



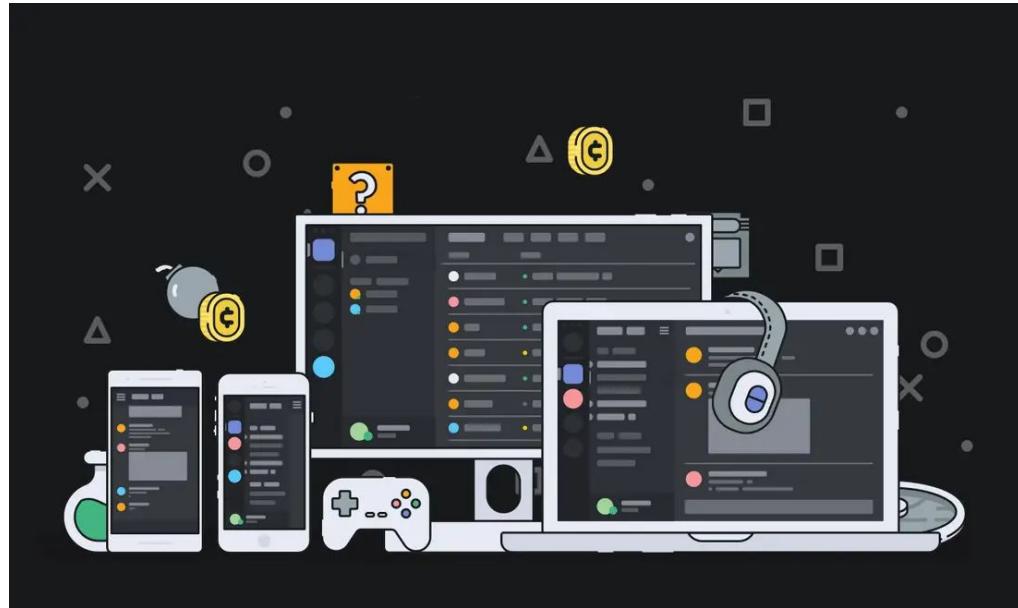
Building a Home Lab

Active Countermeasures and BHIS
Bill Stearns and John Strand



Welcome!

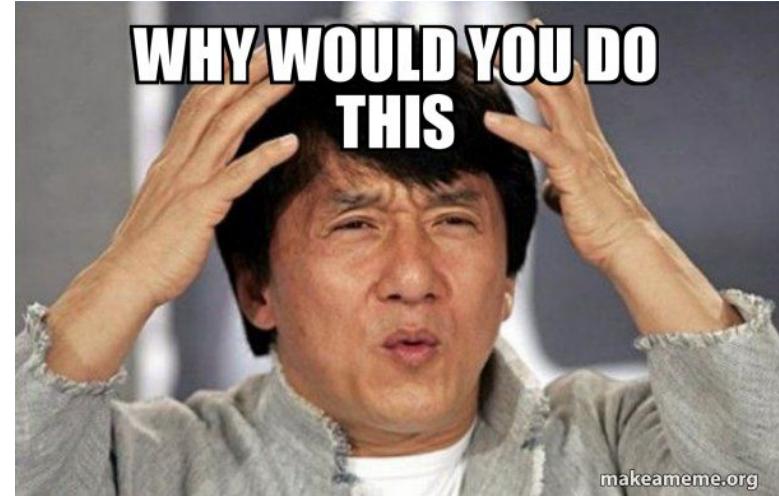
- Discord servers
 - Discussion during and after webcast
 - Threat Hunting community:
<https://discord.gg/w23C3rd>
 - Live discussion in #acm-webcast-chat
 - Slides and materials in #acm-webcast-content
 - Report problems in #feedback
 - Black Hills Information Security:
<https://discord.gg/aHHh3u5>
- Private questions window in GTW
 - We'll answer as many as we can



