BREAKING AND ENTERING: EMULATING THE DIGITAL ADVERSARY IN 2019

Bobby Thompson
National Cybersecurity Assessments and Technical Services (NCATS)

CISA
CYBER+INFRASTRUCTURE

Services Today

If vulnerability is the only element of risk that we can eliminate ....

Cyber Hygiene

- Open Source Intelligence Monitoring
- Phishing Campaigns and Assessments
- System & Application Vulnerability Scanning
- Remote Penetration Testing

Risk Evaluation

- Risk and Vulnerability Assessments
- Validated Architecture Design Reviews

Advanced Operations

- Critical Product Evaluation
- Red Team Assessments

.... lets focus on proactive elimination of vulnerability to reduce risk

CISA
CYBER+INFRASTRUCTURE

Goals

REDUCE

REDUCE RISK AND INCREASE RESILIENCE

- IDENTIFY AND ELIMINATE ATTACK PATHS PRIOR TO THEIR EXPLOITATION BY MALICIOUS ACTORS;
- COLLABORATIVELY EVALUATE PRODUCTS WITH VENDORS IN ORDER TO INCREASE "OUT OF BOX" SECURITY;
- PROMOTE EFFECTIVE CYBERSECURITY RISK MITIGATION STRATEGIES.

ENABLE

ENABLE DATA-DRIVEN DECISIONS

- IMPROVE POLICY MAKERS ABILITY TO MAKE INFORMED, RISK-BASED DECISIONS;
- ENABLE ANALYSTS TO ENRICH THREAT ANALYSIS AND MODELING AND INFORM RISK MANAGEMENT;
- CHAMPION AND PROMOTE DATA-DRIVEN STANDARDS, POLICIES, GUIDELINES AND CAPABILITIES.

INFLUENCE

INFLUENCE OPERATIONAL BEHAVIOR

- MEASURE AND MONITOR THE IMPLEMENTATION OF MATURE OPERATIONAL CAPABILITIES
- NOTIFY STAKEHOLDERS OF SIGNIFICANT FINDINGS AND TRENDS

CISA
CYBER+INFRASTRUCTURE

THREAT EMULATION MODEL COMPARISON

Threat emulation and assessment models means many things to many people

- Vulnerability Assessment
- Penetration Testing
- Red Team Operations

- Used interchangeably and often amalgamated

- Important to establish a clear delineation for *your* purposes
  - Each have advantages and disadvantages

- Caveats….

VULNERABILITY ASSESSMENT

- **Primary objective: Identify vulnerabilities within target scope**

- Vulnerabilities generally discovered via automated tools
- Typically, no exploitation is performed against hosts
  - Additional manual steps required to clear false positives
  - Some tools may provide the capability to attempt exploitation for validation

- This model could be leveraged by leadership to:
  - Discover critical vulnerabilities and recommended mitigations
  - Determine criticality statistics for a target environment
  - Validate patching capabilities in place are effective

