Red Team Tactics For Pentesters

Think Like a Red Teamer

TEXAS CYBER SUMMIT

Disclaimer

All thoughts and opinions expressed by me during this presentation are my own and do not represent those of my employer.

Roadmap

The journey is just as important as the destination.

- Whoami
- Red Teaming Vs. Pentesting
- Importance of Red Team Tactics
- What risks do Adversarial activities pose to our SecOps
- Getting into the mindset of a Threat Actor
- The Red Team Methodology
- How does a Red Team engagement compare to a Pentest
- What are the different types of engagements
- Threat Intel and it's role in offensive security
- Where to get Threat Intel
- Techniques and Tactics that you should know about
- Bringing it all together
- Reporting, and how it can make or break your engagement
- Correlating your actions
- Example of Operation Planning
- Some love for the Blue Team
- Other options
- Keys to success
- Final thoughts

Who Am I

Red Teamer | Pentester

- Specialize in Adversary Emulation
- Built the Internal Red Team at the US-AFCERT
- Have a few certs (GXPN, GPEN, GWAPT, etc…)
- YouTube: ILikeToHackThings
- Twitter: @Valcan_K

TEXAS CYBER SUMMIT

Red Teaming vs. Pentesting

Red Teaming:

"Red Team Assessments focus on giving your security team practical experience combatting real cyber attacks. While avoiding business damaging tactics, these assessments use conventional and advanced attacker TTPs to target agreed-upon objectives."

"Red Team Operations test your internal security staff's ability to safeguard critical assets."

- FireEye

Red Teaming vs. Pentesting

Pentesting:

“A penetration test is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. The test is performed to identify both weaknesses (vulnerabilities), including the potential for unauthorized parties to gain access to the system’s features and data, as well as strengths, enabling a full risk assessment to be completed.”

- Wikipedia

Red Teaming != Fancy Pentesting

The definitions of both are pretty similar, but vastly different when it comes to the intentions behind the actions.

The Importance of Red Team Tactics

Knowledge is power!

Why are they important to Pentesters?

- A pentester's actions are very close to those of a Red Teamer.
- A ton of advancements in offensive tactics come from the Red Team community.
- Pentesters can find better ways to convey the severity of vulnerabilities or their findings.

Why are they important to the rest of us?

- You can't defend against certain attacks if you don't understand how they work.
- Keeping up with the latest trends and offensive security can allow you to tailor your defensive controls.
- Why would you not want to know how adversaries gain access, pivot, and accomplish their objectives?

What risks do Adversarial activities pose to our SecOps?

Why should we as Pentesters, Red Teamers, and Blue Teamers take them into consideration.

69% **Breaches / Attacks** Perpetrated by outsiders

39% **Breaches / Attacks** Conducted by organized criminal groups

23% **Breaches / Attacks** Identified as nation-state or state affiliated

Data from: 2019 Verizon Data Breach Investigation Report

Getting into the mindset of a Threat Actor

The recipe for designing an Adversary or an Adversary profile.

Intel

The intel provided or acquired for an engagement will help you design and build an adversary profile.

This could be based off of multiple Threat Actors and their known behaviors.

Objective

Typically during an engagement you'll have a primary objective and potentially several secondary objectives.

Combined with threat intelligence you should be able to see the adversary profile begin to take shape.

Intent

What is the overall intent behind a Threat Actor's objective and their actions.

Is it the theft of intellectual property, monetary gain, etc.

Red Teaming vs. Pentesting

How does the engagement process differ from the traditional penetration test?

1. There is a considerable amount of planning that goes into a Red Team engagement. Sometimes you may spend months planning for a 3 week operation.
2. Red Teaming is very detail oriented.
3. Utilizing intel is key, that helps when attempting to stick to specific behaviors or tools identified during the Adversary profile creation.

- Remember there are humans behind the toolsets, and behaviors are amongst the hardest things to change.
- Where as with a pentest, you may be willing to try a 100 different avenues or tools to accomplish the next step of your assessment.

The Red Team Methodology

Or rather, the methodology that my team and I utilize.
Also known as PDED.