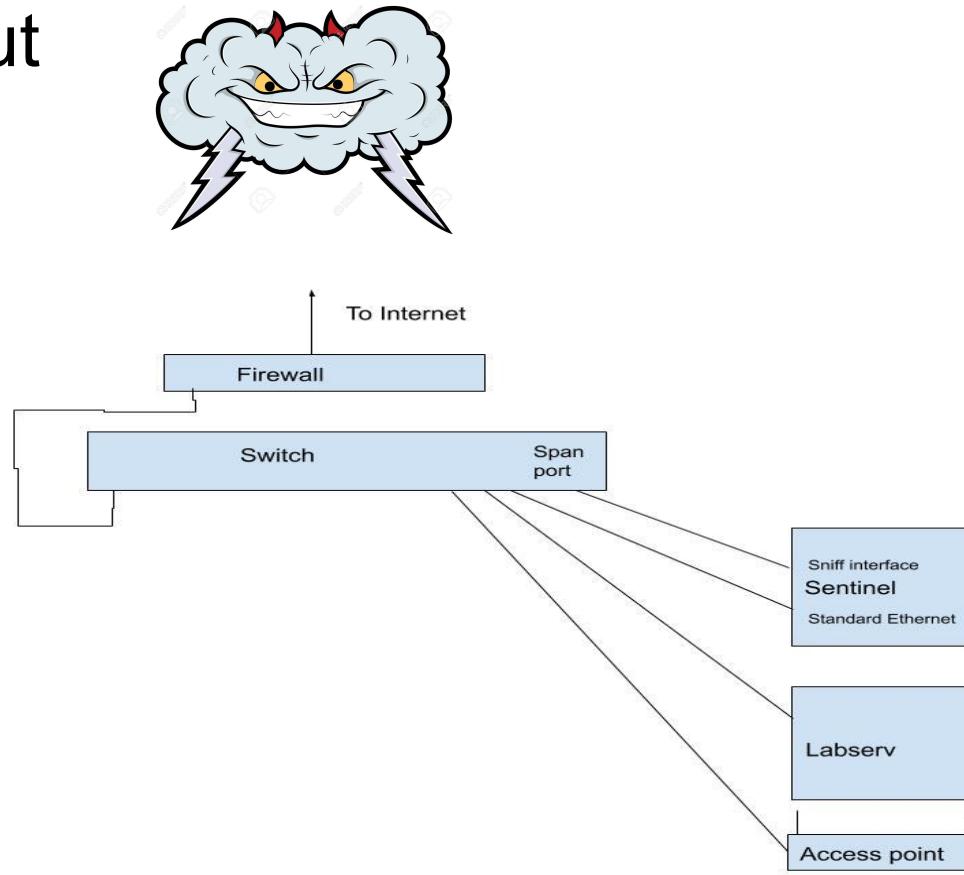
Chaos... Total. Chaos

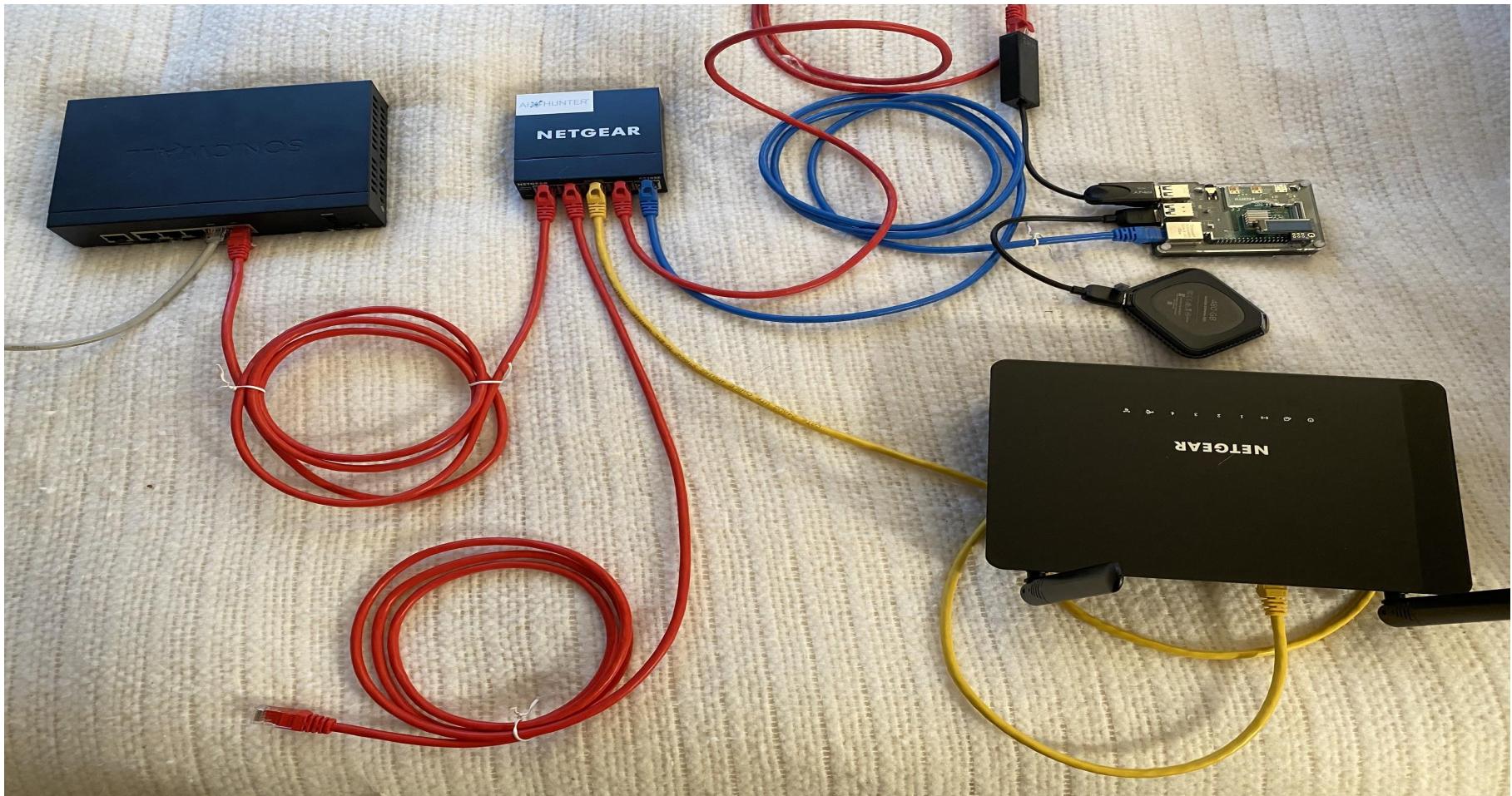
Why?

- Protection
 - Testing software in a controlled environment
- Rules
 - Packet capture and some cracking tools may be prohibited at work
- Learning
 - You can try out applications without risk
 - Document install procedure on a test network
 - Reverse engineering
- Patch testing
 - Apply to these non-production machines first
- Troubleshooting
 - Place to test/repair potentially infected systems
 - Disconnect other systems for this use

