White Hat Operations: Building an Effective Pen Testing Team
Agenda

• Distinctions between Red Team and pen testing
• Selling points for upper management
• Disadvantages and limitations
• Build the foundation and team
• Define the tool set and refine the processes
• Planning, Execution, Post Execution, and Report Writing
• Follow-up
## Pen Testing and Red Team Distinctions

<table>
<thead>
<tr>
<th>Type</th>
<th>Scope</th>
<th>Objectives</th>
<th>Tradecraft</th>
</tr>
</thead>
</table>
| **Penetration Testing** | Network, Web App, Solution, Social engineering (phishing) | - Enumerate vulnerabilities  
- Validate with known exploits  
- Show impact to what is scoped  
- Exercising Blue team is "not" an objective although we will collaborate with them so they can shadow the attack and tighten up their defenses later | - Utilize known TTPs  
- Stealth is not a factor  
  - Phishing requires the targets to be unaware but at the organizational level, this activity is a cooperative one |
| **Red Teaming**       | Organization: Cyber/Comms/Operations/Social/ sometimes physical (Not NCATS) | - Determine minimum necessary vulnerabilities/attack path(s) needed to achieve agreed upon objectives  
- Validate with known/unknown exploits  
- Show impact to what is scoped  
- As a separate activity or as part of the same one, exercise blue teams to measure how well they protect, detect, respond and in some cases recover against adversarial attacks | - For specific threat emulation, exercise known TTPs  
- For other cases, utilize any TTP allowed within the ROE to include 0-days developed by the assessing team.  
- Stealth is everything unless there is a specific threat being emulated that has a particular "signature".  
- Trusted agents are used to aid in insider threat or blue team monitoring situations. |
Why Build a Pen Test Team