1. Planning

- Define objectives
- Most time consuming
- All parties should partake

2. Development

- Collectively develop as a team
- Everyone is continuously briefed

3. Execution

- This is where the fun happens
- Aiming to hit desired objectives

4. Debrief

- All parties should be involved
- Question and answer
- Documentation, reporting, and lessons learned

Red Team Methodology

The Planning Phase Overview

The Planning Phase should consist of these items:

- Determine the primary and secondary objectives.
- Meet with all required parties.
- Build Adversary profile based on target objectives.
- Assign team roles.

Red Team Methodology

The Development Phase Overview

The Development Phase should consist of these items:

- Each team member should have a role in this process, from collecting and compiling TTPs to developing custom implants.
- This will allow everyone to remain informed on the operation's preparation status.
- I suggest using Gitlab or any other form of DevOps task tracking and code collaboration.
- I'll provide an example of this.

Red Team Methodology

The Execution Phase Overview

The Execution Phase should consist of these items:

- This is where all of the hard work and planning comes together.
- Honestly this should be the most enjoyable part of the entire process.
- Documentation is key during this portion, you'll want to make sure all activity is logged. It will help for data correlation, and building the final report.
- Remember to take note of the things that didn't work, and this way they can either be improved or removed.
- This phase may also contain the normal pentesting steps.

Red Team Methodology

The Debrief Phase Overview

The Debrief Phase should consist of these items:

- While the Development and Execution phases get all of the glory, this is where the real value of the engagement is realized.
- There should be a Q&A session with the team members and all other parties involved.
- Documentation -> Lessons Learned -> Reporting
- Begin planning for the next operation! Continuous testing can be extremely valuable for Security Operations.

The Typical Pentest Process

What does normal look like?

Recon

Common Toolsets for both:

- Censys.io
- Google.com
- Wayback machine
- Recon-ng
- Etc..

Scanning/Enumeration

Common Toolsets for both:

- Lazyrecon by nahamsec – super loud
- Nikto, nmap, etc..–pretty loud
- Burp, zap, bloodhound, etc..
- Custom tools may work better

Gaining Access

Common Toolsets for both:

- Phishing
- Exploitation via opensource or custom toolset
- There's probably 100 different ways this can happen

The Typical Pentest Process

What does normal look like?

4

Post-Exploitation

Common Toolsets for both:

- Living off the land techniques
- Empire, various C2 frameworks
- Setting up persistence
- The methods or tools will come down to the objectives

5

Covering Your Tracks

Common Toolsets for both :

- Time stomping
- Log cleanup
- Using valid accounts
- Various Anti-Forensic techniques

6

Reporting

- Overview
- Executive summary
- High level findings
- Technical findings
- Summary

These steps were combined from SANS: building a better Pen Tester & Daniel Holdsworth

The Different Types of Red Team Engagements

Emulated vs. Simulated Adversary

Adversary Emulation

- The act of emulating a known threat actor based on threat intel.
- The accuracy of this type of engagement will vary, you won't always be able to emulate an adversary to 100% of their known actions.
- Designed to test specific TTPs or behaviors.

Adversary Simulation

- Will most likely consist of a full scope engagement.
- During this type of engagement your team will probably combine TTPs from various Threat Actors.
- The designed adversary profile will be a bit more wide spread and dynamic. More valuable for most organizations.
- In my opinion this is closer to a pentest.

Adversary Emulation

Emulated vs. Simulated Adversary

What are the benefits of this type of engagement?

- Great for validating and testing the defensive posture against specific Threat Actors or Behaviors.
- Allows for the refinement of the implementation of intel into operations.
- Helps to refine and focus the attention and objectives of an engagement.
- The most beneficial piece is that it really helps put the risks into perspective.

Adversary Simulation

Emulated vs. Simulated Adversary

What are the benefits of this type of engagement?

- Probably the most enjoyable part of Red Teaming.
- Allows for the team to create a simulated Adversary that is designed to test their org's environment.
- In my opinion this is much closer to Pentesting.
- Better for orgs with a less mature Defensive poster, will allow for testing of a wide range of capabilities.
- Can combine open source intel and internally developed TTPs.

