NASA's IV&V Program
Safety and Mission Assurance (SMA) Office
Information Assurance/Cybersecurity Support

NASA Blue Team: Determining Operational Security Posture of Critical Systems and Networks

Adam Alley | 681.753.5273
adam.d.alley@nasa.gov

http://www.nasa.gov/centers/ivv

BT-VAP - Overview

- Blue Team Vulnerability Assessment Program (BT-VAP) Defined:

  An evaluation to ascertain the operational security posture of an agency's critical systems/networks; focusing on the IT assets & supporting infrastructures that enable the mission to operate

- Blue Team refers to the tactics and techniques employed: a blue team is done in full coordination with the mission elements being assessed in a transparent manner with no impact to mission ops

- As BT-VAP evaluates missions "end-to-end"; it is often perceived (incorrectly) as duplicative of other assessment type activities:

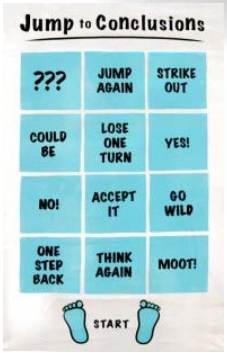
Blue Team VAP Evaluation Focus	Focus of Other Assessment Type Activities
Determine Operational Security Risk Posture	FISMA: State of Regulatory Compliance (per NIST 800-53)
Assist Mission Elements to understand/mitigate Security Risks	Audits: Detecting fraud or error/ evaluate adequacy of controls
Comprehensively Assess all factors (backups, infrastructure etc)	Pen Test: Simulate attack on asset(s) to discover vulnerabilities
Fully evaluate without disrupting mission operations	IG: Examine actions of a government agency; focus on misuse

BT-VAP - Team

- Need for a Blue Team to comprehensively evaluate CS-IA factors in a methodical manner results in needing Subject Matter Expertise across multiple areas to focus on this specific evaluation
- Use of a "risk jury" with SMEs from multiple disciplines with varying perspectives to provide a comprehensive "360°" assessment view

Five Key Role Specialists on this BT-VAP Risk Jury:

Security Analyst / Threat Protection	***Network Security / Information Assurance***	***ICS / SCADA / Computer Network Defense***	***Space Systems / Program Protection***	***Software Security / Cybersecurity Operations***



We evaluate an organization "top to bottom" (from policy/plans to operational posture) to examine IF and HOW they address CS-IA risk factors to determine what their operational security posture is compared to other similar environments

CS-IA = Cybersecurity - Information Assurance

BT-VAP - Testing Capabilities

- **<u>Cybersecurity Evaluation:</u>** determine critical assets, model the "mission thread" that these critical assets use to enable the mission – then do a selective "deep dive" on potential points of vulnerability based on a test plan & approved rules of engagement to cover:
  - Space/Mission Systems (ground)
  - Industrial Control Systems/SCADA
  - Supporting Infrastructure: (Layer-2/Layer-3 Network Devices, Controlled Interfaces/Firewalls, Cybersecurity Defense (CND) mechanisms, etc)
- **<u>Software Security Evaluation:</u>** analyze the software code base which supports critical assets and mission threads
  - Source Code Analysis
  - Binary/Compiled Code Analysis (S/W Origin Analysis)
- BT-VAP Testing Techniques involve a combination of three principal methods:
  - Analytic/Tabletop Analysis
  - In the Lab Testing (modeling-simulation environment)
  - On-Site with a "flyaway" team with mobile assets

We evaluate an organization to examine IF and HOW they address CS-IA risk factors to determine what your operational security posture is compared to other similar environments

CS-IA = Cybersecurity - Information Assurance

BT-VAP - Process

Blue Team VAP coordinates and collaborates with the elements being assessed in order to identify, analyze and evaluate the security risks to critical systems which increasingly rely on a diverse set of IT assets, **without disrupting** *mission operations.*

- Risk Assessment of Missions (from an "outsiders" perspective)
  - Threat & Scope Analysis (TSA) produced using only publically available information
- Site Survey to Finalize Assessment Scope & Perform Data Collection Activities
- Test Planning Phase
  - Rules of Engagement (RoE) & Test Plan for selected mission threads
  - Network Topology modeled (inc. routers, firewalls, & subnets)
  - Host Vulnerability Data overlaid with Network Model
  - Mission Threads with supporting infrastructure (inc. DNS, LDAP, SCADA, etc.)
- Active Assessment Phase
  - Fly-Away team travels on-site to conduct "on-site" testing
- Analysis & Reporting
  - Document detailed evaluation findings; Provide outbrief and final report

BT-VAP Activities

- Scope the Assessment
- Collect network based configurations (layer 2/3)
- Build out network topology in modeling tool
- Collect vulnerability credentialed scans on assets*
- Perform binary analysis on custom mission software
- Perform source code analysis of custom mission software
- Ingest host-based scan data and results of code analysis into model
- Perform detailed path analysis on critical data flows
- Conduct in-depth interviews and analysis
- Identify all access points into the networks
- Validate critical findings*
- Demonstrate potential exploitation scenarios*

