Penetration Tester

<table>
<tr><td><b>NICE Framework Reference</b></td><td colspan="2">None.</td></tr>
<tr><td><b>Functional Description</b></td><td colspan="2">Conducts formal, controlled tests and physical security assessments on web-based applications, networks, and other systems as required to identify and exploit security vulnerabilities.</td></tr>
<tr><td><b>Consequence of error or risk</b></td><td colspan="2">Error, neglect, outdated information, lack of attention to detail or poor judgment could result in mis-identifying or not detecting vulnerabilities which could be comprised. This may have a significant impact on organizational IT systems, capabilities or functions.</td></tr>
<tr><td><b>Development pathway</b></td><td colspan="2">This is often a tier 2 / 3 position within a cybersecurity operations environment that is normally preceded by significant experience (3-5 years) in a cybersecurity operations role including employment within Vulnerability Analysis, Malware Analysis or Technical Analysis of security systems. This is an advanced technical role, which can lead to increasing technical specialization, red team leadership or management roles.</td></tr>
<tr><td><b>Other titles</b></td><td colspan="2">▪ Security Testing and Evaluation Specialist
▪ Advanced Vulnerability Assessment Analyst</td></tr>
<tr><td><b>Related NOCs</b></td><td colspan="2">2171 Information systems analysts and consultants
2147 Computer engineers (except software engineers and designers)
2173 Software engineers and designers</td></tr>
<tr><td><b>Tasks</b></td><td colspan="2">▪ Complete penetration tests on web-based applications, network connections, and computer systems to identify cyber threats and technical vulnerabilities
▪ Conduct physical security assessments of an organization's network, devices, servers, and systems
▪ Develop penetration tests and the tools needed to execute them (e.g. standards, risks, mitigations)
▪ Investigate for unknown security vulnerabilities and weaknesses in web applications, networks, and relevant systems that cyber actors can easily exploit
▪ Develop and maintain documents on the results of executed pen testing activities
▪ Employ social engineering to uncover security gaps
▪ Define and review requirements for information security solutions
▪ Analyze, document, and discuss security findings with management and technical staff
▪ Provide recommendations and guidelines on how to improve upon an organization's security practices
▪ Develop, deliver, and oversee training material and educational efforts</td></tr>
<tr><td rowspan="3"><b>Required qualifications</b></td><td>Education</td><td>Post-secondary education (degree or diploma in related computer science or IT field).</td></tr>
<tr><td>Training</td><td>Training in vulnerability analysis and penetration testing tools, techniques and procedures.</td></tr>
<tr><td>Work experience</td><td>2-3 years' experience in an advanced cybersecurity operations role, preferably with VA experience.</td></tr>
<tr><td><b>Tools &amp; Technology</b></td><td colspan="2">▪ Organizational security policies, procedures and practices
▪ Organizational systems map and network architecture</td></tr>
</table>

	▪ VA tools ▪ Vulnerability management policies, processes and practices ▪ Common vulnerability databases ▪ Penetration testing tools and protocols
Competencies	KSAs applied at an advanced level: ☐ Network security architecture ☐ Advanced threat actor tools, techniques and protocols ☐ Penetration testing principles, tools, and techniques ☐ Risk management processes for assessing and mitigating risks ☐ System administration concepts ☐ Cryptography and cryptographic key management concepts ☐ Cryptology ☐ Identifying security issues based on the analysis of vulnerability and configuration data ☐ Vulnerability management policies, processes and practices ☐ Penetration test planning and scheduling including system risks and mitigations ☐ System and application security threats and vulnerabilities ☐ System administration, network, and operating system hardening techniques ☐ Packet analysis using appropriate tools ☐ Conducting vulnerability scans and recognizing vulnerabilities in security systems ☐ Conducting vulnerability/impact/risk assessments ☐ Reviewing system logs to identify evidence of past intrusions ☐ Using network analysis tools to identify vulnerabilities
Future Trends Affecting Key Competencies	▪ The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their responsibilities for detecting, responding to and recovering from a cybersecurity incident. ▪ If practiced within the organization, there will be a requirement to fully understand the implications of 'bring your own device' (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. ▪ Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into the SOC including implementation of personnel and process changes. ▪ Increased use of automated tools by threat actors pose challenges for organizations that do not have complementary defensive tools. Accordingly, creative, locally relevant mitigation strategies will be required. This will require well-honed critical and abstract thinking abilities. ▪ Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. ▪ The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe

	strategy, understanding system vulnerabilities and how to mitigate quantum-related threats.