THE REGISTERED APPRENTICESHIP OCCUPATIONS AND STANDARDS CENTER OF EXCELLENCE (AOSC)

Penetration Tester
National Occupational Framework

ONET Code: 15-1299.04

RAPIDS Code: 3030

Created: June 2024

This project has been funded, either wholly or in part, with federal funds from the Department of Labor, Employment and Training Administration under Cooperative Grant Number AP-36653-21-75-A-11. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of the same by the US Government.

ABOUT THE URBAN INSTITUTE

The nonprofit Urban Institute is dedicated to elevating the debate on social and economic policy. For nearly five decades, Urban scholars have conducted research and offered evidence-based solutions that improve lives and strengthen communities across a rapidly urbanizing world. Their objective research helps expand opportunities for all, reduce hardship among the most vulnerable, and strengthen the effectiveness of the public sector.

Acknowledgments

We want to thank several people who have contributed to developing and vetting this National Occupational Framework. We would especially like to thank Miranda Santillo, Leslee Haisma, and Diane Jones for their research, support, and contributions to developing the National Occupational Framework. Additionally, we had terrific experts lend their time, review, and support to the framework. They include Gene Ellis, consultant and senior SME at Safal Partners; Ashley Felton, CEO at Tech NIC Ally; Andrea Harston, security researcher and owner of The Cyber Dirt; Ray Sims, global delivery coordinator at X-Force, IBM; Jason Addison, cyber security analyst at the Department of Defense; Brian Correia, director of business development at GIAC, SANS Institute; James Shewmaker, instructor at SANS Institute; Ed Skoudis, SANS fellow and president at the SANS Technology Institute; Kimberly Bashman, business development manager for Security Compliance Associates; Ben Johnson, senior penetration tester for Security Compliance Associates; Jason Miller, lead cyber engineer at ManTech International Corporation; Robert Broughman, director of security for Urban Institute. Finally, we thank Zach Boren and Lexi Mills for their thoughtful review.

Introduction to Using This Document

Under the Registered Apprenticeship Technical Assistance Centers of Excellence award, the Urban Institute leads the Occupations and Standards work. One of the main objectives of Urban's project is to create high-quality, well-researched, consensus-based work process schedules that are nonproprietary and widely available. This document is a product of that work and contains three sections: the occupational overview, the work process schedule, and the related technical instruction.

The **occupational overview** is a general introduction, including alternative job titles, any prerequisites, and, if applicable, the total number of hours needed to complete a time-based or hybrid program.

The **work process schedule** outlines the major job functions, competencies, and/or hours an apprentice completes in a registered apprenticeship program. It outlines what apprentices are expected to learn on the job with the support of a mentor or journeyworker (a worker mastering the competencies of an occupation in a particular industry), including both core competencies and those deemed optional by experts in the field. The work process schedule is the foundational document guiding a program.

Urban works with numerous experts to ensure the content is thoroughly researched and vetted to reflect the expectations of industry, educators, labor unions, employers, and others involved in apprenticeship for this occupation. Sponsors and employers can use the work process schedule as their program standards with assurances it has been approved by experts in the field.

The **related technical instruction** presents considerations for the coursework that apprentices will undertake to supplement on-the-job learning. It is intended to serve as a reference to sponsors exploring their options for the accompanying classroom, virtual, or hybrid training.

How to Use the Work Process Schedule

Sponsors can adapt the work process schedule to accommodate their needs for competency- or time-based or hybrid programs. In a **competency-based** apprenticeship, sponsors assess apprentices' progress across core and optional competencies listed in the work process schedule. In a **time-based** apprenticeship, apprentices complete a predetermined number of hours across major job functions and the program overall. In a **hybrid** apprenticeship, sponsors monitor apprentices' hours spent on major job functions and assess their proficiency across competencies.