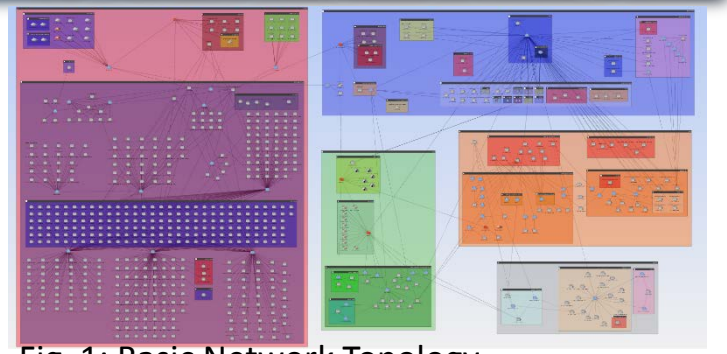


Fig. 1: Basic Network Topology

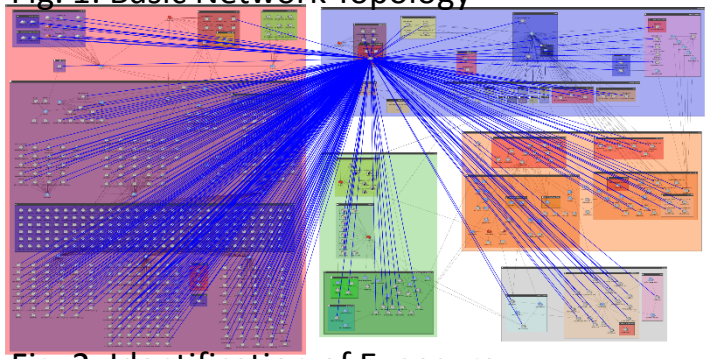


Fig. 2: Identification of Exposure

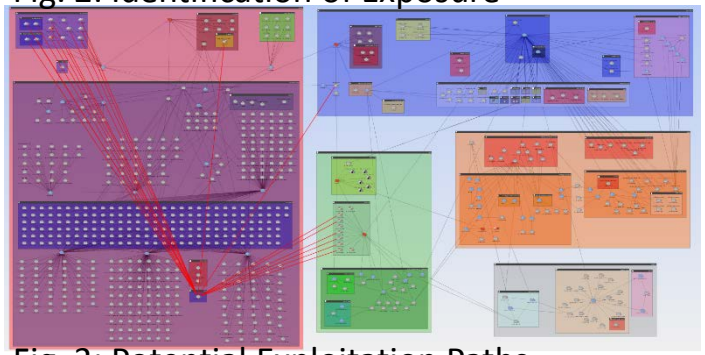


Fig. 3: Potential Exploitation Paths

* Unique virtualization approach deployed to limit impact during assessment. Create virtual "snapshots" of critical assets to perform testing against.

BT-VAP Tools

IV&V Cyber

Activity

"Credentialed" Vulnerability Scans

Mapping of Network Topology:
Layer 2 & 3
Firewalls
CND

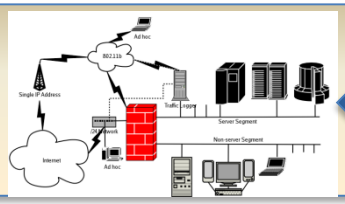
Evaluate Telecommunications Paths for diversity and security

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

- Acquire Snapshot of Critical hosts/servers
- Mock up in Lab
- Scan with host based Tools
- Ingest results of scans Into Modeling tool
- Custom S/W Scans

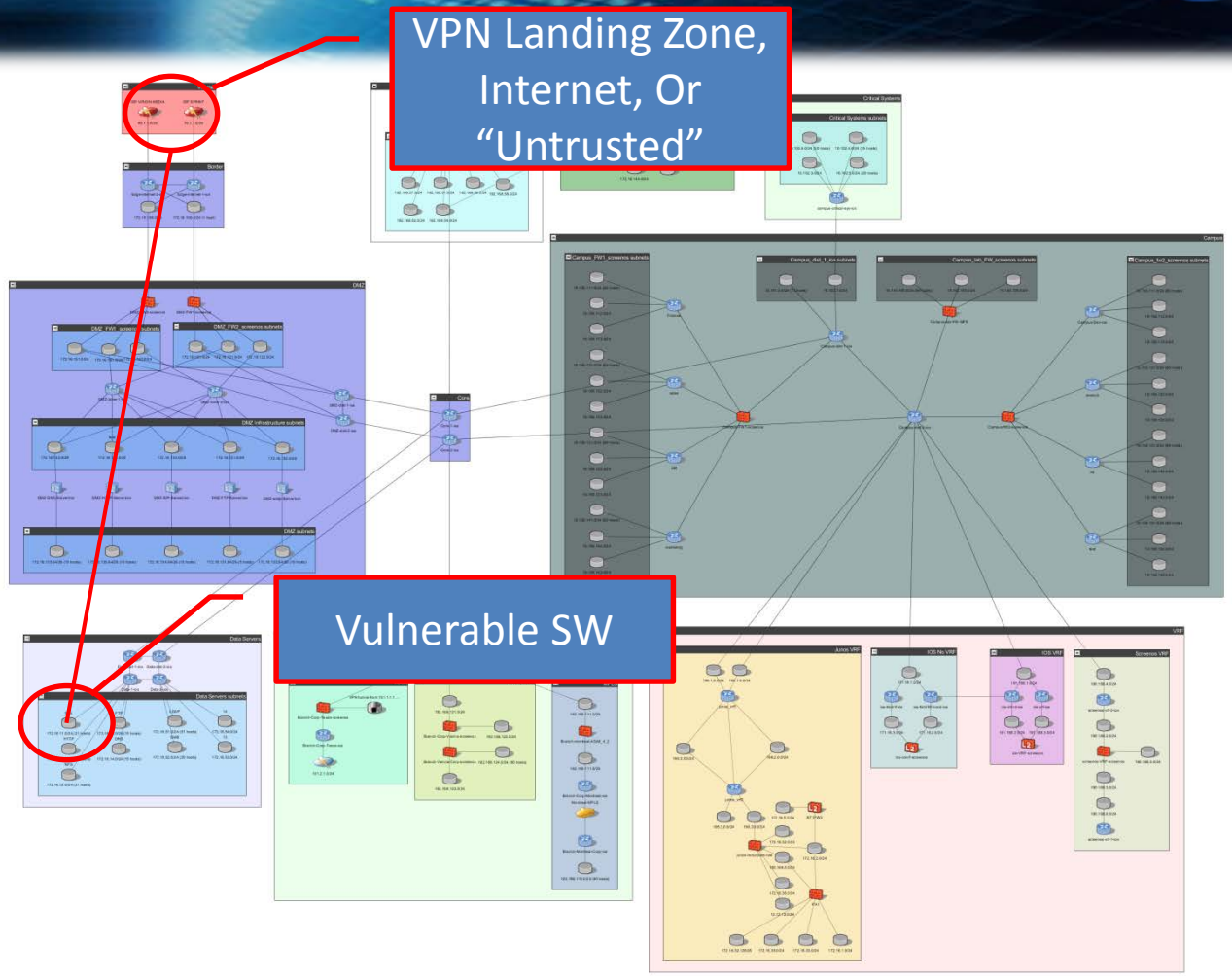
- Provide customer with "Show" commands to run during non-peak times
- Ingest configuration files Into Modeling tool

