GRASSMARLIN

NSA, IAD, I4 – Fusion, Analysis, and Mitigations

Motivating Factors

- Blue Teams did not conduct assessments on ICS/SCADA networks for risk of physical impact
- Minimum situational awareness of devices connected to ICS/SCADA networks
- Lack of GOTS or COTS solutions *specifically* designed for this technology space

How would you passively identify IP-based devices on your ICS/SCADA network?

Constraints & Limitations

- Maintaining ICS/SCADA system availability is paramount
  - Cyber/Physical system faults/failures could result in
    - Loss of life
    - Loss of revenue
    - Loss of equipment
    - Environmental damage
    - Loss of service
- Primary data acquisition - **PASSIVE**

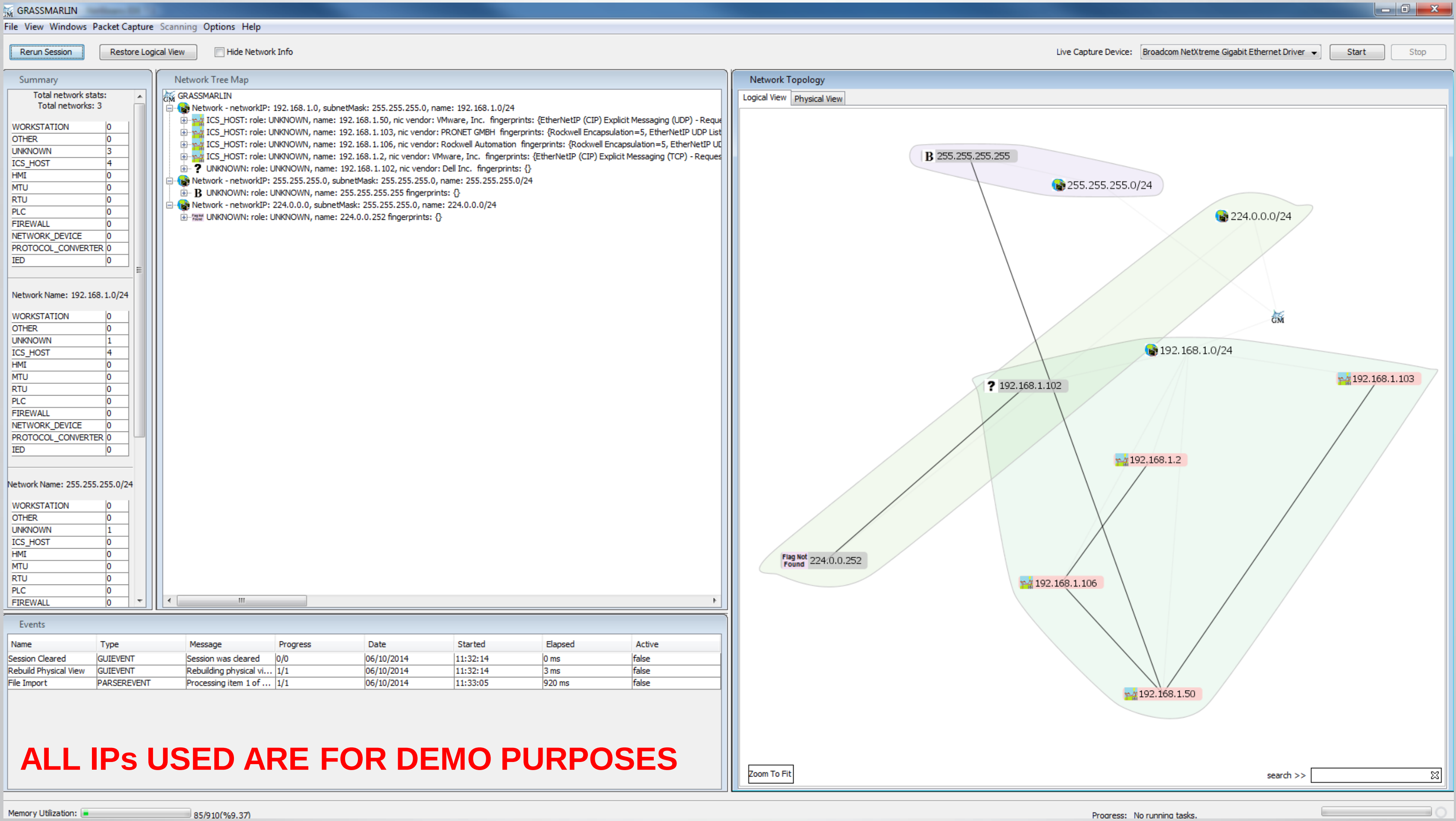
Goals

- Enable Blue Team capabilities on live ICS/SCADA IP networks while rigorously managing risk of harm to the network, process, or physical plant
- Ability to run stand-alone, outside a Blue Team environment for other DoD customers
- Facilitate the development of an ICS/SCADA Knowledge Base

What is GRASSMARLIN?

- Passive Network Mapping Tool
- Lightweight, Java Based graphical tool
- Can be used to do some initial analysis work but is **not an analysis engine**
- Runs in Windows and some versions of Linux
- Two views: Logical and Physical

GRASSMARLIN



Total network stats:
Total networks: 3

WORKSTATION	0
OTHER	0
UNKNOWN	3
ICS_HOST	4
HMI	0
