Skill Sharpening @ the Cyber Range: Developing the next generation Blue Team

Don Murdoch, GSE #99, MSISE, MBA
(and quite a bit more alphabet soup)
Asst. Director, Regent Cyber Range Virginia Beach, VA
Jan 9, 2019 Virginia Beach ISC2 Chapter Meeting
There are three types of people on the Internet:

- Sheep
- Wolves
- **Shepherds**

**Shepherd**

- 27+ years in IT, 17 InfoSec (gosh I feel old…)
- Boat loads of alphabet soup, including EMT/A
- Author BTHb Series
- Scenario Designer and Instructor at Regent U. Cyber Range
  - Come flex your muscles!
Regent Range - In a Nutshell
Blue Team Focused Adversary Emulation

• Four class groups in 2x3 arrangement
  • Five students
  • One trainer station
  • Each class is isolated from each other
  • Live, re-runnable scenarios

• Instrumentation
  • SIEM’s, Firewall’s, Sec Onion, email, DNS, ICS hardware, 15 segments, 40+ OS’s….  
  • Rinse, Wash, Repeat (4 min) as needed

• Students go through
  • Tools Orientation
  • SIEM Instrumentation
  • Intrusion analysis and IR

• Practice Incident Response
  • Working as a team of two
  • Investigate and Document
  • Reconstruct investigative attack timeline
  • Strive for an exec summary

• After action
  • Share tools, techniques, write ups
  • Formal Certification req’s a Don-Cu-Ment grade write up

• Students can actually change the environment and achieve different outcomes, which we encourage
Blue Team Ed. Must Answer Critical Questions for Success

- Why do you need to test internal staff?
- Why is AdSim going to improve internal security over establishing and maturing the “next best thing”?
  - Mature the threat hunting program.
  - Reduce overall elevated account exposure.
- How will internal staff respond to being tested?
  - Hawthorne Effect
  - What will this do to their morale?
  - AdSim generally depends on “assumed compromise”.
  - What are your breach vectors so that AdSim works properly in your environment?
Even more questions

• How are info systems actually instrumented?
  • Avoid building scenario dev with a capability you don’t actually use!

• How do we prioritize?
  • This answer must be BUSINESS RELAVENT and tied to the Value Chain.

• How do we safely build scenarios?
  • What happens if some nastiness “escapes”?
  • Ans: MITRE ATT&CK & Adversary TTP, MISP

• Can we use production? (that might be a RGM…)

REGENT UNIVERSITY
Hawthorne Effect
(because everyone needs some industrial psychology...)

- Research has found that the novelty of being research subjects and the increased attention from such leads to "temporary" increases in workers' productivity; result in short term gain; improvements are not sustainable from direct observation and measurement. For the observer, too....

- BT Application:
  - Personal Observation found that trainees follow the "outline" more when facilitator routinely checks in on them, certain people have more attention applied to them, and professed skill affects the amount of coaching given.
  - Compensator: Develop *and use* timing, process, and output analysis objective criteria

- Originated at Hawthorne Works in Cicero, Illinois, in 1958 by Henry A. Landsberger
BT Training Needs a Plan!

• A training outline has a purpose: it’s about a learning outcome (KSA’s)
  • Title, Learning Objectives, outline, and written learning outcomes
  • OBJECTIVE Scoring vehicle
  • Completion Tool Activity list (did you do X, Y, and Z?)
  • NICE / NICCS INRE and CDA are usable starting points
• A training program needs to include:
  • Initial KSAl assessment, entry points, and progression model
  • Time commitments outlined with a tie in to the organization IDP
  • Charge code::
  • Professional educational development with a scenario costs between 23 to 143 hours per hour of delivery time, based on complexity and delivery method (Assoc for Talent Dev2018 study)
  • Reusable resources (more on that later....)
• Ref: https://www.td.org/insights/how-long-does-it-take-to-develop-one-hour-of-training-updated-for-2017
BT Range Requirements

• Platform management
  • Virtualization is a must – Local VMware, AWS, Azure, ...
  • Cloud = set your VPC to allow to/from your own network to prevent spillage

• Scenarios
  • Static, Dynamic, multiple levels, different duration, ...
  • Training scenario generation and execution for repeatability through scripted ed.

