Context Matters

Tailoring Tradecraft to the Operational Environment

$ whoami

- Fletcher Davis (@gymR4T)
- Senior Red Team Consultant at CrowdStrike
- Specializing in Adversary Simulation Operations and Offensive Security Research
- Previously:
    - Red Team Consultant at Mandiant

Maymont in Richmond, VA

The research expressed here is mine alone and not necessarily representative of views of my employers

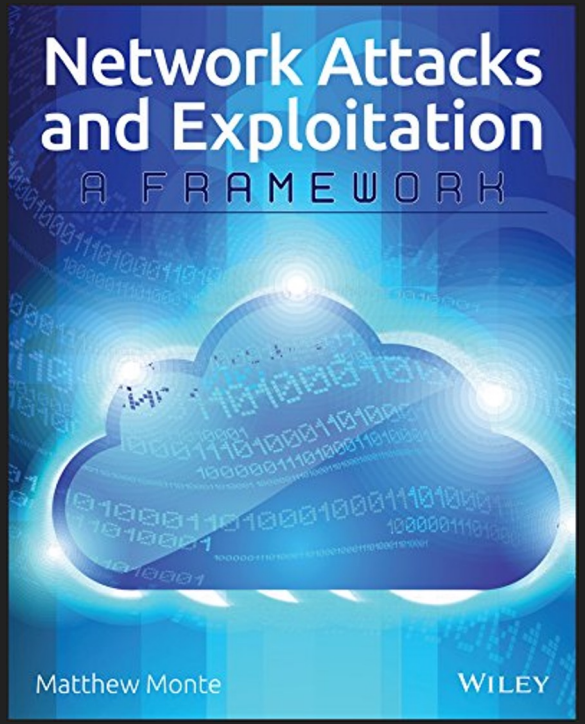
What is this talk about?

- Defining foundational principles for offensive cyber operations
- Redefining how Red Team operators prepare and conduct offensive cyber operations
- Defining a framework for understanding normality
- Discussing operational techniques within target environment

Foundation

Core Principles

- Written by Matthew Monte
- Defines a framework for reasoning about the strategies, technologies, and methods for executing and defending against computer operations
- We must move beyond typical analysis of an event to understand the foundations of computer operations



Foundational Principles

- Humanity
- Access
- Economy
- Knowledge
- Awareness
- Innovation
- Precaution
- Operational Security
- Program Security

Humanity

- Computer operations are grounded in human nature
- Target networks are designed, built, used, and monitored by humans
  - Constrained by human flaws
- Attackers that understand the foundation of humanity in technology will begin to think like its creators
  - Begin understanding and abusing their assumptions

Access

- There is someone with legitimate access and a means to use it
- This extends to data as well
  - Data is generated and stored for the purpose of being accessed later by someone or something with legitimate access
- An adversary's goal is to "assume" the legitimate identity or software agent with access
  - Can be difficult, but not impossible

Economy

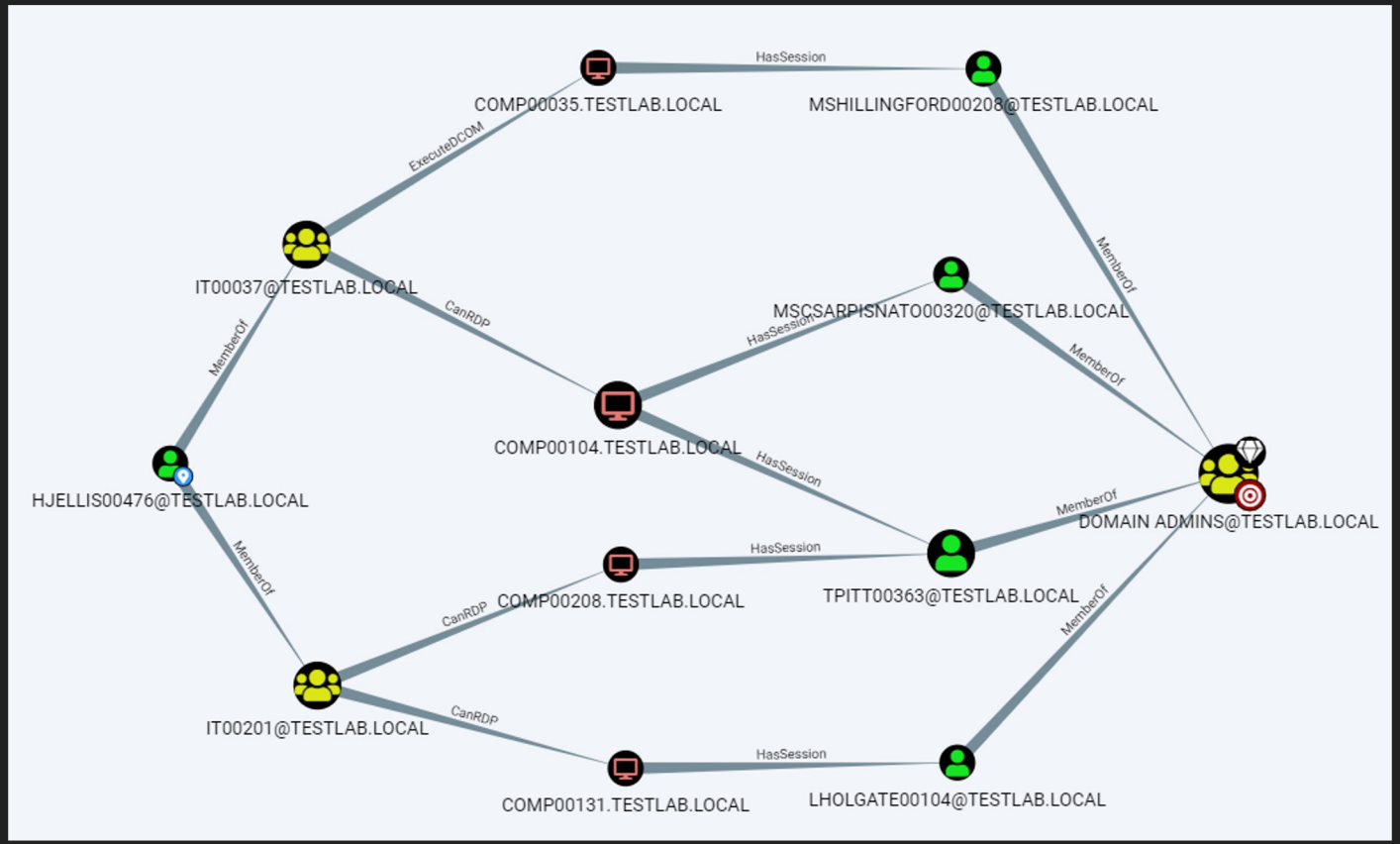
- “Ambitions always exceed available resources”
- There is a priority, cost, and benefit to every operational action and its associated outcome
- Understanding these constraints is important for succeeding during an operation
- Resource constraints depend on the operation:
  - Time
  - Operational Capabilities
  - Expertise