PENETRATION TEST

Primary objective: Effect & outcome of vulnerability exploitation

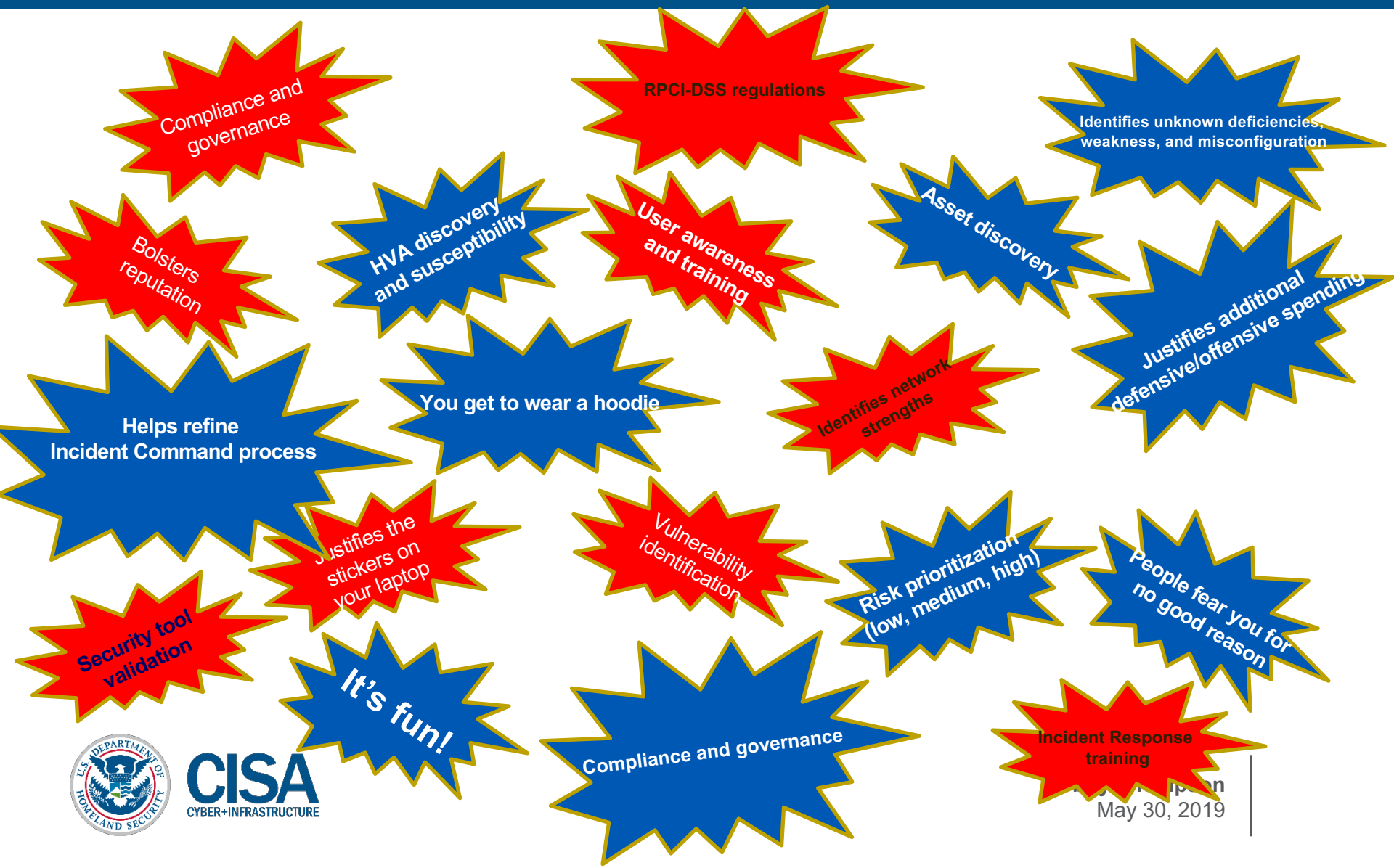
- Emulation is conducted by applying an attacker mindset to discovered vulnerabilities
  - Breadth of testing is limited by scope and legal restrictions
- Tests are collaborative in nature and exploitation is coordinated
  - No obfuscation of activity or evasion of traditional IR
  - Focus is testing technical controls in an environment
- This model could be leveraged by leadership to:
  - Prioritization, management, and mitigation of risk
  - Identify and eliminate attack paths prior to exploitation by malicious actors
  - Find misconfigurations not discovered by vulnerability scans

RED TEAM OPERATIONS

Primary objective: Effective training for blue teams, SOCs, and network defenders

- Emulates real-world threat activity against a target organization
  - Events are not coordinated with security personnel
  - Utilization of evasion, obfuscation techniques, and advanced skill sets
  - Breadth of testing limited by legal restrictions
- Tests people, processes, and technologies
- This model could be leveraged by leadership to:
  - Train defensive personnel against a live threat actor in a controlled scenario
  - Test defensive detection and response capabilities of an organization

WHY EMULATE?



CISA
CYBER+INFRASTRUCTURE

ADVERSARY EMULATION 101

- Authorization of an ethical, professional, and realistic attacker within the confines of your network infrastructure

- Allows stakeholders to:
  - Understand and manage risk
  - Discern what happens if a real-world attacker infiltrates a network
    - Did the SOC detect adversarial activity/entry?
    - Was root cause determined?
    - Were critical assets manipulated?
    - What were the lessons learned?

- Cyclical Process
  - Adversary Emulation
  - Test/Challenge Defense/Blue Teams
  - Report, Review, Revise, Mitigate, & Follow Up

- Log, communicate, collaborate

ADVERSARY EMULATION 101

- Infrastructure setup
  - Team share
  - C2 Infrastructure and redirectors
  - Domain names
  - Payload development
  - Data collection repository
    - Findings
    - Observations
    - Risks and issues
    - Daily summary
    - Persistent and non-persistent
    - Raw data

ADVERSARY EMULATION 201

- Research, Read, Test, and Develop
- Standard, consistent, quantifiable, and ***adaptable*** TTPs, PPPs, and methodology
- Multiple options to exploit the kill chain
- Evolve, Adapt, Thrive
- Administrative statistics, findings, and standards (ATT&CK, NIST, etc.)
- Do not accept the status quo!