• Modeled Networks
  • Server, Client, ICS, DMZ, Internet, Partner, VPN, ...

• Hosts – after all, you need something to attack and defend!
• After action analysis and reporting process and measurement
Cyber Range Scenario Information Flow

Range info flow impacts attendee progress!

• Setup, initiate session using a reusable/repeatable attack generation

• Observation/recording of the trainee
  • Merely observing staff will change their behavior

• Record keeping for meeting objective(s)
  • Did the trainee use the desired technique? Was an alternate suitable?

• Defense tools observe, trainee react and engage, INVESTIGATE

• Confirm the trainee “Solves the case”
  • Implement a change to contain the breach/attack (Remediate)
  • Perform root cause analysis

• Write up at the level required by the organization, using org specific tools
Range Network Layout and Components
How do you select tools?

• What do you own?
  • Is there a “lab” model
    • For example, Palo Alto has a PA-220 Lab Skew w/ a < $1k price point

• Or better yet – do you actually need “tools”?

• Requirements?

• Will FOSS get you there?
  • Remember – many AdSim tools assume the attacker gains at least end user access, and takes it form there. Several FOSS packages support this.
What FOSS tools are out there?

• APT Simulator (batch)***
• Atomic Red Team ***
• AutoTTP
• Blue Team Training Toolkit (BT3) ***
• Caldera
• dumpsterfire
• Infection Monkey
• Invoke-adversary
• Kali – build purpose drive scripts with MetaSploit – Tons of Packt type books!
• Metta
• NSA unfetter
• Endgame’s Red Team Automation
• Unicorn for Pshell Encoding

• Other Blue Tools
  • SiLK
  • BHIS RITA – but Zeek needs TSV
  • QRader @ 50 EPS or less
  • Relkci – whitenoiselist
  • Windows Forensic Toolchest
  • Log MD – Free or Pro ***

• Platforms
  • OpenSOC.io
  • Security Onion ***
Artificial Domain Build Tools

- AutoLab
- AutomatedLab
- Boxstarter
  - Targets Hyper V
- DetectionLab ***
  - Targets VirtualBox, somewhat finicky, but when it works!
- LAN/WAN Specific emulation tools
  - GNS3
  - Cisco VIRL

- DetectionLab
  - Multistage extendable build process
  - Downloads Win2016, Win10, Linux
    - Uses native MSFT build tools
  - Windows AD, DNS Server
    - Strong Windows audit posture
  - Windows Event Forwarding Server
    - Collector & Subscriptions
  - Windows 10 Workstation
    - Highly instrumented sysmon and WEF
  - Logger
    - Splunk, OSQuery, and MITRE Caldera
apt simulator

• Start here
  • Snapshot the VM….
• Solid “stand alone” batch tool
  • Triggers AV, NIDS, HIDS, …
• Cases – highlights
  • Local file collation
  • C2 connection w/WMI
  • Malware RAT, Mimikatz
  • Guest Admin
  • NBTscan, other local Recon
  • Persistence – AT, Run, Sch Tasks
• https://github.com/NextronSystems/APTSimulator
Integrate an Open Source / Inexpensive Option – BT3

BT3 – Encryptio.IO

Several N/C modules in each category
BT3 - https://www.bt3.no/

- Easy implementation
  - Get Kali, install BT3, register for an API key
  - Leverages Maligno – client/server, simulates C2, 4 examples free, others
  - Includes pcapteller for packet capture replay
  - Has files that pass md5sum analysis for malware samples (hash collisions)
  - Download agents, pcaps
- Very low risk – White team is in control of the VMs and script code
  - Can install script code, drop off, we know where the bits go
- Inexpensive content update subscription available