MTU	0
RTU	0
PLC	0
FIREWALL	0
NETWORK_DEVICE	0
PROTOCOL_CONVERTER	0
IED	0

Network Name: 192.168.1.0/24

WORKSTATION	0
OTHER	0
UNKNOWN	1
ICS_HOST	4
HMI	0
MTU	0
RTU	0
PLC	0
FIREWALL	0
NETWORK_DEVICE	0
PROTOCOL_CONVERTER	0
IED	0

Network Name: 255.255.255.0/24

WORKSTATION	0
OTHER	0
UNKNOWN	1
ICS_HOST	0
HMI	0
MTU	0
RTU	0
PLC	0
FIREWALL	0

```
GRASSMARLIN
⊟ Network - networkIP: 192.168.1.0, subnetMask: 255.255.255.0, name: 192.168.1.0/24
    ⊞ ICS_HOST: role: UNKNOWN, name: 192.168.1.50, nic vendor: VMware, Inc.  fingerprints: {EtherNetIP (CIP) Explicit Messaging (UDP) - Reque
    ⊞ ICS_HOST: role: UNKNOWN, name: 192.168.1.103, nic vendor: PRONET GMBH  fingerprints: {Rockwell Encapsulation=5, EtherNetIP UDP List
    ⊞ ICS_HOST: role: UNKNOWN, name: 192.168.1.106, nic vendor: Rockwell Automation  fingerprints: {Rockwell Encapsulation=5, EtherNetIP UD
    ⊞ ICS_HOST: role: UNKNOWN, name: 192.168.1.2, nic vendor: VMware, Inc.  fingerprints: {EtherNetIP (CIP) Explicit Messaging (TCP) - Reques
    ⊞ ? UNKNOWN: role: UNKNOWN, name: 192.168.1.102, nic vendor: Dell Inc.  fingerprints: {}
⊟ Network - networkIP: 255.255.255.0, subnetMask: 255.255.255.0, name: 255.255.255.0/24
    ⊞ B UNKNOWN: role: UNKNOWN, name: 255.255.255.255 fingerprints: {}
⊟ Network - networkIP: 224.0.0.0, subnetMask: 255.255.255.0, name: 224.0.0.0/24
    ⊞ UNKNOWN: role: UNKNOWN, name: 224.0.0.252 fingerprints: {}
```

