Cyber Effects Prediction

Shane Powell, CISSP-ISSEP

Principal Systems Security Engineer

Raytheon – Network Centric Systems

Who am I?

- 14 year Army Veteran
  - Aviation Operations, Tank Commander, Drill Sergeant, Enemy Prisoner of War Collector, Arabic Voice Interceptor, Gulf War, Bosnia-Herzegovina
- Systems Security Engineer
  - Not a Hacker… interests are focused on the design and implementation of systems that are highly resilient to persistent cyber attack
- Martial Artist
  - Shorin-Ryu, Shito-Ryu, White Crane
- Straight-Up, Hard-Core, Old-School Geek!

Now the general who wins a battle makes many calculations in his temple ere the battle is fought. The general who loses a battle makes but few calculations beforehand. Thus do many calculations lead to victory, and few calculations to defeat: how much more no calculation at all! It is by attention to this point that I can foresee who is likely to win or lose.

-Sun Tzu, the Art of War

Perfect Security is a Pipe Dream…

- But, How Good is Good Enough?
  - At what point has sufficient Due Diligence been reached in understanding the security state of your information systems?
- Do you really understand:
  - If your security compliance measures will work?
  - How your networked systems might be attacked?
  - Which systems are truly critical?
  - How the failure of critical systems affect overall capabilities?
  - Your organization's ability to continue to operate when attacked?
- Cyber Effects Prediction is an analytical methodology that aids analysts and engineers by demonstrating the ability of their systems to withstand cyber attack, without exposing production systems to the risks associated with rigorous hands-on testing and analysis

Note: The term System is used interchangeably in this presentation as hosts, servers, networks, networked devices, or combinations which form LANs, Enclaves, Enterprises, etc

Background

- **Original Goal**
  - Facilitate design and planning for the execution lab based network security tests, so as to reduce errors that may occur during test execution

- **Results**
  - Identification of numerous commercial and open source tools that can be used in conjunction to model test environments and identify non-obvious events that may occur as a result of tests… aka Cyber Effects

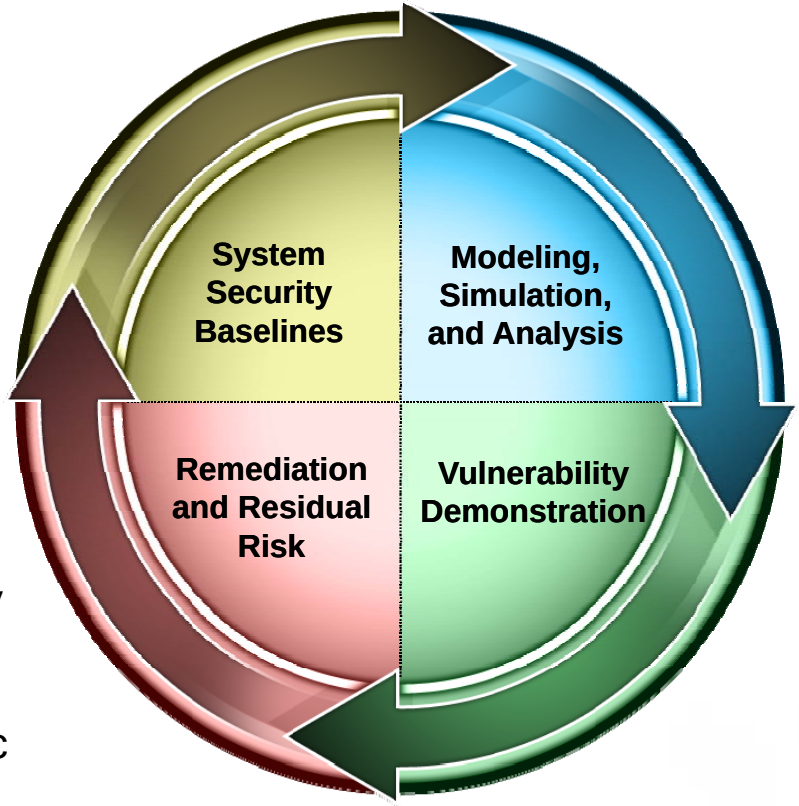
  - Analytical Methodology which allows for:
    - Modeling of network security baseline configurations
    - Analysis of attack vectors against real system configurations
    - Simulation of network conditions while under cyber attack
    - Assessment of mission impacts during system failures

What is Cyber Effects Prediction?

- The Methodology for Cyber Effects Prediction consists of four major components:

1. System Security Baselining
2. Modeling, Simulation, and Analysis
3. Vulnerability Demonstration
4. Allocation of Remediation Actions and Residual Risk

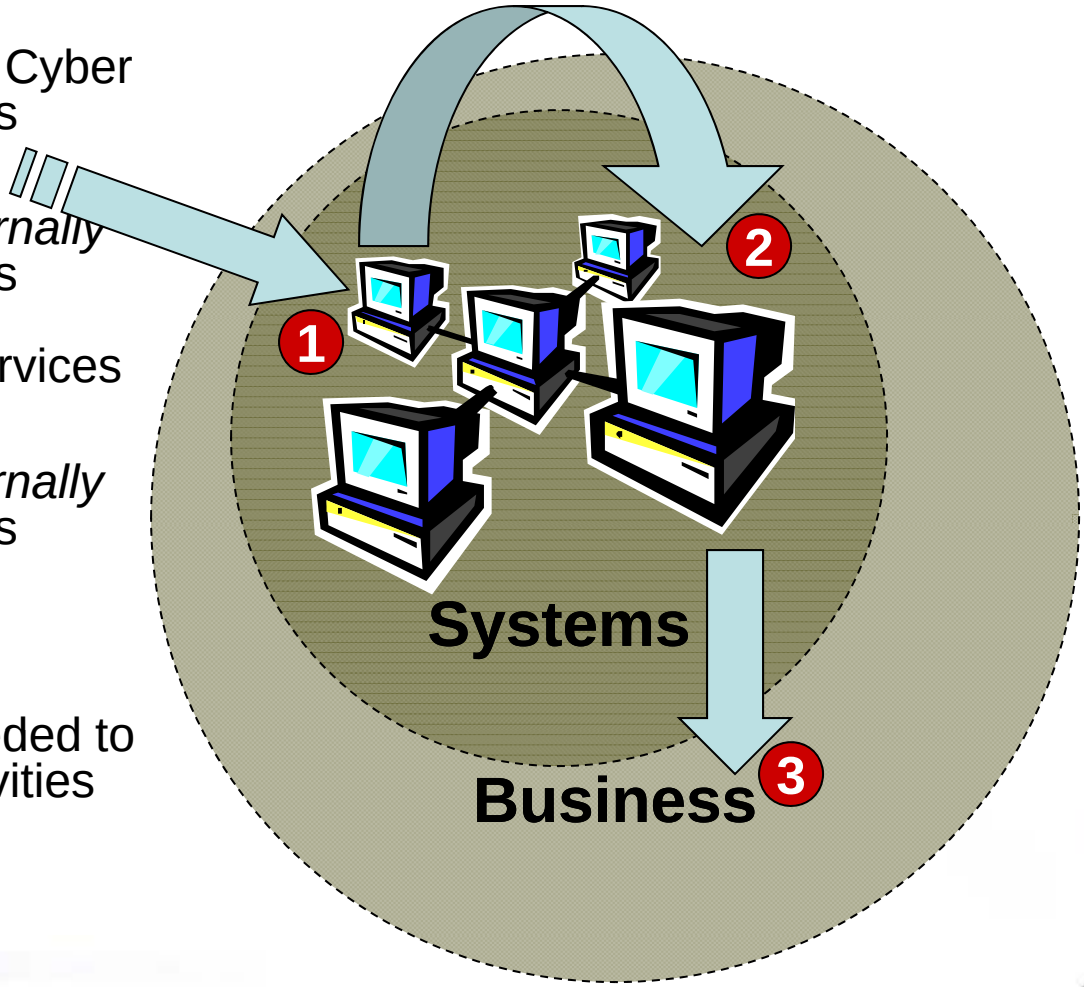
- Why is this important?
  - Vulnerability and risk assessments alone can easily mislead system owners into a false sense of security
  - Cyber Effects Prediction builds upon these tools to provide a more holistic view of a system's security state