- URL: https://www.encripto.no/forskning/whitepapers/BT3_User_Guide.pdf
BT3

- Server side setup – set LHOST, sample profile, and gen the py client code

```
BT3 ~ maligno > show profiles disk

<table>
<thead>
<tr>
<th>File</th>
<th>Size (MB)</th>
<th>Location</th>
<th>Date</th>
<th>Price</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cryptowall_v3.py</td>
<td>0.003</td>
<td>Disk</td>
<td>2015-02-13</td>
<td></td>
<td>Cryptowall v3 ransomware profile.</td>
</tr>
<tr>
<td>etumbot.py</td>
<td>0.003</td>
<td>Disk</td>
<td>2014-07-01</td>
<td></td>
<td>Etumbot APT backdoor profile.</td>
</tr>
<tr>
<td>havex.py</td>
<td>0.004</td>
<td>Disk</td>
<td>2014-03-14</td>
<td></td>
<td>Havex trojan profile.</td>
</tr>
<tr>
<td>standard.py</td>
<td>0.003</td>
<td>Disk</td>
<td>2016-06-26</td>
<td></td>
<td>Default profile with static elements.</td>
</tr>
</tbody>
</table>

[*] Available profiles: 4

BT3 ~ maligno > set profile havex.py

[+] profile => havex.py

BT3 ~ maligno > genclient

[*] Generating Maligno client...
[+] Maligno client successfully generated! Check the "clients" folder.

BT3 ~ maligno > run
```
BT3 Client Side

- Client needs the “maligno_client_havex.py” file onboard – just run it!
- python maligno_client_havex.py  # options abound here....
Snort Picks up the Trojan Behavior
Havex is an espionage focused tool
If you let it run for a day ...
Atomic Red Team

- Simple Atomic Tests
- Mapped To MITRE ATT&CK
- Easy To Use
  - Execute in either PowerShell or Python
- Demystify The Attacks
- Open Source
- Test Multiple Products
---

attack_technique: T1117

display_name: Regsvr32

atomic_tests:
- name: Regsvr32 local COM scriptlet execution
  
  description: |
  Regsvr32.exe is a command-line program used to register and unregister OLE controls

  supported_platforms:
  - windows

  input_arguments:
  - filename:
      
      description: Name of the local file, include path.
      type: Path
      default: Regsvr32.sct

  executor:
  - name: command_prompt
    
    command: |
    regsvr32.exe /s /u /i:{filename} scrojb.dll
Commercial BAS Products

(Breach and Attack Simulation)

- BAS tools
  - AttackIQ
  - Safe Breach
  - Immunity Adversary Simulation
  - Cymulate
  - Immunity Adversary Simulation
  - Office 365 - Attack Simulator
  - Spectre Ops
  - On the horizon
    - randori.com

- Tools that can be leveraged
  - SCYTHE (by Grimm) ***
  - Cobalt Strike
  - BreakingPoint by IXIA
    - > 500 malicious traffic patterns
    - >2300 (?) application traffic patterns
  - And others…
BAS: What Benefits should you hope to find?

• How well do your security focused tools “Work”?  
  • Inform, Prevent, Alarm  
  • Do they really perform deep packet inspection?  
    • Can you validate your $spend?  

• How well have you instrumented your tools?  
  • Do you perform protocol enforcement?  
  • Just how many systems and users can ignore the proxy?  
  • When you *know* what happened, can you find multiple supporting artifacts and traces?

• How porous is your perimeter?  
  • What about that internal segmentation project?  
  • How easy is it for you to data exfiltrate a 1 GB payload with SSNs?
Commercial Product Approaches

• Operate in Isolation
  • Virtualized Company Work A Like Platform using VMware / AWS

• Artificial agent deployment
  • Similar to what a network trojan would do, but under InfoSec control
  • Scan for local vulnerabilities & stays “local”
  • Maps out pathways

• Malicious Network Traffic Generation
  • Virtualized systems, net to net traffic, needs to pass in front of a sensor

• Black Box Multi Vector
  • Agent to cloud service – intends to function as close to a real trojan or persistence tool as possible
Beware: Range-Isms Abound!

