Determining Current Cybersecurity Capabilities

Develop and maintain an unrivaled, globally competitive cybersecurity workforce
NICE Cyber Workforce Inventory Project

Dr. Michael Koehler
Program Analyst
U.S. Department of Homeland Security
NICE Cyber Workforce Inventory Project

Understanding the State of the Cyber Workforce

• Lead – U.S. Department of Homeland Security
Background

National Initiative for Cybersecurity Education (NICE)

• **Goal 2**: Broaden the pool of skilled workers capable of supporting a cyber-secure nation.

• **Goal 3**: Develop and maintain an unrivaled, globally competitive cybersecurity workforce
Mission

Strengthen the overall cybersecurity posture of the United States by collecting data that captures current cyber workforce capabilities and analyzing that data to identify the current state of the workforce.
Vision

Inform the development and enhancement of cybersecurity education to foster a cybersecurity workforce capable of defending the infrastructure and interests of the United States.
Foundation

The NICE Cybersecurity Workforce Framework

- 7 Categories
- 31 Specialty Areas
- Numerous Associated Tasks and KSA
Presentations

To provide an overview of the methods, challenges, and best practices for investigating cybersecurity workforce capabilities and competencies.
Presenters

Maureen Higgins/Dr. Jacqueline Caldwell, OPM
- Federal Cybersecurity Competency Model

Drew Lopez, Booz Allen Hamilton
- DHS Cyber Workforce Initiative

Dr. David Tobey, NBISE
- From Cybersecurity Competencies to a Job Performance Model
The Secretary of the Department of Homeland Security has identified the acquiring, growing, and sustaining of a cyber workforce as one of the Department’s priorities.

- The cyber security mission of DHS will require a federal workforce that possesses the necessary skills to lead cybersecurity missions and solutions, while ensuring the future security of the national critical infrastructure.

- In response, the Office of the Chief Human Capital Officer (OCHCO) and the National Protection and Programs Directorate (NPPD) has established a cross-component team responsible for the development of this initiative.
Implementation: First Steps

To start, Cyber Workforce Development is focused on defining Capability needs, which is accomplished by building competency models

• Why Cyber Competency Models?
  ➢ Objective: Competencies define the skills/capabilities critical for successful job performance across Cyber roles, and the behaviors that exemplify the progressive levels of proficiency associated with these competencies
  ➢ Impact: Provides a solid foundation upon which targeted recruitment, selection, and employee development (learning and training) initiatives can be built to increase Cyber Workforce capabilities

What makes a Competency Model?
  ➢ Competencies
  ➢ Behavioral Indicators

<table>
<thead>
<tr>
<th>Competency</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penetration Testing</td>
<td>Designs, simulates, and executes attacks on networks and systems. Leverages existing and emerging methods to attack systems and exploit vulnerabilities. Documents penetration testing methodology, findings, and resulting business impact.</td>
</tr>
</tbody>
</table>
Implementation: Challenges

• How do we minimize the time impact on the managers, supervisors and SMEs?
• How do we ensure consistency in terminology across all agencies and components?
• Who are the DHS Cybersecurity professionals?
• What competency work has been accomplished?
• With so many Occupational Series involved with Cybersecurity, how should the models be built?
Although we still have some outstanding challenges, the NICE Framework presented an exceptional solution for time and consistency. Using the framework as a foundation, DHS can

- Compile initial technical competency models in a compressed timeframe
- Maintain consistency in terminology across all agencies and components, as well as alignment with NICE and OPM
What are Competency Models? – Nuts and Bolts

**CYBER ROLE**

**Cybersecurity Tester:** The Cybersecurity Tester provides compliance-based security testing leveraging automated tools. The Cybersecurity Tester assists in the preparation, development, modification, and management of security products in support of the C&A process. The Cybersecurity Tester provides technical analysis and automated scans to assess their completeness and identify system vulnerabilities and weaknesses.

