent those attacks from succeeding in the first place, detecting those attacks if they do succeed, and respond to them, returning the organization into a state of normal operations. Only through a Red Team / Blue Team exercise we can find all these. Red Teaming is the sharpest weapon available to fight against threats and we need to use it in order to consistently evaluate how good our security is, and to improve the organization's security and also the security staff training.

Because today's attacks are complex, we need to build models in order to try to anticipate the attacker's behaviors. In our days, it is unlikely that organizations have the ability and resources to defend against all threats. A zero-day threat can be a success factor of an attack because all organization rely on signature-based detection mechanisms. Attempting to handle unknown threats without a systematic plan will fail. It is imperative that incident handlers and response teams have a methodology to be able to respond to unknown or unidentified threats to protect the critical assets and data that businesses rely on.

We all know that understanding the problem is half-way to solution. Therefore, we need a way to model threats against our environment. If we can understand all the different ways in which our organization can be attacked we can design effective countermeasures. It is as simple as that: *as better we understand the threats, as better we have chances to defend our environment*.

"Problems are nothing but wake-up calls for creativity" – Gerhard Gschwandtner

So, we need to put our creativity at work to describe and depict potential attacks and build countermeasures to protect our environment. To describe and depict potential threats we will use threat modeling and we will draw the "threat picture" using attack/threat tree.

Before doing that let's underline few important benefits of threat modeling:

- Spots design flaws that traditional testing methods and code reviews might overlook;
- Evaluates new forms of attack that might not otherwise be considered;
- Models threats against the existing infrastructure and evaluate the potential to create damage;
- Evaluates which of the current countermeasures are likely to succeed or fail;
- Helps to design proper remediation countermeasures in order to reduce the threats;

Let's put it in simple words. There are two sides: attackers and defenders. *The side that learns the fastest wins*. The only way to win this game is to find *sooner* than our attackers what makes our organization vulnerable and fix that.

Even we focus on cyber security, we should consider the entire attack surface, which is not always entirely digital. Some attack vectors might be non-technical. In hybrid attacks, attackers frequently leverage physical threat vectors in order to bypass digital controls. Therefore, we should not ignore the physical threat vectors of a potential attack that can start in the parking place or an open location where an employee finds and picks up or gets an USB stick or when an intruder gets into the building together with one of the employees, by smuggling the access control.

Attack tree is a tool to explore vulnerabilities in a system, be it physical, digital or both (technical and non-technical). It is particularly suitable for analyzing the security of a system against malicious attackers. It puts the security expert in the shoes of an attacker to gain new insights in vulnerabilities of the system. It is a structured process to anticipate cyber attacks and reveals the attack surface according to the attack goal we analyze.

The goal of building an attack tree is to explore attacks on a system and expose vulnerabilities. Therefore the root (first node) of an attack tree is a goal an attacker would have (e.g. access customer data or disrupt the flow of business) . After the root is set, the rest of the tree should be created by refining each node until the action in the node becomes trivial.

As building blocks, an attack tree consist of the following components:

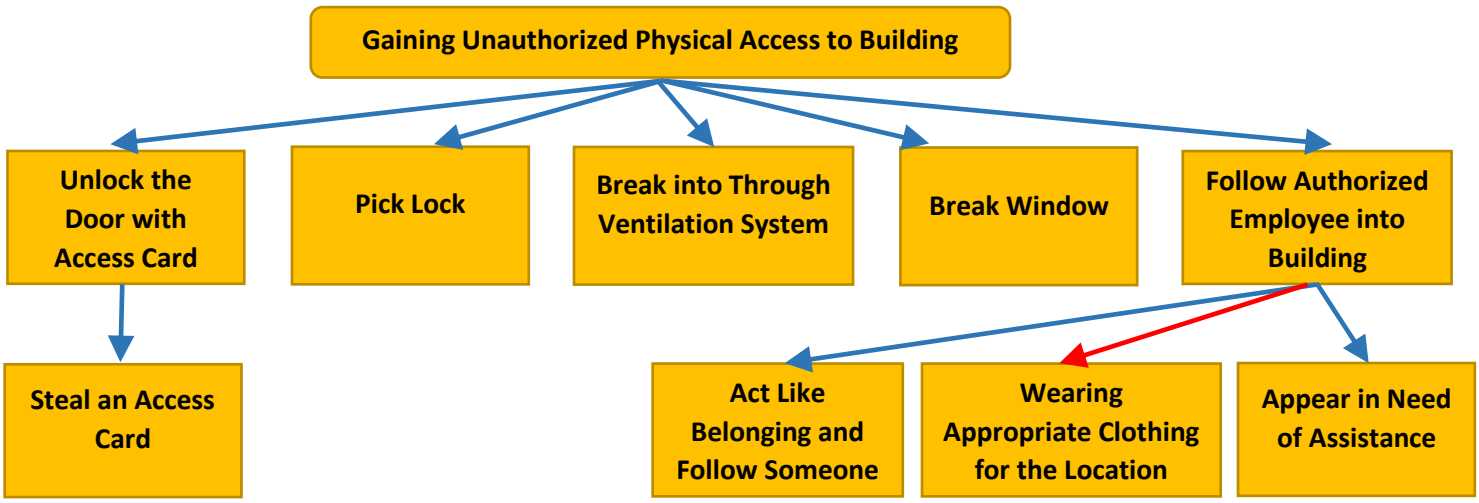
- Root node – the goal of the attack and the starting point of the attack tree;
- OR node – a node of which ONLY ONE of its child nodes needs to be successful;
- AND node – a node of which ALL of its child nodes need to be successful;
- LEAF node – the activity performed by the attacker;

Nodes between the leaf nodes and the root node depict intermediate states or attacker sub-goals. The attacker may gain benefits at any level of the tree.

The following questioning can be used to start the most used form of an attack tree:

1. What would be the goal of an attack to our environment ?
2. What areas can be attacked to reach the goal ?
3. What attacks can be performed on this areas ?
4. What steps are required to execute such an attack ?
5. What alternatives approaches are there to the step ?

Let's take an example in order to simplify the understanding of how to build an attack tree. Let's say we would like to analyze how unauthorized physical access can be gained to one of our buildings. So, the goal of the attacked will be "Gaining Unauthorized Physical Access to Building". In order to do this, there are some alternatives for the attacker, represented in the Fig. 1.



BLUE = OR

RED = AND

Fig 1. Attack Tree Example - Gain Unauthorized Physical Access to Building

Now, what if we will put the attacker's goal on the top of the kill chain and connect the seven phases of the chain to it ? Will it look like an attack tree ? Of course it will! And what if we will use further the MITRE PRE-ATT&CK and MITRE ATT&AK matrices to depict the modus operandi of the attacker ? We have a priceless knowledge base we can rely on to build specific attack trees related to our environment. There is no reasonable reason to not use it. And don't forget to consider the physical threats along with digital threats when you build the attack trees.

OODA Loop

It might happen that we might feel in difficulty to make choices or take decision in certain circumstances when we try to determine what the threats might be to define them as goals and build attack trees. OODA loop might be of a very good help in such situations. OODA (Observe, Orient Decide, Act) loop is a method for dealing with uncertainty. It is a learning system and a decision-making framework helping us orienting to situations and acting faster than our adversary can adapt. It can be applied in threat hunting, but also in other information security areas and in business as well. When the environment is volatile, and uncertainty is high, managers know that the same uncertainty facing them is facing their competitors too. Influencing and shaping the uncertainty in the environment can provide them with the tools needed to create a competitive advantage.

Observe

To effectively observe, we need to have good situational awareness. Our decisions and actions should ideally happen in a way that sets up an opponent and makes him vulnerable to having his rhythm broken. Therefore, the need of developing a clear understanding of your operational environment and

context is crucial for the next decisions we will make. For threat intelligence or threat hunting observation includes our own situation, our opponent's situation and the environment more broadly. It includes all the dimensions of that environment: the physical, mental, and moral dimensions. In other words, this is the data collection phase – we should just aggregate what's available.