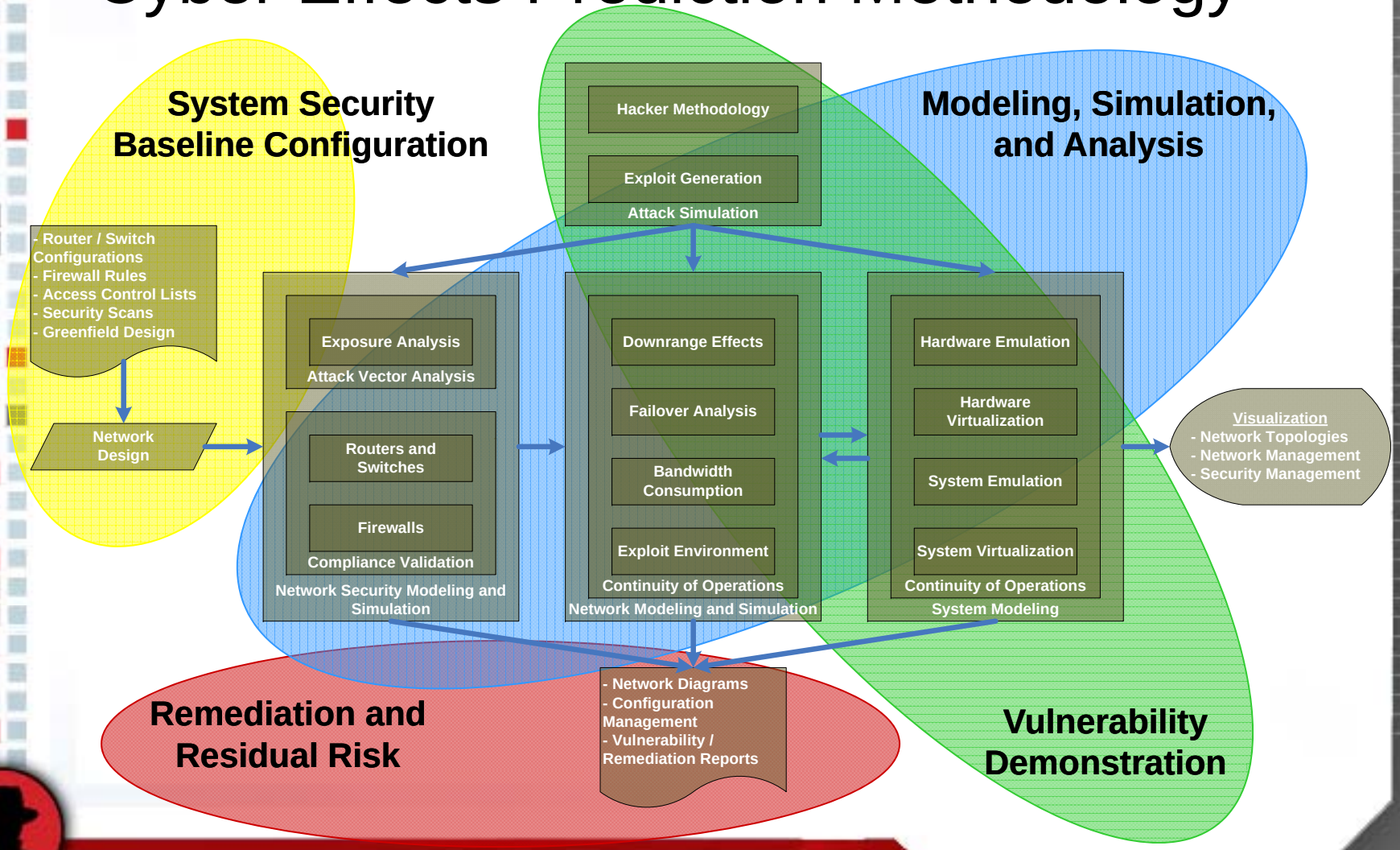
Intent of Cyber Effects Prediction

1. Identify **Primary** (*Direct*) Cyber Effects Affecting Systems
2. Predict **Secondary** (*Internally Cascading*) Cyber Effects Affecting Distributed Communications and Services
3. Postulate **Tertiary** (*Externally Cascading*) Cyber Effects Affecting Operations and Mission

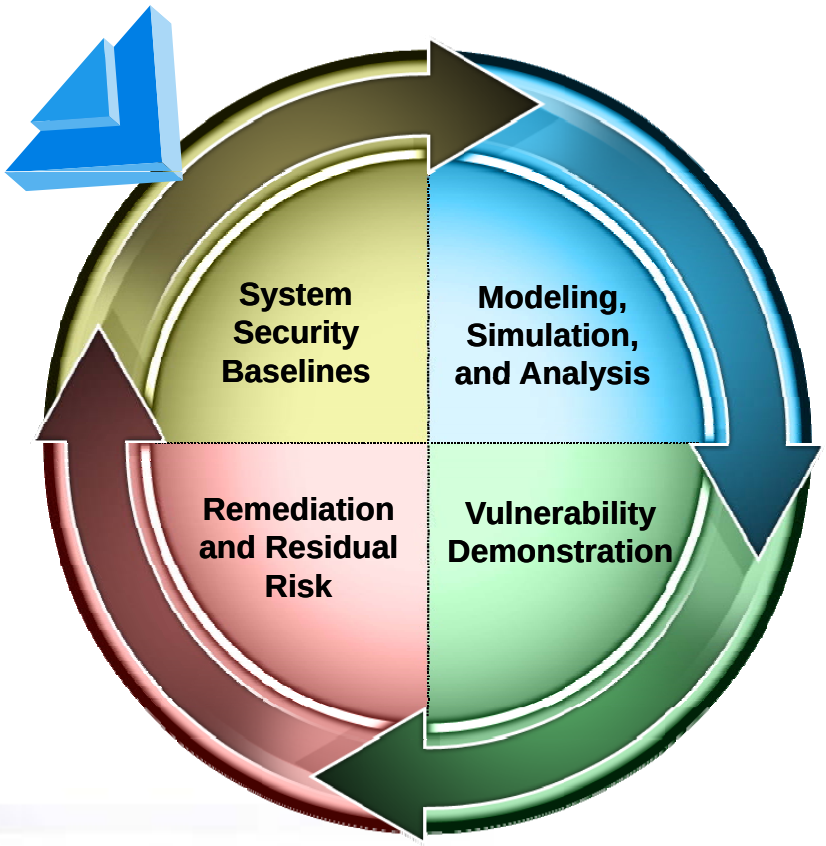
- Output – Knowledge needed to focus cyber security activities



Cyber Effects Prediction Methodology

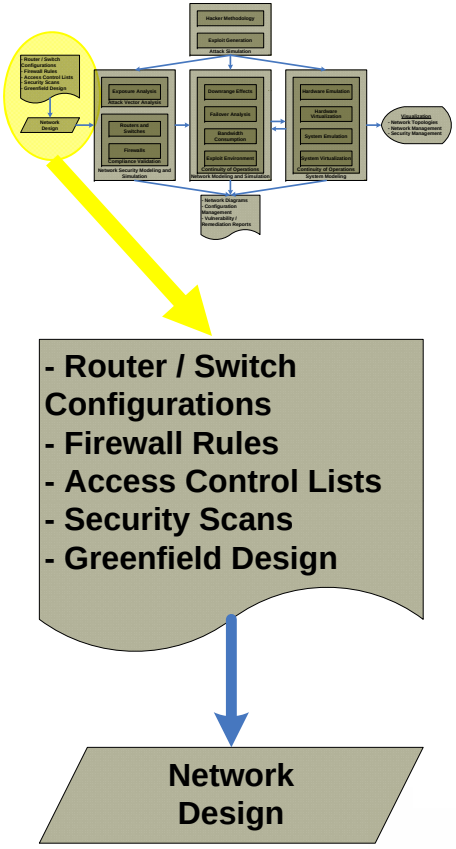


System Security Baselines



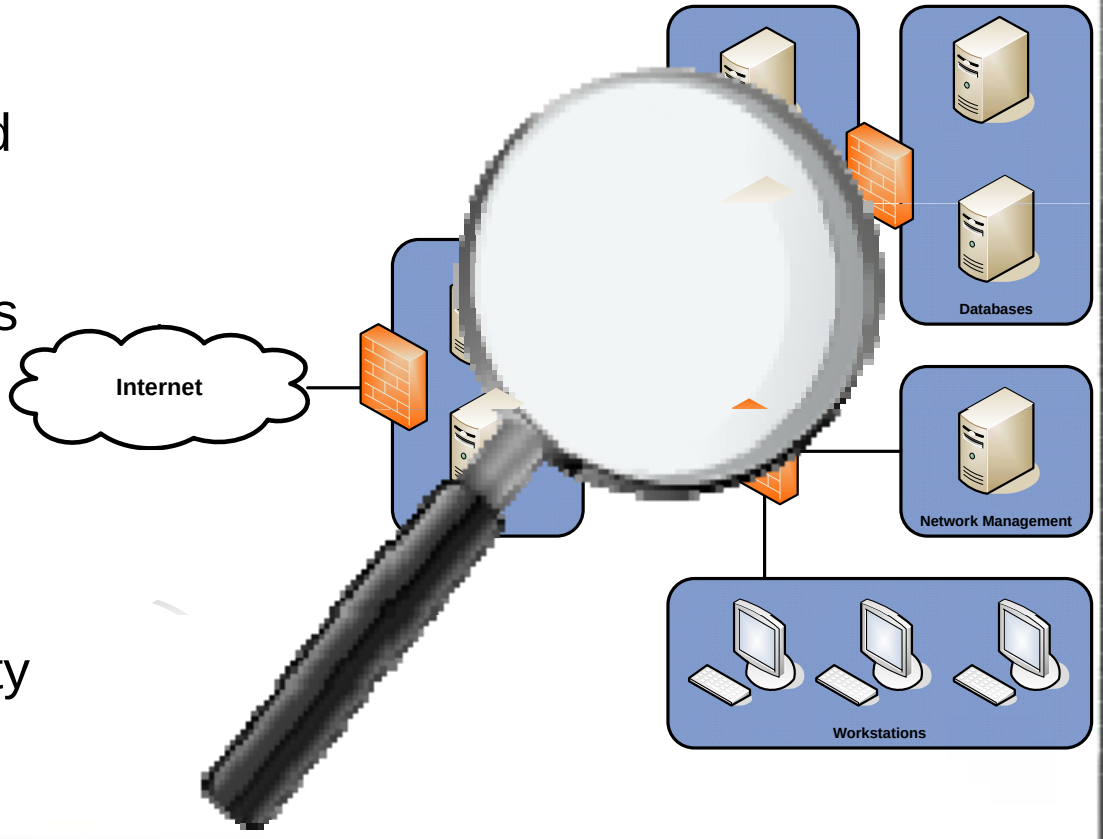
Establishing System Security Baselines

- System Security Baselines are based upon “Known” system configurations
- System Configurations are collected through common Vulnerability Assessment tools
- Require Authoritative (Credential-Based) Scans of Systems and Routing Devices
  - Authenticate to, and scan routers, switches, firewalls, and hard-to-assess devices
  - Check scan logs and verify authentication to target systems
  - Verify that scans completed for each system and device on the target network