Knowledge

- Broad and deep understanding of technology, such as computers and computer networks, as well the behavioral and psychological characteristics of people and organizations
- Knowledge reduces operational friction
- Knowledge has its limitations
  - Generally incomplete and frequently inaccurate
- The best decisions are made by those that have a balance of knowledge of the technical, psychological, and social aspects of operations

Awareness

- Mapping the operational domain and monitoring relevant events in real-time
- Unlike knowledge, awareness is target specific and obtained from the target environment
- Seeks to shift Defender’s advantage of domain control and knowledge
- Helps operators orient themselves within the environment and provides direction towards objective
- An operational example of this is using a tool like BloodHound to map an organization’s Active Directory

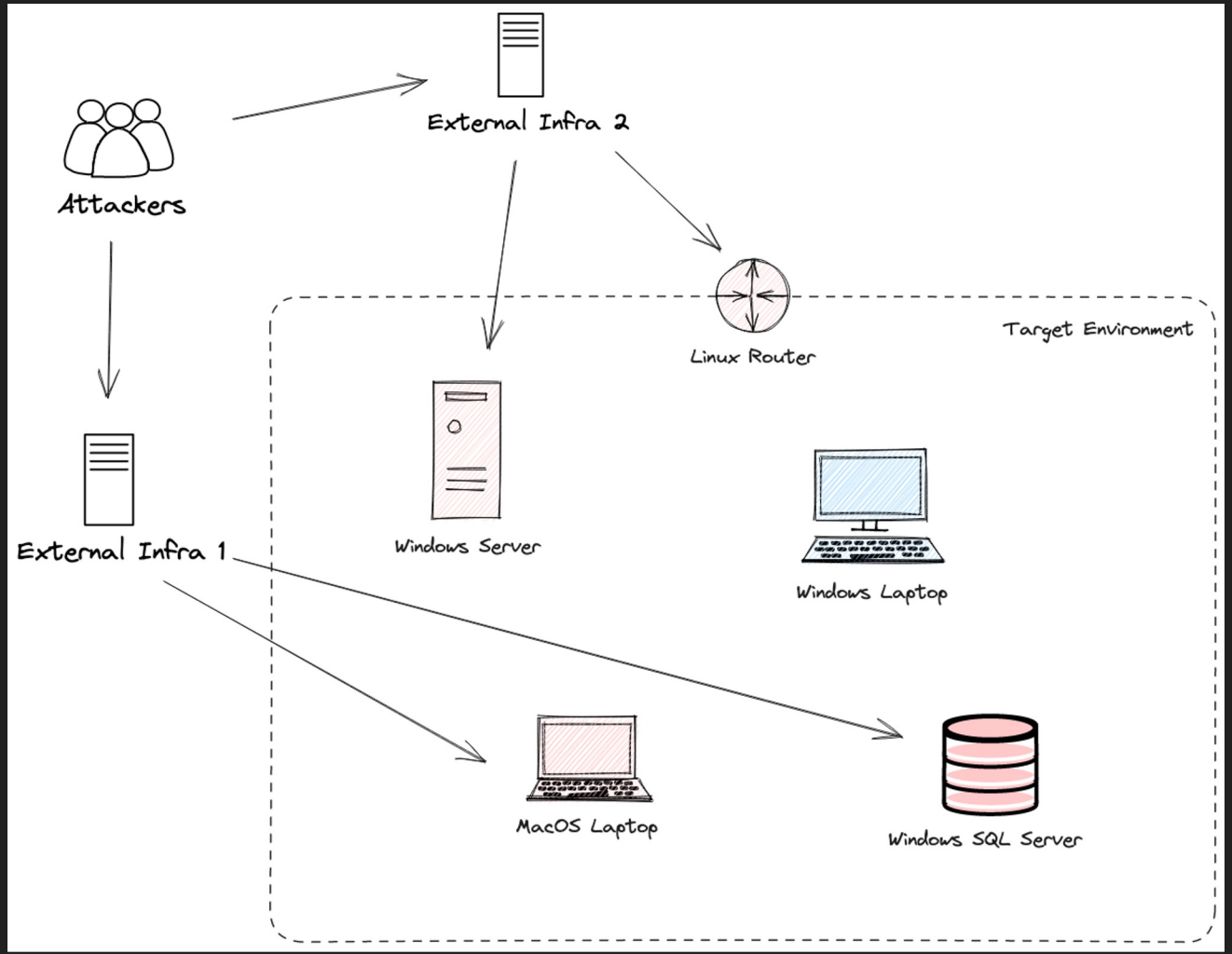

COMP00035.TESTLAB.LOCAL
HasSession
MSHILLINGFORD00208@TESTLAB.LOCAL
ExecuteDCOM
IT00037@TESTLAB.LOCAL
CanRDP
MemberOf
MSCSARPISNATO00320@TESTLAB.LOCAL
HasSession
MemberOf
COMP00104.TESTLAB.LOCAL
HJELLIS00476@TESTLAB.LOCAL
HasSession
MemberOf
DOMAIN ADMINS@TESTLAB.LOCAL
HasSession
COMP00208.TESTLAB.LOCAL
TPITT00363@TESTLAB.LOCAL
CanRDP
MemberOf
IT00201@TESTLAB.LOCAL
CanRDP
HasSession
COMP00131.TESTLAB.LOCAL
LHOLGATE00104@TESTLAB.LOCAL

Innovation

- The ability to create new technology, leverage existing technologies, or develop and adapt operational methods to new circumstances
- Rooted in creativity
- Innovation becomes most effective when combined with awareness and knowledge of humanity within a target organization
- Innovation provides operators with better capabilities

Precaution

- The minimization of the impact of unwitting actions on an operation
- Natural operations within an environment can impact an operator’s activities
  - Employee working late notices system slowdown
  - System updates
  - Power outages
- Precaution mitigates accidental disruptions through two forms:
  - Redundancy
    - Establishing fail-safes, backups, contingency plans, etc.
  - Diversity
    - Leveraging wide range of tools, techniques, and infrastructure
- Sustain access through multiple redundant points of access


External Infra 2
Attackers
Linux Router
Target Environment
External Infra 1
Windows Server
Windows Laptop
MacOS Laptop
Windows SQL Server

Operational Security

- The minimization of defender exposure, recognition, and reaction to the existence of an operation
- One can visualize a target environment as a hostile environment, entirely controlled by the “enemy”
- Relative superiority is gained upon access to the network without the Defender being aware of the presence
- Relative superiority is lost upon discovery by Defenders
  - Defenders sweep networks and quarantine systems
- Operational Security is ultimately all actions done before and during an operation to prevent loss of relative superiority

Program Security

- The containment of damage caused by the compromise of an operation
- Operators do not want one operation to impact another
- “Remaining undetected forever is chasing an impossible reality”
- With the prevalence of managed security providers and threat hunting services, correlation of behaviors and tooling across multiple organizations is becoming easier

Thanks for the Principles, Now What?

Operational Planning

Goals

- Reduce operational uncertainty
- Define most effective route to an objective
- Develop and tailor technical capabilities
- Design redundancy plans
- Develop strong awareness about a target

Objective Abstraction

- Abstraction is a concept by which implementation details are hidden from a user
- Objectives are merely an abstraction of their underlying technical components
- Removing the abstraction layers and understanding the underlying components that make up an objective allows us to make more informed decisions when targeting them

Modeling the Target Objective

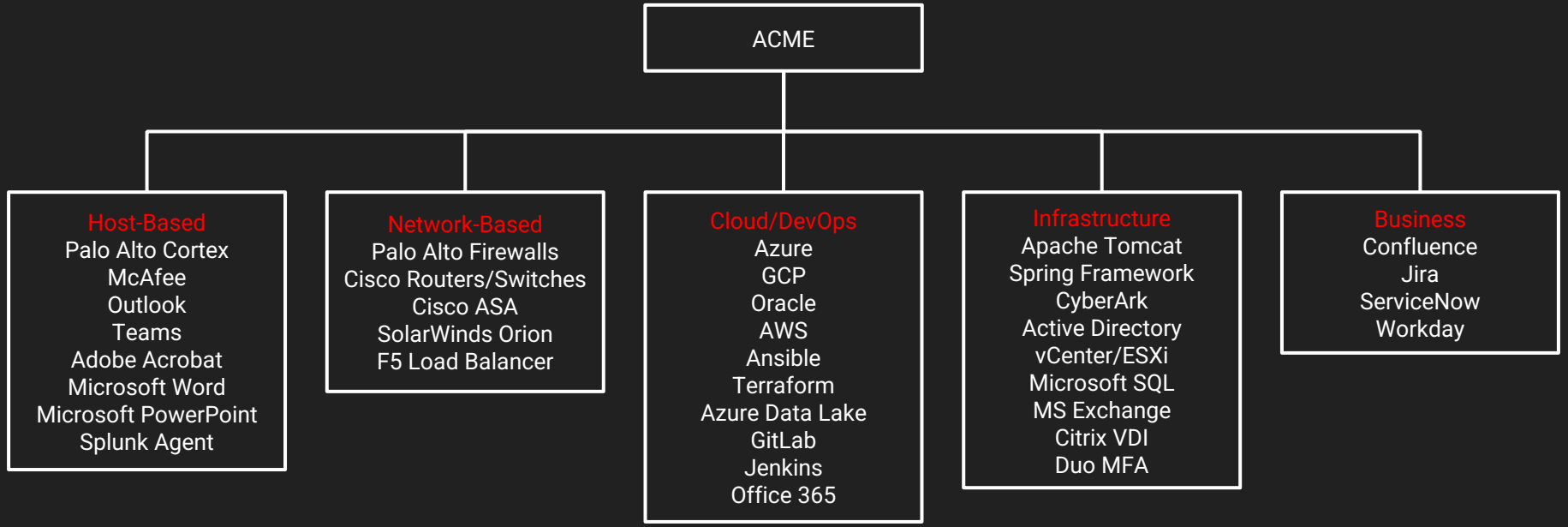
- Target systems rarely exist in isolation
- Usually a component of a complex system
  - Containing a variety of privileged and unprivileged systems, users, and networks
- Sometimes the complex system itself
- Modeling allows us to visualize user interactions, analyze trust between systems, understand data flows, and how data is stored and used
- Modeling target objectives allows us to identify weaknesses and gaps in defender/developer assumptions