• Artificial constructs are not attackers.
  • They do not pivot
  • They do not adjust
  • They go after one thing – Domain Admin
  • They don’t read your email … because they got your C Ring account creds

• Network activity without a “On System Trace” is only half the puzzle.

• Tools that depend on an “agent” aren’t all that “real”
  • Attackers establish persistence that should be removed
  • Agents that need to run and can’t be removed b/c that breaks other things

• Artificially high or low auditing
  • Do not train in a way where you cannot fight
$o how will you measure your training program $u$cce$$?

“What cannot be measured, cannot be managed.”
- W. Edwards Deming.

“Not everything that counts can be counted, and not everything that can be counted counts.”
- William Bruce Cameron

• Resources
  • Don Murdoch, “Blue Team Handbook: SOC, SIEM, and Threat Hunting”
  • Carson Zimmermans “Measure Yo Bad Self” @ SANS SOC Summit 2018
  • Pragmatic Security Metrics, W. Krag Brotby and Gary Hinson
BTHb:SOCTH’s Metrics

- Time to sweep the enterprise (Test Net)
- MTT Close an alarm by Close Category
- MTT Forward an alarm up Tier
- MTT Open a formal Incident
- MTT Implement a use case
- # of Events Received / Analyzed in scope for a given exercise
- # of Alarms by Severity in scope for the given exercise
- ATT&CK Coverage by Exercise

- Impact and Cost per incident – trainees can be asked to assess the impact
- MTT to Detect a Security Incident
- MTT for Detect to Contain
- MTT to expel an intruder
- Incidents opened and closed
- Avoidability of an Incident
- Thoroughness of eradication practices
- MTT Notify Principle, System Owner, or Custodian
Focus in on Timeline Reconstruction

- Mean Time To Decision (MTTD)
  - Is the observable event True or False? (hint – range alarms are usually True!)

- Mean Time to Compromise (MTTC):
  - This starts counting from the minute that the Red Team initiated the attack to the moment that they were able to successfully compromise the target

- Mean Time to Privilege Escalation (MTTP):
  - This starts at the same point as the previous metric, but goes all the way to full compromise, which is the moment that the Red Team has administrative privilege on the target
Log MD – Need this in the toolbox
MalwareArchaeology.com

• Audit Policy compliance, Windows IR, Malware Discovery, Forensics
• Check Windows Advanced Audit Policies against Logging Cheat Sheet
• Harvest both Event Logs and non-log events
  • AutoRuns including all WMI namespaces
  • Large Registry keys (hidden payloads and scripts)
  • Full filesystem hash compare against known good image of hashes
  • List of Locked Files malware often uses to prevent cleanup
  • Full registry compare against known good registry snapshot
  • WhoIs lookups of single IP or a list of IPs
• Feed LOG-MD reports (CSVs) to your Log Management/SIEM if available
Reports

• Focus on what happened

• Empty report?
  • Got Nutthin!

• CSV reports enable downstream processing with a variety of tools

• Create a “baseline”, and then run the scenario, students should be able to compare/contrast
Upgrade to the Pro Version

• Parent / Child Process Tree

• MS Word calling CMD.EXE is not generally a good thing …

<table>
<thead>
<tr>
<th>Parent_PID</th>
<th>Parent_Path</th>
<th>Child1</th>
<th>Child2</th>
<th>Child3</th>
</tr>
</thead>
<tbody>
<tr>
<td>2140</td>
<td>C:\Windows\explorer.exe</td>
<td>C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5140</td>
<td></td>
<td></td>
<td>C:\Windows\SysWOW64\cmd.exe</td>
<td></td>
</tr>
<tr>
<td>7784</td>
<td></td>
<td></td>
<td></td>
<td>C:\Windows\System32\conhost.exe</td>
</tr>
<tr>
<td>7784</td>
<td></td>
<td></td>
<td></td>
<td>C:\Windows\SysWOW64\cmd.exe</td>
</tr>
</tbody>
</table>