Reverse engineer all Physical pathways



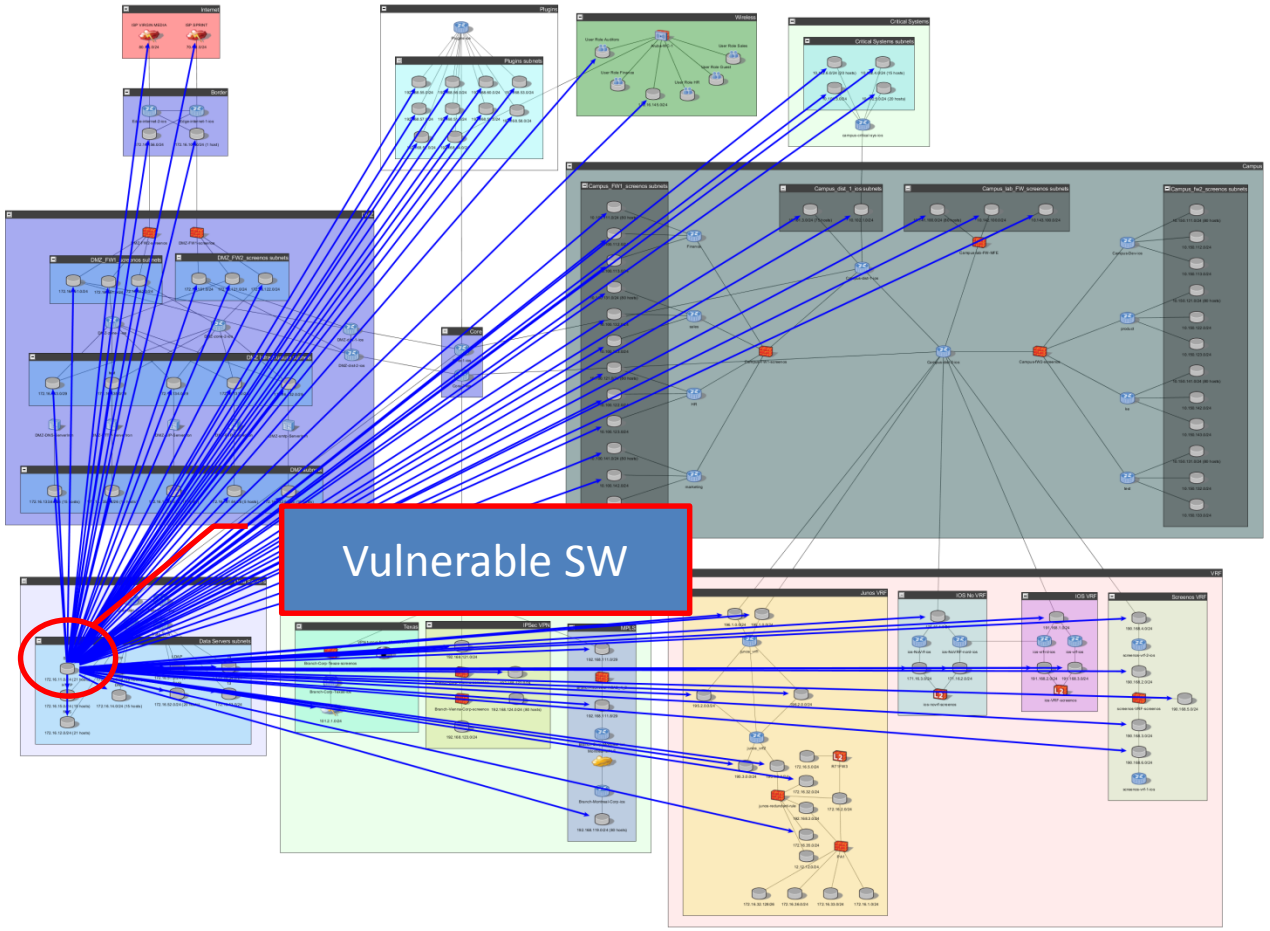
JSTAR Cyber Lab
Fairmont, WV

Sample Exposure



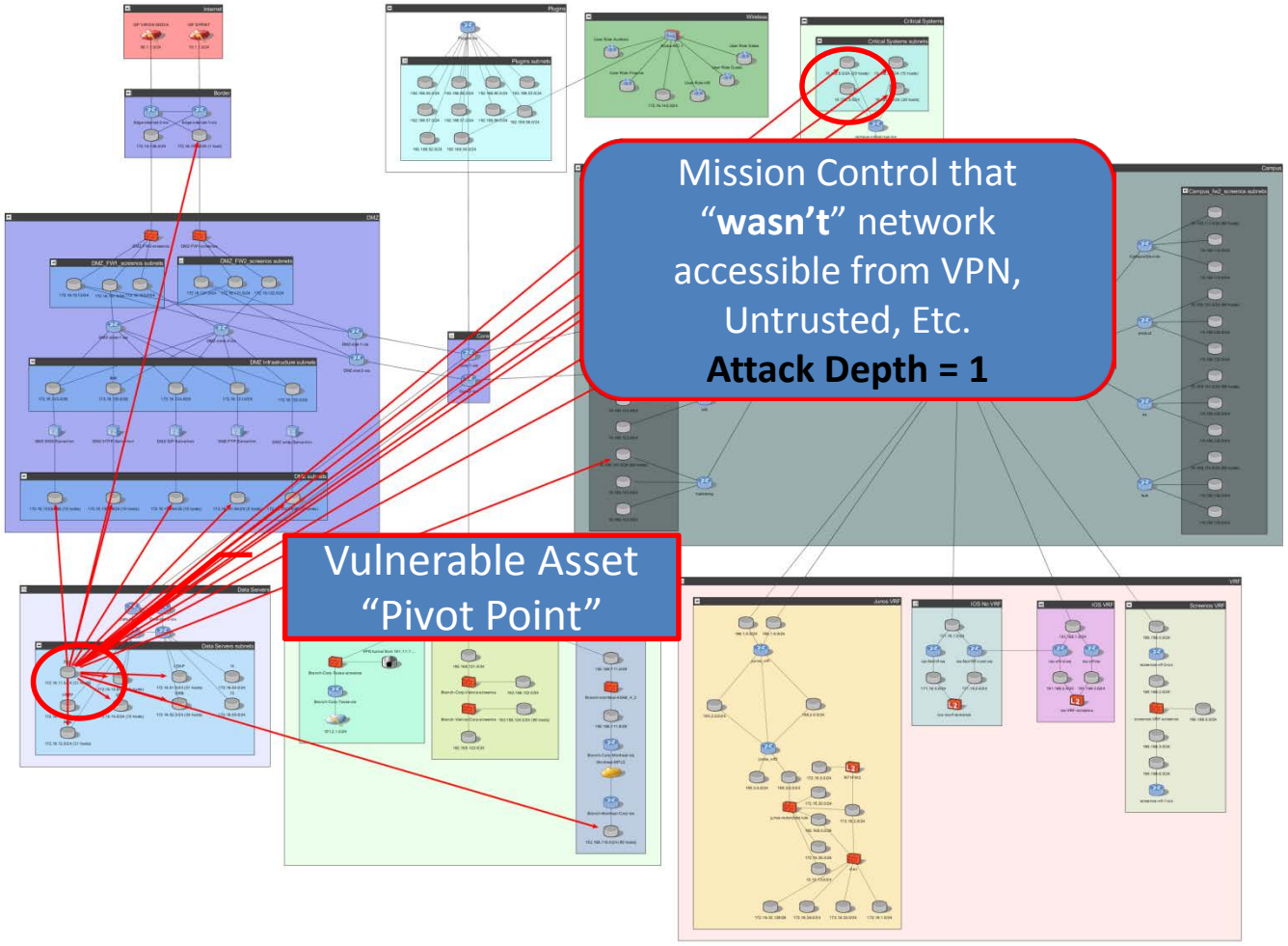
Demonstrates that a pathway exists from the VPN Landing Zone, Internet, Or Untrusted to a vulnerable piece of software

Sample Exposure



Demonstrates all outbound access paths (**Pivoting**) from the vulnerable asset

Sample Exposure



Demonstrates potential vulnerabilities that could be exploited from this server

Lessons Learned: Space Mission Systems

- Tend to be quite different from enterprise (business) systems
  - Tend to include a lot of custom code/customized solutions that are not found in very many places
  - Difficult to modify/patch – unless designed/engineered carefully can be difficult to evaluate (test strings do not always represent the operational environment)
  - Older systems were not designed/engineered to function in a contested, high threat environment (i.e. the Internet)
  - Frequent Lack of Knowledge on exactly what it takes to operate existing systems (ports, protocols, settings)
  - Most space/mission ground systems lack situational awareness capabilities to monitor functionality/performance/security
  - Limited attention paid to the security testing of mission software
  - Designed to be a stovepipe – when joined to other multi-mission environments and moved to an IP enabled architecture, the threats and the attack surface they are exposed to grows exponentially

Lessons Learned: Summary

- Some assets are more critical than others
- Some vulnerabilities are more critical than others
- Different methods of evaluation will yield different results
- The state of A&A documentation does not always match the security posture of the asset
- Most service providers are not fully aware of the traffic on their network; thus detecting what is not “normal” via security monitoring is difficult