How to Model an Objective

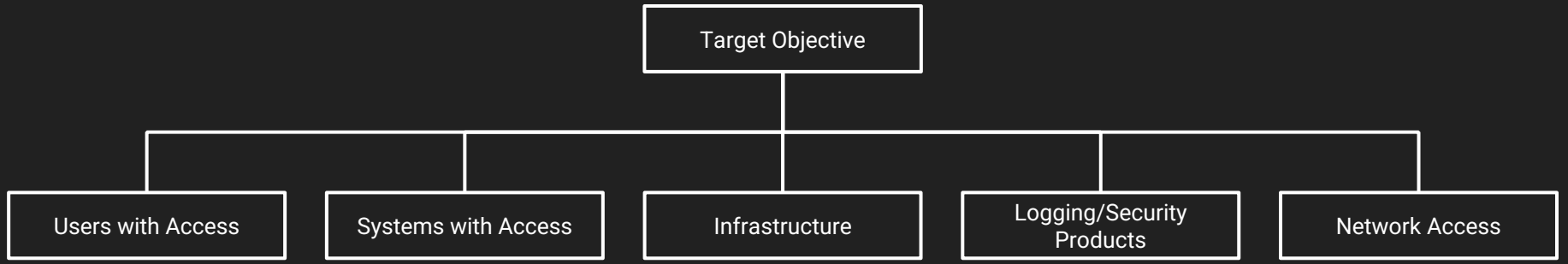
1. Scope: Define objective
2. Gather: Perform reconnaissance against target
3. Process: Analyze obtained information
4. Map: Identify technical and psychological components that comprise objective
5. Visualize: Generate architecture model