Orient

Orientation is the most important part of the OODA loop. The goal of the orientation phase is to find mismatches: errors in your previous judgement or in the judgement of others. As a general rule, bad news is the best kind because as long as we catch it in time, we can turn it to our advantage.

For threat hunting, the goal of Orient should be the identification of a set of possible threats that would be relevant to the operational environment being analyzed, how they would present themselves in various possible scenarios and what could be done to mitigate them. The information collected during Observe phase, now is analyzed, evaluated, and prioritized. If you feel uncertain, make sure you're devoting more time and resources to orienting.

The success factor of the overall OODA loop is to build here models or concepts and try to validate them before operation in order to assure that we have the confidence that our models or concepts will work before we actually will need to use them.

Decide

Invariably, this phase produces a hypothesis: the decision-maker predicts what the best course of action will be based on his understanding of the situation. As decision-makers, we should now be well-positioned to decide on the appropriate response. When we decide, we're essentially moving forward with our best hypothesis about which our model or concept will work. To find out if our hypothesis is correct, we then have to test it.

Act

This step is about testing the hypothesis generated in the decision phase. Action is how we find out if our models or concepts are correct. If they are, we win the battle; if they aren't, then we start the OODA Loop again using our newly observed data.

Ideally, we should have multiple actions or experiments going on at the same time so that we can quickly discover the best model or concept for a particular situation.

Because the OODA loop is, after all, a loop, Act is never the last step of the process. What was learned about the validity of the hypothesis is used during the next cycle of the OODA loop.

The power of OODA loop comes from its simplicity. The one who arrive to run successfully consecutive OODA loops faster than the opponent will win. Remember that "Orient" shapes the way we "Observe", the way we "Decide", and the way we "Act".

RED TEAMING

Now, more than ever before, robust red teams are needed to challenge emerging operational concepts and current security practices, in order to discover weaknesses before real adversaries do. Successful red teaming helps lead to robust decision making, ameliorates risk and helps prepare for the unexpected.

How do we know that our investments in security are doing a good job ? Red Teaming can give the answer to this question. Red Teaming is the only way we have available to measure how well our defenses will hold up to a real-world attack.

Red-teaming is a function that can compare and test approaches and plans, by considering a range of hypotheses or alternative outcomes in order to help the organization mitigate against potential attacks. One of the key role of the red team is to challenge our basic assumptions and to provide a different perspective on the assessment process and should offer also, alternative views on adversaries.

Whatever their particular skill all red team members should have a full understanding of the problem for analysis and ensure they are familiar with relevant systems and processes our organization use. The team should contain critical and creative thinkers who can approach the problem from different perspectives and deal with complex systems and challenging constructs.

When forming a red team the following attributes should be considered and included as appropriate:

- The ability to see things from alternative perspectives;
- Imagination, a particularly desirable attribute, enabling freedom of thought;
- Self awareness. 'Know thy enemy but not yourself, wallow in defeat every time' (Sun Tzu);
- Understanding of the operational environment, its critical variables and the decision making process;
- Familiarity with cyberwar gaming and experimentation best practice;
- The confidence to challenge conventional or established blue thinking;
- The ability to communicate effectively;
- Strong leadership;
- Effective facilitation;

Red teaming is not easy; establishing an effective team and applying sound processes are challenges in themselves but are essential if red teaming is to add value. The red team must:

- Have a clear objective;
- Be independent from blue, but be close to the decision making process and have adequate interaction with blue;
- Contain critical and creative thinkers with relevant expertise;
- Have the full support of the top management;
- Help to detect possible deception and denial strategies by an adversary;
- Assist security team in understanding how much confidence to place in information and judgements derived from it;

Trust is crucial for Red Teaming. In the wrong hands the information they handle can be deadly for our business.