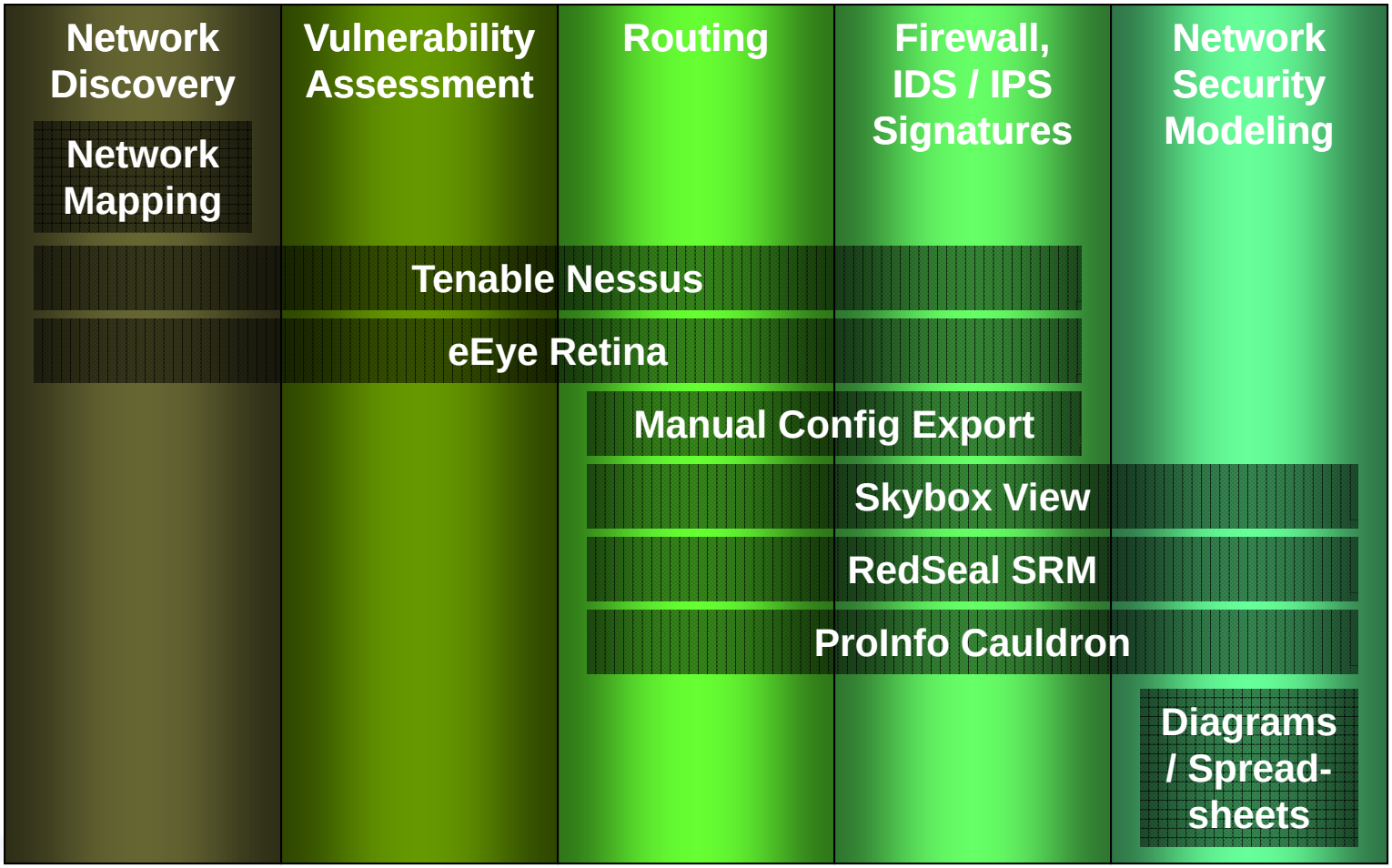


Process: System Security Baselining

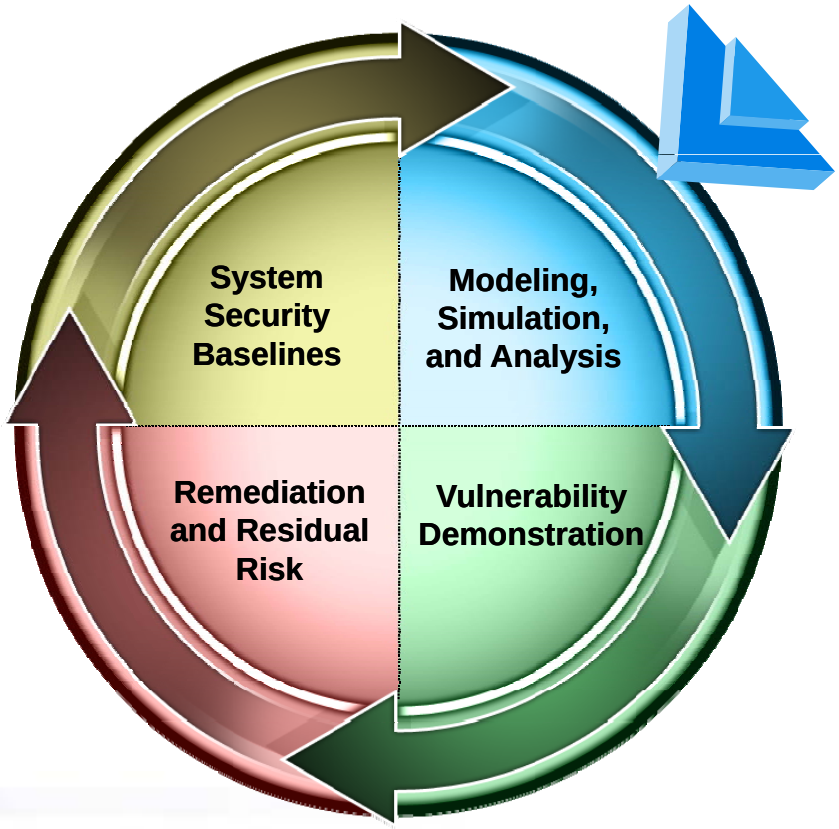
1. Discover Network Assets
2. Perform Authenticated Vulnerability Scans
3. Collect Routing Tables
4. Collect Firewall, IDS / IPS Signatures
5. Consolidate Findings into a Network Security Model… this is your "System Security Baseline"



System Security Baselining Tools

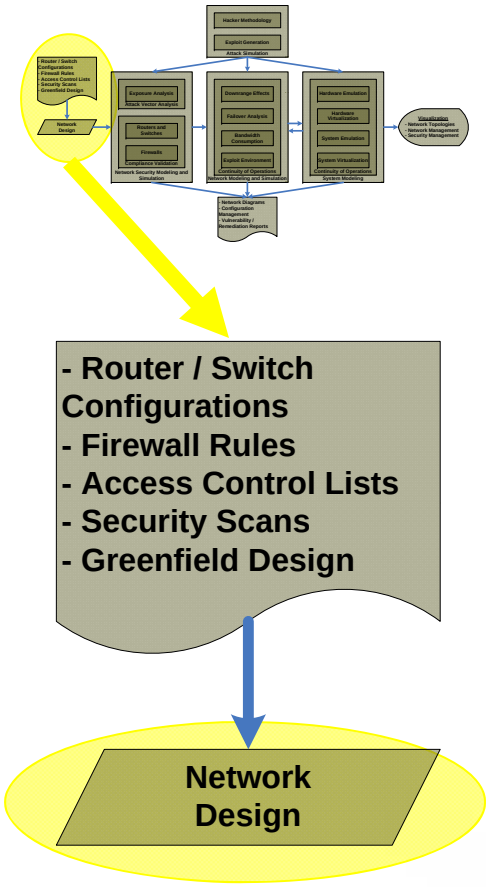


Modeling, Simulation, and Analysis



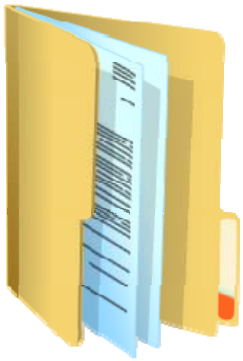
Determining Mission Criticality of Systems

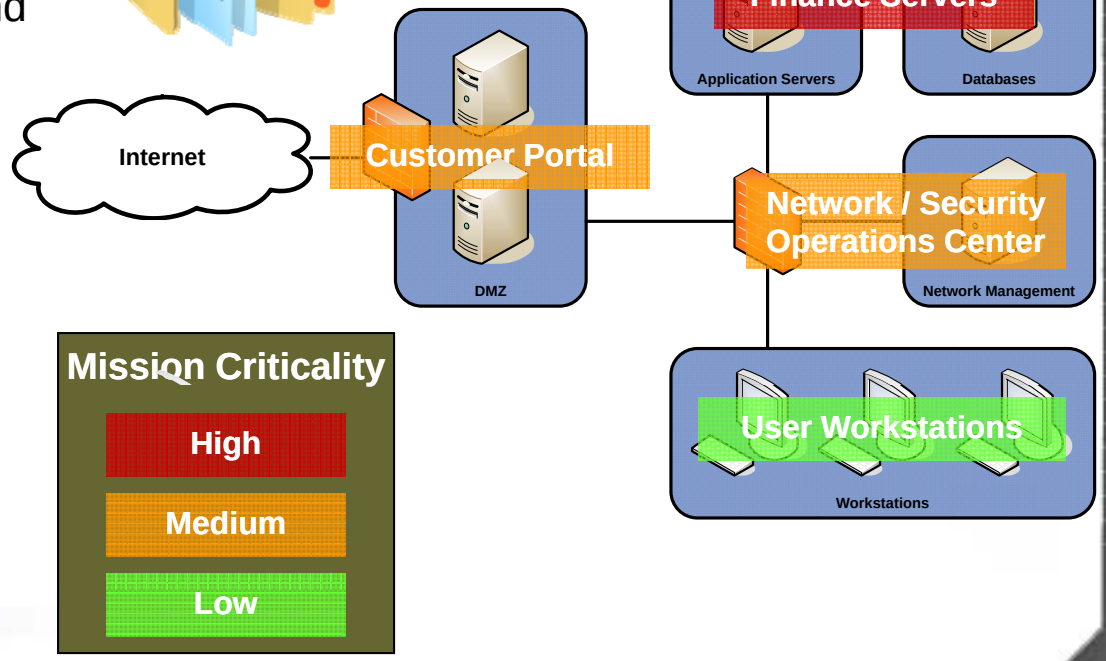
- Determining System Criticality requires an understanding of the Target Organization's Operations and Mission
- Operations and Mission should be analyzed with the same intensity as placed on System Security Baselines
- Sources that can be used to begin understanding an Organization's Operations and Mission include:
  - Mission Statements and Plans
  - Organization Charts
  - Risk Assessments and Business Continuity Plans
- Once Operations and Mission are understood, align Criticalities with System Security Baseline