Target Package

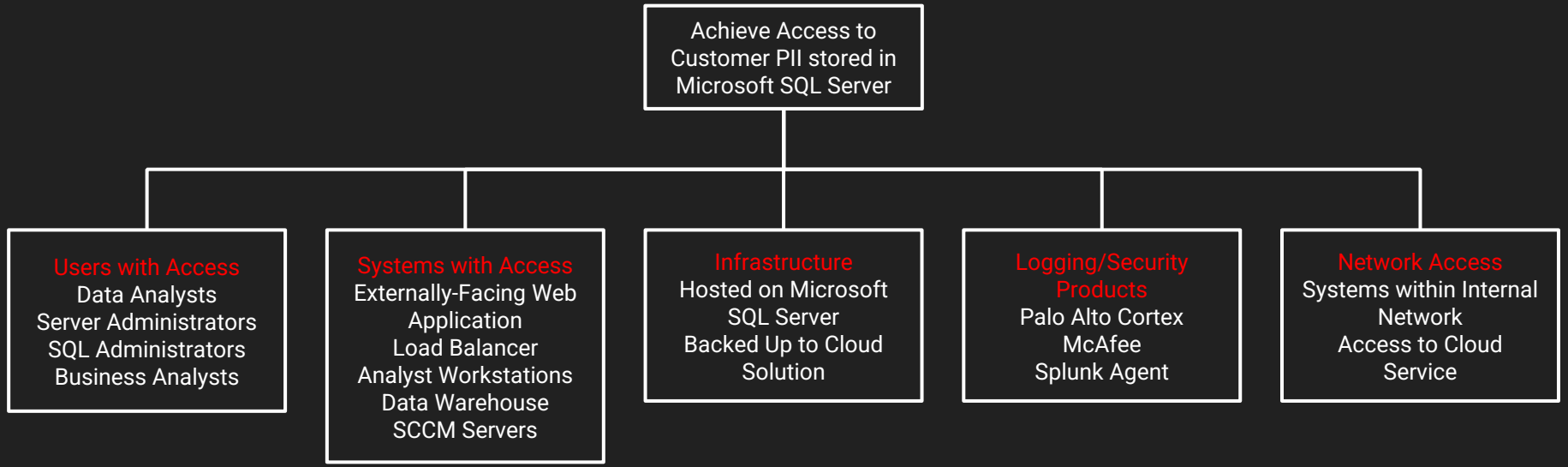
Target Package

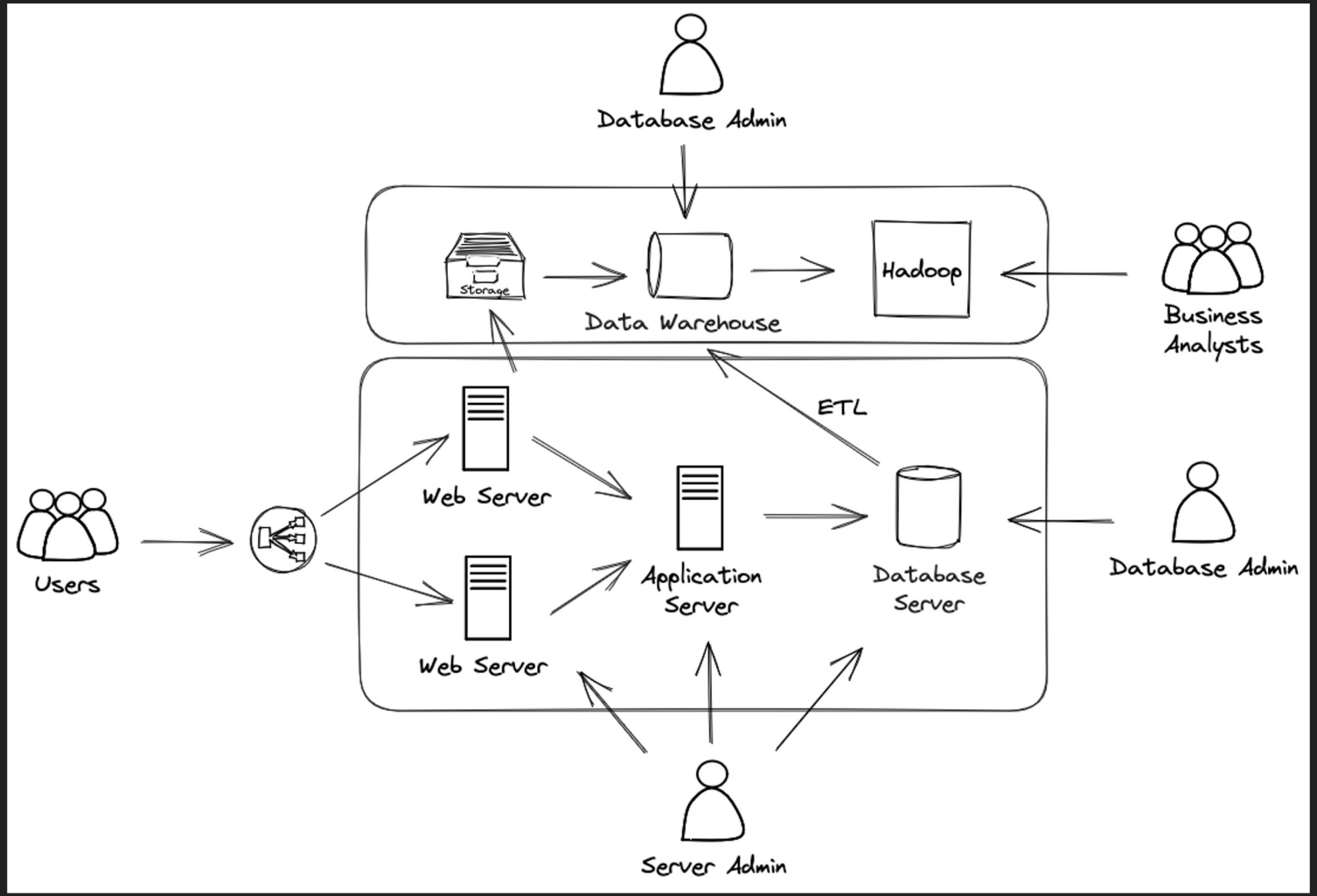


Modeling a Target Objective



Modeling a Target Objective




Database Admin
Storage
Data Warehouse
Hadoop
Business Analysts
ETL
Web Server
Web Server
Application Server
Database Server
Database Admin
Users
Server Admin

Limitations to Modeling Objectives

- Cognitive Biases
  - “Mindsets tend to be quick to form but resistant to change”
- Selective Perception
  - We tend to see what we want to see
- Uncertainty means dealing with incomplete knowledge
- Humans are bad at handling complexity
  - Naturally develop shortcuts to navigate complexity
  - Humans take the path of least resistance