BT-VAP Deliverables

- Network Topology Model (routers, firewalls, & subnets)
  - Provides the "ground truth" of network architecture
  - Allows near-real time analysis of network access/exposure
- Host vulnerability data overlaid with Network Model
  - Provides ability to analyze the overall security posture of each mission should vulnerable components become compromised
- Mission Threads
  - Depicts the components required to perform the critical functions of each mission in a set of diagrams
    - Inc. Routers, Firewalls, Servers, supporting assets, etc.
- Final Report: detailing results, analysis and prioritized set of recommendations

BT-VAP Debrief at the conclusion of the active assessment will include preliminary results, analysis and recommendations to enable stakeholders to make more informed decisions on balancing risks to the security posture of missions evaluated

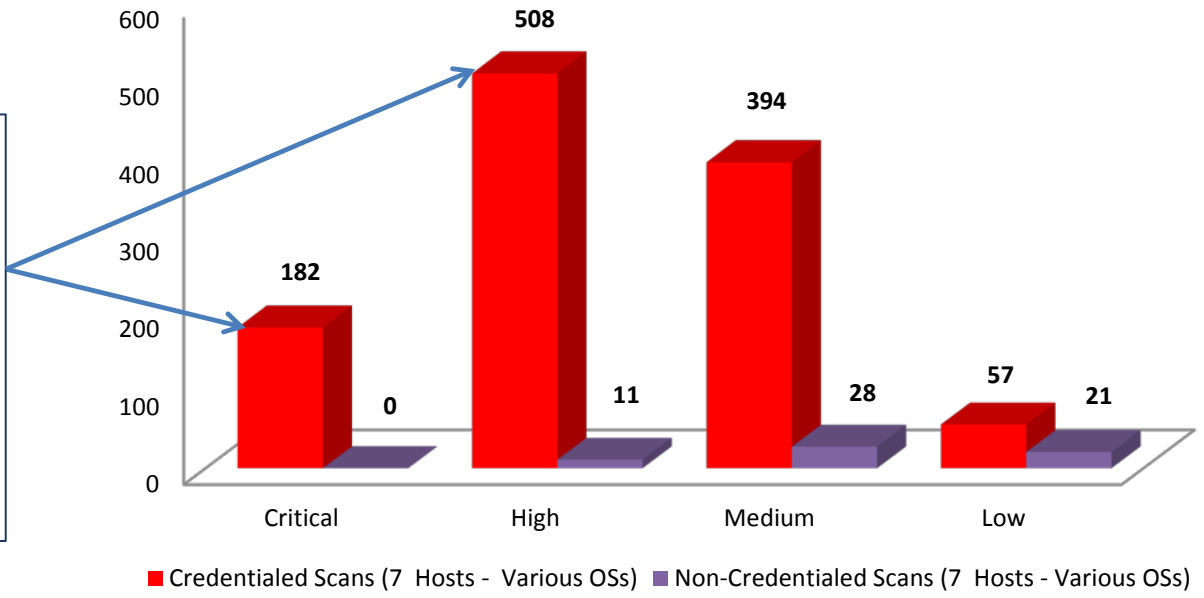
BACKUP SLIDES

Emerging Threats…

- Emergence of Cybersecurity has increased the focus on security risks to Information Technology (IT) assets – going beyond "traditional" Information Assurance (IA) concerns:
  - More sophisticated threats have emerged from increasing sources as advanced "hacker" tools and techniques have emerged and proliferated to broaden the "attack surface" available across globally interconnected networks
- As systems and infrastructures become increasingly interconnected the IT security posture of the linkages between networks, systems and supporting infrastructures has become increasingly difficult to understand, to provide, and to evaluate which requires:
  - **Mission Understanding:** how mission functions are being performed on an "end-to-end" basis and their supporting IT base in order to identify critical assets (e.g. "crown jewels")
  - **Information Technology/Information Assurance:** how to apply security principles to IT assets in order to provide Confidentiality, Integrity and Availability
  - **Ability to evaluate Software security:** is critical as modern system capabilities are increasingly shaped & implemented by software components – as this testing is an emerging discipline - detecting flaws at random intervals occurs frequently in most software code packages
  - **Address Industrial Control Systems (ICS):** an increasing target of choice for many threats as most of these systems are not designed to operate in a high threat environment