- Compliance and governance
- Security tool validation
- HVA discovery and susceptibility
- User awareness and training
- Vulnerability identification
- Risk prioritization (low, medium, high)
- Asset discovery
- Identifies network strengths
- Identifies unknown deficiencies, weakness, and misconfiguration
- Justifies additional defensive/offensive spending
- Helps refine Incident Command process
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- RPCI-DSS regulations
- Inciident Response training
- People fear you for no good reason
- Refines Incident Command process
- Identifies network strengths
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- Security tool validation
- HVA discovery and susceptibility
- User awareness and training
- Vulnerability identification
- Risk prioritization (low, medium, high)
- Asset discovery
- Identifies network strengths
- Identifies unknown deficiencies, weakness, and misconfiguration
- Justifies additional defensive/offensive spending
- Helps refine Incident Command process
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- RPCI-DSS regulations
- Inciident Response training
- People fear you for no good reason
- Refines Incident Command process
- Identifies network strengths
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- Security tool validation
- HVA discovery and susceptibility
- User awareness and training
- Vulnerability identification
- Risk prioritization (low, medium, high)
- Asset discovery
- Identifies network strengths
- Identifies unknown deficiencies, weakness, and misconfiguration
- Justifies additional defensive/offensive spending
- Helps refine Incident Command process
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- RPCI-DSS regulations
- Inciident Response training
- People fear you for no good reason
- Refines Incident Command process
- Identifies network strengths
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- Security tool validation
- HVA discovery and susceptibility
- User awareness and training
- Vulnerability identification
- Risk prioritization (low, medium, high)
- Asset discovery
- Identifies network strengths
- Identifies unknown deficiencies, weakness, and misconfiguration
- Justifies additional defensive/offensive spending
- Helps refine Incident Command process
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- RPCI-DSS regulations
- Inciident Response training
- People fear you for no good reason
- Refines Incident Command process
- Identifies network strengths
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- Security tool validation
- HVA discovery and susceptibility
- User awareness and training
- Vulnerability identification
- Risk prioritization (low, medium, high)
- Asset discovery
- Identifies network strengths
- Identifies unknown deficiencies, weakness, and misconfiguration
- Justifies additional defensive/offensive spending
- Helps refine Incident Command process
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- RPCI-DSS regulations
- Inciident Response training
- People fear you for no good reason
- Refines Incident Command process
- Identifies network strengths
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- Security tool validation
- HVA discovery and susceptibility
- User awareness and training
- Vulnerability identification
- Risk prioritization (low, medium, high)
- Asset discovery
- Identifies network strengths
- Identifies unknown deficiencies, weakness, and misconfiguration
- Justifies additional defensive/offensive spending
- Helps refine Incident Command process
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- RPCI-DSS regulations
- Inciident Response training
- People fear you for no good reason
- Refines Incident Command process
- Identifies network strengths
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- Security tool validation
- HVA discovery and susceptibility
- User awareness and training
- Vulnerability identification
- Risk prioritization (low, medium, high)
- Asset discovery
- Identifies network strengths
- Identifies unknown deficiencies, weakness, and misconfiguration
- Justifies additional defensive/offensive spending
- Helps refine Incident Command process
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- RPCI-DSS regulations
- Inciident Response training
- People fear you for no good reason
- Refines Incident Command process
- Identifies network strengths
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- Security tool validation
- HVA discovery and susceptibility
- User awareness and training
- Vulnerability identification
- Risk prioritization (low, medium, high)
- Asset discovery
- Identifies network strengths
- Identifies unknown deficiencies, weakness, and misconfiguration
- Justifies additional defensive/offensive spending
- Helps refine Incident Command process
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- RPCI-DSS regulations
- Inciident Response training
- People fear you for no good reason
- Refines Incident Command process
- Identifies network strengths
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- Security tool validation
- HVA discovery and susceptibility
- User awareness and training
- Vulnerability identification
- Risk prioritization (low, medium, high)
- Asset discovery
- Identifies network strengths
- Identifies unknown deficiencies, weakness, and misconfiguration
- Justifies additional defensive/offensive spending
- Helps refine Incident Command process
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- RPCI-DSS regulations
- Inciident Response training
- People fear you for no good reason
- Refines Incident Command process
- Identifies network strengths
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- Security tool validation
- HVA discovery and susceptibility
- User awareness and training
- Vulnerability identification
- Risk prioritization (low, medium, high)
- Asset discovery
- Identifies network strengths
- Identifies unknown deficiencies, weakness, and misconfiguration
- Justifies additional defensive/offensive spending
- Helps refine Incident Command process
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- RPCI-DSS regulations
- Inciident Response training
- People fear you for no good reason
- Refines Incident Command process
- Identifies network strengths
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- Security tool validation
- HVA discovery and susceptibility
- User awareness and training
- Vulnerability identification
- Risk prioritization (low, medium, high)
- Asset discovery
- Identifies network strengths
- Identifies unknown deficiencies, weakness, and misconfiguration
- Justifies additional defensive/offensive spending
- Helps refine Incident Command process
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- RPCI-DSS regulations
- Inciident Response training
- People fear you for no good reason
- Refines Incident Command process
- Identifies network strengths
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- Security tool validation
- HVA discovery and susceptibility
- User awareness and training
- Vulnerability identification
- Risk prioritization (low, medium, high)
- Asset discovery
- Identifies network strengths
- Identifies unknown deficiencies, weakness, and misconfiguration
- Justifies additional defensive/offensive spending
- Helps refine Incident Command process
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- RPCI-DSS regulations
- Inciident Response training
- People fear you for no good reason
- Refines Incident Command process
- Identifies network strengths
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- Security tool validation
- HVA discovery and susceptibility
- User awareness and training
- Vulnerability identification
- Risk prioritization (low, medium, high)
- Asset discovery
- Identifies network strengths
- Identifies unknown deficiencies, weakness, and misconfiguration
- Justifies additional defensive/offensive spending
- Helps refine Incident Command process
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- RPCI-DSS regulations
- Inciident Response training
- People fear you for no good reason
- Refines Incident Command process
- Identifies network strengths
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- Security tool validation
- HVA discovery and susceptibility
- User awareness and training
- Vulnerability identification
- Risk prioritization (low, medium, high)
- Asset discovery
- Identifies network strengths
- Identifies unknown deficiencies, weakness, and misconfiguration
- Justifies additional defensive/offensive spending
- Helps refine Incident Command process
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- RPCI-DSS regulations
- Inciident Response training
- People fear you for no good reason
- Refines Incident Command process
- Identifies network strengths
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- Security tool validation
- HVA discovery and susceptibility
- User awareness and training
- Vulnerability identification
- Risk prioritization (low, medium, high)
- Asset discovery
- Identifies network strengths
- Identifies unknown deficiencies, weakness, and misconfiguration
- Justifies additional defensive/offensive spending
- Helps refine Incident Command process
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
- Compliance and governance
- RPCI-DSS regulations
- Inciident Response training
- People fear you for no good reason
- Refines Incident Command process
- Identifies network strengths
- Justifies the stickers on your laptop
- You get to wear a hoodie
- It's fun!
Potential Disadvantages and Limitations