Framework for Understanding Normality

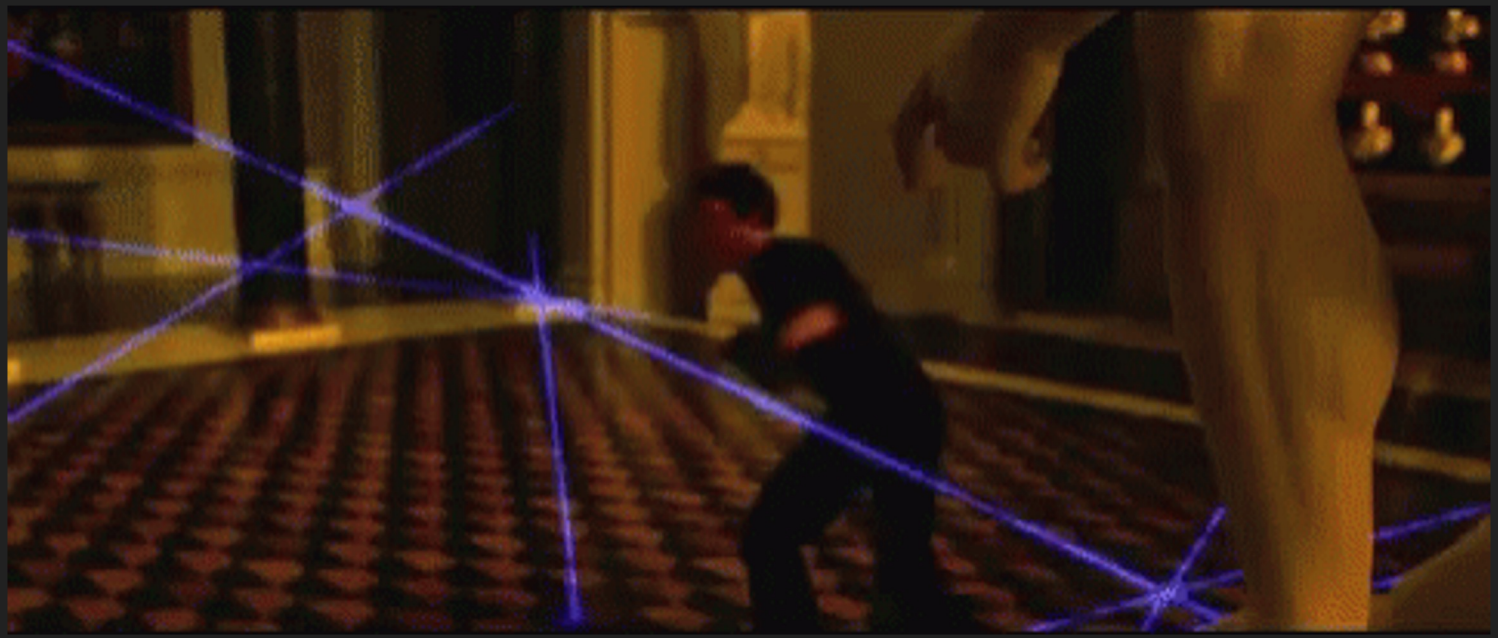
Detection Philosophy

- Detection is difficult
- Analysts must process large amounts of information involving uncertainty
- Analysts leverage indicators to identify adversary activity:
  - Atomic Indicators
    - Known malicious artifacts (hashes, filenames, strings, IPs, etc.)
  - Behavioral Indicators
    - Patterns of known-malicious techniques (remote service creation and execution, etc.)
    - Requires strong contextual data points
  - Anomaly Indicators
    - Anomalous activities outside the presumed baseline
    - Previously unknown within organization’s intelligence corpus