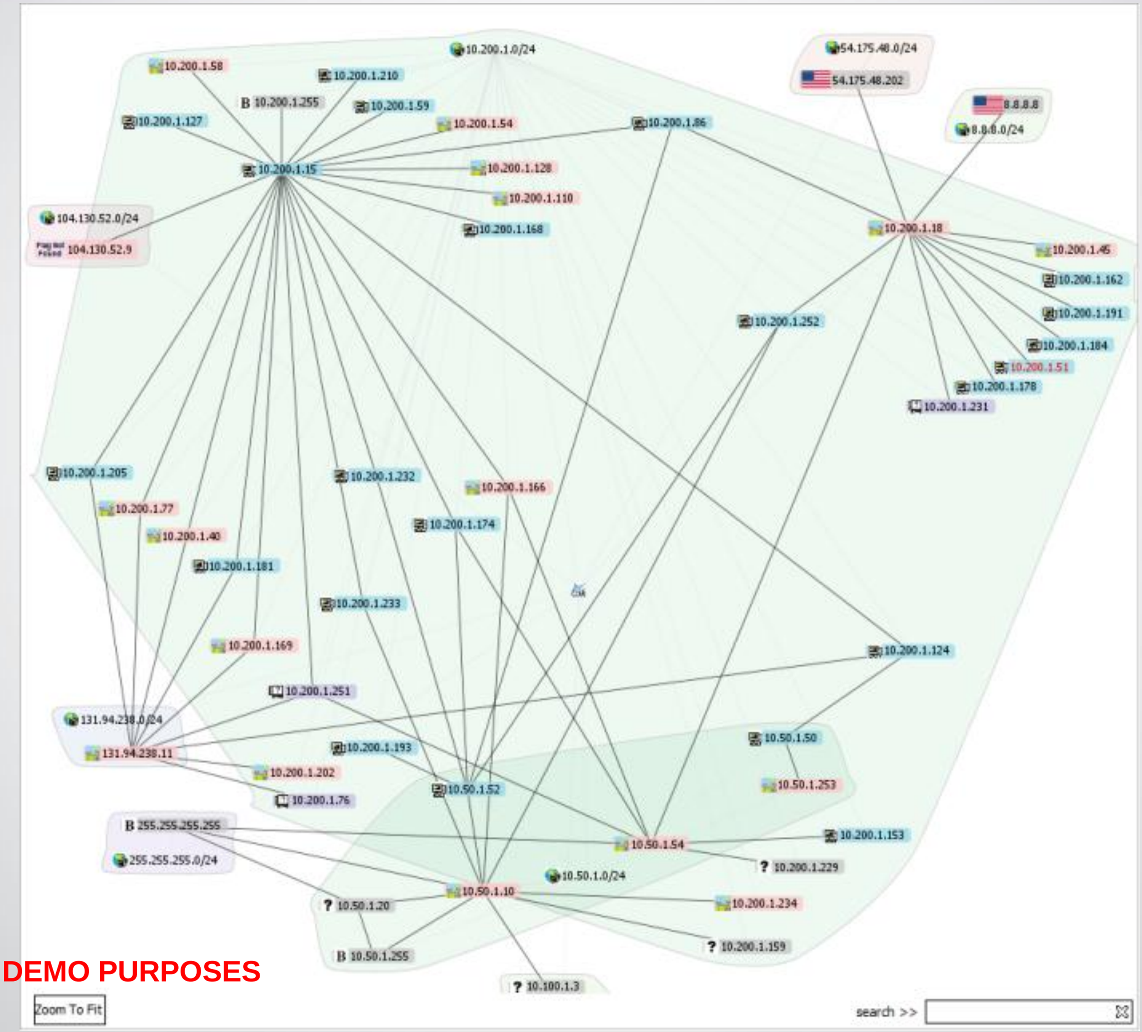
Name	Type	Message	Progress	Date	Started	Elapsed	Active
Session Cleared	GUIEVENT	Session was cleared	0/0	06/10/2014	11:32:14	0 ms	false
Rebuild Physical View	GUIEVENT	Rebuilding physical vi…	1/1	06/10/2014	11:32:14	3 ms	false
File Import	PARSEREVENT	Processing item 1 of …	1/1	06/10/2014	11:33:05	920 ms	false

Memory Utilization: 85/910(%9.37)

Progress: No running tasks.

ALL IPs USED ARE FOR DEMO PURPOSES

Current Capabilities
Logical View



ALL IPs USED ARE FOR DEMO PURPOSES

Current Capabilities Logical View

- Map IP networks from PCAPs
- Ability to do live capture
- Draws a logical map of connections: both one way and two way connections
- Ability to bring up a specific packet in Wireshark
- All traffic (live or ingested) is run against the knowledge base