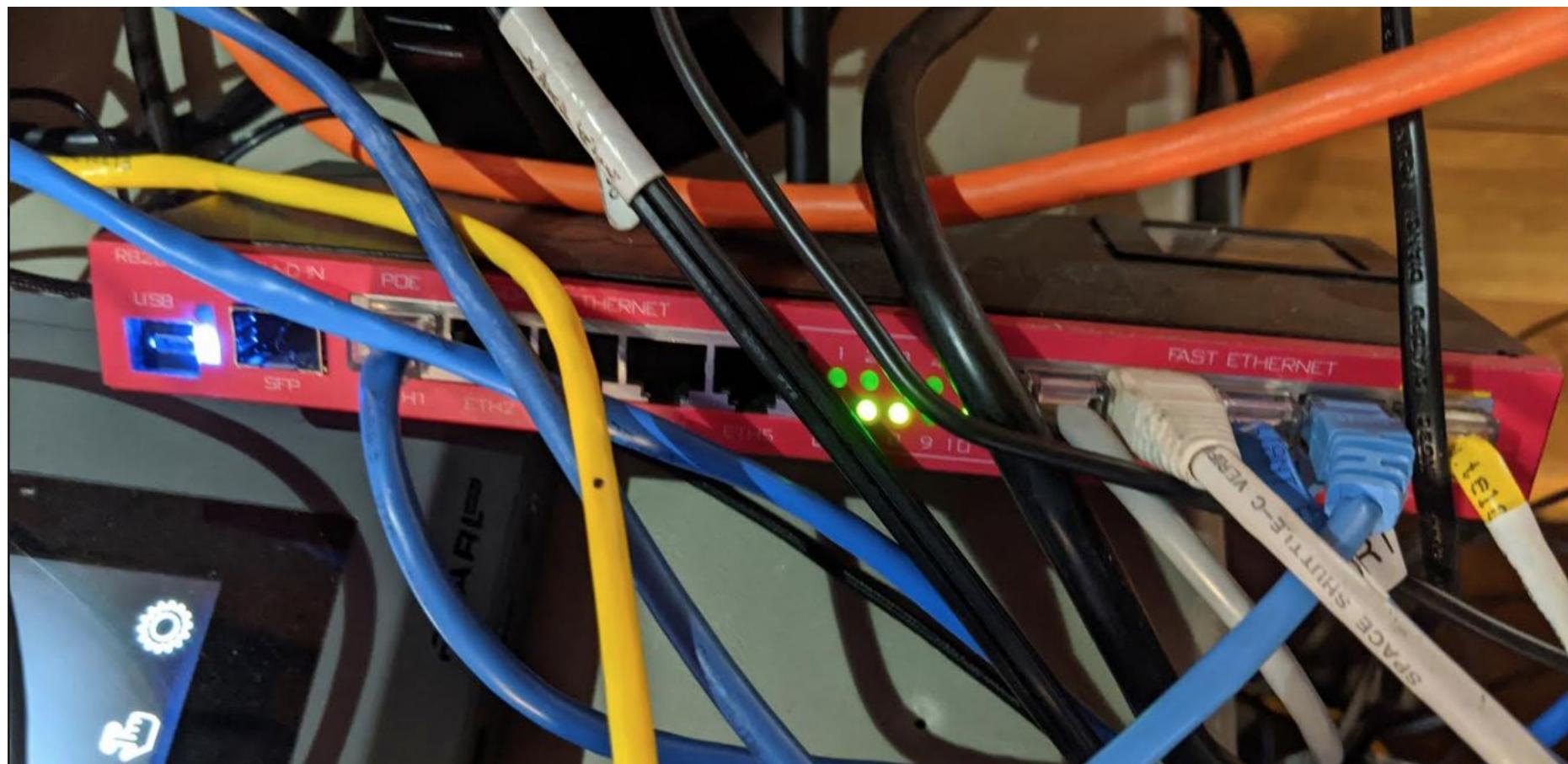


Network layout





John's Lab Network



John's Lab Network

◀ Back to results

 Purchased 1 time.

You last purchased this item on March 25, 2017.

[View this order](#)



Roll over image to zoom in

MikroTik Routerboard RB2011UiAS-2HnD-IN Sfp Port plus 10 Port Ethernet

by MikroTik

 279 ratings | 120 answered questions

Price: \$140.69 

Get \$125 off: Pay \$15.69 upon approval for the [Amazon Business Prime Card](#). Terms apply.

- RouterBOARD 2011UiAS-2HnD has most features and interfaces from all our Wireless routers
- It's powered by the new Atheros 600MHz 74K MIPS network processor, has 128MB RAM, five Gigabit LAN ports, five Fast Ethernet LAN ports and SFP cage
- Also, it features powerful dual chain 2.4GHz (2312-2732MHz depending on country regulations) 802.11bgn wireless AP, RJ45 serial port, USB port and RouterOS L5 license, as well as desktop case with power supply and two 4dBi Omni antennas
- RouterBOARD 2011UiAS-2HnD-IN comes with desktop enclosure, LCD panel and power supply
- The RB2011Ui also has passive PoE output capability on the last port (ETH10), this means you can power another device just by connecting it over regular Ethernet cable

New & Used (6) from \$100.00 + \$5.49 Shipping

[Report incorrect product information.](#)

10Gtek

10Gb/s SFP+ direct attach
cable 3m for Ubiquiti

[Shop now](#)



10Gb/s SFP+ Direct
Attach Copper Cable, 10Gb/s 3m-
Meter SFP+ DAC Twinax Cable...
\$23.49 

[Add feedback](#)

Port Mirroring

Port mirroring lets switch 'sniff' all traffic that is going in and out of one port (mirror-source) and send a copy of those packets out of some other port (mirror-target). This feature can be used to easily set up a 'tap' device that receives all traffic that goes in/out of some specific port. Note that mirror-source and mirror-target ports have to belong to same switch. (See which port belongs to which switch in `/interface ethernet menu`). Also mirror-target can have a special 'cpu' value, which means that 'sniffed' packets should be sent out of switch chip's CPU port. Port mirroring happens independently of switching groups that have or have not been set up.

