CSCI 1800 Cybersecurity and International Relations

Defense in Depth

John E. Savage

Brown University

Outline

- This lecture is based on a talk by Rob Joyce at the 2016 USENIX Enigma Conference entitled Disrupting Nation State Hackers*.
- Joyce was Chief of Tailored Access Operations (TAO) Office in National Security Agency (NSA).
  - TAO is cyber-warfare intelligence-gathering NSA unit
- Watch his great (35min) video with the slides!

*See https://www.youtube.com/watch?v=bDJb8WOJYdA

Joyce's Basic Message

- To protect a network you must understand it
  - Successful attackers take the time to know your network!
  - They will know better it than the people who designed it and those securing it.

Phases of Intrusion

- Reconnaissance
- Initial Exploitation
- Establish Persistence
- Install Tools
- Move laterally, i.e. across the network
- Collect Exfil and Exfiltrate

Cyber Kill Chain

- Every phase of an intrusion is a potential step in the kill chain
  - A point at which you can stop an attacker

Reconnaissance – Understand Target

- Attacker will physically scan the target
- Study important people and activity at target
- Attacker will study your network thoroughly and know it better than you do
  - Attacker will know the technologies you actually used, not just what you intended to use.
  - It will study them closely and find vulnerabilities
- Attacker is focused and pays attention to details

How to Counter Threats

- Know what devices are installed on your network
- Reduce attack surface – drop unused devices
- You must red-team your environment
  - Find vulnerabilities and what's exploitable and act!
- Well run networks make attacker's job harder
- NSA will red-team government sites
  - Often find the same vulnerabilities years later! BAD!

How to Counter Threats

- Don’t assume that a crack is to small to be noticed or exploited
  - NSA does not ignore them; it needs a toe-hole
- Advanced Persistent Threat (APT) attacker is patient
  - He/she/they will look for esoteric edge cases
  - E.g. Will wait for door to open, perhaps on weekend

Know and Protect Your Trust Zone

- Network boundaries are becoming more porous
  - Think smartphones, laptops, and Internet of Things (IoT)
  - Interconnected facilities are not in your trust zone
- Remember:
  - Cloud computing is fancy name for outsourced security
  - Trust boundaries extend to partners
  - HVAC systems can be a point of entry
- Instrument, defend, pay attention to crown jewels
  - How can you instrument high-value files?

Ways to Launch Initial Exploitation

- Phishing
- Watering hole attack
- Using a known CVE for which an exploit exists
  - What is a CVE?
- SQL injection
  - How is SQL defined? Look it up!

Ways to Launch Initial Exploitation

- Zero-days are not skeleton keys
- Persistence and focus will get you into a large network without 0-days!
  - Many other vectors are available and less dangerous
- Continuous defensive work is necessary

Principal Intrusion Vectors

- Email – tempts you to click on a link
- Website – run code from a corrupt website
- Removable media – it gets inserted into a port
- Recall that air-gaped networks can be bridged!
  - Think Stuxnet

Protecting Against Intrusion

- How can we enforce written policy?
  - People will click on email links even after training
- Can your architecture protect you?
- Use MSFT EMET* – anti-exploitation technology
  - EMET uses 12 mitigation techniques including
  - ASLR, DEP, Anti-Return Oriented Programming
- Visit NSA Information Assurance Directorates
  - Host mitigation package (EMET only one method)
  - USG uses just these mitigation practices

* https://insights.sei.cmu.edu/cert/2018/08/life-beyond-microsoft-emet.html

Protecting Against Intrusion

- Take advantage of software improvement
- If there is a known exploitable bug (CVE), fix it.
  - Automatic updating is outstanding security practice
- Replace your OS with a secure host baseline
  - A pre-configured, hardened, machine-ready binary
  - They implement best practices for configurations
  - Special version of Windows 10 created for USG
- NSA teaches and trains employees very well!

Protecting Against Intrusion

- NSA is using best practices for exploitation
- In almost any intrusion, it tries to get credentials
- What is normal inside your network?
  - Is a user operating within norms for credentials?
  - Are they doing what they should be doing
- Are you monitoring credential use
- If a user's activity is anomalous, examine it
- Two-factor authentication protects assets

Protecting Against Intrusion

- Strictly limit administrator privileges – no admins
- Segment the network – make it hard for attacker to get from one segment to another!
- Whitelist applications – only listed apps can run
- Don’t put credentials in scripts to enable logins

Protecting Against Intrusion

- Learn about “pass the hash” – serious weakness
  - Password hash allows Yves* to move around like mad
  - See https://www.beyondtrust.com/resources/glossary/pass-the-hash-pth-attack
- Enable the logs and look at them
  - This is a bedrock way to find intrusions
  - Know your network because the attacker will

* Yves is a well-known, beret-wearing French eavesdropper.