Threat Intel

- Cyber Threat Intelligence is one of the biggest factors when drawing the line between Red Teaming and Pentesting.
- Threat Intel should drive your operations, just like it does with Threat Hunting.
- A Threat Intel cell is critical the in the effectiveness of a Red Team.

Where to get the Intel?

There's a vast array of Threat Intel resources out there.

Which makes it difficult to determine which ones are reputable.

MITRE

www.mitre.org

- A collection of over 290 TTPs
- Helps with TTP development and replication.

Threat Feeds

Various

- Talos Intelligence
- DHS – Automated Indicator Sharing (AIS)
- Open Threat Exchange (OTX) – Alienvault
- Threat feeds will help keep you updated on current trends and threats.

Security Firms & Vendors

Various

- FireEye
- CrowdStrike
- CarbonBlack
- Recorded Future
- Each of these has it benefits.

Types of Tactics you should know about.

There are hundreds of possible Tactics that you could use during an engagement.

MIRTE alone lists over 290.

What are some common ones that your team should consider using:

- Living off the Land – So hot right now, and will continue to be for the foreseeable future.
- Specifics:
  - LOLbins
  - WMI for lateral movement, persistence, etc..
  - Native PowerShell commands
    - With PowerShell 5, you could most likely run an entire operation with it alone.

- Why are these TTPs so important for you to utilize as a Pentester or Red Teamer?
- Because they are most likely not being logged, if they are you can probably assume they're not being monitored.
- Looking at it from the Defensive side, there's going to be so much noise that most of your actions will blend in with the rest of the activities. That is of course, if a tuned EDR solution + continuous monitoring + behavior correlation is being employed.


LIVING OFF
THE LAND TECHNIQUES
SO HOT RIGHT NOW
imgflip.com

Use What Is Available!

- Adversaries are going to take advantage of what is on the environment!
- So why shouldn’t we do the same?
- No reason to reinvent the wheel.

Engagement Type Selection

Let's go with an Emulated Adversary Enagement

Intel

APT 77 is known to use WMI for lateral movement and persistence.

Sourced from various threat intel feeds.

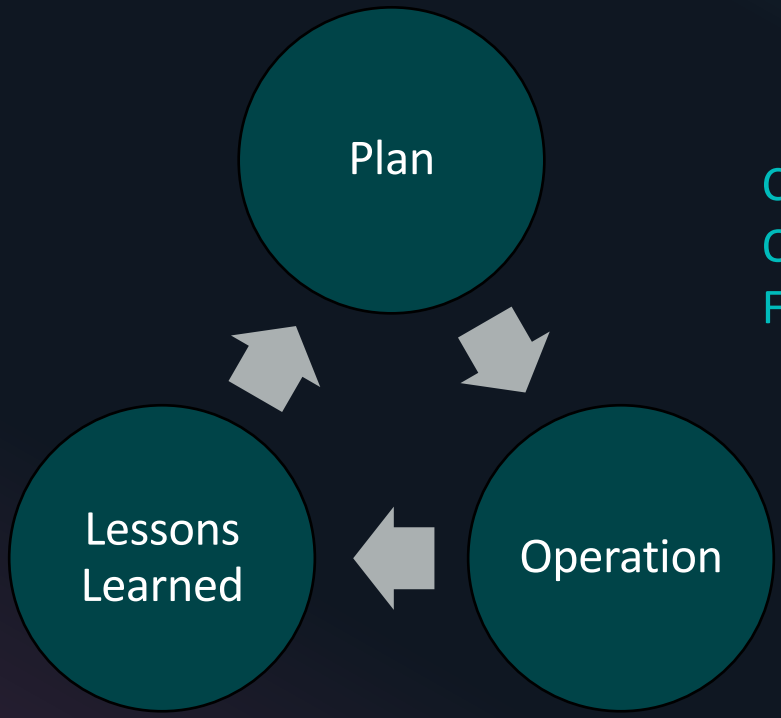
Objective

APT 77 has been observed targeting financial institutions along with R&D organizations.