**CYBER SKILLS**
- Systems Requirements Analysis
- Testing
- Vulnerability Assessment
- Threat Assessment
- Penetration Testing
- Certification & Accreditation
- Secure Network Design

**BEHAVIORAL INDICATORS**
- Performs technical planning, system integration, verification and validation, and supportability and effectiveness analyses for total systems
- Analyzes all levels of total system products to include: acquisition, concept, design, test, installation, operation, maintenance, and disposal
- Translate operational requirements into technical requirements
- Organizes and analyzes stated requirements into categories throughout the system lifecycle such as functionality, usability, performance, operational, security, etc.
- Proficient at using a requirements management tool (e.g., DOORS)
- Identifies and documents security requirements

**SYSTEMS REQUIREMENTS ANALYSIS:** Translates functional security requirements into secure design technical and operational specifications. Reviews requirements documentation to determine security impact and requirements. Conducts security risk assessments and business impact analyses to detect weaknesses and depth/breadth of security controls needed. Evaluates current state of security systems, processes, and controls. Performs gap analyses and makes recommendations for gap mitigation.

**TRANSLATION:**
- Leads the definition and flow-down of functional, performance, and design requirements
- Performs functional analysis, timeline analysis, requirements allocation, and interface definition studies to translate customer requirements into hardware and software specifications
- Distinguishes testable requirements
- Conducts gap analyses between requirements and proposed architecture to identify security performance and other weaknesses in the system
- Verifies security requirements through collaboration with DAA/IA/Engineering & Systems Administration
- Conducts vulnerability & risk assessment analyses
- Advises on new techniques and estimated costs associated with new or revised programs and utilities, taking into consideration personnel, time, and hardware requirements
- Interprets mission objective and applies knowledge to requirements and implementations
- Advises customer of gaps in security policy and guidance; provides recommendations
- Monitors industry developments and evolving instruction/policy/guidance on IT security concerns
- Oversees large-scale requirements development and management efforts to include the definition of new requirements and the implementation of changes to existing requirements.

**PERFORMANCE STANDARDS**

<table>
<thead>
<tr>
<th>CYBER SKILL &amp; PROFICIENCY STANDARDS</th>
<th>PERFORMANCE LEVEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems Requirements Analysis</td>
<td>INT</td>
</tr>
<tr>
<td>Testing</td>
<td>2</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>1</td>
</tr>
<tr>
<td>Threat Assessment</td>
<td>2</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>1</td>
</tr>
<tr>
<td>Certification &amp; Accreditation</td>
<td>1</td>
</tr>
<tr>
<td>Secure Network Design</td>
<td>1</td>
</tr>
</tbody>
</table>
Applying the NICE Framework

DHS SPECIFIC CYBER ROLE

**Cybersecurity Tester:** The Cybersecurity Tester provides compliance-based security testing leveraging automated tools. The Cybersecurity Tester assists in the preparation, development, modification, and management of security products in support of the C&A process. The Cybersecurity Tester provides technical analysis and automated scans to assess their completeness and identify system vulnerabilities and weaknesses.

<table>
<thead>
<tr>
<th>SPECIALTY AREAS</th>
<th>BEHAVIORAL INDICATORS</th>
<th>PERFORMANCE STANDARDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems Requirements Planning</td>
<td>Performs gap analyses and makes recommendations for gap mitigation, depth/breadth of security controls needed. Evaluates current standards. Conducts security risk assessments and business impact analyses for total systems analyses for total systems and supportability and effectiveness analyses for total systems</td>
<td>Systems Requirements Planning 2 3 3</td>
</tr>
<tr>
<td>Test and Evaluation</td>
<td>Identifies and documents security requirements through collaboration with DAA/IA/Engineering &amp; Systems Administration</td>
<td>Test and Evaluation 2 3 3</td>
</tr>
<tr>
<td>Investigation</td>
<td>Translates functional security requirements into secure design through the system lifecycle such as functionality, usability, performance, operational, security, etc.</td>
<td>Investigation 1 2 3</td>
</tr>
<tr>
<td>Computer Network Defense</td>
<td>Proficient in using a requirements management tool (e.g., DOORS)</td>
<td>Computer Network Defense 2 2 2</td>
</tr>
</tbody>
</table>

Built by SMEs with alignment to respective NICE Framework KSAs

- Advises on new techniques and estimated costs associated with new or revised programs and utilities, taking into consideration personnel, time, and hardware requirements
- Interprets mission objective and applies knowledge to requirements and implementations
- Advises customer of gaps in security policy and guidance; provides recommendations
- Monitors industry developments and evolving instruction/policy/guidance on IT security concerns
- Oversees large-scale requirements development and management efforts to include the definition of new requirements and the implementation of changes to existing requirements.