Process: Determining Mission Criticalities

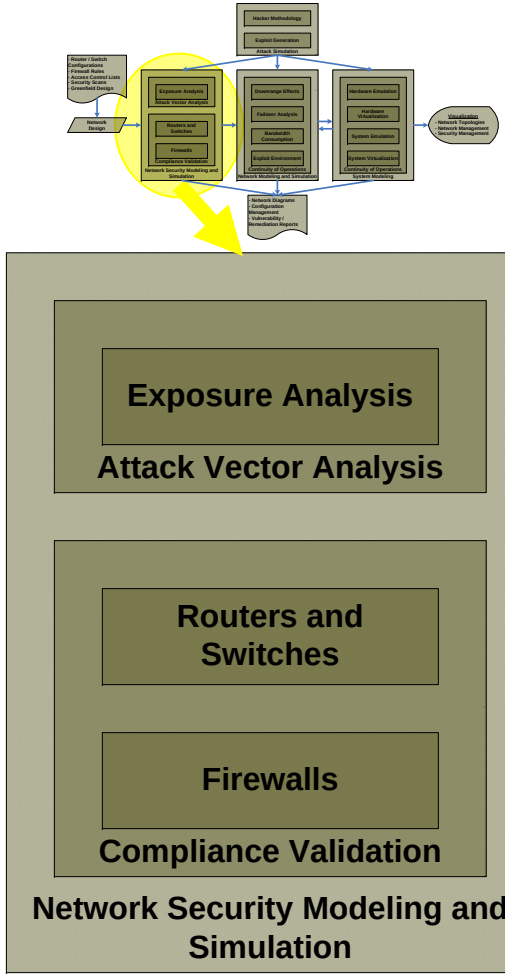
1. Obtain Network Security Model / System Security Baseline
2. Obtain and Analyze Supporting Operations and Mission Documentation
3. Determine Systems Necessary for Operations support and Mission Execution
4. Define System Roles and Relations to Operations Support and Mission Execution





Identifying Organizational Exposure

- Organizational Exposures refer to vulnerable or mis-configured hosts, servers, and network devices that serve as entry points for cyber attacks on information systems
- Entry points may either reside at the perimeter of an information system, or at a less obvious internal points of origin
- Organizational Exposures should not be confused with attack sources… with the exception of some forms of Internal Organizational Exposures, many attacks originate from outside either the physical or logical perimeters of an information system
- Corresponding to any Organizational Exposure is a Cyber Threat, which can be described in terms of actors and methods which present the potential to exploit a given Organizational Exposure



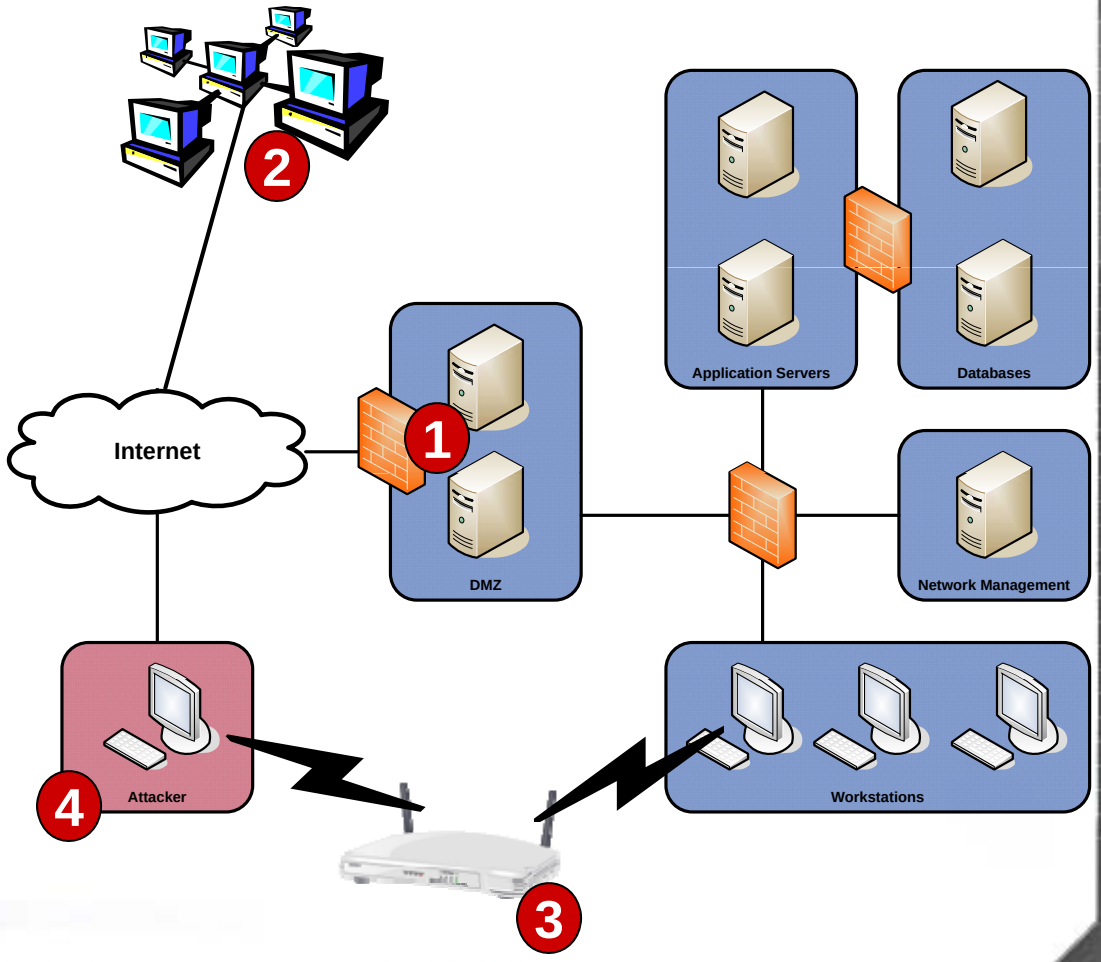
External Exposures

- External Exposures represent vulnerabilities at network perimeters, which allow access to internal systems once exploited
- This category of exposure acts as a hop-point for network based attacks to enter protected infrastructures from the internet, and may take advantage of weakly configured or non-hardened systems, such as:
  - Routers
  - Firewalls
  - Intrusion Detection / Prevention
  - Mail Routers
  - Data Guards
  - Content Filters
  - Other edge protection or routing devices

Example: External Exposures

- External Exposures are Vulnerabilities in:

1. Internet facing services
   - Web Servers
   - Mail Servers
   - Remote Access Servers
   - Perimeter Routers
   - Perimeter Firewalls
2. Trust Relations with other networks
3. Wireless Access Points
4. Allow Network-Based Attacks to enter protected systems



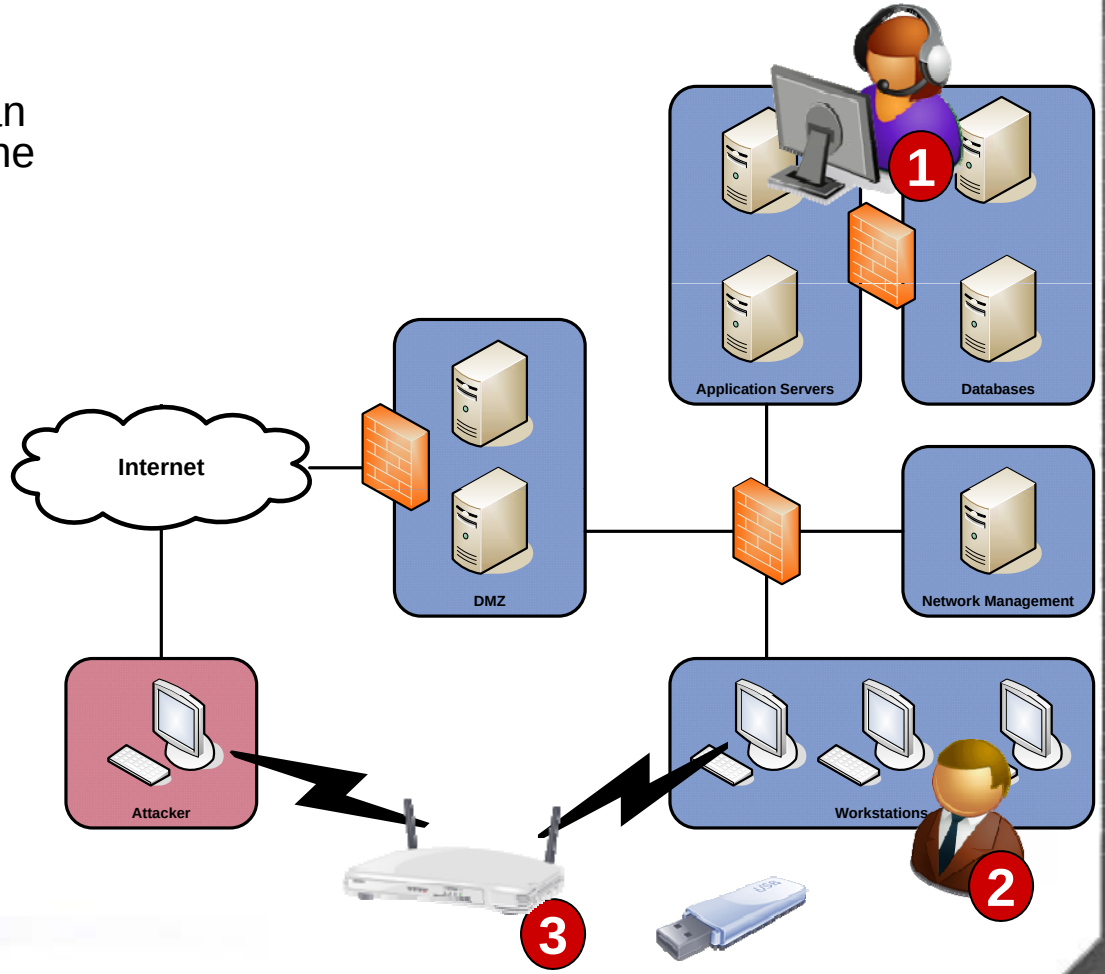
Internal Exposures

- Internal Organization Exposures require access to information systems, and are performed by either knowing or unknowing actors… once exploited, further access to target systems may be gained
- When External Exposures are mitigated within well configured networks, attackers shift to the weakest security link in a given target system, its users
- Attempts to compromise Internal Organization Exposures are local in nature, and focus on gaining access to computing resources, through:
  - User Interaction
  - Introduction of External Media and Communications
  - Theft
  - Social Engineering