- Port mirroring configuration example:

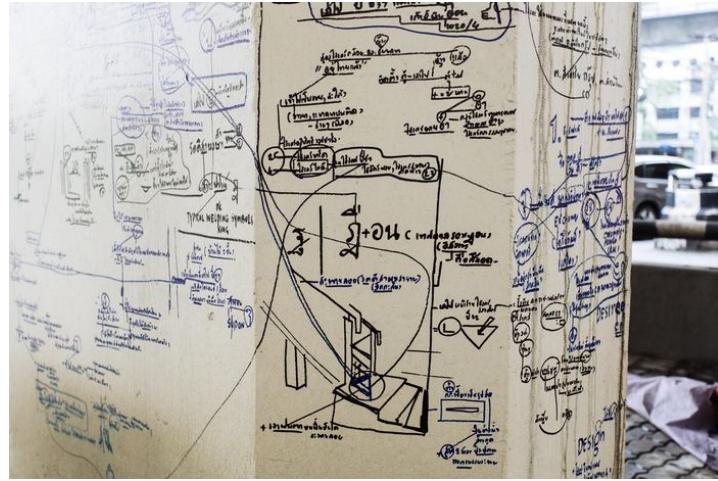
```
/interface ethernet switch
set switch1 mirror-source=ether2 mirror-target=ether3
```

John's Lab Network



Network layout

- From the outside in:
- Ethernet from firewall to internet gateway
- Lab Firewall
 - Choke point, good for isolation and capture
- Switch with span port
 - Dedicated Sentinel capture system
 - Dedicated Labserv service system
- Wireless AP
 - By connecting this to the lab switch, Sentinel can capture all wired and wireless clients



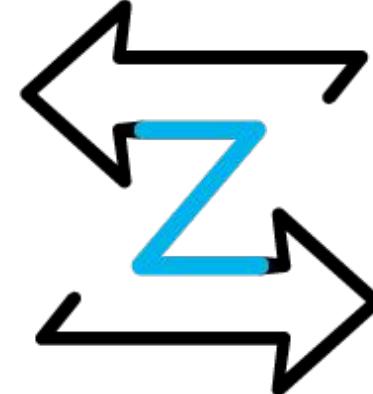
Hardware for the project

- Firewall
- Switch with span port
- Wireless AP
 - wired ethernet outbound
- KVM switcher, monitor, KB, mouse
 - 4x PC -> KB/Mouse/HDMI: <https://www.amazon.com/Switch-HDMI-1080P-Supported-Cables/dp/B083VWW9N9/>
- Used hardware - excellent!
 - All that stuff you have in your basement already. :-)
- Gigabit ethernet
 - Needed for imaging
- Extra sata drives, flash drives, and microSDs
 - One for each project



Firewall or IPS

- Severely limit all traffic
 - Both directions
 - Do **not** open up for all outbound traffic
 - Open up ports as needed (coming up in this talk)
- IDS/IPS
 - Look for signatures of malicious traffic and beacons
- Bro/Zeek
 - Feed output to Rita (<https://github.com/activecm/rita/>)
 - Feed output to devprof (<https://github.com/activecm/devprof>)



Marcus Ranum's Ultimate Firewall

http://www.ranum.com/security/computer_security/papers/a1-firewall/



The Ultimately Secure DEEP PACKET INSPECTION AND APPLICATION SECURITY SYSTEM
Featuring signature-less anomaly detection and blocking technology with application awareness and layer-7 state tracking!!!

Now available in Petabyte-capable appliance form factor!

Which firewall?

- Anything!
- Requirements
 - At least 2 network interfaces - inside and outside
 - Fast enough for needed data
 - Per-port firewall rules (ideally, per-port and per-client)
 - IPv4 and IPv6 support
- For this example, Sonicwall TZ300
 - Left over from a previous project
 - Serves the above needs



Switch



- Span port for capture leading to Sentinel
 - Second normal port for Sentinel incoming/outgoing access
- One port leading up to the firewall
- One port leading down to the wireless AP
- One port leading down to labserv
- Remaining N-5 ports for client systems
- Netgear GS116E (managed, 16 port)
 - Has span port capability (1 monitor port only)
 - <https://www.amazon.com/gp/product/B00GG1AC7I/>
 - \$130, \$108 with discount
- Mikrotik
 - <https://www.amazon.com/Mikrotik-Routerboard-RB2011UiAS-2HnD-Port-Ethernet/dp/B00BGIXOHQ>



Wireless AP

- Wired Ethernet going out to switch
- Optional additional Ethernet ports for lab machines
 - Though prefer main switch so all traffic captured
- Wireless Ethernet for wireless devices
 - Needs to support 2.4 ghz and 5 ghz
- Use management interface to monitor new systems
- Disable NAT here so you see the wireless IPs at your firewall



Free Wifi!!

Sentinel

- SSH accessible from home machines
 - Allows for port forwarding in and out as needed
 - Jump to other hosts from here
- Has network tools for testing
 - Kali Linux or Security Onion
- VPN gateway software if needed
 - Discouraged - can be a way around the firewall
- Block all listening ports from lab IPs
- Extra drive space
 - Forensic images
 - Pristine images for rebuilding
- Second ethernet interface connected to span port
 - Need to capture inside packets with internal IP addresses

File and drive image transfer

- Make sure Sentinel system and devices support at least USB 3.0
- Flash drives
 - For manual file transfer
 - Pay attention to infection
 - Read-only before inserting into infected system
- USB 3 SATA cable or bay
 - <https://www.amazon.com/s?k=USB+3+sata>
- USB 3 memory card reader
 - <https://www.amazon.com/s?k=USB+3+card+reader>
 - <https://www.amazon.com/SmartQ-C368-Multi-Card-Compatible-Supports/dp/B06Y1G18KS/>
- Make image before starting forensics
- Create pristine images for all lab systems

Memory Analysis

- Volatility
 - <https://www.volatilityfoundation.org/>
- FTK Imager
 - <http://vcodispot.com/ram-acquisition-ftk-imager-volatility/>



Labserv

- SSH accessible from home machines
- System that provides services to lab systems
 - DNS
 - SMTP
 - Syslog
 - Squid web proxy
 - Hides the requestor IP
- Enable logging of all requests
 - DNS and squid request logging, /var/log/maillog
- Turn on file sharing with SMB/NFS/SSH if needed
 - If you need to share files with lab machines, do it from here
- Connections: Labserv -> lab systems

Do Firewall, Sentinel, and Labserv have to be separate?