**CYBER SKILL & PROFICIENCY STANDARDS**

- **Systems Requirements Planning:**
  - INT 2
  - EXP 3
  - FEL 3
- **Test and Evaluation:**
  - INT 2
  - EXP 3
  - FEL 3
- **Investigation:**
  - INT 1
  - EXP 2
  - FEL 3
- **Computer Network Defense:**
  - INT 2
  - EXP 2
  - FEL 2
Current challenges using NICE Framework

• Specialty Areas not “perfectly” aligned to DHS cyber roles/mission

• Limited coverage for programmatic and other roles
Current challenges: Our solutions

• Specialty Areas not “perfectly” aligned to DHS cyber roles/mission
  – Using Behavioral Indicators and proficiency levels to make models “aligned” to DHS cyber roles

<table>
<thead>
<tr>
<th>Basic</th>
<th>Intermediate</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>At this level, individuals perform behaviors that show they have</td>
<td>At this level, individuals perform behaviors that show they have substantial knowledge/awareness of the competency. They can apply the competency</td>
<td>At this level, individuals perform behaviors that show exceptional knowledge/awareness of the</td>
</tr>
<tr>
<td>fundamental knowledge/awareness of the competency. They have limited capability in applying this competency but are capable of performing tasks, applying this competency with guidance and supervision.</td>
<td>and are considered capable to fully perform work that requires application of this competency. These individuals are capable of demonstrating this competency in straightforward and routine situations and can contribute knowledge or new ideas in applying this competency. They implement the competency with little help and work independently most of the time.</td>
<td>competency and are looked to as experts in this competency. Others view these individuals as role models capable of leading or teaching others in this area, and they consult with them for assistance or guidance with work requiring this competency. These individuals obtain best-in-class results, setting the standard for performance.</td>
</tr>
</tbody>
</table>
Current challenges: Our solutions

• Limited coverage for programmatic and other roles
  – Provide feedback to NICE from what we gather in the field

To: Burgess, Roy (Roy.Burgess@dhs.gov)
Subject: One other piece of feedback from the field

Roy,

...so I am forwarding it to the NICE folks for their consideration, banter, decision and action as they deem appropriate.

**Current Specialty Area and Definition:**
Vulnerability Assessment and Management: Conducts assessments on threats and vulnerabilities, determines the level of risk, deviations from acceptable configurations, enterprise or local policy, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

**Feedback/Recommendation received from CICPA on the Specialty Area and Definition:**
Capability Assessment and Management: Conducts evaluations to determine the state of repeatable process, procedure, and management of IT operations delivering a critical infrastructure service. Utilizes a standard process improvement framework to determine levels of capability, maturity, and resilience of these operations, including focused inquiry of asset, technology, risk (vulnerability, threat, and consequence), continuity, dependency, and situational awareness management. Develops and/or recommends appropriate options for consideration to reduce risk exposures under normal circumstances and in times of operational stress.
From cybersecurity competencies to a job performance model

David H. Tobey, Ph.D.
VP, Director of Research
National Board of Information Security Examiners
From cybersecurity competencies to a job performance model

1. The Science of Cybersecurity Competency Development
   A. Are we measuring the right things?
   B. Are we measuring the right way?
   C. Are our measures meaningful and predictive?

2. Methods, Best Practices and Challenges
   A. Methods and best practices
      i. Eliciting organizational context through vignettes and role/responsibility relationships
      ii. Achieving alignment through goal and objective elicitation
      iii. Defining proficiency at multiple levels for multiple roles
      iv. Identifying critical and differentiating tasks that explain differences in skill level
      v. Job Performance Models: The path from apprentice to master
   B. Challenges
      i. Competency modeling at ground truth speed
      ii. Facilitating the translation of competency models into workforce development programs

3. Why Job Performance Models Are Important
What is a competency?

- **Knowledge** (understanding of strategy or procedure)
- **Skills** (consistency of performance)
- **Ability** (transfer across domains)

- Narrow
- Broad
- Shallow
- Deep
- Consistent
- Inconsistent

- Novice
- Apprentice
- Journeyman
- Master

Are we measuring the right things?