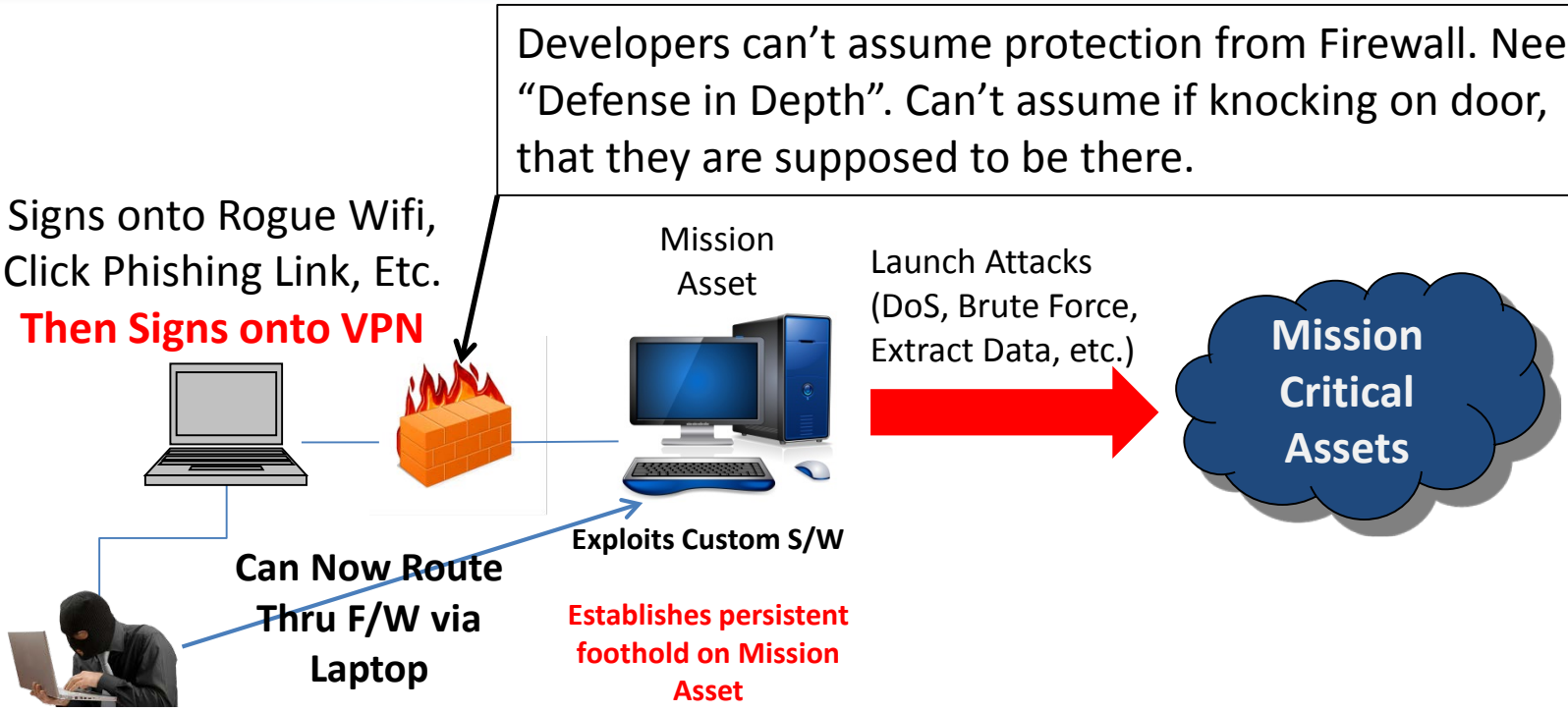
Cred vs Non Cred Scans

Not performing credentialed scans misleads missions to think their security posture is better than it really is



Back

Example SW Impacting Mission



This example will depict how unsecure software within a network can potentially impact critical mission assets

Open Source Scanning

Vulnerability	Affected File	Mitigation
CVE-2006-1546: Allows remote attackers to read or write data belonging to a signed applet.	XXXXXX.jar	Upgrade Jar file to 1.2.9 or newer
CVE-2006-1547: Allows remote attackers to cause a denial of service via a multipart/form-data encoded	XXXXXX.jar	N/A (new versions exist but also contain vulnerabilities). Implement host based restrictions (i.e., IP tables, file integrity detection, Host based IDS)
CVE-2013-4002: Allows remote attackers to affect availability via unknown vectors.	XXXXXX.jar	N/A (new versions exist but also contain vulnerabilities). Implement host based restrictions (i.e., IP tables, file integrity detection, Host based IDS)
CVE-2013-4002: Allows remote attackers to affect availability via unknown vectors.	XXXXXX.jar	N/A (new versions exist but also contain vulnerabilities). Implement host based restrictions (i.e., IP tables, file integrity detection, Host based IDS)
CVE-2014-0107: Allows remote attackers to bypass expected restrictions and load arbitrary classes or access external resources via a crafted messages	XXXXXX.jar	Upgrade Jar file to 2.7.2 or newer
CVE-2014-0114: Allows remote attackers to "manipulate" the ClassLoader and execute arbitrary code via the class parameter	XXXXXX.jar	N/A (new versions exist but also contain vulnerabilities). Implement host based restrictions (i.e., IP tables, file integrity detection, Host based IDS)
CVE-2015-0254: Allows remote attackers to execute arbitrary code or conduct external XML entity (XXE) attacks	XXXXXX.jar	Upgrade Jar file to 2.7.2 or newer
CVE-2003-1516: Allows remote attackers to read or write data belonging to a signed applet.	XXXXXX.jar	Upgrade Jar file to 2.7.2 or newer
CVE-2007-4575: Allows user-assisted remote attackers to execute arbitrary Java code via crafted database documents	XXXXXX.jar	Upgrade to Jar file 1.8.0.10 or newer
CVE-2010-2227: Allows remote attackers to cause a denial of service (application outage) or obtain sensitive information via a crafted header	XXXXXX.jar	N/A (new versions exist but also contain vulnerabilities). Implement host based restrictions (i.e., IP tables, file integrity detection, Host based IDS)
CVE-2011-2894: Allows remote attackers to bypass intended security restrictions and execute untrusted code	XXXXXX.jar	Upgrade to Jar file 3.0.6. or newer