Intent

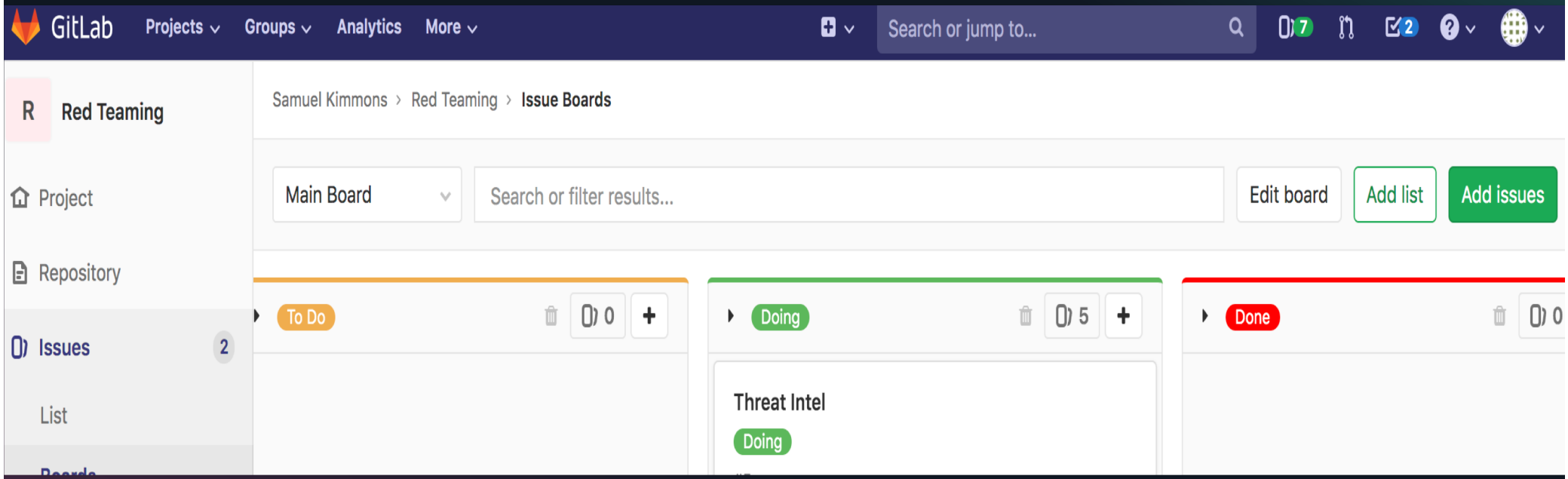
It is believed that APT 77 targets these specific entities for their access to money and their desire to steal intellectual property.

Overview of the Red Team's Operation lifecycle



Continuous Operations & Feedback

Planning with GitLab



Planning with Gitlab

Name	Last commit
Red Team Scripts	Add new file
README.md	Update README.md

README.md

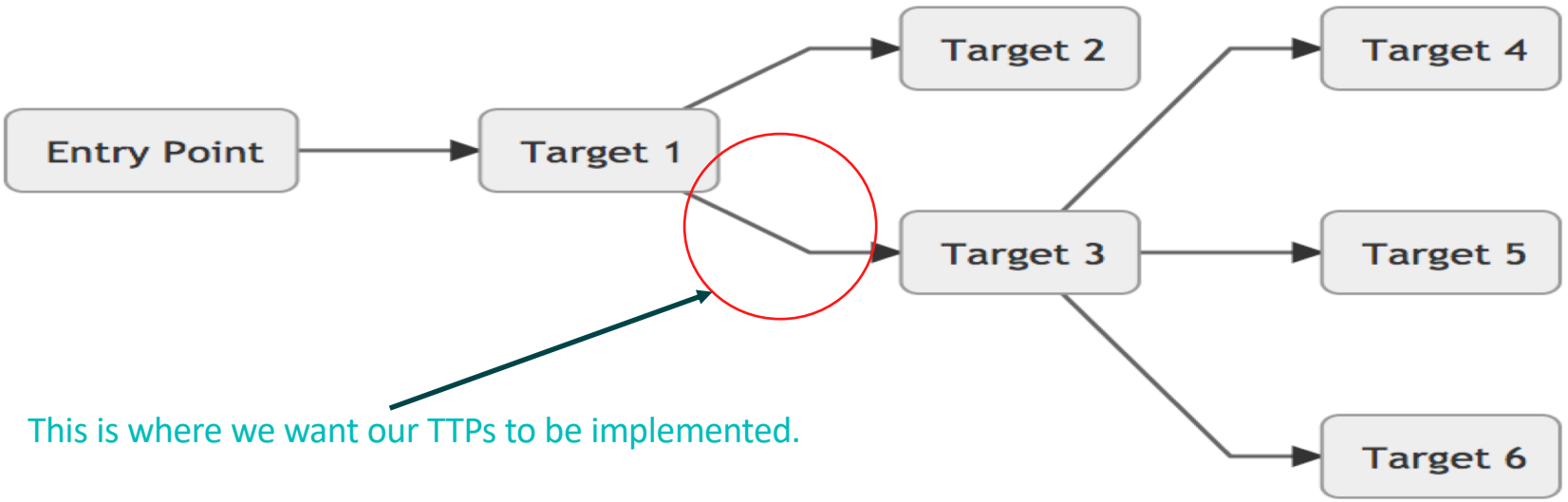
Welcome to the Red Team Repo for Operation TCS