Each program type has a different method of assessment:

- **For a competency-based program**, apprentices engage in activities and make progress toward proficiency in the identified competencies. Sponsors overseeing apprentices' work assess their mastery of the outlined competencies using the following rating scale:

  4—Competent/proficient (able to perform all elements of the task successfully and independently)

  3—Satisfactory performance (able to perform elements of the task with minimal assistance)

  2—Completed the task with significant assistance

  1—Unsuccessfully attempted the task

  0—No exposure (note the reason—absence, skill isn't covered, etc.)

  The competencies may be completed in any order. Apprentices must perform at a level 4 or 3 in all competencies listed as "core" to complete the apprenticeship program successfully.

- **For a time-based program,** sponsors monitor apprentices' completion of hours in training across major job functions. The total number of hours recommended for this occupation is listed in the occupational overview and is based on guidance from the US Department of Labor. Generally, apprentices must have at least 2,000 hours overall for on-the-job learning, but occupations of greater complexity may require more hours. Sponsors will provide apprentices with supervised work experience and allocate the total number of hours across the major job functions to adequately train their apprentices.

- **The hybrid approach** blends both competency- and time-based strategies. Sponsors measure apprentices' skills acquisition through a combination of completing the minimum number of hours of on-the-job learning successfully demonstrating identified competencies. Sponsors will assess apprentices' proficiencies as described for competency-based programs with a rating scale of 0–4 for every core competency. Generally, apprentices have at least 2,000 hours overall for on-the-job learning, but occupations of greater complexity may require more hours. Sponsors will document apprentices' completion within a minimum and maximum range of hours assigned for each major job function.

Penetration Tester Occupational Overview

Occupational Purpose and Context

Penetration testers evaluate network system security by conducting simulated internal and external cyberattacks using adversary tools and techniques. They attempt to breach and exploit critical systems and gain access to sensitive information to assess system security.

Potential Job Titles

Systems security tester, cyber assessor, security application tester, tester, hacker, information security assessor, hardware hacker, cyber tester, vulnerability analyst

Apprenticeship Prerequisites

Apprentices should have a high school diploma or equivalent, and benefit from a bachelor's degree in a related field (information technology, computer science, etc.) and strong problem-solving skills. Apprentices may have gained working knowledge of computer networks, information technology, and security technologies. They may also have the ability to script or write code.

Recommended Length of Apprenticeship (Time/Hybrid Programs Only)

The recommended time for on-the-job learning in a penetration tester apprenticeship is 2,000–3,000 hours.

Work Process Schedule

Penetration Tester

ONET Code: 15-1299.04

RAPIDS Code: 3030

Instructions for Use:

Competency-based programs: In the "performance level achieved" column of the work process schedule (see examples starting on the next page), assess apprentices' performances on each competency with the scale below. No monitoring of hours is required for this approach. See "Guidelines for Competency-Based, Hybrid and Time-Based Apprenticeship Training Approaches," US Department of Labor, Employment and Training Administration, Office of Apprenticeship, October 20, 2015, https://www.apprenticeship.gov/sites/default/files/bulletins/Cir2016-01.pdf.

4—Competent/proficient (able to perform all elements of the task successfully and independently)

3—Satisfactory performance (able to perform elements of the task with minimal assistance)

2—Completed the task with significant assistance

1—Unsuccessfully attempted the task

0—No exposure (note the reason—absence, skill isn't covered, etc.)

Time-based programs: In the "hours" row, specify the number of hours apprentices will fulfill for each job function. No assessment of competencies is required for this approach.

Hybrid programs: In the "performance level achieved" column, assess apprentices' performances on each competency using the 0–4 scale above. In the "hours" row, identify a range of hours apprentices should spend working on each major job function.