• Especially if there is a PowerShell call later on in the process tree
After Action Reporting and Analysis

- Each “team” discusses their findings and how they got there
- Have an objective grading criteria
  - Write your own discovery timeline
- Request each participant or team list observation in writing
  - Put each person’s observations up on the screen
  - Open discussion promotes “What they said” responses
- IR can look like a tree
  - Many branches – encourage different approaches
- IR skills will develop over time
Incident Response Report

• Incident Response is a *team sport*
  • *Document* as you go
  • *Screen shots* really help
  • *IR Template* is a professional learning experience – you will use each template throughout the week
    • *PICERL format and an Executive Summary/Timeline format*
    • *Write Ups and the Template are yours to keep*

• During After Action Review
  • Go over each team’s IR document and executive summary
  • Everybody is asked to contribute, talk through and take notes
  • Emphasis on Timeline Reconstruction – this is one of the *hardest skills to master* when it comes to Incident Response
Thank you!

Questions and Possible Answers for the balance of our time.
Other Slides that may be used
Level Set on the AdSim Lingo

• Gartner’s BAS term – next slide!
• Red Team
  • Generally: externally hired to test physical, psychological, and technical defenses while they avoid detection and “find the crown jewels”
  • Should make every effort to use APT type attack patterns (A’la MISP)
• Blue Team (DART) – This is our focus area
  • Quite simply, YOU, the internal defender – the maintainer of the security posture
  • Detect, analyze, respond, weaken, and thwart the Red team
  • Focus on log analysis, network pattern analysis, and persistence detection and response
• Purple, White, Green
  • Conceptual, Transient – oversee and optimize RvB exercise, staffed with senior staff
Breach and Attack Simulation and its position on the Gartner Hype Cycle
Leveraging the Gartner Model
Breach & Attack Simulation (BAS) Technologies

• Gartner Definition
  • Tools that allow enterprises to continually and consistently simulate the full attack cycle (including insider threats, lateral movement and data exfiltration) against enterprise infrastructure, using software agents, virtual machines, and other means

• Search Terms
  • Breach and Adversary Simulation will be a search term
  • Vendors will ensure that SEO works here (Marketecture™)

• Beginning process of feature comparison
  • CIO/CISO’s on the edge will start paying attention to this tech category
  • Posture testing – just starting to be a “purchased” item, as benefit is “high”
You do not need to actually spend much to test your infrastructure...

- Create an isolated segment
  - Install workstation with your golden image and common application
    - Amp it up a bit ... sysmon, check the stance with LogMD
    - Install a “rollback” app
  - Install a copy of Sec Onion on the same segment
    - Must mirror LAN traffic for this to be effective
  - Limit connectivity to internal segments
  - Build scripts to:
    - Retrieve “recent” malware lists (MDL, RBL, ISC)
    - Reach out, retrieve, curl, etc.

- Technique used for several years (by me) to demo security products for clients
Example Test

Why does the Palo Alto treat these differently?
Note that the protective system behaved differently...

