Cyberspace Trapping
The Offensive Defender
whoami

- Former Air Force
- Counterhacker
- Founder Open Security
- Instructor with the SANS Institute
- Author of the SEC460 Course
I Am Red

• Offensive Perspective is Critical for Defense
  – This is True for Defense Software Vendors as too!
• Targeting Threat Tactics Requires Intimate Understanding
Losing is Inevitable

Defense Needs to Be Successful 100%
Offense just Needs to Win Once
Losing is Inevitable

• The quickest way to lose is to cede victory
  – It stifles Creative Thinking
  – It’s the Easy Way Out
• If a catastrophic breach feels inevitable how can we change this?
• Military Science gives us parallels from which to Learn
Introspection

• Is your Defense at the Boundary or Behind it?
• Do you know how your Vendor Tools Work?
• Breaches Happen!
  – The Maginot Line Style of Defense is Outdated and Dangerous
  – It is Time to Invest and Empower People to Customize Defense
Fighting the Right Fight

Is your Defensive Strategy Targeted to Address True Threats?
Cyberspace Trapping

• It’s not You it’s Me
• Poison vs Venom

Cyberspace trapping is the practice of poisoning threat Tactics, Techniques, and Procedures in order to weaponize your environment
Tactics, Techniques, and Procedures (TTP)

• TTP is a widely used term in the information security community but many misuse or incorrectly delineate the term.
  – Tactics - "The employment and ordered arrangement of forces in relation to each other. See also procedures; techniques."
  – Techniques - "Non-prescriptive ways or methods used to perform missions, functions, or tasks. See also procedures; tactics."
  – Procedures - "Standard, detailed steps that prescribe how to perform specific tasks. See also tactics; techniques."
Know thy self, know thy enemy. A thousand battles, a thousand victories
Finding Threat TTP

- Techniques grouped within a subset of overarching tactics
- Many listed techniques are in use by most threat groups

ATT&CK Matrix for Enterprise
Mimikatz and LSASS Passwords

- According to the NSA Red Team, Mimikatz is the number one threat to US Government Environments.
Task Manager LSASS Dump
Other Mimikatz Implementations

- PowerShell
- Cobalt Strike
- C#
- Metasploit
- Many Many Others
Poisoning LSASS

Tactic
• Escalate privileges to domain admin using stolen credentials

Technique
• Use Mimikatz to retrieve credentials from LSASS memory

Procedures
• Steps to accomplish the techniques mentioned above

Traditional Defense
1. Do more user awareness training
2. Write a Mimikatz signature and pray

Cyberspace Trapping
• Create fake accounts configured to lockout after one failed attempt
  – Use RunAs to seed LSASS with fake creds
Configuring Fine-Grained Password Policies

![Diagram showing Active Directory Users and Computers interface with HoneyTokenUsers properties window open.]
Sneaking Fake Credentials into LSASS

runas /user:domain.com\admin /netonly cmd.exe
Sneaking Fake Credentials into LSASS

https://github.com/FuzzySecurity/PowerShell-Suite

**Invoke-Runas**

Functionally equivalent to Windows "runas.exe", using Advapi32::CreateProcessWithLogonW.

```
Start cmd with a local account.
C:\PS> Invoke-Runas -User SomeAccount -Password SomePass -Binary C:\Windows\System32\cmd.exe -LogonType 0x1

Start cmd with remote credentials. Equivalent to "/netonly" in runas.
C:\PS> Invoke-Runas -User SomeAccount -Password SomePass -Domain SomeDomain -Binary C:\Windows\System32\cmd.exe -Logon
```
Monitoring and Scaling with PowerShell

- Tracking LockedOut Status Provides us with Additional Sensors within the Environment
- Correlating this Information with the IP Address of the system where the Trap is in Place Allows for Increased Reaction Speed
Other Implementations

- Passwords.txt Files
- Poisoned Password Managers
- Network Passwords
  - Telnet
  - FTP
  - HTTP

*The threat actor can no longer know whether to trust the password gifts of careless users. They might just be poisoned.*
Trap Master 101

Pretend inferiority and encourage his arrogance.
The OODA Loop

• When the Threat can no longer trust their Own Tools
  Their ability to Decide has been Disrupted
Poisoning Documents
Other Traps

• Fake Login Portals
  – Site Cloning
• Robots.txt Disallowed References
• Port Traps
• Decoy Shared Drives
• Local Admin Access Group Traps
• Many More
Traps vs Honeypots

• Traps are Built to Poison Adversary Tactics to Produce Indicators of Compromise
  – Because the Trap is Based on Fake Information they are Difficult to Turn Against You
• Honeypots Collect Threat Intelligence by Providing a Low-Risk Target for Adversary Exploitation
Intel Gain/Loss

- Threat Intelligence is Vital, but Most Commercial Feeds are Pure Snake Oil
- Personalized Indicators of Compromise are the only Valid Ones
- In the Private Sector we are Extremely Quick to Burn our Threat Intelligence
Cyberspace Trapping

- Cyberspace Trapping is an aggressive strategy for defense
- The objective is not to block attacks
  - Blocking all attacks, you can see, leaves fewer options to identify the attacks you cannot
  - Poison the root of their methodology
  - Then follow the effects along the tree until you see fruit they are after and deny them.
- Engaging adversaries by tactic as opposed to tool is not a static, trivially bypass-able defense like AV signatures
- When the opponent is uncertain they are vulnerable. When deceived they are weak. Cyberspace trapping about sowing confusion, disorder, and chaos along the attacker’s path