Job Function 1: Performs pretesting engagement tasks		
Hours (time-based and hybrid programs only):		
Competencies	**Core or optional**	**Performance level achieved (0–4)** (competency-based and hybrid programs only)
A. Operates using ethical hacking standards during all risk assessment operations	Core	
B. Defines the scope of testing, statement of work, and rules of engagement and understands the risks associated with the testing	Core	
C. Identifies the designated points of contact within the organization being penetrated, along with the mode of contact	Core	
D. Establishes timeline for testing phases and tasks	Core	
E. Obtains written permission from the organization to perform testing	Core	
F. Collects stakeholder data to evaluate risk and mitigation strategies	Core	
G. Collaborates with internal and external partner organizations on target access and operational issues	Core	
H. Develops testing methodologies, such as wireless, data networks, application, and telecommunication security tests	Core	

Job Function 2: Conducts reconnaissance		
Hours (time-based and hybrid programs only):		
Competencies	**Core or optional**	**Performance level achieved (0–4)** (competency-based and hybrid programs only)
A. Gathers information about known threats to the organization and industry to identify current vulnerabilities	Core	
B. Conducts passive reconnaissance within the scope of work by searching publicly available information, including Domain Name System (DNS) records, websites, social media, tax, and other publicly available information	Core	

C. Conducts active reconnaissance within the scope of work, including working with the network, operating system, user accounts, mail servers, Cloud footprints, and web domains	Core	

Job Function 3: Performs scanning		
Hours (time-based and hybrid programs only):		
Competencies	**Core or optional**	**Performance level achieved (0–4)** (competency-based and hybrid programs only)
A. Analyzes physical and logical digital technologies to identify potential avenues of access	Core	
B. Runs discovery scans of the network to identify connected systems	Core	
C. Performs vulnerability scans of discovered assets to determine system weaknesses	Core	
D. Conducts network and security system assessments using reconnaissance and tools	Core	
E. Tests the security of the network by using social engineering strategies	Optional	
F. Prioritizes identified avenues of attack based on their value and potential impact	Core	

Job Function 4: Conducts vulnerability assessments		
Hours (time-based and hybrid programs only):		
Competencies	**Core or optional**	**Performance level achieved (0–4)** (competency-based and hybrid programs only)
A. Evaluates vulnerability assessments of local computing environments, networks, infrastructures, or segmentation boundaries using either automated or manual processes	Core	
B. Identify security system weaknesses to be exploited and evaluate the associated risks from vulnerabilities using the National Vulnerability Database (NVD)	Core	
C. Demonstrates understanding of tools and setting/safety protocols before running production testing, including third-party systems	Core	

D. Identifies the existence of vulnerabilities using tools and manual techniques	Core	
E. Identifies environmental and mitigating factors that may influence the severity of vulnerabilities	Core	
F. Researches exploits to determine risk and relay to the client before performing exploitation attempts	Core	

Job Function 5: Performs exploitation of networks, applications, and systems		
Hours **(time-based and hybrid programs only):**		
Competencies	**Core or optional**	**Performance level achieved (0–4)** (competency-based and hybrid programs only)
A. Conducts network and security system assessment using ethical specialized tools	Core	
B. Develops and executes infiltration tests that simulate the techniques of known cyber threat actors to exploit device vulnerabilities	Core	
C. Tests the security of systems by attempting to gain access to networks, web-based applications, or computers	Core	
D. Avoids detection during exploitation by using strategies such as living off the land, data exfiltration, covering tracks, steganography, or establishing a covert channel	Core	
E. Deploys Command-and-Control (C2) framework for remote control and access of exploited system(s)	Core	
F. Attempts various techniques for lateral movement through compromised systems to discover other systems and penetrate deeper into the target environment	Core	
G. Handles all sensitive data ethically by proper protocols	Core	
H. Documents exploitation attempts, including steps taken to gain access	Core	