- 3 systems available
 - Keep all three separate
- 2 systems available
 - sentinel and firewall together
 - Labserv separate
 - **OR**
 - sentinel and labserv together
 - firewall separate
- 1 system available
 - discouraged, but can place all three on 1



Guinea Pigs

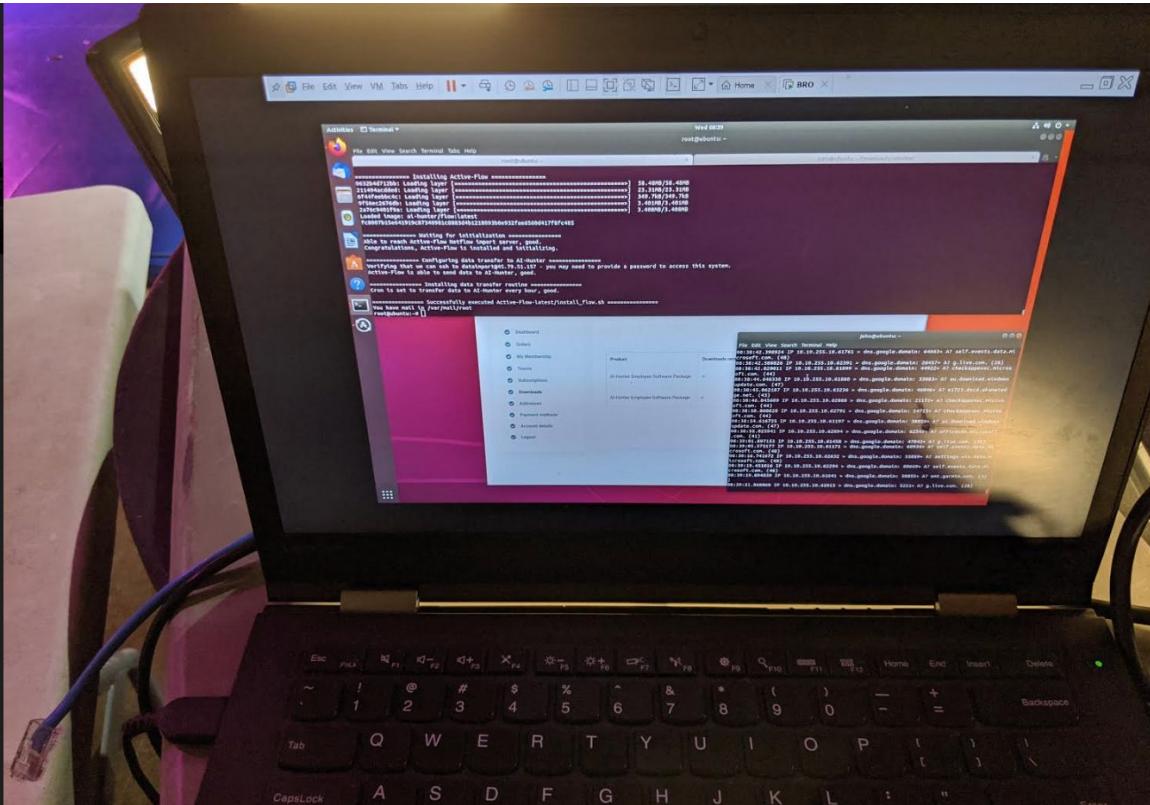
- Different platforms
 - Windows, Mac, Linux
 - IOT devices
 - Software you're testing or don't trust
 - Devices you're testing or don't trust
 - Android phone
 - Raspberry Pi
 - Multiple microsd cards for different Linux distributions
 - Potentially infected systems for forensics and imaging
- Virtual machines
 - Much easier to snapshot and restore
- They can *only* get internet access through this lab network



John's Systems



Zeek System



AI-Hunter for home

ACTIVE COUNTERMEASURES



ACTIVE COUNTERMEASURES



HELK

Discover

New Save Open Share Inspect

process.name:chrome.exe

KQL Last 15 minutes Show dates Refresh

logs-endpoint-winevent-syamon-* (change)

Count @timestamp per 30 seconds

44 hits Apr 16, 2020 @ 03:27:30.870 - Apr 16, 2020 @ 03:42:30.870 — Auto

Time _source

process.name: chrome.exe record_number: 2,910 provider_guid: 5770385F-C22A-43E0-BF4C-06F5698FB09 event.created: Apr 16, 2020 @ 03:38:02.887 event.action: File stream created (rule: FileCreateStreamHash) event.provider: Microsoft-Windows-Syamon event.kind: event.event_code: 15 event.module: syamon event.id: 15 task: File stream created (rule: FileCreateStreamHash) process.exe: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe best_version: 7.6.2 #file.date_creation: Apr 16, 2020 @ 03:37:33.968 agent.hostname: TheBoss agent.version: 7.6.2 agent.id: d86bf02d-d6c8-4e5d-bf8f-9e3b3ccb055b agent.type: winlogbeat agent.ephemeral_id: 2a94100c-5cfb-4ab2-9aad-bf5ceb2b78e4 process_id: 1,240 user.reporter_type: User user.reporter_name: SYSTEM @version: 1 file.path: C:\Users\Sec504\Downloads\atomic-red-team-master.zip Zone.Identifier z.original_message: File stream created: RuleName: UtcTime: 2020-04-16 09:38:01.754 ProcessGuid: {AC64AE42-26D0-5E98-0000-0010F8319800} ProcessId: 2688 Image: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