Example: Internal Exposures

- Internal Exposures result from vulnerabilities and mis-configurations that can be exploited from within the physical boundaries of systems

1. Misuse of Legitimate Access
2. Inadvertent or subversive use of system resources
3. Covert use of systems
   - Rouge Access Points
   - Physical Access
   - Removable Media



Hybrid Exposures

- Hybrid Exposures take advantage of Internal Exposures to facilitate the exploitation of External Exposures from within protected infrastructures

- These exposures may originate from:

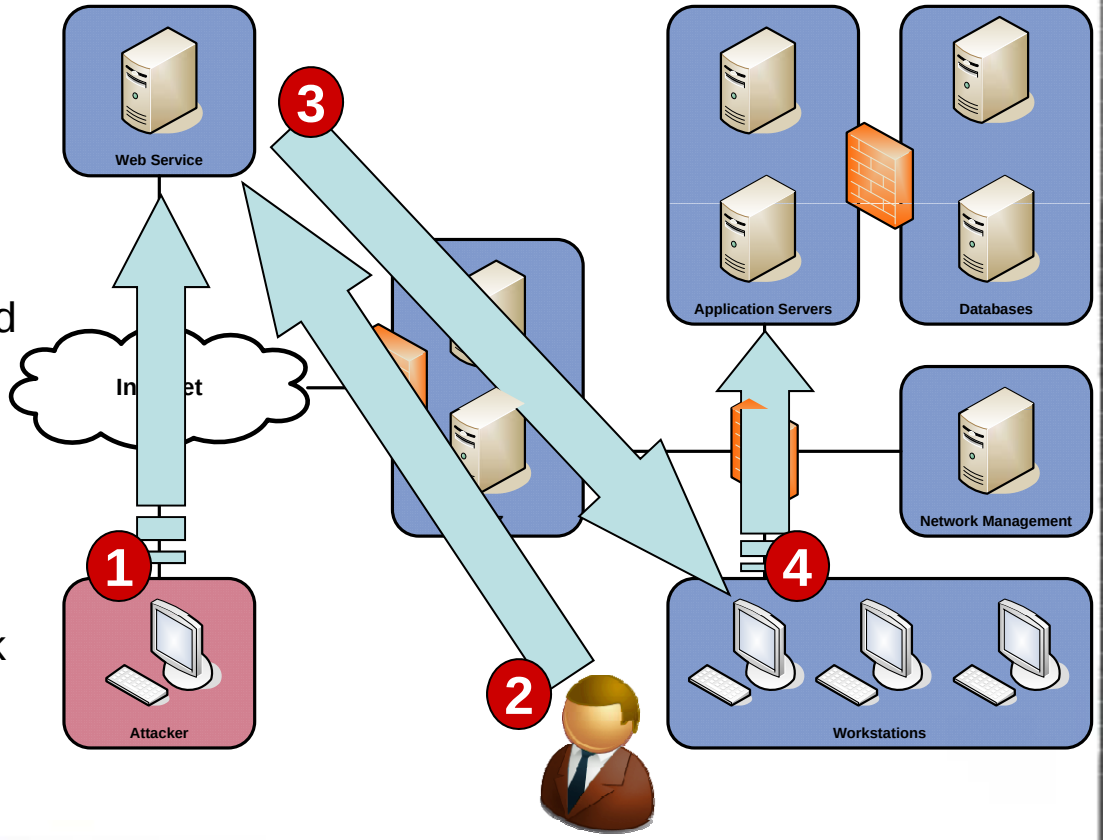
  - Intentional mis-configuration of systems
  - User circumvention of security controls from within networks
  - Negligent use of Internet or E-Mail resources, resulting in the introduction of malicious code with reverse shells

    - Phishing Attacks
    - Trojans
    - Root-Kits

Example: Hybrid Exposures

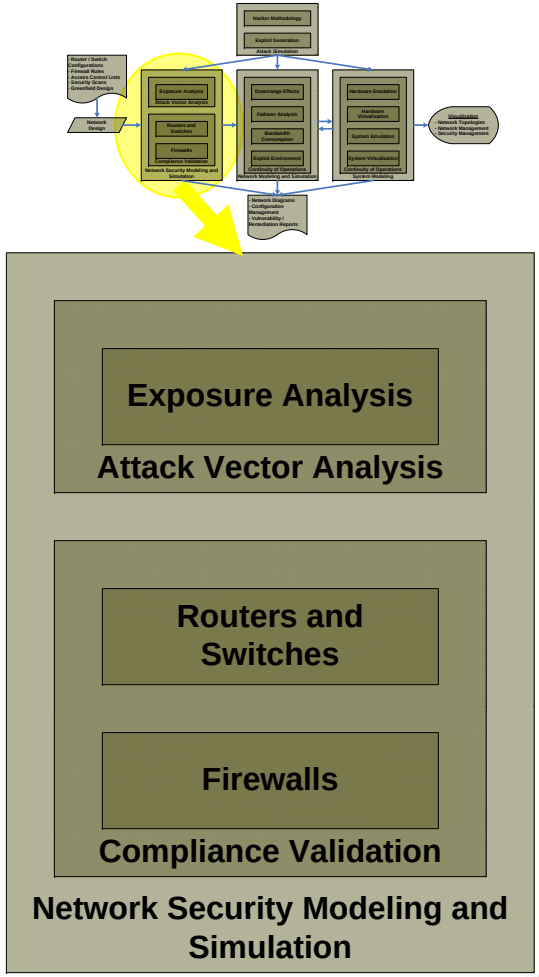
- Hybrid Exposures have characteristics of both Internal and External Exposures

1. Attacker plants exploit in public web service
2. User access compromised public web service
3. Malicious Code exploits User's workstation
4. Provides potential jump point for attacker to attack deeper into system



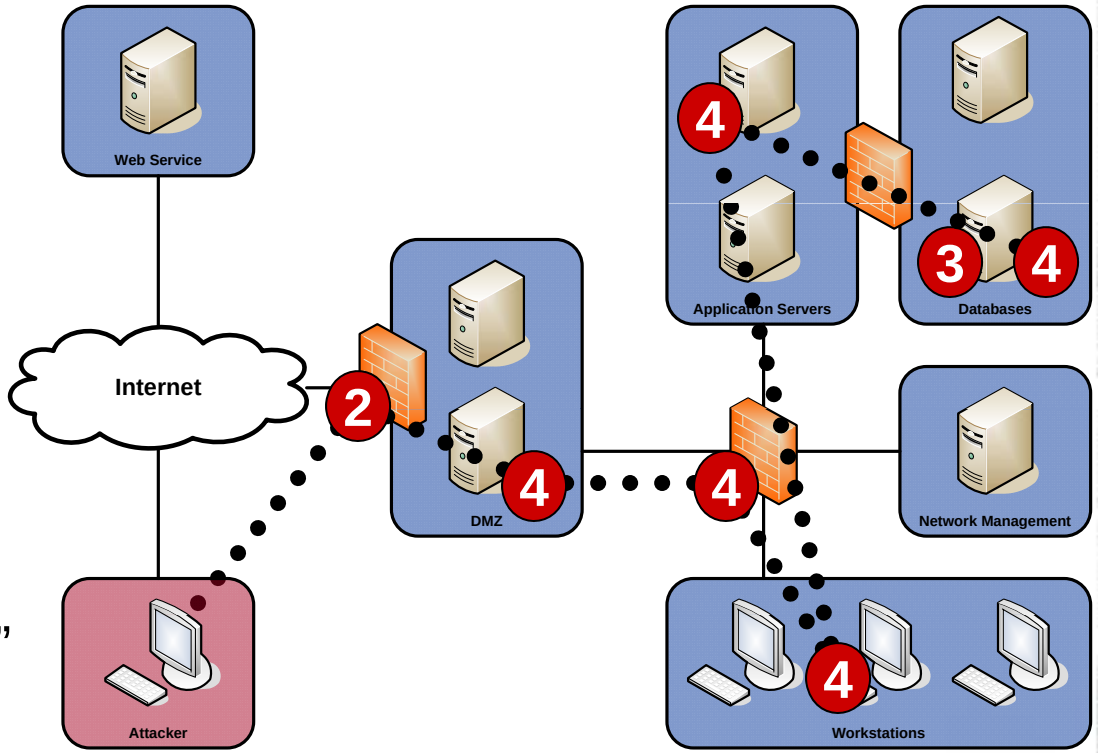
Cyber Attack Vectors

- Cyber Attack Vectors consist of the physical and logical paths a particular attack takes to reach its ultimate target
- This allows for the identification of an Organization's exposure to cyber threats as the result of thorough vulnerability analysis and the establishment of network security baselines
- Whether performed manually or using analytical tools, the end result is an understanding of the pathways of vulnerabilities that lead to critical systems