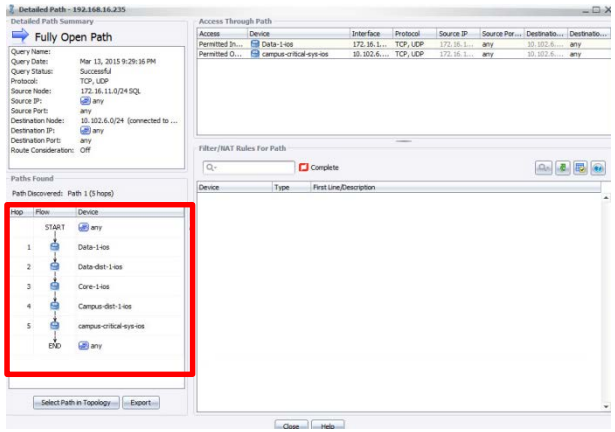
Back

Source Code Analysis

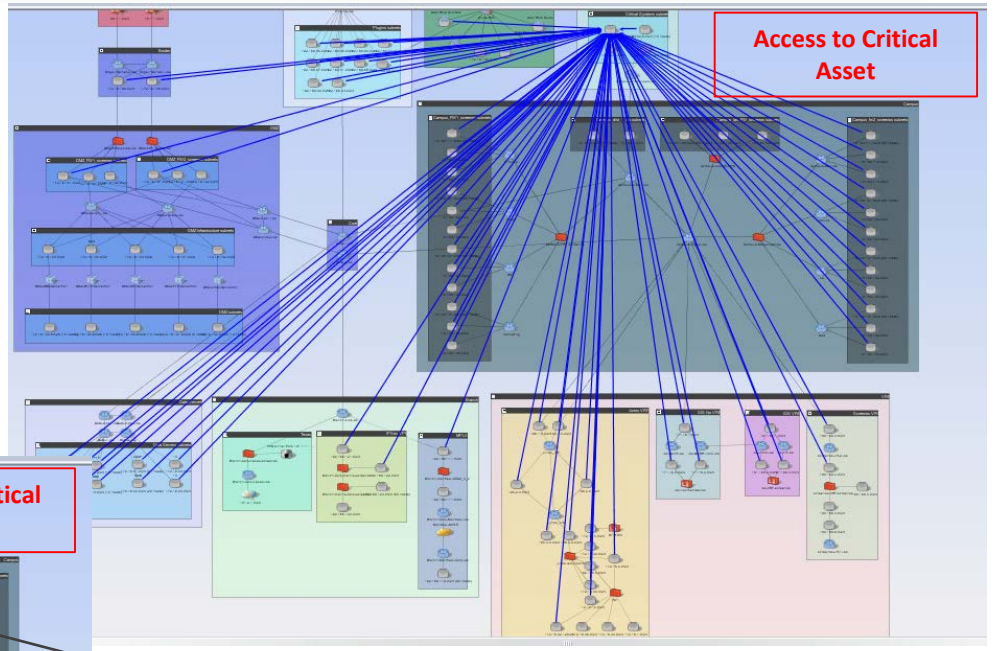
SCA Tool's Default Security Categorization	
Critical	XXXXXX
High	
SANS Top 25 Most Dangerous Software Programming Errors	
Insecure Interaction - CWE ID 078	XXXXXX
Insecure Interaction - CWE ID 079	
Insecure Interaction - CWE ID 089	
Insecure Interaction - CWE ID 601	
Porous Defenses - CWE ID 798	
Risky Resource Management - CWE ID 022	
Porous Defenses - CWE ID 807	
Porous Defenses - CWE ID 863	
OWASP Top 10 2013	
A1 Injection	XXXXXX
A2 Broken Authentication and Session Management	
A3 Cross-Site Scripting (XSS)	
A4 Insecure Direct Object References	
A5 Security Misconfiguration	
A6 Sensitive Data Exposure	
A9 Using Components with Known Vulnerabilities	
A10 Unvalidated Redirects and Forwards	

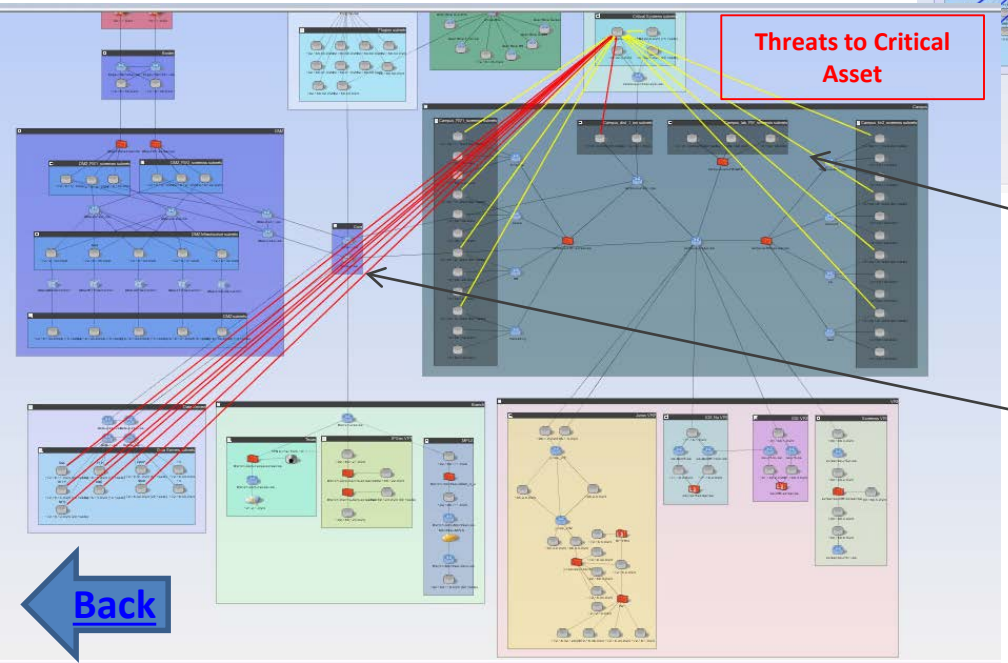
Back

Detailed Path Analysis



Shows all devices on critical path





Indirect exposure is vulnerabilities that can be exploited from “untrusted” address space via leapfrog (pivot) through a different trusted source

