RED TEAM ENGAGEMENT GUIDE: HOW AN ORGANIZATION SHOULD REACT

By Jason Lang in Red Team Adversarial Attack Simulation, Security Testing & Analysis

A lengthy Red Team engagement is coming. What should the defense do if they catch the offense? Reimage systems? Notify and allow? What is the course of action that allows the engagement to proceed and deliver maximum value to the organization? These can be difficult questions to answer, but ones that companies procuring these tests should be asking. This article is meant to be a preparation guide for an organization that has an upcoming Red Team engagement and wants to get the most out of it!

This article makes several important assumptions, as indicated below. They are referred to throughout the post and are critical to a proper understanding of a successful Red Team engagement.

1. Neither the offense (Red Team) nor the defense (Blue Team) are simply out to 'win' the engagement. Let me clarify this: I'm all for healthy competition, but in this case, 'winning' means competition + ego (best summarized by Ross the Boss in Superman III, "It's not enough that I succeed. Everyone else must fail." *#Dated*) This is a destructive attitude that, when adopted by either party, immediately devalues the engagement.
2. There is genuine desire on the part of both the offense and [illegible] security of the target organization. When this happens, the [illegible] receive the most value from a Red Team engagement.
3. The organization is ready for a Red Team from a maturity st[illegible] being aggregated, alerts are configured, multiple purple teams have been performe[illegible] etc.

Typically, the technical defense teams are not made aware that a Red Team engagement [illegible] occur. This post will proceed from that perspective.

Each of these phases has ways to diffuse the specific attack without compromising the engagement's overall value.

DETECTED: EXTERNAL INTRUSION ATTEMPTS

This includes brute-force attacks, port/service scanning, and anything odd hitting your perimeter. Assuming the Red Team is using decent opsec and not sending attacks from an IP address that betrays themselves, it is rare that a detection on an external attack has any lasting bearing on the engagement as a whole. Detecting and responding to external attacks should be considered 'business as usual' for the defense. Block IPs, block domains, and perform your standard operating procedure. Even for more advanced clients who may have authentication honeypots in place, if a wire is tripped, proceed as you normally would.

Bottom line: SOP applies. Act as you would if this were a real attack.

DETECTED: PHYSICAL INTRUSION ATTEMPTS

Physical attacks are gaining popularity against clients with more sophisticated endpoint and network controls, simply because physical controls can still (usually) be easily evaded. Our rate of physical success on Red Teams is very high, even against large organizations.

The physical tester should, of course, have a get out of jail letter, but it should only have the numbers of those who are on the internal need-to-know team, such as the main engagement point of contact (POC), as well as the CISO and Security Operations Center (SOC) manager. For engagements that include a physical intrusion attempt, the need-to-know team **must** include the owners of the building!

If the tester is caught by an employee or guard and forced to reveal the existence of the test, the POC should immediately reach out to the building security contact and ensure that communication between departments is limited to those with a need-to-know. This will help protect the integrity of the testing process.

Bottom line: If it is previously determined that the tester should proceed upon detection, then allow the tester to proceed; otherwise, allow them to leave the building. In both cases, send relevant logs and screenshots to the Red Team engagement lead and ensure communication is limited to those on the need-to-know team.

DETECTED: PLANTED PHYSICAL DEVICES

device. This can quickly escalate into panic, requiring internal deconfliction, and is another great reason for including the SOC manager in the testing planning process ahead of time. Multiple courses of action are possible if a network device is detected, and depending on the objectives of the test, the device could be either disconnected, as per SOP, or left online for the tester to proceed using.

Bottom line: The action of disconnecting or leaving the implant device should be decided during the kick-off call. If detected, refer to the Internal Actions and The Informed SOC sections below.

DETECTED: INTERNAL ACTIONS

The Red Team has acquired internal network access, but the SOC is investigating one or more alerts related to the Red Team's activities. The alert looks legitimate and they are unaware that a Red Team engagement is taking place, so they commence full-scale Incident Response activities to get to the bottom of things. For those who are aware of the engagement, this is usually a tense but valuable moment! How is the team going to respond to what appears to be genuinely malicious activity? Will they track down the artifacts and follow their playbook, or will they close the events prematurely because it's Friday and they're tired? This is the true value of a Red Team exercise!

What happens next will determine how the remaining weeks of the engagement play out, so it is important for the organization POC to take an active hand (when needed) to avoid unnecessary service interruptions while allowing the test to proceed on schedule.