process.name: chrome.exe record_number: 2,900 provider_guid: 5770385F-C22A-43E0-BF4C-06F5698FB09 event.created: Apr 16, 2020 @ 03:38:02.887 event.action: File created (rule: FileCreate) event.provider: Microsoft-Windows-Syamon event.kind: event.event_code: 11 event.module: syamon event.id: 11 task: File created (rule: FileCreate) process.exe: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe best_version: 7.6.2 #file.date_creation: Apr 16, 2020 @ 03:37:33.968 agent.hostname: TheBoss agent.version: 7.6.2 agent.id: d86bf02d-d6c8-4e5d-bf8f-9e3b3ccb055b agent.type: winlogbeat agent.ephemeral_id: 2a94100c-5cfb-4ab2-9aad-bf5ceb2b78e4 process_id: 1,240 user.reporter_type: User user.reporter_name: SYSTEM @version: 1 file.path: C:\Users\Sec504\Downloads\atomic-red-team-master.zip Zone.Identifier z.original_message: File created: RuleName: Downloads UtcTime: 2020-04-16 09:38:01.754 ProcessGuid: {AC64AE42-26D0-5E98-0000-0010F8319800} ProcessId: 2688 Image: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe TargetFilename:

process.name: chrome.exe record_number: 2,988 provider_guid: 5770385F-C22A-43E0-BF4C-06F5698FB09 event.created: Apr 16, 2020 @ 03:38:02.887 event.action: File stream created (rule: FileCreateStreamHash) event.provider: Microsoft-Windows-Syamon event.kind: event.event_code: 15 event.module: syamon event.id: 15 task: File stream created (rule: FileCreateStreamHash) process.exe: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe best_version: 7.6.2 #file.date_creation: Apr 16, 2020 @ 03:37:33.968 agent.hostname: TheBoss agent.version: 7.6.2 agent.id: d86bf02d-d6c8-4e5d-bf8f-9e3b3ccb055b agent.type: winlogbeat agent.ephemeral_id: 2a94100c-5cfb-4ab2-9aad-bf5ceb2b78e4 agent.id: d86bf02d-d6c8-4e5d-bf8f-9e3b3ccb055b agent.type: winlogbeat agent.hostname: TheBoss process_id: 1,240 user.reporter_type: User user.reporter_name: SYSTEM @version: 1 file.path: C:\Users\Sec504\Downloads\atomic-red-team-master.zip Zone.Identifier z.original_message: File stream created: RuleName: UtcTime: 2020-04-16 09:38:01.674 ProcessGuid: {AC64AE42-26D0-5E98-0000-0010F8319800} ProcessId: 2688 Image: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe TargetFilename:

process.name: chrome.exe record_number: 2,987 provider_guid: 5770385F-C22A-43E0-BF4C-06F5698FB09 event.created: Apr 16, 2020 @ 03:37:59.877 event.action: Dns query (rule: DnsQuery) event.provider: Microsoft-Windows-Syamon event.kind: event.event_code: 22 event.module: syamon event.id: 22 task: Dns query (rule: DnsQuery) process.exe: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe process.entity_id: {AC64AE42-26D0-5E98-0000-0010253C9800} process.pid: 3392 process.executable: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe best_version: 7.6.2 agent.version: 7.6.2 agent.hostname: TheBoss agent.id: d86bf02d-d6c8-4e5d-bf8f-9e3b3ccb055b agent.type: winlogbeat agent.ephemeral_id: 2a94100c-5cfb-4ab2-9aad-bf5ceb2b78e4 process_id: 1,240 user.reporter_type: User user.reporter_name: SYSTEM @version: 1 z.original_message: Dns query: DNS: QueryName: ab-ssl.google.com QueryStatus: 0 QueryResults: type: 5 sb-ssl1.google.com:216.58.192.286; Image: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe host_name: theboss action: dnsquery syamon.dns.status: SUCCESS

process.name: chrome.exe record_number: 2,986 provider_guid: 5770385F-C22A-43E0-BF4C-06F5698FB09 event.created: Apr 16, 2020 @ 03:37:35.846 event.action: File created (rule: FileCreate) event.provider: Microsoft-Windows-Syamon event.kind: event.event_code: 11 event.module: syamon event.id: 11 task: File created (rule: FileCreate) process.exe: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe process.entity_id: {AC64AE42-26D0-5E98-0000-0010F8319800} process.pid: 2688 process.executable: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe best_version: 7.6.2 #file.date_creation: Apr 16, 2020 @ 03:37:33.968 agent.version: 7.6.2 agent.ephemeral_id: 2a94100c-5cfb-4ab2-9aad-bf5ceb2b78e4 agent.id: d86bf02d-d6c8-4e5d-bf8f-9e3b3ccb055b agent.type: winlogbeat agent.hostname: TheBoss process_id: 1,240 user.reporter_type: User user.reporter_name: SYSTEM @version: 1 file.path: C:\Users\Sec504\Downloads\2964bd9f-cd7a-43e1-9379-a24246515909.tpm

```

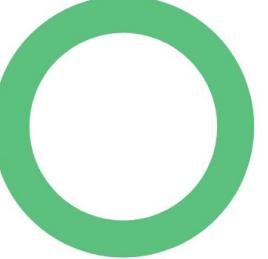
graph TD
    beats[beats] --> kafka[kafka]
    kafka --> logstash[logstash]
    logstash --> elasticsearch[elasticsearch]
    elasticsearch --> kibana[kibana]
    elasticsearch --> esHadoop[ES-Hadoop]
    elasticsearch --> spark[spark]
    spark --> jupyter[jupyter]
    elasticsearch --> elastalert[elastalert]
    elasticsearch --> sigma[sigma]
    elasticsearch --> graphframes[GraphFrames]
    elasticsearch --> helk[HE-LK]
    helk --> beats
    helk --> kafka
    helk --> logstash
    helk --> elasticsearch
    helk --> esHadoop
    helk --> spark
    helk --> jupyter
    helk --> elastalert
    helk --> sigma
    helk --> graphframes
  