Job Function 6: Conducts post testing analysis		
Hours (time-based and hybrid programs only):		
Competencies	**Core or optional**	**Performance level achieved (0–4)** (competency-based and hybrid programs only)
A. Identifies any systemic root causes of security system weakness using penetration test results	Core	
B. Interprets design or operational test results	Core	
C. Determines severity of identified risks using the Common Vulnerability Scoring System (CVSS) and prioritizes vulnerabilities	Core	
D. Tests computer system operations to ensure proper functioning and removes any system or network alterations made during exploitation	Core	
E. Collaborates with IT team to ensure vulnerabilities are appropriately patched and mitigated	Core	
F. Conducts post report delivery activities	Core	
G. Demonstrates understanding of post engagement clean-up, client acceptance, follow-up actions, and retests	Core	
H. Identifies data remnants and demonstrates an understanding of the data destruction process	Optional	

Job Function 7: Reports findings to appropriate stakeholders		
Hours (time-based and hybrid programs only):		
Competencies	**Core or optional**	**Performance level achieved (0–4)** (competency-based and hybrid programs only)
A. Writes reports for appropriate audiences (e.g., executives, third-party stakeholders, technical staff, and developers)	Core	
B. Develops an executive summary presentation on threat intelligence	Core	
C. Prepares operational, analytical, or technical reports or presentations	Core	
D. Develops and submits reports documenting and describing the results of security fixes	Core	

E. Recommends remediations on security solutions to information technology teams or management	Core	
F. Makes recommendations on design or technical features of products or services with technical personnel	Core	

Job Function 8: Participates in ongoing professional development		
Hours (time-based and hybrid programs only):		
Competencies	**Core or optional**	**Performance level achieved (0–4)** (competency-based and hybrid programs only)
A. Stays informed about current industry-specific developments	Core	
B. Keeps up with new penetration testing tools and methods	Core	
C. Maintains up-to-date skills in hacking trends; demonstrates an understanding of the current threat actors and tactics, techniques, procedures	Core	
D. Maintains up-to-date skills in networking and network authentication protocols and systems such as Lightweight Directory Access Protocol (LDAP), Kerberos, New Technology LAN Manager (NTLMv2), Link-Local Multicast Name Resolution (LLMNR), and other active directory services	Core	
E. Maintains advanced skills in internal network architecture, boundaries, zone, cloud environments, Internet of Things (IOT), and zero trust architecture	Core	
F. Maintains cloud specific knowledge of accounts/projects, users, Identity and Access Management (IAM), Kubernetes, serverless computer, and storage	Core	

Related Technical Instruction

Penetration Tester

ONET Code: 15-1299.04
RAPIDS Code: 3030

Instructions for Use:

Registered apprenticeships must include at least 144 hours of related technical instruction (RTI). Courses offered by accredited colleges and universities may be assigned a credit hour determination rather than a contact hour determination. In general, an academic credit unit is the equivalent of 15 clock hours of instruction. [Insert specifications for this occupation]

Development and Use of This RTI Outline: Employers and academic institutions may approach RTI in markedly different ways. Our goal was not to identify the single best way to provide RTI or to identify a single provider whose content we deemed to be superior. Instead, our goal was to survey numerous education providers, including employers, institutions of higher education, high schools, private continuing education providers, labor organizations, professional associations and, in some cases, municipalities that provide worker training, to identify topics or courses common among those providers that align with the job functions included in this work process schedule. Those common topics or courses are reflected in the RTI outline provided below, which may be useful in developing your RTI program or communicating your needs to an educational partner.

Licensure or certification requirements: Although states do not require penetration testers to be licensed or certified, for those working with the Department of Defense or Department of Defense contractors, a Global Information Assurance Certification (GIAC), Penetration Tester Certification (GPEN), or GIAC Cloud Penetration Tester Certification (GCPN) may be required. Some employers may require penetration testers to hold other certifications, such as CompTIA PenTest.
Degree requirements for licensure or certification, if applicable: None
Accreditation requirements of instructional provider for licensure or certification, if applicable: Not applicable
Anticipated changes in licensure or certification requirements, if known: None
Examples of state licensure or certification requirements: None

Examples of RTI providers for this occupation

Professional associations and labor organizations: ISC2, a member association for cybersecurity professionals, offers training in various aspects of cybersecurity, although they do not offer specific training or certification programs for penetration testers.