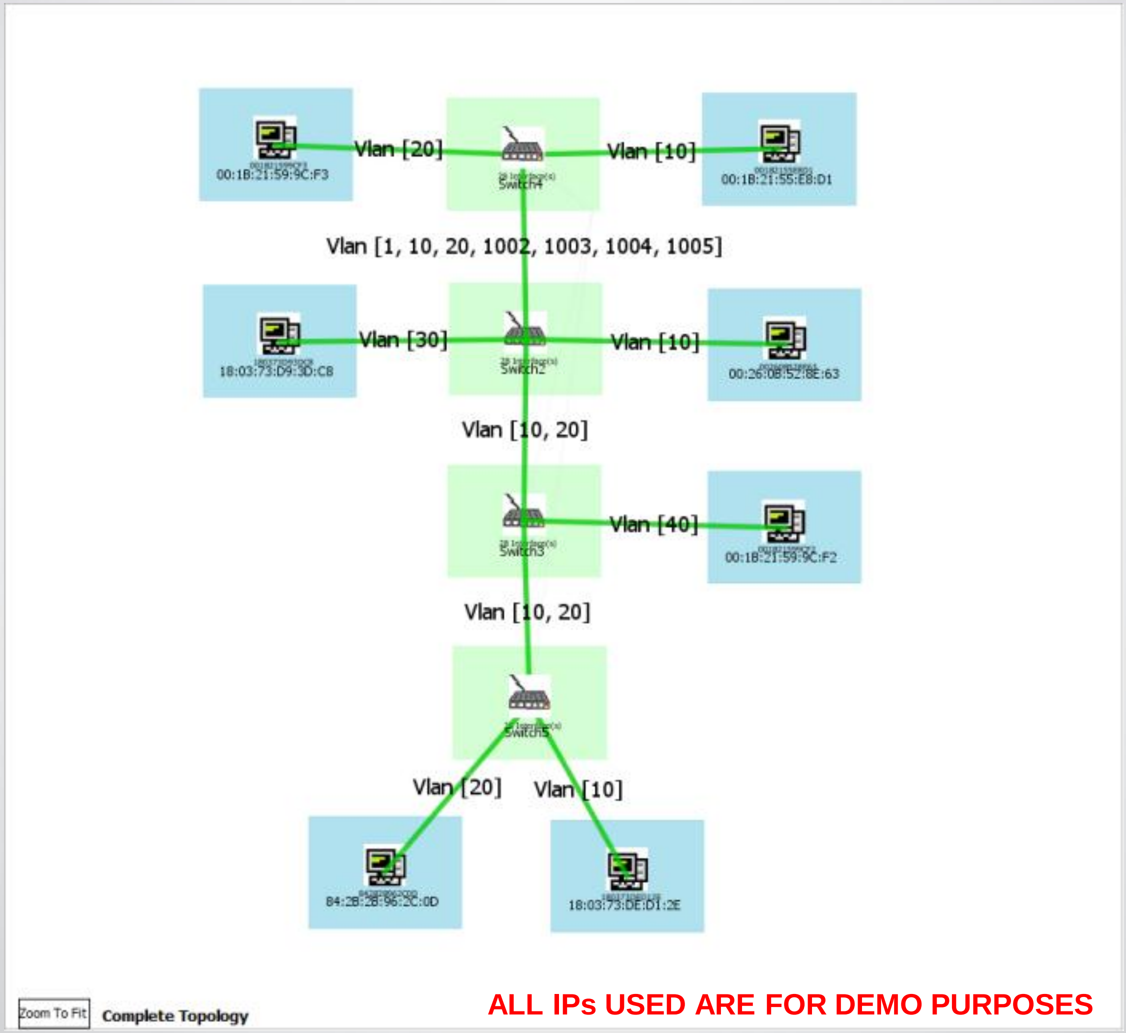
Knowledge Base

- Consists of the GeoIP database, fingerprints and Vendor IDs
- Displays the country's flag based on the GeoIP
- Vendor IDs identify the vendor of the Network Interface Card (NIC)
- Currently over 100 fingerprints, but continues to expand as we get more data
- Fingerprints are based on the contents of the individual packet
- Ability for users to create custom fingerprints