ADVERSARY EMULATION 201

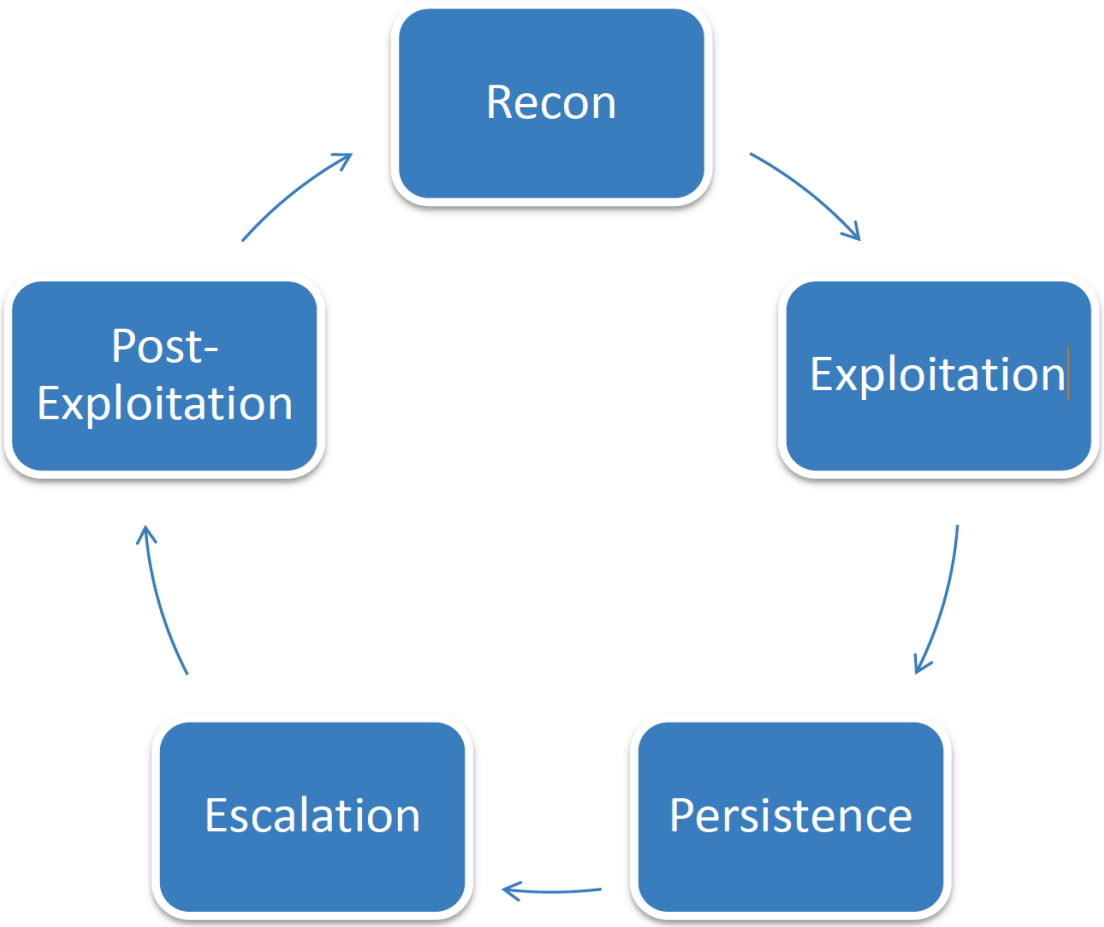
CVSS Score	Number Of Vulnerabilities	Percentage
0-1	1322	8.60
1-2	126	0.80
2-3	472	3.10
3-4	840	5.40
4-5	3653	23.70
5-6	2432	15.80
6-7	2367	15.30
7-8	2528	16.40
8-9	68	0.40
9-10	1620	10.50
Total	15428	

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	74	1.60
1-2	30	0.70
2-3	179	3.90
3-4	319	6.90
4-5	1151	24.90
5-6	795	17.20
6-7	755	16.40
7-8	802	17.40
8-9	29	0.60
9-10	481	10.40
Total	4615	

ADVERSARY EMULATION 301

- Assume breach
- Replicate threat landscape specific to each customer – adversarial modeling
- Wealth of intel reports, malware analysis sites, and formal collaboration groups
- Allow for adaptable TTPs
- Total and complete transparency
- Automation

THREAT EMULATION METHODOLOGY



METHODOLOGY: RECON

- OSINF and *passive/active* recon is the primary activity for the initial phase
- Information gathering, passive fingerprinting, social media monitoring
  - Personnel, roles, e-mail addresses, organization schemas, infrastructure
- Multitude of sources provide a wealth of valuable data
  - Google Dorking, LinkedIn, social media, and publicly hosted information
- Analytics are applied to tie the information into a bigger picture
  - Initial targets are developed based off this information
  - Specially crafted spear-phishing campaigns are developed
- Restriction: establishment of personas, impersonation, etc.