```



Beaker

ACTIVE COUNTERMEASURES

Top 10 Destination Ports



Source IP: 10.55.100.108 | Source Hostname: WKS-12-11 | Destination IP: 68.183.138.51

Events



Program List

Executable	PID	User	Destination Port	Protocol	Transport	Count
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	1,392	Anthony.Caldwell	80	http	tcp	2,670

Time: Apr 5, 2020 @ 17:59:27.433 | Source: @timestamp

> Apr 5, 2020 @ 17:59:27.433 @timestamp: Apr 5, 2020 @ 17:59:27.433 destination.ip: 68.183.138.51 destination.port: 80 user.name: Anthony.Caldwell user.domain: WLABV2 host.name: WKS-12-11 event.code: 3 event.module: sysmon event.provider: Microsoft-Windows-Sysmon event.action: Network connection detected (rule: NetworkConnect) event.created: Apr 5, 2020 @ 18:01:59.477 event.kind: event process.entity_id: {bbfc056b-3559-5e44-0000-0010b325724b} process.pid: 1,392 process.executable: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe process.name: powershell.exe message: Network connection detected RuleName: UtcTime: 2020-04-05 23:58:27.433 ProcessGuid: {bbfc056b-3559-5e44-0000-0010b325724b} ProcessId: 1392 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: WLABV2\Anthony.Caldwell Protocol: tcp Initiated: true SourceIpv6: false SourceIp: 10.55.100.108 SourceHostname: WKS-12-11.wlabv2.local SourcePort: 65511 SourcePortName: DestinationIpv6: false DestinationIp: 68.183.138.51 DestinationHostname: DestinationPort: 80 DestinationPortName: http network.transport: tcp network.protocol: http network.direction: outbound network.type: ipv4 network.community_id: 1:DBf6Lk2Hty+Walq08KG2QvSD8= source.ip: 10.55.100.108 source.domain: WKS-12-11.wlabv2.local source.port: 65,511 agent.type: winlogbeat agent.ephemeral_id: 4d96af00-6da5-4b9d-8e68-d9f452201477 agent.hostname: WKS-12-11 agent.id: 2ded2d9-6f3c-41c7-9549-c69d19fe85e agent.version: 7.5.2 ecs.version: 1.1.0 winlog.provider_guid: {5770385f-c22a-43e0-bf4c-06f598fbfd9} winlog.api: wineventlog winlog.task: Network connection detected (rule: NetworkConnect) winlog.process.pid: 2,672 winlog.process.thread.id: 3,584 winlog.computer.name: WKS-12-11.wlabv2.local winlog.version: 5 winlog.user.name: SYSTEM

> Apr 5, 2020 @ 17:58:57.290 @timestamp: Apr 5, 2020 @ 17:58:57.290 network.type: ipv4 network.community_id: 1:pwVxbB3oKHM7gUcYxJp8YAZ2= network.transport: tcp network.protocol: http network.direction: outbound source.ip: 10.55.100.108 source.domain: WKS-12-11.wlabv2.local source.port: 65,508 host.name: WKS-12-11 winlog.task: Network connection detected (rule: NetworkConnect) winlog.record_id: 453516 winlog.provider.guid: {5770385f-c22a-43e0-bf4c-06f598fbfd9} winlog.user.name: SYSTEM winlog.user.domain: NT AUTHORITY\SYSTEM winlog.user.type: User winlog.user.identifier: S-1-5-18 winlog.provider.name: Microsoft-Windows-Sysmon winlog.api: wineventlog winlog.opcode: Info winlog.version: 5 winlog.process.thread.id: 3,584 winlog.process.pid: 2,672 winlog.channel: Microsoft-Windows-Sysmon/Operational winlog.event_id: 3 winlog.computer.name: WKS-12-11.wlabv2.local message: Network connection detected RuleName: UtcTime: 2020-04-05 23:58:57.290 ProcessGuid: {bbfc056b-3559-5e44-0000-0010b325724b} ProcessId: 1392 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: WLABV2\Anthony.Caldwell Protocol: tcp Initiated: true SourceIpv6: false SourceIp: 10.55.100.108 SourceHostname: WKS-12-11.wlabv2.local SourcePort: 65508 SourcePortName: DestinationIpv6: false DestinationIp: 68.183.138.51 DestinationHostname: DestinationPort: 80 DestinationPortName: http process.executePath: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe process.name: powershell.exe process.entity_id: {bbfc056b-3559-5e44-0000-0010b325724b} process.pid: 1,392 destination.ip: 68.183.138.51 destination.port: 80 user.domain: WLABV2 user.name: Anthony.Caldwell agent.ephemeral_id: 4d96af00-6da5-4b9d-8e68-d9f452201477 agent.hostname: WKS-12-11 agent.id: 2ded2d9-6f3c-41c7-9549-c69d19fe85e

ACTIVE COUNTERMEASURES

Creating Evil

- Atomic Red Team
- Metasploit
- Scythe
- Cobalt Strike

```
msf5 > [metasploit v5.0.29-dev
+ --=[ 1897 exploits - 1068 auxiliary - 329 post
+ --=[ 547 payloads - 44 encoders - 10 nops
+ --=[ 2 evasion
]
msf5 > ]
```



- Open source
- Discrete unit tests
- Mapped to MITRE ATT&CK framework



Recording



Incrementally opening up the Firewall

- Top of the list
 - Allow from Home network to Sentinel, Firewall and Labserv on ssh (22/tcp)
 - And responses
 - Block all traffic from lab network to Home network subnets
 - And responses
- End of firewall rules, add a "Block and Log everything not yet allowed" rule
- Wait for a new entry in the firewall log
- Create a rule for it above "Block and Log everything" rule
 - Make it an "Allow" rule if you agree with it, a "Block/Drop" rule otherwise
- Repeat
- Mason!