Best Practices in Competency Modeling

Analyzing Competency Information (Identifying Competencies)
1. Considering organizational context
2. Linking competency models to organizational goals and objectives
3. Start at the top
4. Using rigorous job analysis methods to develop competencies
5. Considering future-oriented job requirements
6. Using additional unique methods

Organizing and Presenting Competency Information
7. Defining the anatomy of a competency (the language of competencies)
8. Defining levels of proficiency on competencies
9. Using organizational language
10. Including both fundamental (cross-job) and technical (job-specific) competencies
11. Using competency libraries
12. Achieving the proper level of granularity (number of competencies and amount of detail)
13. Using diagrams, pictures, and heuristics to communicate competency models to employees

Using Competency Information
14. Using organizational development techniques to ensure competency modeling acceptance and use
15. Using competencies to develop HRs systems (hiring, appraisal, promotion, compensation)
16. Using competencies to align the HR systems
17. Using competencies to develop a practical “theory” of effective job performance tailored to the organization
18. Using information technology to enhance the usability of competency models
19. Maintaining the currency of competencies over time
20. Using competency modeling for legal defensibility (e.g., test validation)

Source: Campion et al. (2011) p. 230

NBISE Job Performance Methodology

Analyzing Competency Information (methods)
- Context: Vignette Elicitation
- Goals and objectives: PRISM method
- Rigorous/Future-oriented job analysis: JTCA

Organizing Competency Information
- Anatomy of a competency: KSA*MT
- Levels proficiency: JAQ – multiple performance levels for multiple roles
- Org. Language/Hard/Soft Skills: technical and operational tasks prescribed by methods
- Level of analysis: KSA Quadrant analysis
- Diagrams: Predictive Performance Model (PPA)
- Competency libraries: ADAPTS

Facilitating use of Competency Information:
Establish standards based on validated curricula, assessment, and simulation libraries
Are we measuring the right way?

Not all validation is the same

Most competency model or assessment validations focus on whether the model statements and assessment questions relate to the job and are fair; rather than that they identify the critical elements that are predictive of job performance.

Validating construct and predictive validity

- Item Difficulty Index
- Item Discrimination Index
- Distractor Analysis
- Homogeneity Analysis
- Reliability Index
Are the measures meaningful and predictive?

Predictors of Performance
- Situational judgment
- Behavioral consistency

Achievement vs. Aptitude Assessment
- Achievement tests measures the **proficiency** of recall of past knowledge. These tests are **descriptive** – they classify people into categories based on the depth of understanding of a domain. They measure the observed score on a test.

- Aptitude tests measure future **potential**. These tests are considered **predictive** – forecasting how the tested individual can be expected to perform. These tests seek to separate knowledge from skill from ability. They use adaptive testing techniques and statistical analyses to measure the true score on a test.

Source: Schmitt, Cortina, Ingerick & Wiechmann (2003), p. 79
Eliciting organizational context through vignettes

<table>
<thead>
<tr>
<th>Vignettes</th>
<th>Security Operations Center Role</th>
<th>IT Security Role</th>
<th>Network Administration Role</th>
<th>Incident Handling Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>START HERE &gt;&gt;&gt; Vignette: A new security vulnerability has been announced that affects your organization, such as a Microsoft vulnerability.</td>
<td>1. Update relevant detection mechanisms (e.g. IDS signatures)</td>
<td>1. Oversee patching process</td>
<td>1. Implement mitigating controls related to network infrastructure (e.g. potentially a firewall/proxy/router block)</td>
<td>1. Prepare to respond to any incidents related to exploitation of the vulnerability</td>
</tr>
<tr>
<td></td>
<td>2. Ensure operational procedures updated to respond to new alerts</td>
<td>2. Coordinate with application administrators, system administrators for patch testing and deployment.</td>
<td>2. Implement firewall blocks, router ACLs, ensure bandwidth SLAs, review router/firewall logs for suspicious traffic</td>
<td>2. Respond to new compromises</td>
</tr>
<tr>
<td></td>
<td>3. Situational awareness of emerging threats related to the vulnerability</td>
<td>3. Assist in determining patch release timelines based on associated risk.</td>
<td>3. Implement new network mitigations related to this vulnerability</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Coordinate with the firewall, network, antivirus and intrusion detection teams to understand the signature coverage, status of vulnerability scans, firewall blocks in place, etc.</td>
<td>4. Implement associated security mitigations, such as intrusion detection signatures, host-based intrusion detection signatures and controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Develop a notification/alert to be disseminated to all relevant parties.</td>
<td>5. Create new rules in security tools to watch for new compromises exploiting this new vulnerability</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Monitor logs and IDS for new compromises that may be related to this new vulnerability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vignette: Data exfiltration: Company information/operations leaking to outside actor</td>
<td>1. Update relevant detection mechanisms (e.g. IDS signatures)</td>
<td>1. Evaluate recommendations in post mortem</td>
<td>1. Implement mitigating controls related to network infrastructure (e.g. potentially a firewall/proxy/router block)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Ensure operational procedures updated to respond to new alerts</td>
<td>2. Mitigate exfiltration and update security tools to monitor for exfiltration attempts</td>
<td>2. Assist in data gathering/monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Reviewing all sources of information relating to the data leakage to determine extent, time, location, etc.</td>
<td>3. Collect network information, netflow, router logs to assist in response.</td>
<td>3. Oversee remediation effort</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Monitor for exfiltration</td>
<td>4. Apply mitigations to firewalls and other network devices</td>
<td>4. Interface with law enforcement</td>
<td></td>
</tr>
</tbody>
</table>