METHODOLOGY: EXPLOITATION*

- Primary attack vector is phishing
- Non-technical personnel are generally targeted
  - Human Resources, contract managers, press, hiring managers
  - Everyone and anyone
- Out of office replies can provide a wealth of information
- A rapport is built with the target before payload delivery
  - This establishes trust so suspicion is not raised upon payload execution
  - This also provides an avenue to test payload success
  - 1-3 campaigns, no rapport, lure is moderate in sophistication
- Payload delivers code execution and the code establishes C2
- Once exploitation is successful, the method can be replicated


Check out this tweet!
Inbox x
ABC Twitter <twitter@abc.com
Mar 10 (7 days ago)
to me
Oh my, look at what somebody posted on Twitter http://twitter.com/ABC
Someone is getting FIRED for this!!
Click here to Reply or Forward

METHODOLOGY: PERSISTENCE

- Once access is obtained, an initial triage and enumeration is performed
  - Triage is a series of steps taken to learn about the host environment
- Persistence may be required as C2 runs in memory
  - Persistence will provide us the opportunity to maintain access through reboots
  - Risk: artifact to be left on disk-potential point of detection
- Persistence is established based on the triage results
- Examples of persistence could include registry or schtask modification
  - Different lanes will use different methods of persistence so tactics are varied
- Persistence may be established or removed as required

METHODOLOGY: ESCALATION

- 2 primary actions in the escalation stage go hand in hand:
  - Lateral movement is using available data to establish C2 on another host
  - Privilege escalation is the act of raising permission levels on a host or network
  - These two actions often rely on each other for overall success
- Primary methods of escalation utilize misconfigurations
  - Shares and local drives are also searched for passwords or other information
  - "Living off the land" helps maintain stealth throughout operations
  - Performing exploitation for escalation could trigger technical controls
- Data on accounts and groups are pulled from Active Directory
  - An analytical process is applied to determine relationships and an attack path
  - If discovered, the attack path is then executed IAW available data

METHODOLOGY: ESCALATION

- End-goal for escalation is enterprise admin when possible
  - Can be abused to obtain unfettered access to most areas in the environment
  - Enterprise or domain administrator access not required when other paths to compromise sensitive business systems exist
- As a high level example:
  - May have local administrator rights to systems, but not domain rights
  - Can use local admin account to move laterally to other hosts on the network
  - Hosts are triaged and searched for new data or account information
  - Having local administrator rights on a host with a domain admin logged in could result in the compromise of the domain administrator account
- New accesses are used to further entrench in the environment

METHODOLOGY: POST-EXPLOITATION

- At this point the cyclical methodology can repeat itself
  - Once entrenched, operators can further perform internal reconnaissance
  - Based on that recon the sensitive business systems can be targeted
  - Privileges acquired in the escalation stage can be used to move to the SBS
  - Artifacts validating successful access to the SBS can be obtained

- Can also include additional:
  - Recon
  - PrivEsc
  - Lateral Movement
  - Obfuscated data pilfering

PLANNING, EXECUTION, POST-EXECUTION

Planning

- Establish Rules of Engagement
- Confirm Dates and Time Frames
- Conduct Pre—Assessment Briefs
- Define the Purpose
- Identify Target Systems
- Procure Scoping Documents
- Notify SOC and External Partners

PLANNING, EXECUTION, POST-EXECUTION

Execution

- Commence Assessment
- Stay in Scope
- Conduct Assessment
- Identify and Exploit Vulnerabilities
- Maintain Communications
- Complete Assessment
- Evidence Collection and Cleanup

PLANNING, EXECUTION, POST-EXECUTION

Post-Execution

- Customer Out-brief
- Validate Evidence
- Report Writing
- Assist with Remediating Weaknesses
- Create Post-Assessment Follow Up
- Strategic Roadmap
- Self Assessment/Lessons Learned

ADVANCED THREAT ANALYTICS

- What does ATA do?
- ATA technology detects multiple suspicious activities, focusing on several phases of the cyber-attack kill chain including:
  - Reconnaissance
  - Lateral Movement
  - Domain Dominance (persistence)
- **Malicious attacks** are detected deterministically, by looking for the full list of known attack types including:

•Pass-the-Ticket (PtT)
•Pass-the-Hash (PtH)
•Overpass-the-Hash
•Forged PAC (MS14-068)
•Golden Ticket
•Malicious replications
•Reconnaissance
•Brute Force
•Remote execution

CISA
CYBER+INFRASTRUCTURE

https://docs.microsoft.com/en-us/advanced-threat-analytics/what-is-ata

CISA
CYBER+INFRASTRUCTURE

For more information:
cisa.gov

Questions?
NCATS@hq.dhs.gov:

CISA

CYBER+INFRASTRUCTURE