Here are some general guidelines for when to inform the SOC about the engagement versus just letting things play out:

1. If an alert is received that the SOC begins investigating, the POC should inquire to the Red Team as to whether it is a genuine Red Team activity or legitimate malicious activity. If the alert is not related to the Red Team's activities, skip the rest of these steps and follow the Incident Response playbook to the letter.
2. If the SOC is investigating, let them investigate. Let them dig to the bottom and look at the files, pull apart attachments, and sift through traffic. This kind of learning is priceless because it couples genuinely malicious artifacts with a bit of real-world stress, and that is better than any training classroom setting.
3. Memory imaging and forensic analysis can be an incredible exercise for the mature SOC. Encourage it. They will get to see real-world command and control artifacts and traffic on one of their own systems. This can be a terrifying but extraordinarily valuable experience.
4. *The POC should consider intervening when a business disruption is imminent, i.e., when the SOC wants to start rebooting critical systems, reimaging any system, or contacting upper*

machine to a separate VLAN while the investigation takes place, as opposed to reimaging.

A personal note from the Red Team: We understand that in the course of an investigation, our artifacts may be uploaded to sites like VirusTotal. We understand that this is part of the job, but if it can be avoided, we appreciate it. We like to make things from scratch, and our artisanal, hand-crafted, 'pharm-to-cable' payloads are made just for you, our clients. 🙂

From Tyler Hudak, TrustedSec's Incident Response Practice Lead: "A personal note from the Blue Team: Artifacts from an ongoing investigation should NEVER be uploaded to any public sandbox site like VirusTotal. There are two primary reasons for this. First, attackers are smart. They are monitoring these sites. If they see you upload their malware to them, they know they have been caught and may change their tactics. Second, public sandboxes are public. They share data with researchers and security companies. If the files you uploaded have any indication that they were targeted against your organization, someone will eventually find out and it will be revealed that you've been attacked."

Bottom line: Allow any investigation to proceed as naturally as possible without interfering, including memory forensics. The time to interfere is when the investigations team wants to reboot critical systems, reimage any system, or notify upper management. If that happens, and the team must be made aware of the engagement, move to The Informed SOC section below. Do not inform the SOC about the specific engagement trophies.

THE INFORMED SOC

The SOC has been made fully aware of the engagement. What now? Is the engagement over? No! While this can be the best part if handled properly, caution and a heavy hand of guidance must be used as the engagement goes forward. This is the moment when the engagement is most vulnerable to devaluing if all three of the assumptions are not met.

Here's how to handle the informed SOC:

1. First and foremost, do not actively block the Red Team from doing their job. This does not mean that you remove controls or somehow downgrade the security of the environment. What it does mean is that you don't turn all the controls up to 11 to make it unrealistically impossible for the Red Team. The only thing that is being 'burned' in that moment is the money spent on the engagement. Leave the environment as is, but feel free to follow along.
2. Encourage the SOC to observe the Red Team's activities in as near real time as the alerts will allow. It gives the SOC a glimpse of an attacker who is actively experimenting (and failing) on a particular system, and that is priceless experience for the defense.

4. If you are working with a mature Red Team, feel free to ask questions! We love nothing more than watching defenses improve real-time and will even try requested attacks if it is within our abilities and time. The Red Team shouldn't reveal the specific trophies, but it is highly likely the Blue Team already knows what they are. How awesome to see a Blue Team ready defenses on specific systems they think might be target goals! Can you find the path the Red Team is likely to take and follow them all the way there?
5. Send the Red Team all the alerts you get (or at least summaries of the highlights) and include screenshots. I love making my client's defenses look good in the report, and any Red Team that doesn't has failed assumption number 1. Start looking for a different provider.

Post-engagement, the Red Team should sit down with the SOC and compare activities performed to the detections or artifacts that were documented during investigation or forensic analysis. This is the perfect time for the SOC to improve their forensic skills by finding out exactly what was done on a system versus what they were able to find or what they interpreted the data to be.

CONCLUSIONS

Red team engagements, when done right, are emotional roller coasters for both the attackers and defenders. We get to watch weeks' worth of work come crashing down in hours, while defenders get to see what a real compromise looks like from the ground up with a safety net in place. A successful Red Team engagement is rarely one of capability and almost always one of mindset and maturity, and when it is done correctly, it can be one of the most valuable services performed for a mature defensive team.

