Anatomy of a Hack

John H. Sawyer
Senior Managing Consultant
InGuardians, Inc.

Bryce Lay - Comsys
Agenda

• Introduction
• Threat Hunting
• Deception
• Powershell Tools
• Additional Tools
• Adversarial Emulation
• Conclusion
Purpose of this Workshop

• Introduction to Threat Hunting / Hunt Teaming
• Learn about different analysis types
• Hands-on with endpoint-focused tools
• Have Fun!!
Who Am I?

• InGuardians Senior Managing Consultant
  – Red Team Operator / Penetration Tester
  – Social Engineering
  – Web, Mobile, and Desktop Apps
  – Incident Response & Forensics
• Dark Reading and InformationWeek author and speaker
• Infosec Volunteer and Mentor
• DEF CON 14/15 Capture the Flag (1@stplace)
My Awesome Employer

- InGuardians, Inc. (formerly IntelGuardians)
- Founded 2003 by Mike Poor, Ed Skoudis, Jay Beale, Jimmy Alderson, and Bob Hillery
- If it’s security-related, we do it.
  - Red Team Assessments
  - Penetration Testing
    - Network, Web, Mobile, Wireless, Hardware, People, and Physical
  - Incident Response Management and Digital Forensics
Thank You

- My Wife and family
- Bryce Lay – ComSys
- Interop Team
- InGuardians
- UBM, Dark Reading, and Tim Wilson
Or is it Hunt Teaming?

THREAT HUNTING
Threat Hunting Defined

• Proactively searching through endpoints and/or logs to detect threats that bypass traditional security tools.

• Human hunting efforts bolstered by threat intelligence and automated tools.
Hunting: Humans vs. Technology

LITTLE BOBBY

WHAT ARE YOU DOING?!

HUNTING THREATS.

WELL THREAT HUNTING DOES REQUIRE THE HUMAN FOCUS --

-- BUT MORE WITH FORENSICS AND SECURITY OPERATIONS THAN WITH BOWS AND ARROWS!

by Robert M. Lee and Jeff Haas

I CAN STILL FULLY AUTOMATE THIS RIGHT?

REMOVING THE HUMAN WOULD BE WRONG.
Threat Hunting Requires...

• A mindset change to understand an attacker WILL get in at some point.
• Knowing your network <- VISIBILITY!
• Understanding the threats your company faces
• Tools and Training
Understanding Threats

• Threat profiling
  – Who is targeting YOU?
• Tactics, Techniques, and Procedures (TTPs)
• Threat Intelligence
  – Internal
  – External
Prioritizing the Hunt

• Identify the commonalities between intrusions
• Enumerate the artifacts left by those types of attacks
  – What are high-confidence indicators?
  – What can be easily observed?
Threat Intelligence

- **External**
  - Known attackers
  - Reputation lists
  - TTPs
    - Tactics
    - Tools
    - Procedures
  - Industry-specific
    - Peers (ISAC)
    - Vetted by 3rd party

- **Internal**
  - DNS
  - Web proxy
  - FW/IDS/IPS
  - Endpoints
    - configuration
    - AV/HIPS
    - process tracking
    - certificates
Attackers Lateral Movement

- Native operating system tools
  - wmic
  - netsh
  - Powershell
- Common syadmin tools
  - Pstools!!
- File shares
- Sharepoint
- Local filesystem
- Passive network monitoring
- Remote access
  - RDP, Citrix, SSH, VPN
The more, the merrier...

TEAM BUILDING
Digital Forensic/IR + Enterprise Security?

**LITTLE BOBBY**

Is threat hunting more forensics and incident response or more enterprise security focused?

**BOTH! Good security operations require a wide set of skills!**

The key is to focus threat hunters on **REAL THREATS** --

**-- not areas like patch management and tuning firewalls!**

by Robert M. Lee and Jeff Haas
Hunters Blend In

• Blue Team
  – Enterprise Defense
  – Forensics and Incident Response
  – Systems Administration and Development

• Red Team
  – Penetration Testing
  – Adversarial Simulation
Getting Your Team Ready

• Build visibility enterprise-wide at the network and host level.
• Ensure that traditional active and passive defenses are working correctly with the appropriate level logging and monitoring.
• Train your team on hunting techniques and tools, offensive techniques, and identification of indicators of compromise.
• Collect internal and external threat intelligence to aid hunting efforts.
The Threat Hunter’s Skillset

- Natural curiosity
- Ability to think like an Attacker
- Motivated and passionate about learning
- Well rounded with wide range of IT and security experience
- Familiarity with the enterprise environment
- Analytical with ability pivot quickly and “think on their feet”
Quick Start Guide for Hunters

• Start small with something you know
  – Data sources
    • DNS, Web proxy, Windows
  – Tools
    • configuration management
    • PowerShell
So you wanna hack some stuff?