Current Capabilities
Physical View

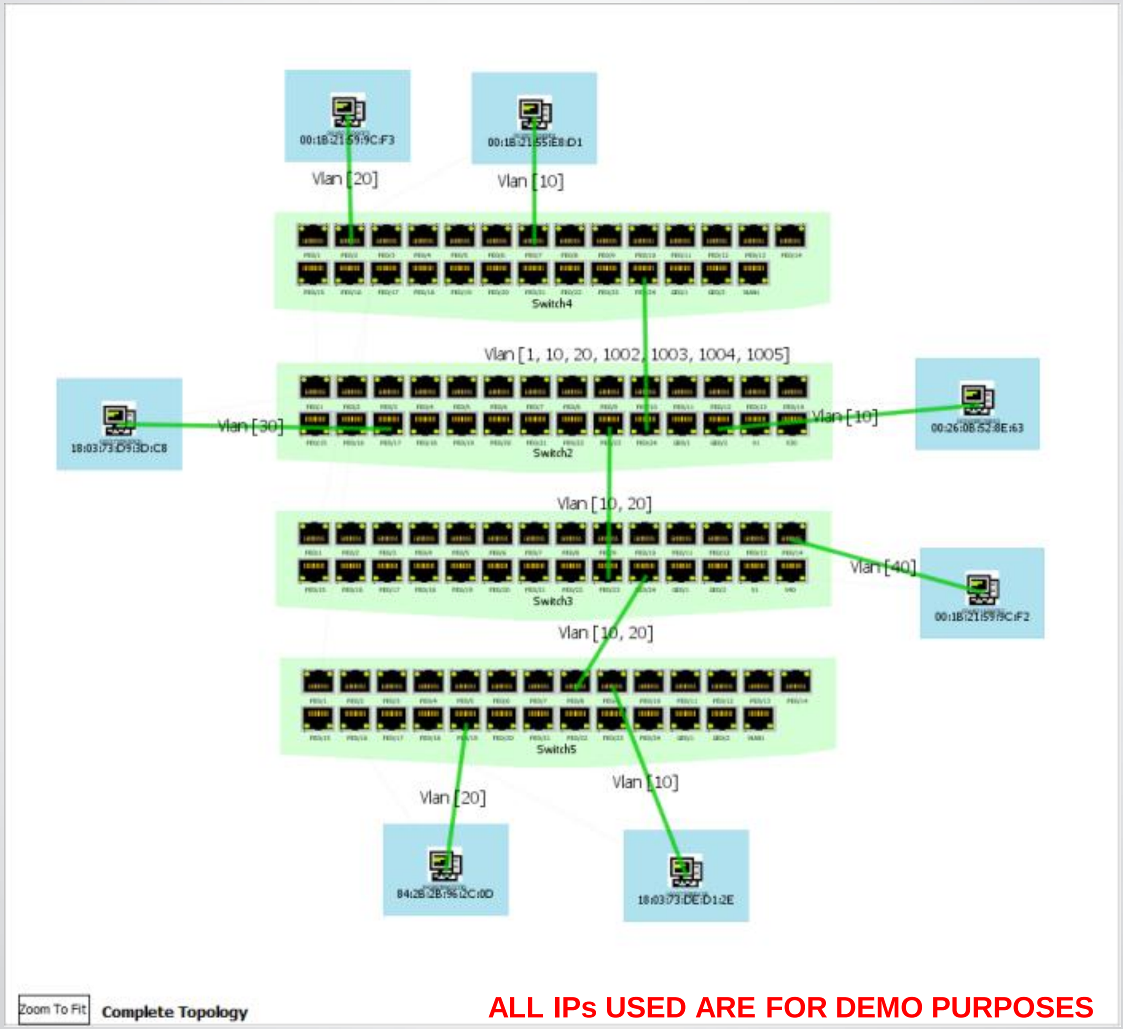
- Phase 1 of implementation
- Renders a visual representation of the physical network
- The current implementation of the physical view can only be rendered through the ingest of the results of “show” commands.
- Requires the result of three Cisco commands
  - *show running-config*
  - *show ip arp *OR* show mac address-table*
  - *show interfaces*

Current Capabilities
Physical View



ALL IPs USED ARE FOR DEMO PURPOSES

Current Capabilities
Physical View



ALL IPs USED ARE FOR DEMO PURPOSES

Common Misconceptions

- GM is currently limited to ingest smaller size pcaps (About half your available memory)
- Cannot ingest GB upon GB of data
- Shows when hosts appear in a network but does not remove the host if the host leaves the network
- Is not meant to turn hosts red or do intrusion detection
- **Can only see and map hosts based on where you are capturing data from**
- Not an active tool
- Cannot capture serial data

Questions?