#Vim4lyfe

BROWSE BY CATEGORY

All Categories

MORE LIKE THIS

Automation Testing With Ansible, Molecule, and Vagrant

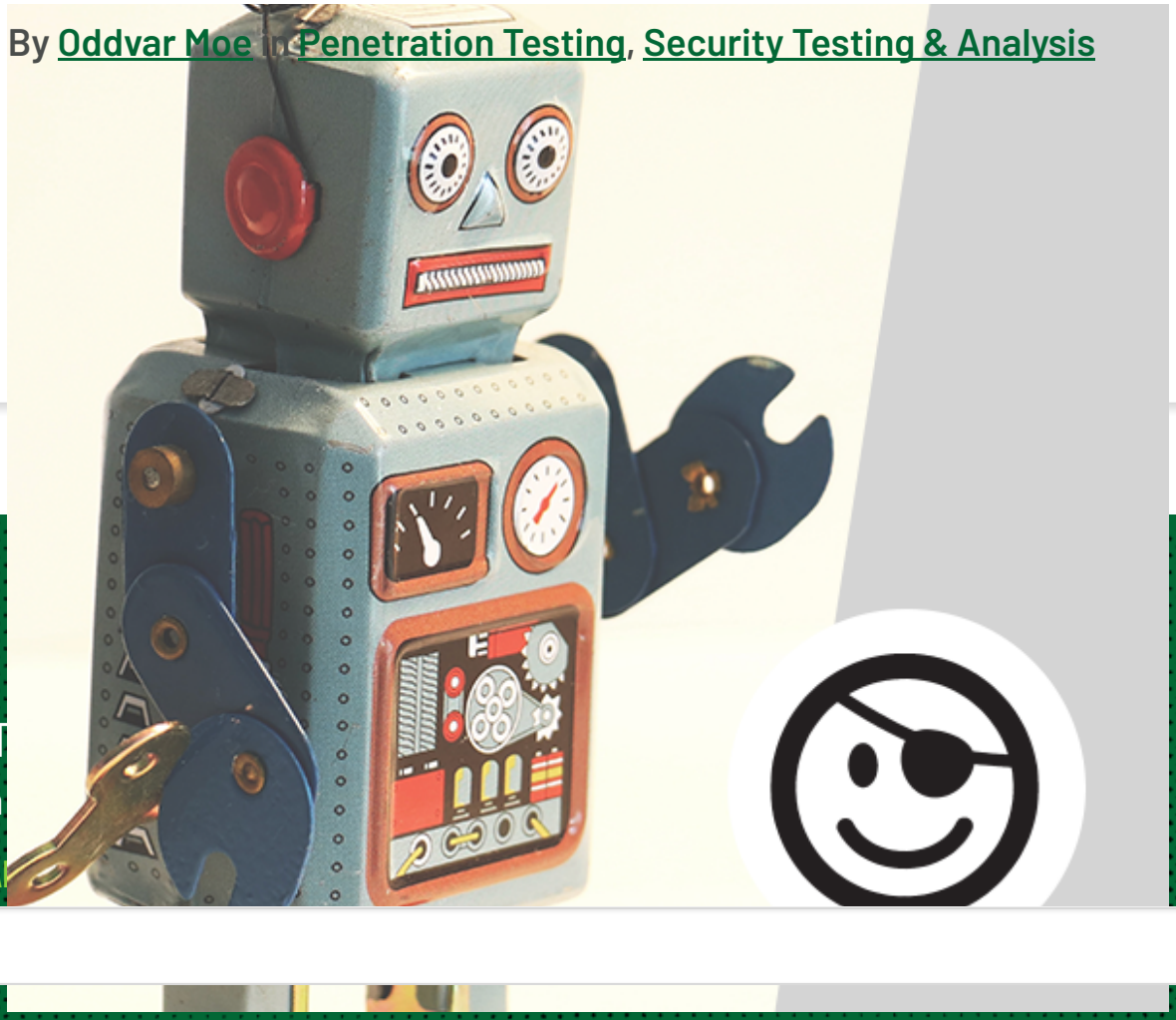
December 3, 2019
By Mike Spitzer in Application Security Assessment, Penetration Testing, Security Testing & Analysis

Creating Honey Credentials with LSA Secrets

November 21, 2019

By Scot Berner in Application Security Assessment, Penetration Testing, Security Testing & Analysis

By Oddvar Moe in Penetration Testing, Security Testing & Analysis



GET
Sign
EMA

By submitting this form, I agree to receive marketing communications from TrustedSec, which I can unsubscribe from at any time.

SUBMIT

14780 Pearl Road, Suite 300
Strongsville, OH 44136

1-877-550-4728