Eliciting context through overlapping roles/responsibilities

<table>
<thead>
<tr>
<th>Update overarching policies and procedures</th>
<th>Security Operations Center Role</th>
<th>IT Security Role</th>
<th>Network Administration Role</th>
<th>Incident Handling Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure procedures address Phishing</td>
<td>Review SOP created by IT Security for detection and response</td>
<td>Create definitions for the different types of phishing attacks</td>
<td>Review SOP created by IT Security for detection and response</td>
<td>Review SOP created by IT Security for detection and response</td>
</tr>
<tr>
<td>Task ====&gt;</td>
<td>Implement the SOP created by IT Security for detection and response</td>
<td>Determine steps to respond to the various phishing attacks</td>
<td>Work with IT Security on the feasibility of the mitigations</td>
<td>Provide lessons learned feedback to IT Security as the SOP is followed and needs modifications</td>
</tr>
<tr>
<td>Task ====&gt;</td>
<td>Refer to the end-user training to educate end-users who call in</td>
<td>Create end-user training</td>
<td>Work with IT Security to update the SOP as new technologies are implemented</td>
<td></td>
</tr>
<tr>
<td>Task ====&gt;</td>
<td>Create SOP for responding to and mitigating phishing attacks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task ====&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**INSERT ROWS ABOVE THIS LINE AS NEEDED**

Policy/procedure definition to clarify process owner

| Task ====> | Work with the other roles to determine the various processes and who should own them | Work with the other roles to determine the various processes and who should own them | Work with the other roles to determine the various processes and who should own them | Work with the other roles to determine the various processes and who should own them |
| Task ====> | Create the process documentation for the Security Operations Center Role | Create the process documentation for the IT Security Role | Create the process documentation for the Network Administration Role | Create the process documentation for the Incident Handling Role |
| Task ====> | Review process documentation with the other roles | Review process documentation with the other roles | Review process documentation with the other roles | Review process documentation with the other roles |
| Task ====> | Obtain buy-in from the other roles on the Security Operations Center processes | Obtain buy-in from the other roles on the IT Security processes | Obtain buy-in from the other roles on the Network Administration processes | Obtain buy-in from the other roles on the Incident Handling processes |
| Task ====> | Lead an annual process documentation review for all roles | | | |