ADVERSARIAL EMULATION
Red Teams and Penetration Tests

- Red Team and Blue Team collaboration
  - “Purple” Teaming
- Full scope, no holds barred penetration testing
- No time constraints
- Multi-disciplinary
Purple Team to the Rescue

https://blog.netspi.com/common-red-team-techniques-vs-blue-team-controls-infographic/
Living off the land

POWERSHELL TOOLS
PShunt

- Designed to scan remote endpoints for indicators of compromise

- Survey endpoints for more comprehensive information related to state of those systems
  - active processes
  - Autostarts
  - Configurations
  - Logs

https://github.com/Infocyte/PShunt
PSRecon

- Gathers data from a remote Windows host using PowerShell
- Organizes collected data into folders
- Hashes all extracted data
- Hashes PowerShell and various system properties
- Sends the data to a share, email, or retained locally.

- Self-contained HTML report
- Endpoint lockdown functionality
  - Disables NIC
  - Logs user out
  - Disables AD account

https://github.com/gfoss/PSRecon
PSRecon - Demo

- Run against localhost
  - PS C:\> .\psrecon.ps1
- Run against remote host
  - PS C:\> .\psrecon.ps1 -remote -target [computer]
HostRecon

- Current Hostname
- IP Information
- Current Username
- Current Domain Name
- All Local Users
- Local Admins Group
- Netstat Information
- DNS Cache Information
- Shares

- Scheduled Tasks
- Web Proxy Information
- Process Listing
- AntiVirus Information
- Firewall Status
- Local Admin Password Solution (LAPS)
- Domain Password Policy
- Domain Admins Group Members
- Domain Controllers
- Checks for Common Security Products
- Egress Filter Check

http://www.blackhillsinfosec.com/?p=5824
HostRecon - Demo

- Import the script
  - PS C:> Import-Module HostRecon.ps1
- Run HostRecon
  - PS C:> Invoke-HostRecon
- To perform an egress filter check on the top 100 ports run the following command:
  - PS C:> Invoke-HostRecon -Portscan -TopPorts 100
Kansa

- A modular incident response framework in Powershell
- Collects volatile information for initial triage and hunting

https://github.com/davehull/Kansa
Invoke-IR / PowerForensics
http://www.invoke-ir.com

- “All inclusive framework for hard drive forensic analysis”
- Supports NTFS and FAT file systems
  - Extended File System and HFS+ support is in progress
- CMDlets
  - Boot Sector
  - NTFS
  - Ext4
  - Windows Artifacts
  - Registry
  - Timeline
  - Disk Imaging

Invoke-IR
Digging in deeper

USEFUL TOOLS
FTK Imager

- Free
- Disk Imaging
- Memory Imaging
- Forensic Image
  - Viewing
  - File Extraction
  - Mounting
Process Hacker

- Free
- Process Listing
- Network connections
- Kill processes
- Load DLLs
- And more!
Volatility Framework

- Free
- Memory Analysis
  - Processes
  - Modules
  - Strings
  - Command line
  - MORE!
It’s all about the logs

DATA-CENTRIC HUNTING
Data Mining

- DNS
- Web proxy
- Network Security Devices
- Intrusion Detection/Prevention System (IDS / IPS)
- Firewall

- Endpoint Data
  - Configuration management
  - AV/HIPS
  - Process tracking
  - Certificates

- Active Directory Logs
Free & Open Source Tools

• Osquery
  – https://github.com/facebook/osquery
• El Jefe
• Google Rapid Response (GRR)
  – https://github.com/google/grr-doc
• FIDO
  – https://github.com/Netflix/Fido
• Mozilla InvestiGator (MIG)
  – http://mig.mozilla.org
• The RITA Framework
• BloodHound
These are not the honeypots you’re looking for.

DECEPTION TECHNOLOGIES
Honeypots: Deception Technology

- Not Your Granny’s Honeypot is the new Buzzword
- Combines Threat Intelligence for better deceptions
- Network- and host-based solutions
Deception Tool Types

- Honeypots
- Honeynets
- Honeytokens
- Honeycreds
- Honeydocs
- Webbugs
Person of Interest

- Fake employees on LinkedIn
  - How can you use lure them in?
    - Marketing, HR
    - folks whose job it is to open email attachments
    - Link them to real employees
- Monitor for emails or attempted logins to those accounts
- Flag them as keywords to find in Help Desk support calls
All UR P@ssw0rds Are Belong To US

• Fake “leaked” credentials
  – Disgruntled employee
  – Data dumps / doxing
• Monitor for attempts to login to the “leaked” accounts
• Injected credentials?!?
Is that all there is?

NEXT STEPS
Next Steps

• Build your own lab
  – VMWare (ESXi), VirtualBox, Hyper-V, AWS, Docker
  – Network equipment (HW or SW)
• Try all the tools, see what works for you
• Team up with Red Teamers
Threat Hunting: Research

- Reading List
- Hunting Platform
- Hunting Procedures
  - By Goal
  - By Data

http://www.threathunting.net
MITRE: ATT&CK

https://attack.mitre.org/wiki/Main_Page

- Adversarial Tactics, Techniques & Common Knowledge
Conclusions

- There is no single “Threat Hunting” tool to save the day and make you the hero...YOU must be the hero.
- Situational awareness requires visibility, humans, tools, and threat intelligence to succeed.
- Free and open source hunting tools exist for organizations to get started with their own hunt team operations.
- Diligence is required to actively learn about new threats and adapt to finding them in your network.
Contact Information

• Contact information:
  John H. Sawyer
  john@sploitlab.com
  @johnhsawyer
  352-389-4704

• Slides - https://www.sploitlab.com