Offensive Perspective to Detections

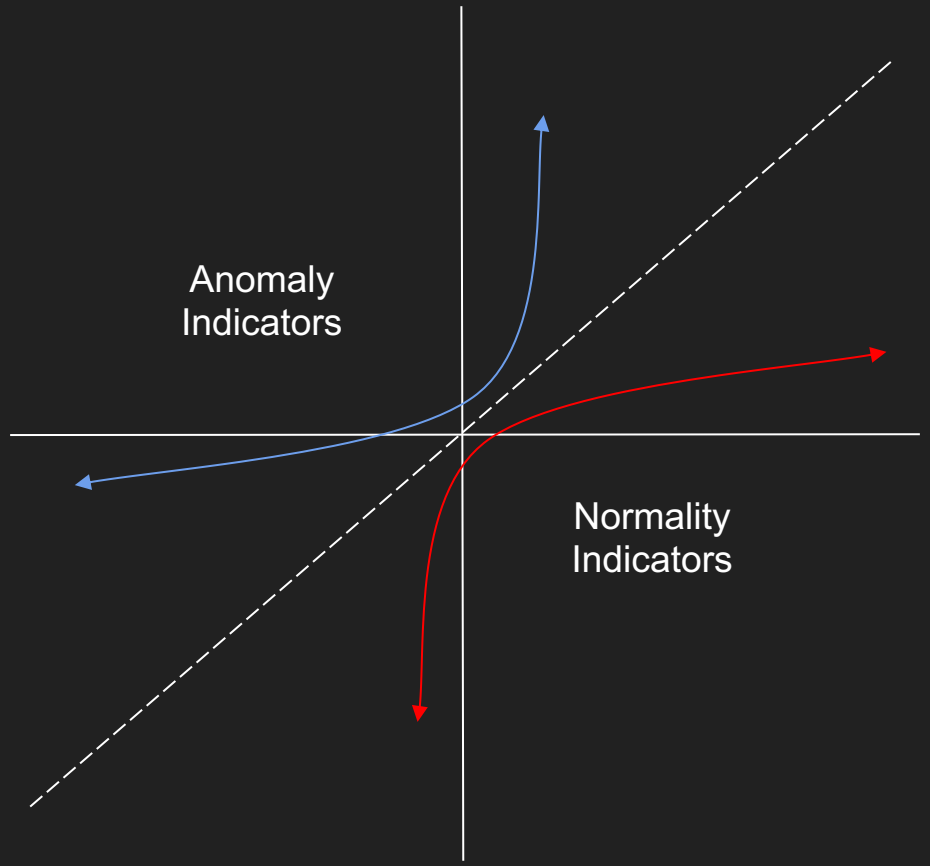
- The Information Security industry is infatuated with “bypassing EDRs”
- There is no such thing as true evasion. Operators need to shift the focus from “bypasses” to tailoring tradecraft to each operational environment
- “Every contact leaves a trace” - Locard’s Exchange Principle
- The absence of telemetry is equally as much of an indicator of malicious activity

