Red Teaming

Why Organizations Hack Themselves

Disclaimer

The opinions stated here are my own, not those of my company.

The scenario described is entirely hypothetical and does not reflect any real-world events.

About Me

- Senior Security Engineer, Google
  - Tech Lead, Offensive Security Team
- Security Researcher
  - CVE-2014-4182, CVE-2014-5204, CVE-2017-17704, CVE-2019-10071
- CTF Player
- Twitter: @Matir
- Blog: https://systemoverlord.com/

Offensive Security

- Using adversarial techniques to test security controls
- “Ethical Hacker”*
- Spectrum of Activity
  - Penetration Testing
  - Red Teaming

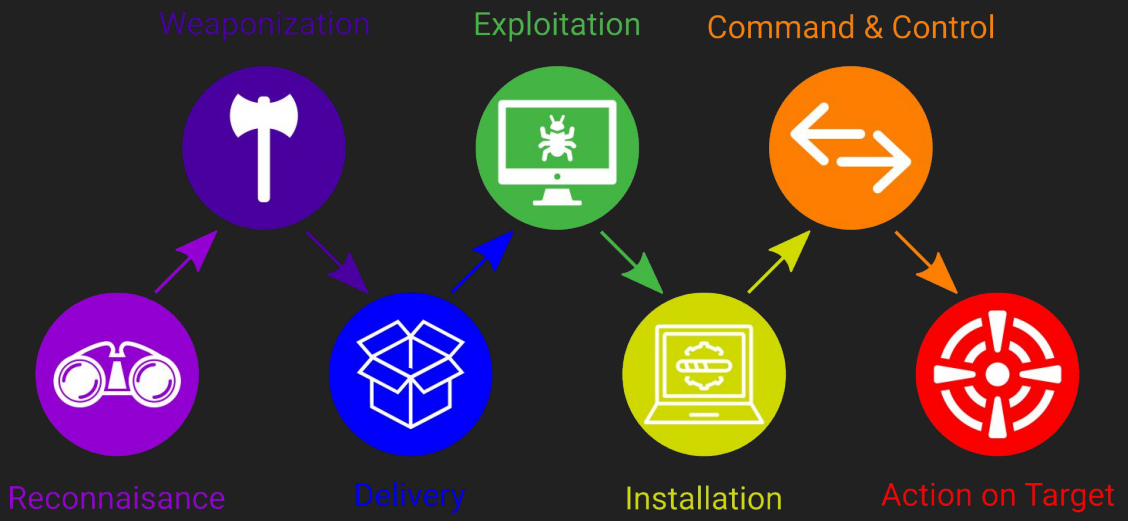
* Or at least Authorized

Penetration Testing

- Enumerating vulnerabilities, testing exploitability
- Breadth of coverage
- Not normally stealthy

Red Teaming

- Business Objective-Driven
- Adversary Emulation
- Testing Entire “Cyber Kill Chain”

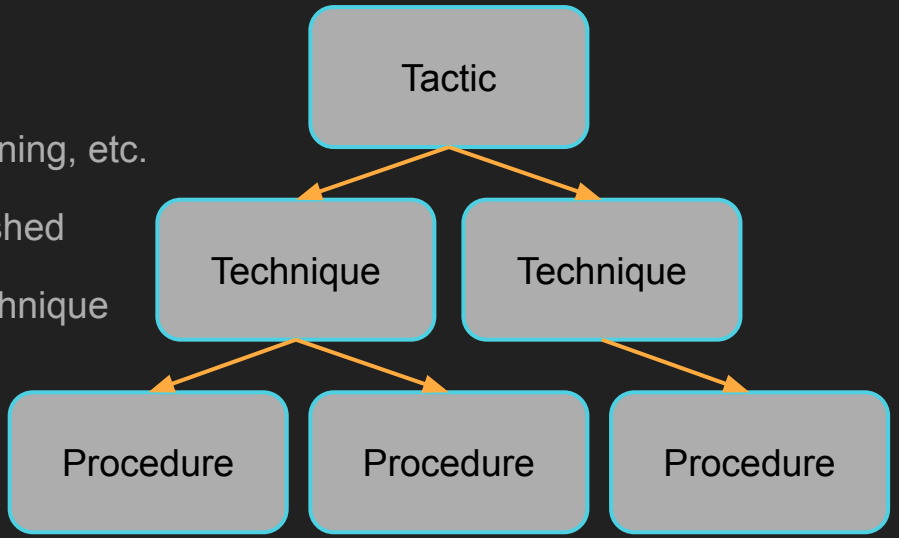


But Why?