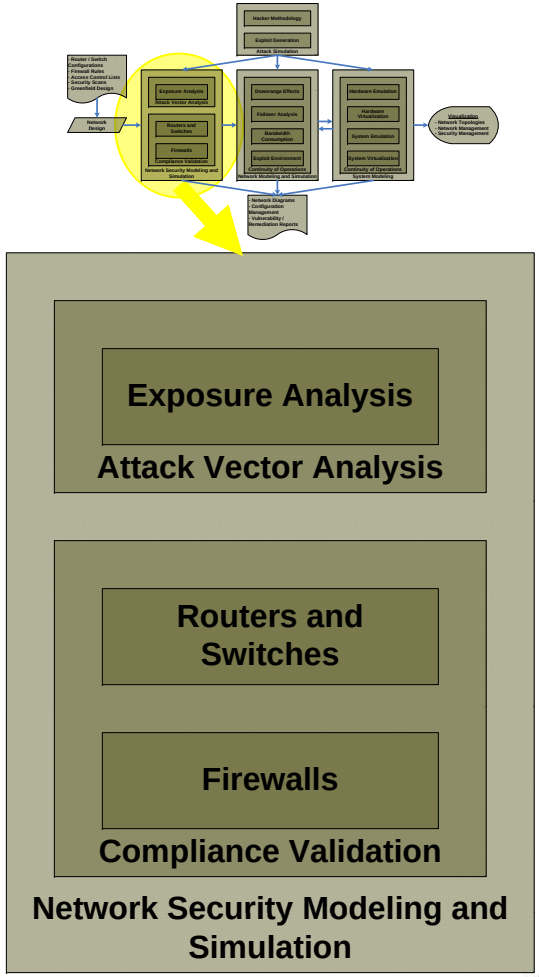
Process: Attack Vector Analysis

1. Generate model of System Security Baseline
2. Identify Organizational Exposures
3. Identify Mission Critical Systems
4. Identify Systems Attackers can “Own” or “Hop” from
5. Connect the Dots



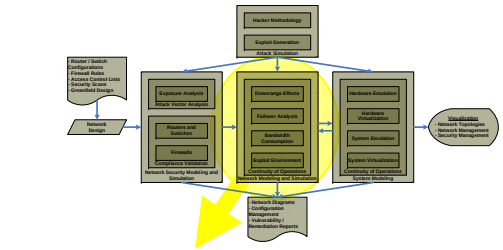
Primary Cyber Effects

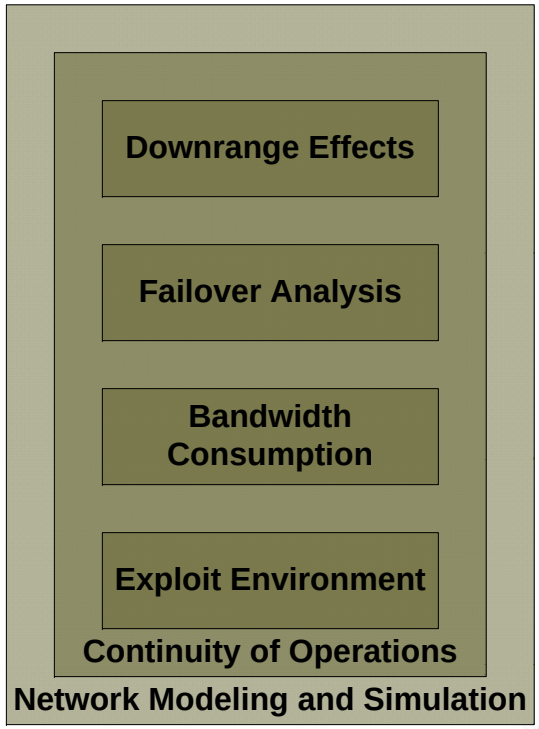
- **Primary Cyber Effects** - The resulting impact to information systems from direct exploitation of vulnerabilities during cyber attack
  - Associated with Attack Graphing / Attack Vector Analysis
  - Includes analysis of Point-to-Point and Multi-Hop Attacks
- Expands upon traditional vulnerability assessments by examining the link-node relationships between vulnerable systems
- Focus is on vulnerabilities that could provide attackers sufficient access to target systems needed to “Own” the target system for use as an attack platform



Secondary Cyber Effects

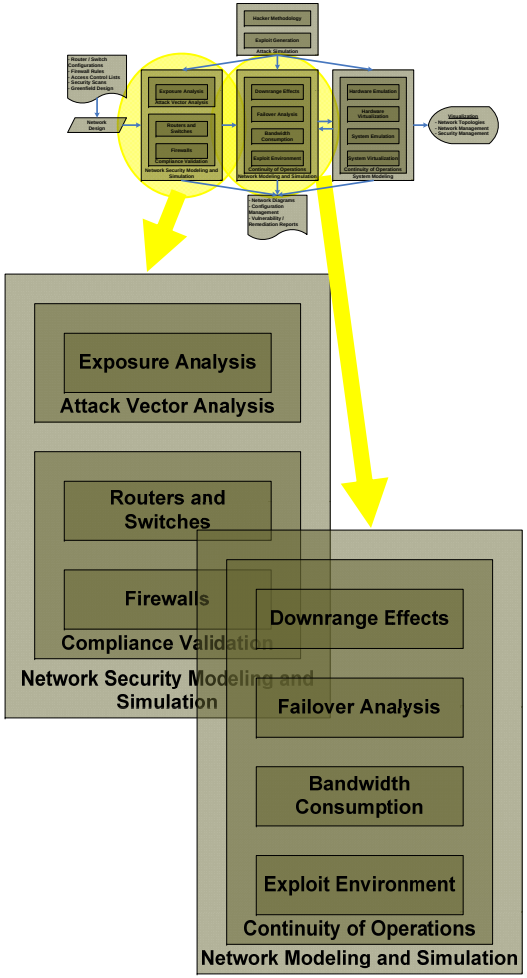
- **Secondary Cyber Effects:** The indirect impact information systems experience when network services and communications are lost or restricted due to cyber attack
  - Indirect in nature, and consist of downstream effects of system failures triggered by cyber attack
  - Characterized as Internally Cascading Effects that occur within systems
  - Exploits the interdependency of networked services
  - Results from the failure of systems dependant upon those affected by direct attack or other internally cascading effects





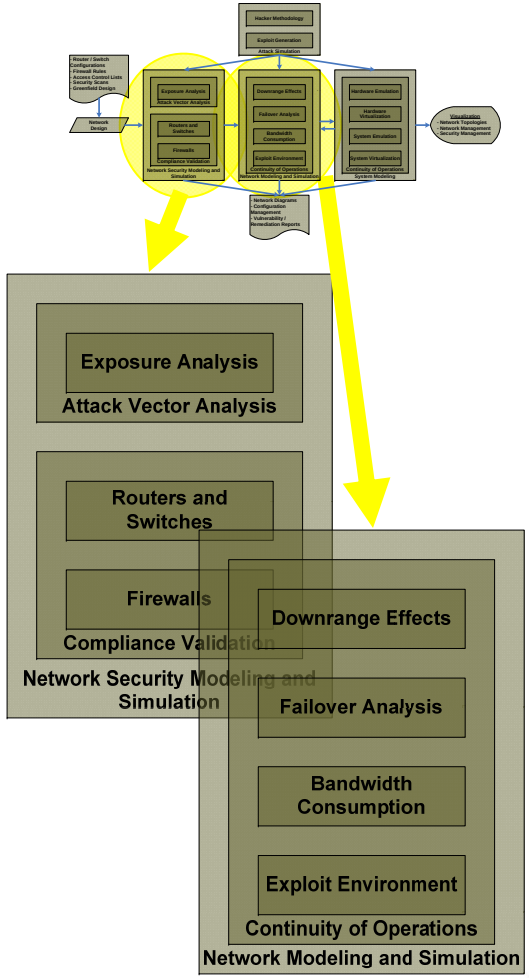
Tertiary Cyber Effects

- **Tertiary Cyber Effects:** The overall impact of Primary and Secondary Effects which result in the loss or degradation Operational or Mission Capabilities that are external, yet dependant upon information systems
  - Characterized as Externally Cascading since Tertiary Effects occur outside of systems
  - Example… an obvious effect of financial systems failing can be employees not being paid, a non-obvious effect could be that logistics systems are unable to complete transactions