What Operators Want to Do



What Operators Should Do

Inverting the Detection Philosophy

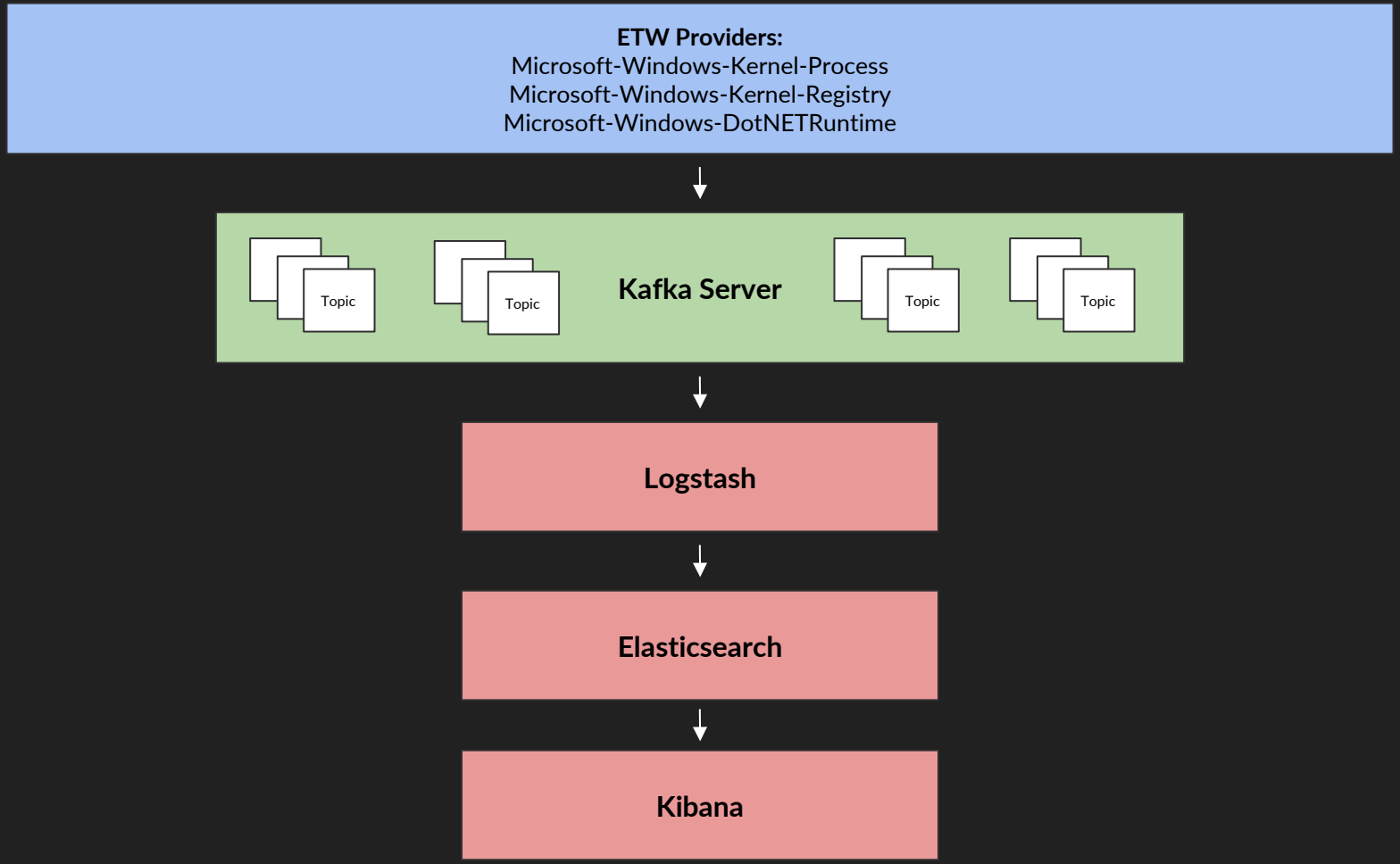


Understanding Normality

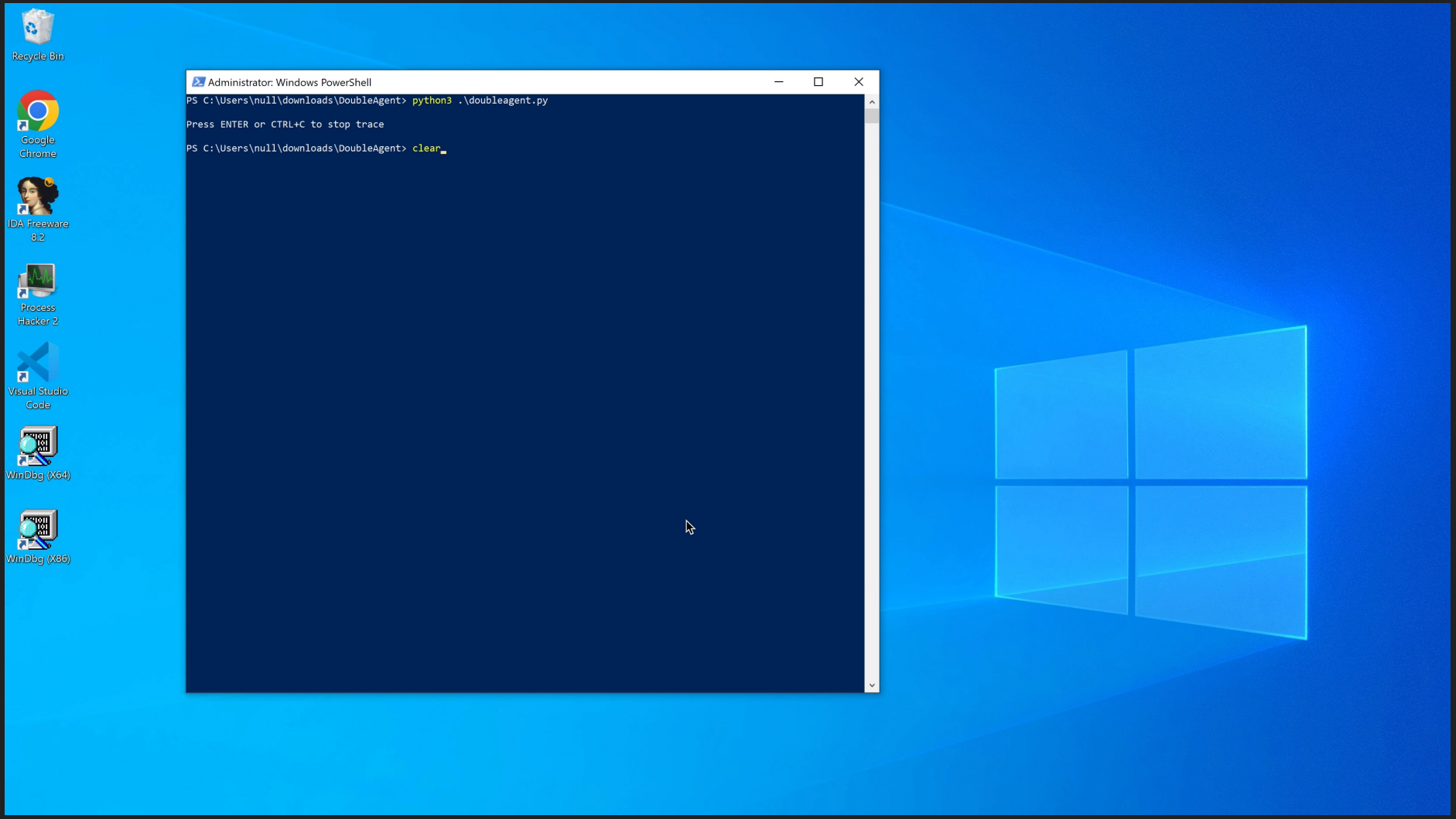
- Operators can leverage Windows telemetry to identify benign contexts for otherwise malicious post-exploitation behaviors
- Understanding the behavior allows operators to make more nuanced tradecraft decisions to better blend-in to the operational environment
- Requires operators to analyze and understand events generated by “benign” applications
    - Ex. Identify applications that normally make outbound network connections to Azure CDN