## Achieving alignment through goal/objective elicitation (PRISM)

<table>
<thead>
<tr>
<th>Goal</th>
<th>Priority</th>
<th>Objective measure</th>
<th>PRISM (\rightarrow)</th>
<th>(\rightarrow)</th>
<th>Improved</th>
<th>Satisfactory</th>
<th>Moot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update overarching policies and procedures</td>
<td>Primary</td>
<td>The time frame policies and procedures are updated to reflect the changing threat landscape</td>
<td>Policies and procedures are updated in real time as incidents are worked and new threats are discovered</td>
<td>Premier</td>
<td>Robust</td>
<td>Improved</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Perform gap analysis of ability to detect or identify vulnerable systems</td>
<td>Primary</td>
<td>Time frame required to determine gaps</td>
<td>Gap analysis performed within 1 hour of vulnerability notification</td>
<td>Premier</td>
<td>Robust</td>
<td>Improved</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Classify data properly and regularly review</td>
<td>Secondary</td>
<td>Percentage of data classified Frequency of review</td>
<td>100% of data classified and reviewed monthly</td>
<td>Premier</td>
<td>Robust</td>
<td>Improved</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Monitoring sources for vulnerability notices and changes in the threat environment</td>
<td>Primary</td>
<td>Person/Resource assigned task to monitor sources</td>
<td>Dedicated threat intelligence team Automated solution to monitor and provide information automatically to the team based on asset profiles, or risk profiles of members</td>
<td>Premier</td>
<td>Robust</td>
<td>Improved</td>
<td>Satisfactory</td>
</tr>
<tr>
<td>Respond to intrusion events</td>
<td>Primary</td>
<td>Monitor security events real time</td>
<td>24x7 security staff monitor security events real time</td>
<td>Premier</td>
<td>Robust</td>
<td>Improved</td>
<td>Satisfactory</td>
</tr>
</tbody>
</table>

Defining proficiency at multiple levels for multiple roles

1. How important is it that a person at the listed level of expertise, or filling the listed job role, be skilled at accomplishing this task?

<table>
<thead>
<tr>
<th>Entry Level</th>
<th>Intermediate</th>
<th>Expert Level</th>
<th>Commercial</th>
<th>Red Team</th>
<th>Blue Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Apprentice):</td>
<td>(Journeyman):</td>
<td>(Master):</td>
<td>Pentester:</td>
<td>Team:</td>
<td>Team:</td>
</tr>
<tr>
<td>2: Low</td>
<td>2: Low</td>
<td>2: Low</td>
<td>2: Low</td>
<td>2: Low</td>
<td>2: Low</td>
</tr>
<tr>
<td>3: Moderate</td>
<td>3: Moderate</td>
<td>3: Moderate</td>
<td>3: Moderate</td>
<td>3: Moderate</td>
<td>3: Moderate</td>
</tr>
<tr>
<td>5: Extremely</td>
<td>5: Extremely</td>
<td>5: Extremely</td>
<td>5: Extremely</td>
<td>5: Extremely</td>
<td>5: Extremely</td>
</tr>
</tbody>
</table>

1. Develop strategies for local traffic analysis
2. Develop mission/attack plan to assess security posture of client/target network
3. Use nontraditional problem-solving skills to solve complex problems
4. Apply filters to pull the correct protocols and ports
5. Develop an understanding of TCP/IP flow
6. Use packet captures to determine if a service is alive
7. Capture legit websites; add instrumentation for redirection and exploitation
8. Map the route between the engagement point and target(s)
9. Analyze e-mail communication for information leakage
10. Analyze active directory information
11. Interpret error messages
12. Map web server directory structure
13. Identify targets for planned attacks
14. Identify ownership of gateway devices
15. Attack vectors associated with error messages