- Challenge Assumptions
  - Security controls may be different between “as designed” and “as implemented”
  - Discover misconfigurations
  - Find unexpected approaches
- Test Detection & Response
  - Only adversary you get to compare notes with
  - Find blind spots

Replicating Attacker Behavior

- Learning About Attackers
  - Public Threat Intelligence (FireEye, etc.)
  - Internal Threat Intel (Larger Organizations)
- Tactics, Techniques, and Procedures
  - Tactics - High-Level Consideration, for planning, etc.
  - Technique - Specific Action to be Accomplished
  - Procedure - Implementation details of a technique



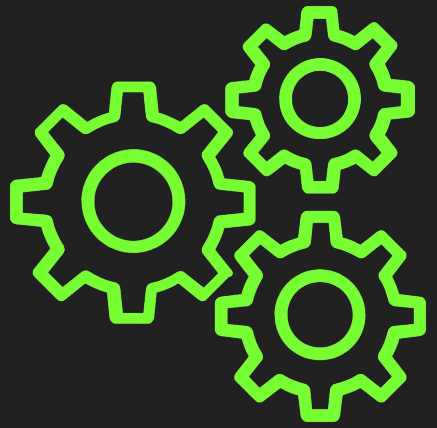
Running a Red Team Exercise

Identify Actor and Objective

- Cybercrime group stealing credit card data
- Student changing grades/transcripts
- Business competitor stealing intellectual property
- Nation state accessing email of dissidents
- Hacktivists defacing popular page

Red Teaming for Spacely's Sprockets

- Simulated Adversary: Cogswell's Cogs
  - Well resourced, but not at the level of a intelligence agency
  - Very interested in not being caught
- Objective: Steal Intellectual Property
  - Designs for the new Series 2020 Sprocket
  - List of Top Customers



Verify Rules of Engagement

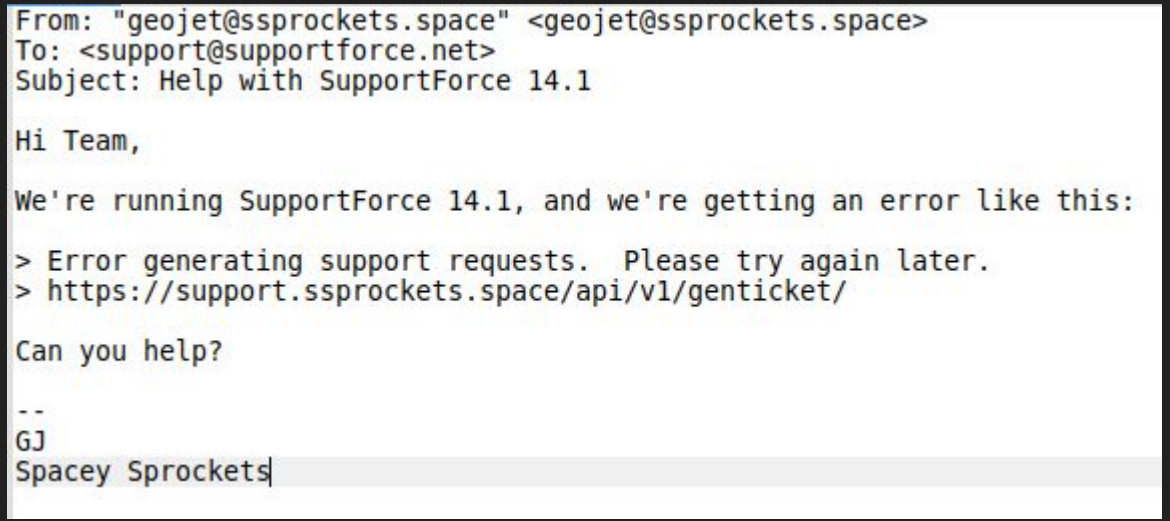
- Rules of Engagement Limit Team Actions
  - Define Scope -- Hosts/Networks that can be targeted
  - Limits on social engineering
  - Physical attacks allowed or not
  - Respect the User (and their privacy)
- Get Leadership/Legal Sign-Off
  - Avoid “Career Limiting Moves”

Reconnaissance

- Information on target
- “Passive” Options
  - Read Job Listings (Skills, Technologies, etc.)
  - Look for News Articles
  - Look for Employees Posting to Support Forums, etc.
- “Active” Options
  - Port Scanning
  - Brute Forcing

Reconnaissance on Spacely's Sprockets

- Find mail server, VPN, etc. by guessing domain names
- Find the software that runs their support portal



```
From: "geojet@ssprockets.space" <geojet@ssprockets.space>
To: <support@supportforce.net>
Subject: Help with SupportForce 14.1

Hi Team,

We're running SupportForce 14.1, and we're getting an error like this:

> Error generating support requests.  Please try again later.
> https://support.ssprockets.space/api/v1/genticket/

Can you help?

--
GJ
Spacey Sprockets
```

Initial Access (Getting In)