Establish Persistence

- The goal is to dig in and hold on
- Privilege escalation is done first
- Then tools are downloaded, e.g. RAT (what?)
  - Defender looks for download tools
- Application whitelisting make this hard
- Find out what you need to protect, segment it and whitelist within it
- This make is hard for the attacker

Hacker Installs Tools

- Attack installs small tool followed by big tool set
  - Attacker wants to establish a beachhead
- Old anti-virus software poor, but being upgraded
- Reputation services are important
  - Hash every piece of software on your system and push the hashes to a reputation service for testing
  - If software has been seen once, be very afraid
  - Such services make an attacker's job more difficult

Install Tools

- Most tools want to talk out
  - Reputation services work well in domain name world
- Domain names
  - Good to block known bad domains
  - Better to block names not known to be good
  - It is hard for a domain to acquire a good reputation

After Inside, Attackers Move Laterally

- Can you defend against lateral movement?
- How can you make movement difficult
  - Network segmentation is best
  - Monitoring movement is good – why is this data moving?
  - Caring about privilege allocation
  - Two-factor authorization good
- Advanced attackers go after crown jewels
  - Defend by limiting admin privileges, segment accesses
- Frustrating to be inside & unable to reach jewels

Managing Trust

- Connecting from remote location?
  - Require use of approved comm app when outside
  - Where are you calling from? What time of day?
  - Use dynamic privileges, e.g. limit access if data is TS
- Segment & manage trust to most important data
- Assume that you are already hacked
  - Do you have means and methods to monitor hacker?
  - Verizon report: Intrusions go on for years undetected

Managing Trust

- An incident response plan is necessary
  - It must also be exercised – trial runs during training
  - Frequently not done!
- The Internet of Things (IoTs)
  - Much easier to attack personally managed IoTs
  - Why allow home laptops into secure environment?
- SCADA networks
  - Very sensitive – they must also be made secure

Collect, Exfiltrate and Exploit

- Data theft is obvious
- Destructive attacks less obvious but important
  - Instrument and protect your valuable data
  - Plan for data destruction, manipulation, corruption
    - Do off site backups
- Differentiate between cyber criminals and APT
  - Mass malware is looking for low hanging fruit
- Nation-state attacker is persistent
- You need to defend, improve, continuously

Good Advice

- Can be found at NSA Information Assurance
  - Mitigation Guidance
  - Show chart

Forrester Zero Trust Concepts

- All resources should be accessed in a trusted and a secure manner regardless of location.
- Access must be on a “need to know” basis and strictly enforced.
- Inspect and log all traffic.
- Forrester Zero Trust:
  - https://go.forrester.com/government-solutions/zero-trust/

The Problem

- Perimeter-based security is ineffective.
  - Limiting access by port is insufficient
  - Signature-based analysis easy to evade
- Guiding principle: “Never trust, always verify!”
- Approach:
  - Identify user of each device
  - Label content of each file by security level
  - Establish policies concerning access to files
  - Enforce access policies by devices, locations, users, geolocation and time of day

Segementation Techniques

- Virtual Local Area Networks (VLANs)
  - Used only to segment networks, no security checks
  - Deploy next-generation firewalls between them
- Secure communication via IPsec, VPN, etc.
- Control access to and movement of files
- White- & black-list IP addresses & domain names
- White- & black-list applications
- Use signed code (see lecture on encryption)
- Try to detect anomalous activity

paloalto networks
Network Segmentation/Zero Trust

- Secure access
  - IPsec and SSL VPN
- Inspect of ALL traffic
  - Truly granular access control
- Advanced threat protection
  - Anti-virus, intrusion detection, and advanced threat prevention technologies

Review

- Based on Rob Joyce 2016 USENIX Enigma talk
- To protect a network, you must understand it
- Exploitation phases
  - Know and protect your trust zone
- Protect against intrusions
- Activity inside a network
- Deploy Forrester Zero Trust concepts