Key Responsibilities of a Red Team

- Test the effectiveness of the organization's security programs and the performance of the internal security team;
- Improves the organization's ability to respond to real-world threats and incidents;
- Assess the internal security standards and practices in order to take needed steps to maximize the performance of the Blue Team;
- Identify and mitigate sophisticated security flaws before an attacker does;
- Use appropriate tactics to discover exploitable vulnerabilities , get access to the target, steal sensitive information, and, at the end, take proper measures to fix and improve the overall organization's security;
- Compiles detailed security assessment reports of discovered vulnerabilities and the measures taken to mitigate them;
- Checks the overall organization's security and creates a strategy to fix and enhance it;
- Educates Blue Team members and senior management to maintain and improve the organization's security;
- Complies with all laws, regulations, policies, programs and Rules of Engagement;

The following mind map depicts the main activities of a Red Team engagement:

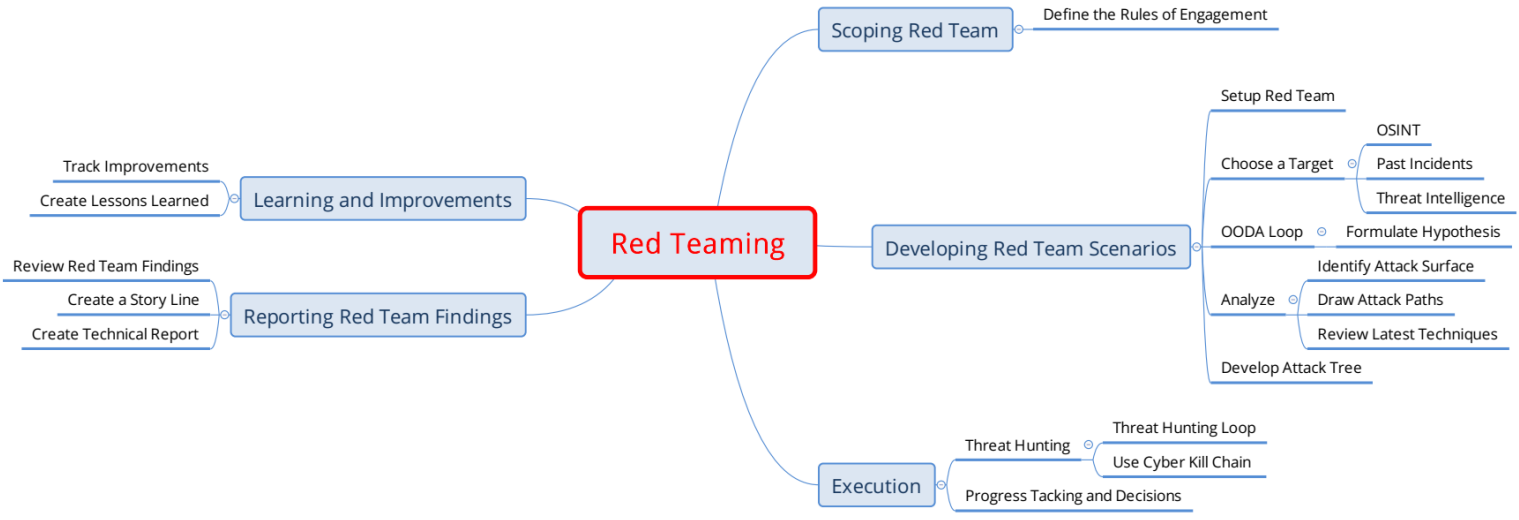


Fig. 2. Red Teaming Mind Map

All organizations are facing with two main choices when setting-up a red team: setting-up a red team with internal resources or to outsource the red team to get an independent perspective ? Both approaches have pluses and minuses. What is really important to get an effective red team is to find appropriate skills for it. In most cases, you cannot find all required skills within your internal team and you will build a red team using internal and external resources. There are two areas of expertise you should consider – technical and tactical. Technical means specialized expertise to build and run the tools needed during the Execution phase. Tactical means specialized expertise to threat model and to develop red team

scenarios. By default, the ability to communicate effectively with the business is a must for each member of the red team.