Identifying indicators that differentiate skill levels

Relative Importance of Penetration and Operational Security Goals

## Identifying indicators that differentiate skill levels

<table>
<thead>
<tr>
<th>CRITICALITY</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DIFFERENTIATION</strong></td>
<td><strong>HIGH</strong></td>
</tr>
<tr>
<td>1. Recognize when tools provide inaccurate data</td>
<td></td>
</tr>
<tr>
<td>2. Multi-task between multiple phases of testing</td>
<td></td>
</tr>
<tr>
<td>3. Develop mission/attack plan to assess security posture of client/target network</td>
<td></td>
</tr>
<tr>
<td>4. Identify vulnerable network aware appliances on the target network.</td>
<td></td>
</tr>
<tr>
<td>5. Ensure all project goals and objectives are clear to team</td>
<td></td>
</tr>
<tr>
<td>6. Explain results of attacks to clients</td>
<td></td>
</tr>
<tr>
<td>7. Identify targets for potential exploitation</td>
<td></td>
</tr>
<tr>
<td>8. Establish control of Windows machines</td>
<td></td>
</tr>
<tr>
<td>9. Communicate best practices in security to clients</td>
<td></td>
</tr>
<tr>
<td>10. Identify major attack targets and assets</td>
<td></td>
</tr>
<tr>
<td>11. Identify specific vulnerabilities on identified hosts</td>
<td></td>
</tr>
<tr>
<td>12. Escalate privileges on an Active Directory network</td>
<td></td>
</tr>
<tr>
<td>13. Utilize pass the hash to compromise additional systems and privilege escalation to gain root access of a system.</td>
<td></td>
</tr>
<tr>
<td>14. Compromise individual host or service</td>
<td></td>
</tr>
<tr>
<td>15. Understand and attack standard data protection mechanisms</td>
<td></td>
</tr>
<tr>
<td>16. Survey environment to develop situational awareness of the environment.</td>
<td></td>
</tr>
<tr>
<td>17. Establish control of remote access mechanisms from inside</td>
<td></td>
</tr>
<tr>
<td>18. Demonstrate robust post-exploitation capability</td>
<td></td>
</tr>
<tr>
<td>19. Analyze data found on compromised machines for strategic value as seen by a worst case actual attacker</td>
<td></td>
</tr>
<tr>
<td>20. Analyze data found on compromised machines to enable exploitation deeper into the network.</td>
<td></td>
</tr>
<tr>
<td>21. Exploit web applications</td>
<td></td>
</tr>
<tr>
<td>22. Educate others to translate the cyberrisk to operational risk.</td>
<td></td>
</tr>
</tbody>
</table>

Defining the path to performance

Masters

Apprentices

Journeymen

Challenge 1: Competency modeling at ground truth speed

Process based on O*NET methodology
Challenge 1: Competency modeling at ground truth speed

Process based on critical incident elicitation methodology
Challenge 2: Facilitating alignment - The case of ATR

The 31 Cybersecurity Specialties:

**Securely Provision**
- Systems Requirements Planning
- Systems Development
- Software Engineering
- Enterprise Architecture
- Test and Evaluation
- Technology Demonstration
- Information Assurance Compliance

**Operate and Maintain**
- System Administration
- Network Services
- Systems Security Analysis
- Customer Service and Technical Support
- Data Administration
- Knowledge Management
- Information Systems Security Management

**Support**
- Legal Advice and Advocacy
- Education and Training
- Strategic Planning and Policy Development

**Protect and Defend**
- Computer Network Defense Infrastructure Support
- Vulnerability Assessment and Management
- Incident Response
- Computer Network Defense
- Security Program Management

**Investigate**
- Investigation
- Digital Forensics

**Operate and Collect**
- Collection Operations
- Cyber Operations Planning
- Cyber Operations

**Analyze**
- Cyber Threat Analysis
- Exploitation Analysis
- Targets
- All Source Intelligence
Challenge 2: Achieving alignment - The case of ATR

31 Specialty Areas (functional roles) organized in 7 categories

- Securely Provision
- Operate & Maintain
- Support
- Protect & Defend
- Investigate
- Operate & Collect
- Analyze

Advanced Threat Response Panel
4 Roles with 706 tasks

Incident Response (Specialty Area Label)
- Computer Crime Investigator
- Incident Handler (Job Title)
  - Incident Responder
  - Intrusion Analyst

Incident Handling Role
226 tasks

Incident Handling Role Item Pool

Technical tasks are prioritized by degree of differentiation and criticality

Exploratory factor analysis will yield a causal model of job performance

Technical tasks (reusable libraries populate Job Performance Models of multiple job roles)
Why job performance models are important

- Facilitate translation of functional roles into job roles
- Clearly distinguish knowledge, skill, and ability
- Determine factors that differentiate performance at varying levels of skill
- Identify the critical factors that predict performance
- Competency models describe
  Job performance models prescribe

JPM’s help to determine who should be developed (aptitude), how to develop them (skill profiles), and when they are ready to take the next step (performance-based learning)
Discussion

Thoughts

• How might the Framework be applicable to a staffing challenge you are facing?

• What could be the best method to evaluate individual cybersecurity competency (e.g. testing, hands-on application, etc.)?

• How might your organization make use of and benefit from a competency assessment methodology?
Determining Current Cybersecurity Capabilities

Develop and maintain an unrivaled, globally competitive cybersecurity workforce