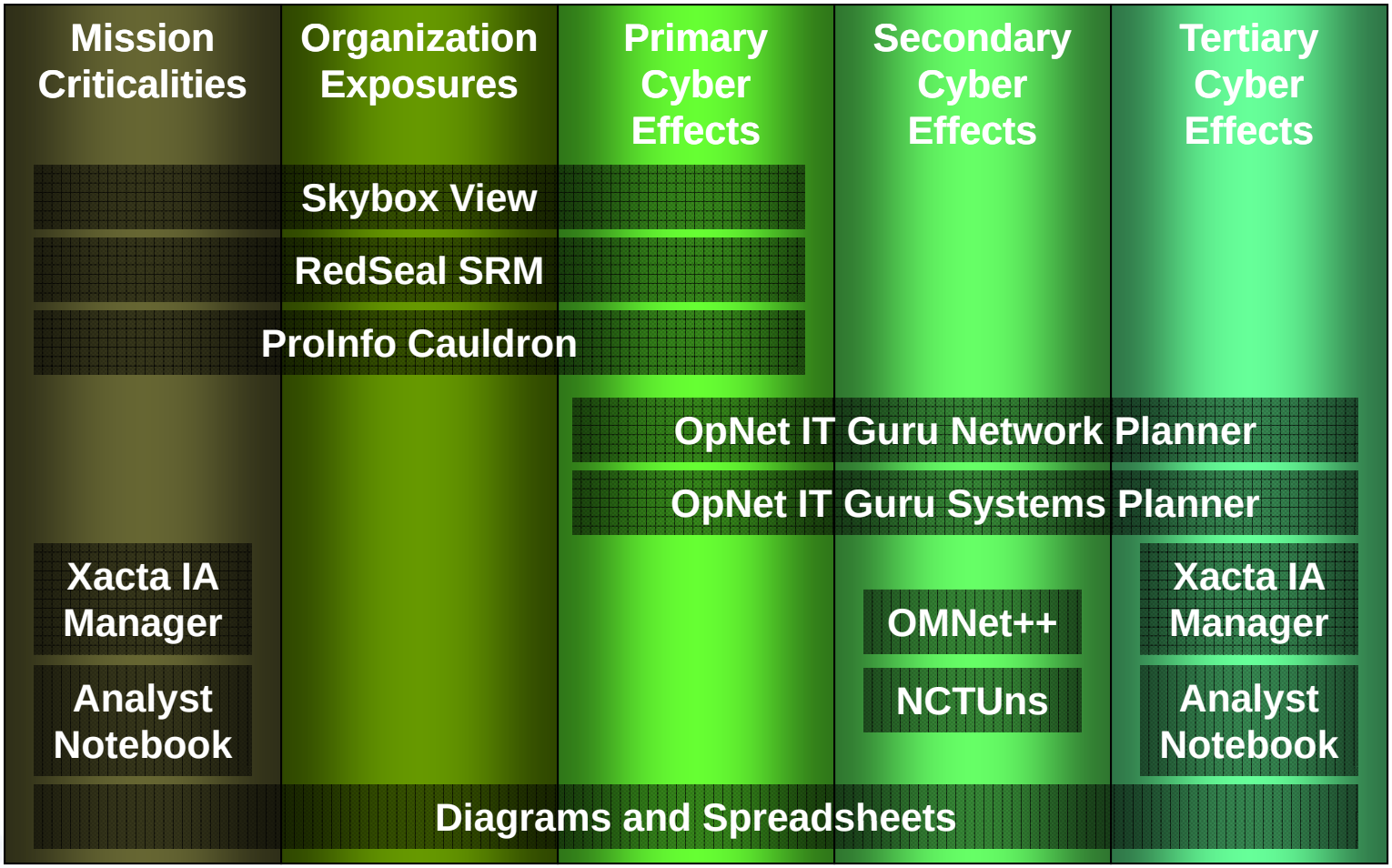


What About 0-Days?

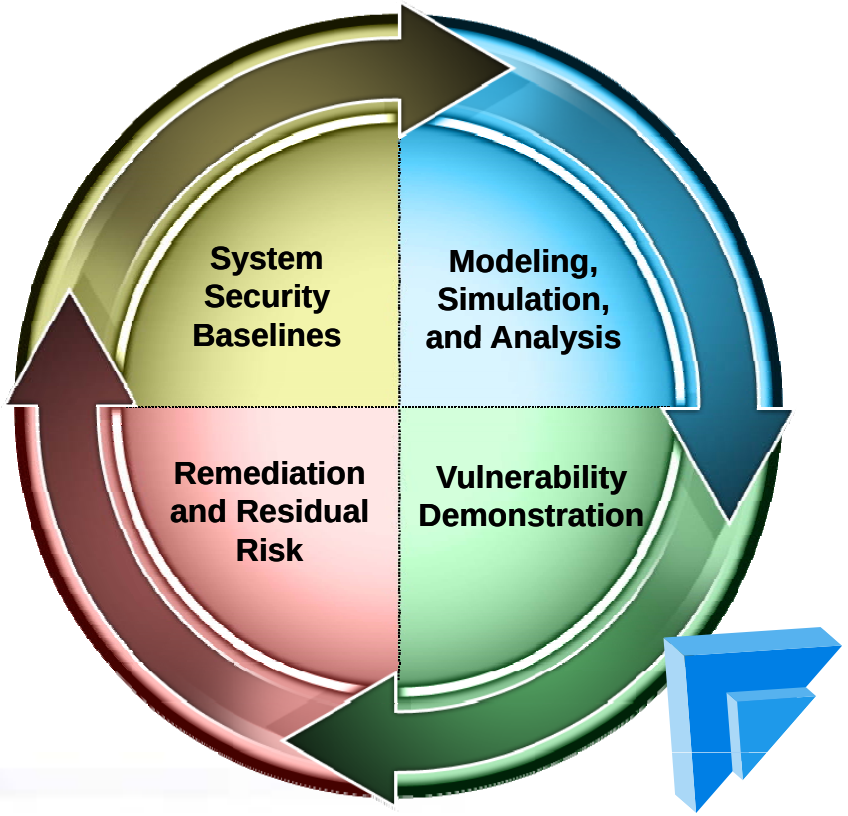
- Perform What-If Analysis…
  - Example – New Vulnerabilities are suspected in systems which are built on Operating System “A”, running Application “B”, with Service “C”, and Port “D”, exploitation allows administrative access
  - Modify Network Security Models to account for this new vulnerability, and re-work analysis
  - New Organizational Exposures and Attack Vectors may emerge depending upon the distribution of systems possessing vulnerable characteristics



Modeling, Simulation, and Analysis Tools

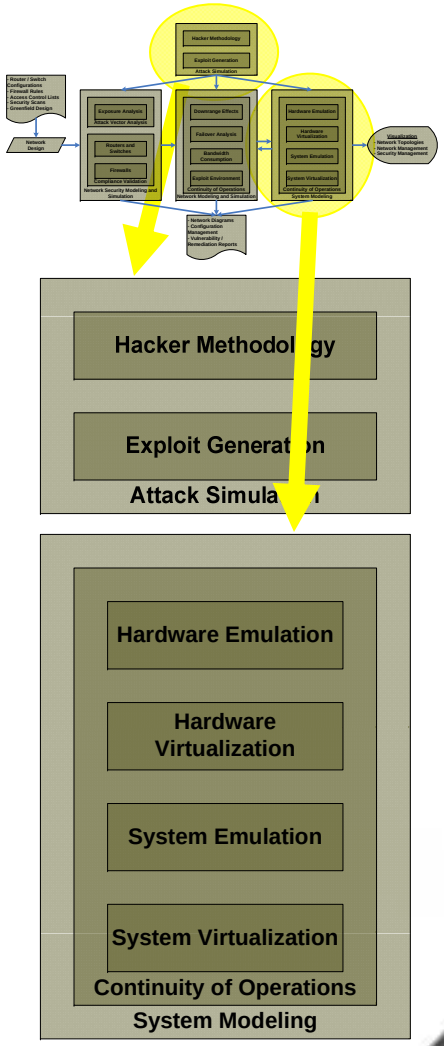


Vulnerability Demonstration



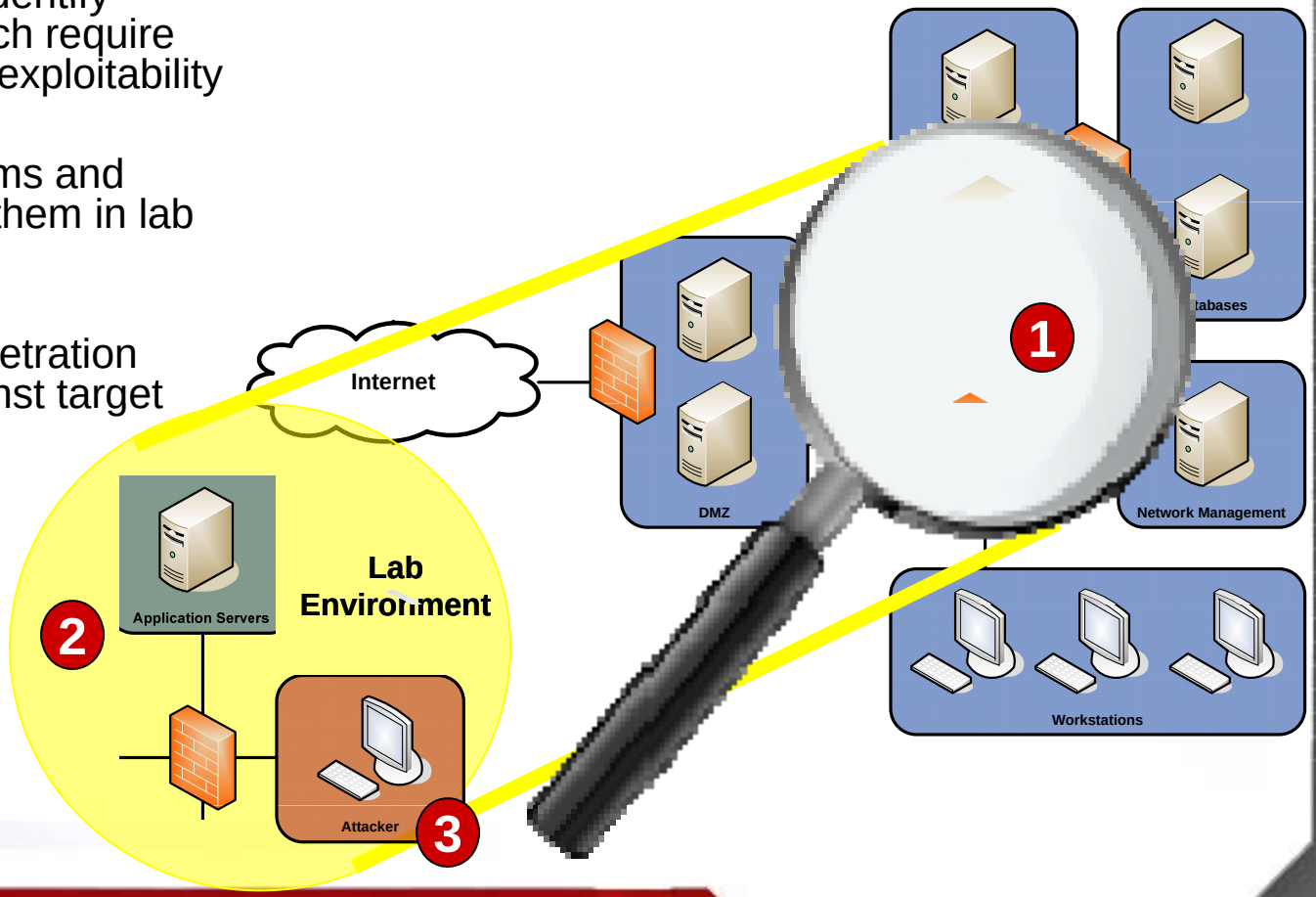
Targeted Penetration Testing

- Pentests generally target black box (unknown) or white box (known) systems
- Cyber Effects Prediction lends itself to white box pentests, eliminating discovery since analysts possess a Network Security Model… aka System Security Baseline
- Pentesting within this methodology is used to demonstrate and prove vulnerabilities that system owners may not otherwise acknowledge
- Tools such as Core Impact (Commercial) or Metasploit (Open Source) are well suited to demonstrating targeted pentests against lab systems
- Vulnerabilities exploited through custom developed code can be worked into Network Security Model based on attributes of systems and software targeted