Software

- IDS/IPS
- Forensics tools for your OS's
 - Statically linked binaries if possible: write protected drive
- Packet capture
- Port and network scanners
- Disk imaging



AUTOPSY
DIGITAL FORENSICS



The RITA logo includes a circular portrait of a woman with dark hair, a blue "DOWNLOAD" button at the bottom, and the text "REAL INTELLIGENCE THREAT ANALYTICS" above it. To the right, there is descriptive text about the tool.

RITA is an open source framework for network traffic analysis.

ACTIVE COUNTERMEASURES



IDS/IPS

- Snort
 - <https://www.snort.org/>
 - <https://github.com/snort3/snort3>
- Suricata
 - <https://suricata-ids.org/>
- Security Onion
 - <https://securityonion.net/>
- Rock NSM
 - <https://rocknsm.io/>



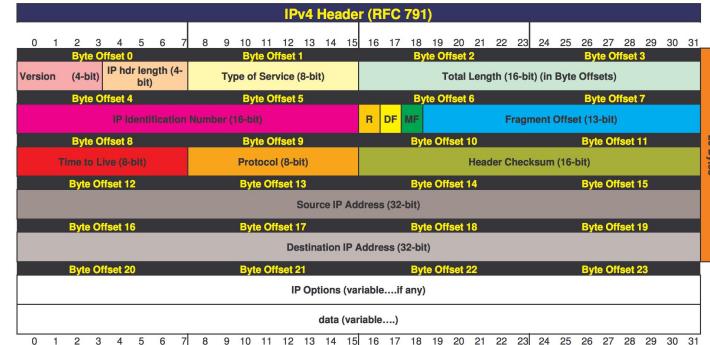
Packet capture

- tcpdump
- Zeek/RITA
- tshark/wireshark
 - "ssh -x sentinel" if you want to run wireshark on sentinel and display on your laptop
- All will read live from an interface or read from pcaps
- Continuous capture, use BPF to drop local-local traffic

```
mkdir -p /opt/pcaps
```

```
screen -S capture -t capture -d -m bash -c "nice -n 15 tcpdump -i eth0 -G 3600 -w '/opt/pcaps/'`hostname -s``.%Y%m%d%H%M%S.pcap` -z bzip2 'not (src net 172.27.0.0/16 and dst net 172.27.0.0/16)'"
```

```
screen -S capture -t capture -d -m bash -c "nice -n 15 tcpdump -i eth0 -G 3600 -w '/opt/pcaps/'`hostname -s``.%Y%m%d%H%M%S.pcap` -z bzip2 '(`tcp[13] & 0x17 != 0x10) or not tcp)` and not (src net 172.27.0.0/16 and dst net 172.27.0.0/16)'"
```



Network monitoring

- Nagios/Icinga/Shinken
 - <https://www.nagios.org/>
 - <https://icinga.com/>
 - <http://www.shinken-monitoring.org/>
- Bandwidth monitoring tools
 - <https://www.dnsstuff.com/linux-network-monitoring-tools>
 - <https://www.binarytides.com/linux-commands-monitor-network/>

Nagios®



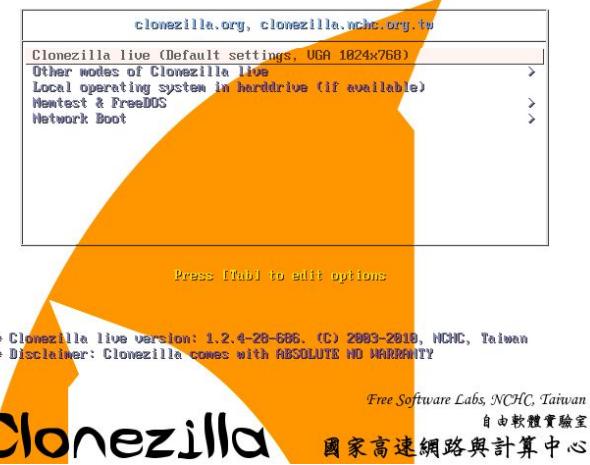
Scanning

- nmap
 - <https://nmap.org/>
- Kali Linux
 - <https://www.kali.org/>
- Passer
 - <https://github.com/activecm/passer>



Disk imaging

- Clonezilla
 - <https://clonezilla.org/>
 - Specifically Clonezilla Live: <https://clonezilla.org/clonezilla-live.php>
- Pi
 - <https://github.com/billw2/rpi-clone>
 - <https://github.com/johntcw/Forensic-Imager>
- FOG
 - <https://fogproject.org/>



Clonezilla

Free Software Labs, NCHC, Taiwan
自由軟體實驗室
國家高速網路與計算中心



On a budget - what's critical?

- >>> Network Isolation <<<
 - Severely limit what gets in and out
- Packet capture
 - Usually needs a span/mirror port
- Storage for pcaps, system images, and forensics
- Network and forensic tools
- Rest is negotiable
 - Network speed, type, and number of ports
 - Number and performance of support systems
 - Wireless vs wired



Closing notes

- Do not connect other systems to this network!
 - Come in over ssh to Sentinel
- Keep infected systems isolated
 - Disconnect the rest while working with one
 - Don't open up ports on the firewall until you know why they're needed.
- Play!
- Restore pristine image after trying new code



**YOUR
LAPTOP?!?**

**YOUR
TEENAGERS'
LAPTOPS!**

Credits

- John Strand
- Chris Brenton
- Bill Stearns
- Ethan Robish - thanks for the ideas!
 - <https://www.blackhillsinfosec.com/home-network-design-part-1/>
 - <https://www.blackhillsinfosec.com/home-network-design-part-2/>
- Shelby and Jason for pulling this all together
- Thanks to KC, Deb, Keith, Rick, David, Joff, Beau, Derek, Kent, James, Darin, and CJ for answering questions.
- Ongoing discussion: Discord servers

But Wait!!!!



<https://www.activecountermeasures.com/documents>