Examples to Monitor

- Identify processes that create Application Domains and load assemblies into them
  - Understand normal assembly names
- Identify processes that make LDAP requests
- Identify network behavior from a particular process
- Identify module load events from a particular process


ETW Providers:
Microsoft-Windows-Kernel-Process
Microsoft-Windows-Kernel-Registry
Microsoft-Windows-DotNETRuntime
Topic
Topic
Kafka Server
Topic
Topic
Logstash
Elasticsearch
Kibana

Demo


Recycle Bin
Google Chrome
IDA Freeware 8.2
Process Hacker 2
Visual Studio Code
WinDbg (X64)
WinDbg (X86)
Administrator: Windows PowerShell
PS C:\Users\null\downloads\DoubleAgent> python3 .\doubleagent.py
Press ENTER or CTRL+C to stop trace
PS C:\Users\null\downloads\DoubleAgent> clear

On-Network Operations

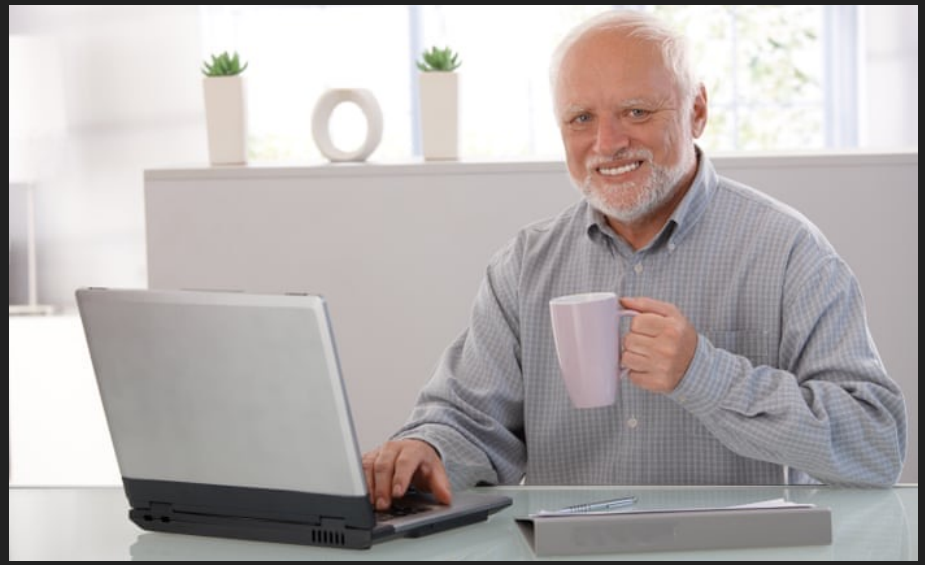
Typical Red Team On-Network Activity

Operate like a Newly Onboarded Employee

- The goal of an operation is to ultimately assume an identity
  - Ex. Business Analysts have access to data in X system
- Attempt to answer questions:
  - Where is onboarding/process information stored?
  - How would a user find that system?
  - Is access federated through some sort of IdP / Azure AD / ADFS?

Host-Based Recon

- DNS Cache
- Browser Data
  - Bookmarks
  - History
- Messaging Clients
- Installed Applications
- File System Enumeration
  - API Tokens
  - Credentials
  - Documentation
- Network Drives



Network-Based Recon

- Internal SharePoint/Confluence/Wiki
- Office 365
- DevOps Environment
  - SCM (GitHub, GitLab, Bitbucket)
  - Automation Servers (Jenkins)
  - Artifact Repository (Artifactory)
- Other Environment-Dependent SaaS/Web Applications

Actions on Objectives

- Be mindful of lateral movement
  - Only do it if you need to
- You do not need to get Domain Admin to achieve your objective
  - Assuming an identity does not require Domain Administrative privileges
  - Principle of Least Privilege -> Principle of Least Access
- Application Layer vs Host
- Objectives are/are a component of complex systems

Takeaways

Offensive Takeaway

- Understand your target more holistically
  - You’re targeting a complex system built for humans, by humans
- The more you prepare externally, the less you need to do internally
  - Less artifacts you leave / the more tailored your operation is
- Offense and Defense are two sides of the same coin
- Don’t be an anomaly, be the baseline

Defensive Takeaway

- Your opposition is also human
  - Constrained by the same cognitive and behavioral limitations
- When identifying malicious behavior, ask WHY an adversary might have made a particular decision?
- Extend beyond your tooling
  - Understand your environment more holistically, instead of technically
- Challenge your own assumptions
- Innovate or be out innovated

References

- Network Attacks and Exploitation: A Framework by Matthew Monte
- Psychology of Intelligence Analysis by Richard J. Heuer, Jr.
- https://jackson_t.gitlab.io/it-depends.html
- https://jackson_t.gitlab.io/edr-reversing-evading-01.html
- https://sansorg.egnyte.com/dl/e9FeMxp8G3
- https://en.wikipedia.org/wiki/Locard%27s_exchange_principle
- https://www.trustedsec.com/blog/walking-the-tightrope-maximizing-information-gathering-while-avoiding-detection-for-red-teams/

Thank You For Listening!

Website: https://www.barbellsandrootshells.com

Twitter: https://twitter.com/gymR4T

GitHub: https://github.com/gymR4T