Scoping the Red Team

A Red Team engagement aims to simulate a real-world attack by expanding the initial scope of the engagement to include the entire organization (in case of gaining access to the target). Therefore, the scope of a Red Team cannot be limited to specific systems. It should be scenario driven, with specific goals, based on real security threats. Those scenarios can be developed with to the input of other security teams, such as the Threat Intelligence team.

The Rules of Engagement for the Red Team should include the following details:

- A list of goals to be achieved by the Red team during the exercise
  Some examples of goals might be:
  - Obtaining physical access to a server room;
  - Gaining access to an environment holding sensitive data;
  - Taking control of a mobile device;
  - Compromising the account credentials of a top manager;
- Specific techniques that are excluded from the engagement (if applicable);
- Specific areas or assets excluded from the scope and Red Teaming exercise (if applicable);
- The official testing period;
- References to the applicable legislation, policies, code of conduct & ethics, etc. (some service providers have their own set of guidelines for performing assessments; they also require proper permission to be obtained before performing any assessment);
- Communication and collaboration rules:
  - Functional and operational escalation points the Red Team can use and in what circumstances;
  - When to share the knowledge with the Blue Team members (if the organization's intent is to test its response to a security event without prior warning, the Red Team will be allowed to share knowledge with the Blue Team at the end of the exercise);
- Incident response rules:
  - In case of critical vulnerabilities and exploits found during the engagement;
  - In case of emergency;

A letter of authorization should be prepared and provided to the Red Team for all on-site activities performed during the testing period. The opening of the Red Team engagement can be done only through a written authorization given by the organization's representative.

Developing Red Team Scenarios

Once the Red Team receives the written authorization, it will start the black-box assessment. The initial work done in black-box assessment is information gathering. The goal is to gathering data on the target organization, and it is critical to the operation because this information is the basis for the development of the early plans for the attack. This should be regarded as initial reconnaissance to identify

what potential targets are the most vulnerable, then to analyze the intel information and define the potential attack surface and develop the attack tree.

Execution

This phase involves the execution of the attack on the identified targets based on the attack plan and scenarios that are formulated in the previous phase. The attack execution phase should be closely monitored. All steps taken by the Red Team and their observations should be continuously captured in the Exercise Log Report with the level of details as defined by the Rules of Engagement.

Reporting Red Team Findings

At the end of the exercise, the main responsibility of the Red Team is to remediate immediate issues found during the exercise, as well as eradicate any left-over attack tools and artefacts.

Then, Red Team will prepare the Exercise Report, capturing all aspects of the exercise where the attack was detected, observed, reacted upon, tracked, contained and eradicated, or lost sight of. This reconciliation should be used to identify security controls, either missing or in need of improvement, that would otherwise have prevented or detected the attack.

For learning purposes, a joint post-attack exercise can be organized to enable a step-by-step replay of the attack for the Blue Team members learning benefit. Also, this post-attack exercise can be organized in the actual live environment, to demonstrate failed controls in real-time.

At the very end, Red Team will prepare the Final Report of the exercise. The Final Report will include security strengths, comprehensive analysis of organizational capability, with recommendations for remediation and enhancements. This report will also contain the methodology, evidence of goals achieved, details of the attack paths undertaken and the concessions, if any, used.

Once the Red Team has completed their exercise, an in-depth debrief should occur with the Blue Team. During this debrief, the Red Team should describe the conclusions they have arrived at, successes, failures, as well as preventative measures and security controls they recommend.

Learning and Improvements

This phase should be under the lead of the Blue Team. The Blue Team should prepare the lessons learned of the exercise and implement the recommendations and enhancement proposed by the Red Team. At the end of the implementation a new overall security check would be required to assure that the risks are under control.

Conclusions

As already mentioned, Red Teaming is the only way we have available to measure how well our defenses will hold up to a real-world attack. Only through Red Teaming we can get all the peace of mind we need to operate safely and maintain the security of our organization and its data.