<table>
<thead>
<tr>
<th>Receive Time</th>
<th>Category</th>
<th>URL</th>
<th>From Zone</th>
<th>To Zone</th>
<th>Source</th>
<th>Destination</th>
<th>Application</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/09 23:34:52</td>
<td>dating</td>
<td>tinder.com/</td>
<td>LocalLAN</td>
<td>Internet</td>
<td>Dons_Window...</td>
<td>hit-adult.opendns.com</td>
<td>ssl</td>
<td>block-url</td>
</tr>
<tr>
<td>10/09 23:34:52</td>
<td>dating</td>
<td>tinder.com/</td>
<td>LocalLAN</td>
<td>Internet</td>
<td>Dons_Window...</td>
<td>hit-adult.opendns.com</td>
<td>ssl</td>
<td>block-url</td>
</tr>
<tr>
<td>10/09 23:34:47</td>
<td>dating</td>
<td>tinder.com/</td>
<td>LocalLAN</td>
<td>Internet</td>
<td>Dons_Window...</td>
<td>hit-adult.opendns.com</td>
<td>ssl</td>
<td>block-url</td>
</tr>
<tr>
<td>10/09 23:34:47</td>
<td>dating</td>
<td>tinder.com/</td>
<td>LocalLAN</td>
<td>Internet</td>
<td>Dons_Window...</td>
<td>hit-adult.opendns.com</td>
<td>ssl</td>
<td>block-url</td>
</tr>
<tr>
<td>10/09 23:34:47</td>
<td>dating</td>
<td>tinder.com/</td>
<td>LocalLAN</td>
<td>Internet</td>
<td>Dons_Window...</td>
<td>hit-adult.opendns.com</td>
<td>ssl</td>
<td>block-url</td>
</tr>
<tr>
<td>10/09 23:34:47</td>
<td>dating</td>
<td>tinder.com/</td>
<td>LocalLAN</td>
<td>Internet</td>
<td>Dons_Window...</td>
<td>hit-adult.opendns.com</td>
<td>ssl</td>
<td>block-url</td>
</tr>
<tr>
<td>10/09 23:34:38</td>
<td>dating</td>
<td><a href="http://www.eharmony.com/favicon.ico">www.eharmony.com/favicon.ico</a></td>
<td>LocalLAN</td>
<td>Internet</td>
<td>Dons_Window...</td>
<td>hit-adult.opendns.com</td>
<td>ssl</td>
<td>block-url</td>
</tr>
<tr>
<td>10/09 23:34:38</td>
<td>dating</td>
<td><a href="http://www.eharmony.com/">www.eharmony.com/</a></td>
<td>LocalLAN</td>
<td>Internet</td>
<td>Dons_Window...</td>
<td>hit-adult.opendns.com</td>
<td>ssl</td>
<td>block-url</td>
</tr>
<tr>
<td>10/09 23:34:32</td>
<td>dating</td>
<td><a href="http://www.okcupid.com/">www.okcupid.com/</a></td>
<td>LocalLAN</td>
<td>Internet</td>
<td>Dons_Window...</td>
<td>hit-adult.opendns.com</td>
<td>ssl</td>
<td>block-url</td>
</tr>
<tr>
<td>10/09 23:34:32</td>
<td>dating</td>
<td><a href="http://www.okcupid.com/">www.okcupid.com/</a></td>
<td>LocalLAN</td>
<td>Internet</td>
<td>Dons_Window...</td>
<td>hit-adult.opendns.com</td>
<td>ssl</td>
<td>block-url</td>
</tr>
<tr>
<td>10/09 23:34:32</td>
<td>dating</td>
<td><a href="http://www.okcupid.com/">www.okcupid.com/</a></td>
<td>LocalLAN</td>
<td>Internet</td>
<td>Dons_Window...</td>
<td>hit-adult.opendns.com</td>
<td>ssl</td>
<td>block-url</td>
</tr>
<tr>
<td>10/09 23:34:32</td>
<td>dating</td>
<td><a href="http://www.okcupid.com/">www.okcupid.com/</a></td>
<td>LocalLAN</td>
<td>Internet</td>
<td>Dons_Window...</td>
<td>hit-adult.opendns.com</td>
<td>ssl</td>
<td>block-url</td>
</tr>
</tbody>
</table>
### Detailed Log View

<table>
<thead>
<tr>
<th>General</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>User</td>
<td>User</td>
</tr>
<tr>
<td>Action</td>
<td>Address 192.168.1.15</td>
<td>Address 146.112.61.106</td>
</tr>
<tr>
<td>Application</td>
<td>Country 192.168.0.0-192.168.255.255</td>
<td>Country Austria</td>
</tr>
<tr>
<td>Rule</td>
<td>Port 6058</td>
<td>Port 80</td>
</tr>
<tr>
<td>Virtual System</td>
<td>Zone Local/LAN</td>
<td>Zone Internet</td>
</tr>
<tr>
<td>Device SN</td>
<td>Interface ethernet1/2</td>
<td>Interface ethernet1/1</td>
</tr>
<tr>
<td>IP Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log Action</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generated Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receive Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tunnel Type</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### HTTP Headers