Direct exposure is vulnerabilities that can be exploited directly from “untrusted” address space

Back

Analysis Example

IV&V Cyber

Public Threats CA

Source Host	Source IP	Target Host	Target IP	Protocols	Ports	Exposure	Vulnerability	Severity	Impact	Patch	Type	On Attack Path	Ticket	Known Exploit	CVE Description
Untrusted	Internet*, 1.1.255.255	X.X.nasa.gov	X.X.X.X	TCP	80	0.938	CVE-2014-3513	HIGH	A	Yes	CONFIRMED	Yes		None	Memory leak in d1_srtp.c in the DTLS SRTP extension in OpenSSL 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted handshake message.
Untrusted	Internet*, 1.1.255.255	X.X.nasa.gov	X.X.X.X	TCP	21	0.789	CVE-2001-1335	MEDIUM	C	No	CONFIRMED	Yes		Exploit DB Download Available	Directory traversal vulnerability in CesarFTP 0.98b and earlier allows remote authenticated users (such as anonymous) to read arbitrary files via a GET with a filename that contains a ...%5c (modified dot dot).
Untrusted	Internet*, 1.1.255.255	X.X.nasa.gov	X.X.X.X	TCP	9898	0.858	CVE-2014-3566	MEDIUM	C	No	CONFIRMED	Yes		MSF Aux	The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

Threat IP Source

Give CVE details

Exploit easily available (i.e. script kiddie threats)

Untrusted Threats CA

Source IP	Target Host	Target IP	Protocols	Ports	Exposure	Vulnerability	Severity	Impact	Patch	Type	On Attack Path	Ticket	Known Exploit	CVE Description
X.X.X.X	X.X.nasa.gov	X.X.X.X	UDP	111	0	CVE-1999-0632	LOW	A	No	CONFIRMED	No		None	The RPC portmapper service is running.
X.X.X.X	X.X.nasa.gov	X.X.X.X	TCP	443	0.99	CVE-2014-3566	MEDIUM	C	No	CONFIRMED	Yes		MSF Aux	The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.
X.X.X.X	X.X.nasa.gov	X.X.X.X	TCP	445	0.99	CVE-2015-0027	HIGH	ACI	Yes	CONFIRMED	Yes		None	Microsoft Internet Explorer 10 and 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-0035, CVE-2015-0039, CVE-2015-0052, and CVE-2015-0068.
X.X.X.X	X.X.nasa.gov	X.X.X.X	TCP	445	0.99	CVE-2014-6352	HIGH	ACI	Yes	CONFIRMED	Yes		exploit	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allow remote attackers to execute arbitrary code via a crafted OLE object, as exploited in the wild in October 2014 with a crafted PowerPoint document.
X.X.X.X	X.X.nasa.gov	X.X.X.X	TCP	445	0.99	CVE-2014-4076	HIGH	ACI	Yes	CONFIRMED	Yes		Exploit DB Download Available	Microsoft Windows Server 2003 SP2 allows local users to gain privileges via a crafted IOCTL call to (1) tcpip.sys or (2) tcpip6.sys, aka "TCP/IP Elevation of Privilege Vulnerability."

Analysis Example (cont.)

Hostname	OS			Applications /Custom Software	Host Protection				Exposure			Exploitability		
	Sup Port ed	Patc hed	Vul Ner able		HIDS	Mal ware	Iptabl es	Inte Grit y	"inter net"	UT	Trust ed	"inter net	UT	Trus ted
Host #1	Med	No	Yes	N/A	No	No	N/A	N/A	No	Yes	Yes	No	Yes	Yes
Host #2	Low	No	Yes	N/A	No	No	N/A	N/A	No	Yes	Yes	No	Yes	Yes
Host #3	Low	No	Yes	N/A	No	No	N/A	N/A	No	Yes	Yes	No	Yes	Yes
Host #4	Low	No	Yes	Yes	No	No	N/A	N/A	No	Yes	Yes	No	Yes	Yes
Host #5	Low	No	Yes	N/A	No	No	N/A	N/A	No	Yes	Yes	No	Yes	Yes
Host #6	Low	No	Yes	N/A	No	No	N/A	N/A	No	Yes	Yes	No	No	Yes
Host #7	Low	No	Yes	N/A	No	No	N/A	N/A	No	Yes	Yes	No	Yes	Yes
Host #8	Low	No	Yes	N/A	No	No	N/A	N/A	No	Yes	Yes	No	Yes	Yes
Host #9	Low	No	Yes	N/A	No	No	N/A	N/A	No	Yes	Yes	No	No	Yes
Host #10	Low	No	Yes	No	No	No	N/A	N/A	No	Yes	Yes	No	Yes	Yes

Consolidate results/analysis into graphical stoplight chart depicting each critical assets security posture to include network exposure

Back