This repo will include:

- Threat Intel for the enagement
- Code developed by the team members
- Rules of Engagement

Planning with Gitlab

Example Execution



Planning with Gitlab

Reporting

Last edited by **Samuel Kimmons** just now

New page | Page history | Edit

This page will serve as a place to document notes from the engagement

Please document anything relevant to the engagement, it will help during the correlation and reporting phases.

Execution notes (example)

- Executed TTP 1 on target 7
  - TTP 1 - Lateral movement via wmi was successful
- Executed TTP 4 on target 7
  - TTP 4 - Persistence via Run Keys was successful

Speaking of Reporting

- As a Pentester or Red Teamer the Reporting phase is probably the most important.
- It’s not as glorious and exhilarating as the Development or Execution phases, but it can make or break an engagement’s success.

How can we better convey the severity of our findings?

Through the correlation of our actions with Threat Intel.

Correlation!

Correlating our actions with those of known Threat Actors can bring immense value to your engagements as a Red Teamer or Pentester.

Example:

- A report states that APT28 Targets the financial sector, which happens to be the same industry of the org you're testing.
- The report also states that they utilize WMI for lateral movement, and during your engagement you find that you're able to openly use the same TTPs with nothing attempting to stop you.
- If they're not able to detect, let's say wmiprvse.exe spawning child processes then they might have a bigger issue.

- Correlation is key, imagine how quickly findings might get remediated.
- Or rather, as a Pentester you'll have more firepower to get even low vulnerabilities taken care of.
- Utilizing Threat Intel in our reporting can bring a substantial amount of value to the results of your engagements.

Some Love for the Blue Teamers

Tools are easy to change, but behaviors are far more complicated to modify.

What can you use to test TTPs?

- Tools, Labs, and Engagements such as:
  - Caldera
  - Atomic
  - Red Hunt OS
  - Detection Lab
  - Dedicated & Replicated environment
  - Try new tools you find on various blogs
  - Purple Teaming!

How can you stay informed?

- MITRE
- Threat Feeds
- Security Vendors
- Twitter
- Blogs

What Else Can We Do?

Purple Teaming!

Purple Teaming

A Pentesting team can fill the gap if a Red Team isn't an option. Just refer to the: Intel, Objective and Intent

Keys to Success!

What are the secrets to success?

Planning

Planning is going to be the biggest factor in the success of any engagement.

Documentation

Without proper documentation, how can you expect to learn from your successes and mistakes?

Communication

All parties should be in contact when necessary. Daily communication is preferred.

Keeping everyone informed

Gitlab – for Process/task tracking

Once again, communicate!

Think Like a Red Teamer

Final Thoughts

Samuel Kimmons

Twitter:
@Valcan_K

Website:
https://valcank.github.io/

References and links can be found on my website.

It is truly up to us as offensive security professionals to convey the severity of potential adversary actions targeting our organization.