- User-Agent
- Referrer
- X-Forwarded-For

#### Details

- **Severity**: Informational
- **Repeat Count**: 1
- **URL**: www.eharmony.com/

#### Flags

- Captive Portal: False
- Proxy Transaction: False
- Decrypted: False
- Packet Capture: False
- Client to Server: True
- Server to Client: False
- Tunnel Inspected: False
- Credential Detected: False

<table>
<thead>
<tr>
<th>PCAP</th>
<th>Receive Time</th>
<th>Type</th>
<th>Application</th>
<th>Action</th>
<th>Rule</th>
<th>Bytes</th>
<th>Severity</th>
<th>Category</th>
<th>Verdict</th>
<th>URL</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018/10/09 23:34:52</td>
<td>end</td>
<td>web-browsing</td>
<td>allow</td>
<td>dons_com...</td>
<td>4857</td>
<td></td>
<td>Informational</td>
<td>dating</td>
<td></td>
<td><a href="http://www.eharmony.com/">www.eharmony.com/</a></td>
<td></td>
</tr>
<tr>
<td>2018/10/09 23:34:38</td>
<td>url</td>
<td>web-browsing</td>
<td>block-url</td>
<td>dons_com...</td>
<td>Informational</td>
<td></td>
<td>dating</td>
<td><a href="http://www.eharmony.com/">www.eharmony.com/</a></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How about another application?

```
10/09 23:56:18  shopping  www.amazon.com/  LocalLAN  Internet  192.168.1.34  a23-211-128-116.deploy.static.akamaitechnolo...  ssl  alert
10/09 23:53:37  dating    www.okcupid.com/   LocalLAN  Internet  192.168.1.34  hit-adult.opendns.com  ssl  block-url
10/09 03:32:07  computer-and-internet-info  rules.emergingthreats.net/  LocalLAN  Internet  192.168.1.34  96.43.137.99  ssl  alert
10/09 03:32:07  computer-and-internet-info  rules.emergingthreats.net/  LocalLAN  Internet  192.168.1.34  204.12.217.19  ssl  alert
```
Ideas... There are MANY!

- Study each phase of the ATT&CK framework
  - Find / deploy a tool / tech for each phase grouping
  - Red needs to learn how, Blue needs to learn to find
- Build out a persistence lab, starting w/ an infected NBK that walks back in
  - Get some lateral movement going on
  - then use the JPCert LogonTracer to go find ‘em
- Build out an OWASP Top 10 lab
  - Red: perform attacks using MetaSploit, CobaltStrike, etc.
  - Blue: active monitor using SecOnion, bro (now zeek)
- Grab some Kali books, see what is a current attack technique, and detect it
- Review MetaSploit attacks against your deployed technology stack, spin up a P2V copy, defang the data, attack and defend
Attack IQ

• 1,500+ distinct attacks built into the tool
  • Active user community
• Designed to support tool, team, and process testing
• Staff can create (build) scenario steps
• Cannot change the deployed EXE name
• Significant remediation assistance and advice
Cymulate - Instrument Agents, Local ENV

• Mimic myriad of attack strategies and tools that malicious hackers and cyber criminals deploy

• Test all phases of an attack, from pre-exploitation to post-exploitation
Overview

- Complex Adversary Simulation
- Modular Framework
  - Communication
  - Capabilities
- Flexible Implant Delivery
  - EXE & DLL
  - Phishing & Web
- Variable Reporting
  - Executive Summary
  - Detailed Exports
- Industry Aligned
  - MITRE ATT&CK & LM Kill Chain
- Module Development Guide
Communication Modules

Communication modules:
- DNS
- Google
- HTTP
- HTTPS
- SMB

Capabilities Modules

Capabilities modules:
- ARP
- Clipboard
- Controller
- Crypto
- Downloader
- Elevate
- EnumWin
- File
- Keylogger
- Loader