- Covers just the target application, infrastructure, or environment that has been selected.
- Focuses on the exposures in technical infrastructure, so it is not intended to cover all the ways in which critical or sensitive information can leak out of your organization.
- *Plays only a small part (despite often including social engineering tests) in reviewing the people element (often the most important element of an organization's defense system)*.
- Is only a snapshot of a system at a point in time.
- Can be limited by legal or commercial considerations, limiting the breadth or depth of a test.
- May not uncover all security weaknesses, for example due to a restricted scope or inadequate testing.
- Provides results that are often technical in nature and need to be interpreted in a business context.
- Ensure that the organization has reached at least a moderate level of INFOSEC maturity and cyber hygiene.
Lay the Groundwork and Build a Foundation

• Leadership and legal approval
• Funding
• Create and develop documentation
  o Mission statement
  o Organizational charts
  o Rules of Engagement
  o Scoping documents
  o CONOPS, test plans, FAQs, process flows
  o Reporting templates and/or generators
  o Follow-up processes
  o Measure success
• Align with an existing, established framework such as NIST cybersecurity framework, ISO 27001, ISF, etc.
Define the services and tools
Build the team

Apprentice

Journeyman

Master

Skill Sets

Established skill in compliance system fundamentals, basic network systems techniques, and software and the ability to maintain and advance systems, services, and infrastructure.

CISPP, Security+ Certified

1-3 Year Experience

Bachelor's degree

DNS, GCIH
Refine the processes

- Customer Out-brief
- Validate Evidence
- Report Writing
- Assist with Remediating Weaknesses
- Create Post-Assessment Follow Up
- Strategic Roadmap
- Self Assessment/Lessons Learned

Post-Execution
Establish Rules of Engagement
Define the Purpose
Identify Target Systems
Conduct Preliminary Assessment Briefs
Confirm Dates and Time Frames
Notify SOC and External Partners
Procure Scoping Documents

### SELECTION OF ASSESSMENT SERVICES

*Acronym* authorizes DHS to perform the required service(s) as part of the HVA RVA, on the networks/systems listed below in this Appendix A, as described in the *Risk & Vulnerability Assessment Catalog, Version 3.2, Appendix C*.

External testing will be conducted by the RVA team from a range of attributed or unattributed IP addresses that may not be identified to *Acronym*, and that may change periodically without notice to *Acronym*. Agency defense systems, such as intrusion detection or prevention systems, may detect and react to this testing activity. As such, the agency Site Monitor should be prepared to react accordingly by, for example, ensuring a perceived attempted intrusion related to this testing is not incorrectly reported outside of the agency as an incident. Internal testing will be conducted by the RVA team either on-site or through a virtual private network (VPN) provided by *Acronym*.

<table>
<thead>
<tr>
<th>Site Name/Address</th>
<th>IP For Assessment</th>
<th>IP Excluded</th>
<th>Need for Admin Access?</th>
<th>Select: External, Internal/On-Site</th>
<th>Authorized Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Name/Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Authorized Testing Sites & Services

1. Penetration Testing
2. Phishing Assessment
3. Web Application Assessment
National Cybersecurity Assessment and Technical Services (NCATS)

Data Handling and Storage Guide (DHG)

Prepared for
Department of Homeland Security Headquarters (DHS HQ)
CS&C
1110 Glebe Rd. Arlington, VA 22201

Prepared by
National Cybersecurity Assessment and Technical Services (NCATS)

September 30, 2014
Customer Out-brief

Self Assessment/Lessons Learned

Strategic Roadmap

Create Post-Assessment Follow Up

Assist with Remediating Weaknesses

Validate Evidence

Report Writing

Post Execution
Penetration Testing Guidelines and Frameworks

- NCATS Training and Qualification (TAQ)
- National Institute of Standards (NIST) 800-115
- Penetration Testing Execution Standard (PTES)
- Open Source Security Testing Methodology Manual (OSSTIMM)
- Information Systems Security Assessment Framework (ISSAF)
- Open Web Application Security Project (OWASP)
The NCATS team provides a robust training and qualification (TAQ) program to federal departments and agencies encompassing the methodologies, processes, policies and procedures employed by the NCATS Risk and Vulnerability Assessment (RVA) program to conduct vulnerability scanning and penetration testing. As part of the training, practicums are used to validate individual skills and qualify third party teams for participation in DHS-led surge force activities should the need arise.

[1] Planning and Pre-Qualification
- Candidate registration
- Sign and return registration documents
- Candidate pre-qualification evaluation

[2] Training
- Attend virtual classroom training
- Complete RVA training modules

[3] Qualification
- Conduct pre-assessment activities
- Perform all technical assessment activities on the Skills Range as a team
- Deliver report and oral briefing
- Receive qualification certification

[4] Activation
- Notification of surge force activation
- Commence assessment activities

DHS-validated teams share non-attributional summary data and findings with NCATS in order to create trending across the federal government on systemic weakness and effective countermeasures.

NCATS_INFO@hq.dhs.gov
Questions?