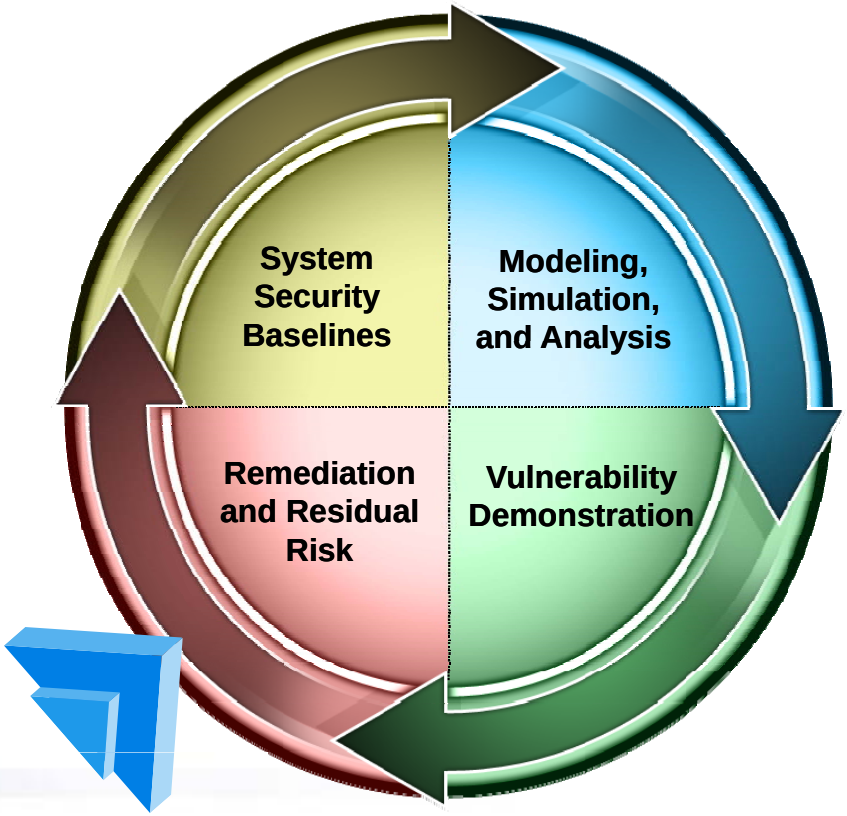


Example: Targeted Penetration Testing

1. Based on analysis conducted, identify systems which require validation of exploitability
2. Image systems and reconstitute them in lab environment
3. Execute Penetration Testing against target systems



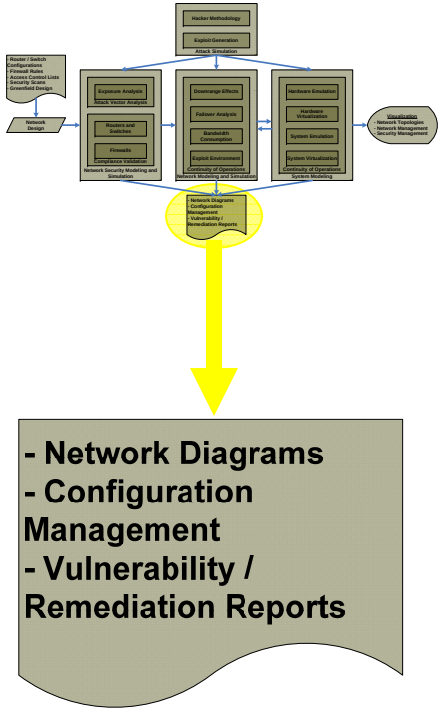
Remediation and Residual Risk



Prioritizing Remediation Actions

- As a result of thorough analysis through Cyber Effects Prediction, vulnerability mitigation for systems aligned as mission critical can be escalated
- Analysis allows for vulnerability mitigation to directly target systems affected, or upstream systems that can access the critical system if exploited
- Goal of remediation is to harden critical systems so that they:

1. Are not vulnerable to known exploits
2. Are not reachable for exploitation through other vulnerable systems
3. Retain the ability to provide the services they are designed for



Allocating Remediation Resources

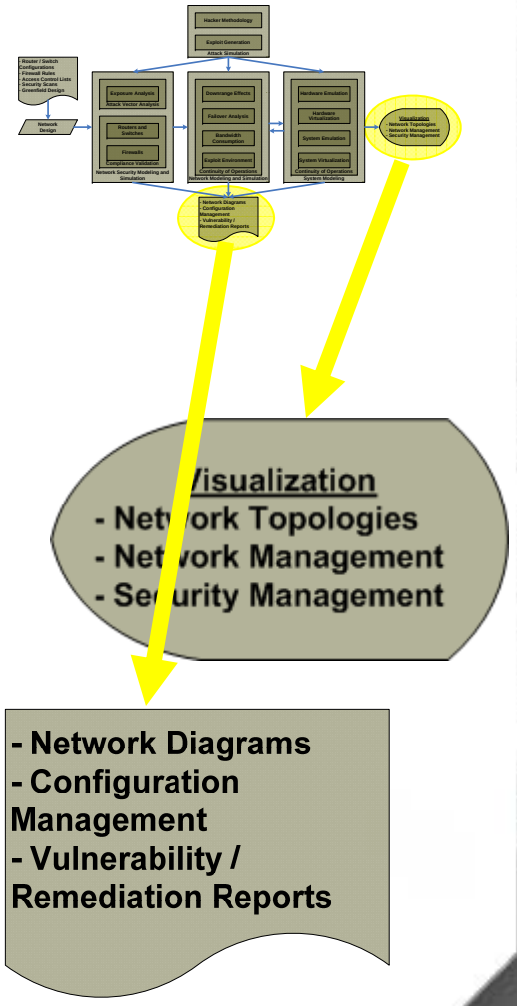
- Analytical results of Cyber Effects Prediction also allows efficient allocation of resources needed to conduct remediation actions:
  - Personnel
  - Time
  - Budget
  - Equipment
- Organizations are often hard pressed to fully patch systems or implement dynamic defense-in-depth strategies
- Allocation of resources to remediate vulnerabilities is discretionary in nature, using Cyber Effects Prediction, resource allocation can be aligned with those vulnerabilities that are:
  - Reachable
  - Assigned to Mission Critical Systems
  - Time Critical
  - Proportionate to Resource Availability

Addressing Residual Risk

- No approach to system security is perfect
  - Cyber Effects Prediction is based on Knowing your System Security Baseline and assessing it against published vulnerability databases
  - 0-Day Vulnerabilities can be worked into your Network Security Model, and should be considered
- Residual Risk will remain that system owners will need to acknowledge and accept responsibility for
- However, Cyber Effects Prediction provides a holistic view of System Security Baselines with an understanding of how Mission Critical Systems may affected by Cyber Attack
- By adding realistic cost models of resources, possible to obtain quantitative analysis

Additional Benefits

- Demonstrates Extreme Due Diligence for Security Compliance
- Captures System Configurations and Supports Configuration Management Processes
- Supports development of Situational Awareness
- Facilitates Rapid Analysis during Incident Response Actions
- Allows Organizations to take Pro-Active approaches to Information Security



What's Next for Cyber Effects Prediction?

- Cyber Effects Prediction today ranges from manual to semi-automated processes, to increase speed of analysis:
  - Work with product vendors to integrate databases used for modeling
  - Tailor Open Source products to better address attack vector analysis
  - Decision Metrics - Perfect Security Pipedream vs How Good is Good Enough?
- System owner's still express reluctance to implement Cyber Effects Prediction
  - Increase awareness of the benefits that can be derived from non-intrusive analysis
  - Refine and decompose Cyber Effects Prediction further into formal processes
  - Build a portfolio of models and analysis that can be released to share with system owners, showing Cyber Effects Prediction in action
- Determine how Systems for Cyber Effects Prediction can be integrated into production environments to support near-real-time situational awareness

Resources

Vulnerability Assessment

- Tenable Nessus - http://www.nessus.org/nessus/
- eEye Retina - http://www.eeye.com/Products/Retina.aspx

Security Risk Management

- Skybox View - http://www.skyboxsecurity.com/
- RedSeal SRM - http://www.redseal.net/
- ProInfo Cauldron - http://www.proinfomd.com/

Modeling and Simulation

- OpNet IT Guru Network Planner - http://www.opnet.com/
- OpNet IT Guru System Planner - http://www.opnet.com/
- OMNet++ - http://www.omnetpp.org/
- NCTUns - http://nsl.csie.nctu.edu.tw/nctuns.html

Penetration Testing

- Metasploit - http://www.metasploit.com/
- Core Impact - http://www.coresecurity.com/

Security Compliance

- Telos Xacta IA Manager - http://www.telos.com/solutions/

Relational Analysis

- i2 Analyst Notebook - http://www.i2group.com/

Questions?

Discussion…