- Phishing for Username & Password
- Compromise Internet-Facing Server
- Email Malicious Attachment
- Drop a Flash Drive in the Parking Lot
- Bribe Insider

https://shop.hak5.org/products/usb-rubber-ducky-deluxe

Initial Access on Spacely’s Sprockets

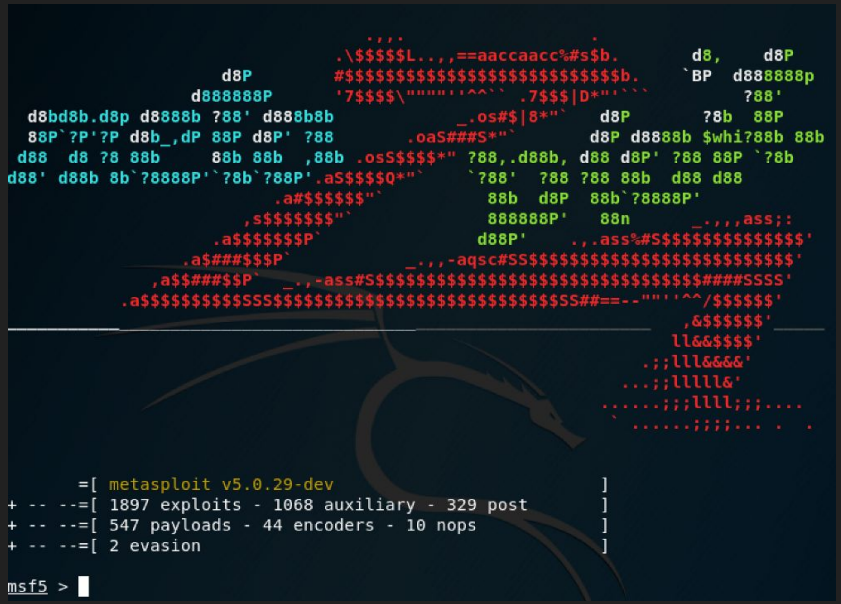
- We send an email to support
  - Links to clone of support site login page
  - Captures Username/Password
- Use credentials to login to remote access
  - Remote desktop session
  - Access as support agent

Command & Control

- Allow remote access to systems
- Usually intended to obfuscate traffic
- Can use existing/legitimate tools
  - Remote Desktop
  - Secure Shell (SSH)

Establishing C&C on Spacely's Sprockets

- Use software like "Metasploit" to Establish Connection
- Sends connection back to Red Team Server
- Provides
  - Run Commands
  - File Transfer
  - Dump Saved Credentials
  - Route Network Traffic



Movement Within Network

- May not be able to access objective immediately
- Need to gain privileges/move to other machines
- Achieved By:
  - Compromising Internal Hosts
  - Reusing Credentials
  - Transitive Trust

Movement within Spacely’s Sprockets

- On a Support Rep’s Workstation
  - No Access to Data we Want
  - Need to move to another account & computer
- Upload Metasploit to File Server
- Ask IT Staff to Help with Issue
- Gain Session Running as Helpdesk
- Use Helpdesk to Create New Account
  - Grant access to all servers

Actions on Objectives

- Access or Modify Data/Systems
  - Exfiltrate Sensitive Data
  - Modify Records
  - Knock Systems Offline
  - Add a long-term access

Actions on Spacely’s Sprockets

- Access File Server
  - Archive Product Designs
  - Archive Customer Lists
- Copy Data Back to Support Computer
- Slowly Upload to Server on Internet
  - Encrypted
  - Avoid Detection

Having an Impact

Reporting

- Communications skills are most underrated security skill
- Reports Read By:
  - Other Security Professionals
  - IT Staff
  - Software Developers
  - Physical Security
  - Leadership
  - Lawyers

Actionable

- Suggest fixes, not just point out flaws
  - Not necessarily implementation, but what the ideal state is
- Advise on hardening measures
- Focus on detection as well as prevention

Improvements for Spacely's Sprockets

- Use "2 Factor Authentication"
  - Security Tokens
  - Something you know (password), Something you have (token)
- Scan File Server for Malware
- Detect Large File Copies to Workstations
- Require 2 Techs to Create New Accounts

https://www.yubico.com/

Becoming a Red Teamer

Background of Red Teamers

- Software Engineer
- System Administrator
- Penetration Tester
- Security Analyst
- Military/Intelligence
- Others

Technical Skills

- Networking
- Authentication/Authorization
- Operating Systems
- Threat Modeling
- Vulnerability Analysis
- Exploitation

Soft Skills

- Written Communications
  - Report Writing
  - Convincing Phishing Emails
- Attacker Mindset
- Social Engineering
  - Convincing People to Do Something
  - Pretexting

Attacker Mindset

- Curiosity About How Things Work
- What-If Scenarios
- Thinking about Attacker Motivations
- Ill-defined
  - Is somewhat “I know it when I see it”
  - Some people are naturals
  - Others learn the skills

Resources

- Twitter: https://twitter.com/Matir
- Blog: https://systemoverlord.com/
- Slides & Notes: https://1337.fyi/redteaming
- Red Team Reading List: https://1337.fyi/want-to-red-team
- Red Team: How to Succeed By Thinking Like the Enemy: https://amzn.to/3mgVP23

Questions?