Military: The armed services provide cybersecurity training and opportunities for cybersecurity specialists to earn GIAC certifications. Military service members must undergo a background check and polygraph to gain top-secret clearance. They will then be assigned to a Texas, Georgia, Virginia, Maryland, or New York base to train in this area.

States/municipalities: N/A

Colleges and universities: Colleges and universities often provide education in cybersecurity; however, penetration testing education programs are often postgraduate programs available only to those with a bachelor's degree in computer science or information technology. Several community colleges offer associate degree programs in penetrating testing that will prepare individuals for industry certifications, such as CompTIA's Security+ and EC=Council's Certified Ethical Hacker (CEH). Many colleges and universities offer noncredit programs and "boot camps" to prepare individuals to pass the CompTIA Security+ certification exam.

No-cost online providers: No-cost online providers, such as Coursera, EdX, and Udemy, offer penetration testing courses, including those delivered by colleges and universities and corporate providers (such as the IBM Skills Network Team). Google also offers a professional cybersecurity certificate through Coursera.

Continuing education or specialty education providers: Several private sector cybersecurity education and training providers offer training and certification in penetration testing.

Prerequisite knowledge, skills or experience typically required by RTI providers for this occupation

RTI providers may require individuals to have experience working with computers. Some employers may also require penetration testers to pass a background check or qualify for a security clearance.

Communication

Hours: 20–30

Sample learning objectives

- Demonstrate the ability to send and receive phone calls, emails, text messages, instant messages, and other forms of electronic communication
- Compose emails, formal letters, memorandums, and reports using appropriate format, spelling, capitalization, grammar, and punctuation
- Provide detailed instructions verbally and in writing to explain how a particular process is done, how a product is made, or to explain decision logic
- Describe effective strategies for engaging in active listening and assessing whether another party understands your message
- Work as part of a team to create a report or complete a project

- Demonstrate effective strategies for managing conflict and maintaining calmness and composure under stressful conditions

Introduction to Computer Systems
Hours: 20–30
Sample learning objectives ▪ Describe the basic elements of computer systems typically used in homes, offices, small businesses, large companies, manufacturing facilities, academic institutions, and government agencies. ▪ Describe the purpose of computer software and the basic processes used to develop, test, and implement various software packages. ▪ Explain the advantages and disadvantages of open-source software. ▪ Discuss the principles of Cloud computing as well as the advantages and disadvantages of using Cloud-based systems, software, and storage solutions. ▪ Discuss the basic processes used to develop, test, and launch new software and applications. ▪ Compare and contrast computers, tablets, and smartphones. ▪ Explain the strategies used by individuals, organizations, system and network specialists, and software developers to improve data and system security.

Introduction to Cybersecurity
Hours: 30–45
Sample learning objectives ▪ List and explain the three principles of cybersecurity. ▪ Explain the types of vulnerabilities that cyber attackers can leverage to penetrate computer systems, steal data, shut down computer-operated equipment or machines, or render computers/computer systems inoperable. ▪ Identify instances of attempted cyberattacks, such as phishing, ransomware, password attack, malware, spyware, disruption of service, man-in-the-middle attack, denial of service attack, structured query language (SQR), injection, zero-day exploit, and Domain Name System (DNS) tunneling. ▪ Explain the strategies used to prevent cyberattacks. ▪ Explain the importance of passwords in reducing cyber threats. ▪ Describe the purpose of the National Institute for Science and Technology (NIST) Cybersecurity Framework and demonstrate the ability to use the framework to manage cybersecurity risk. ▪ Describe the purpose of ISO/IEC 29001 standards for information security controls.

Introduction to Software Development
Hours: 20–30
Sample learning objectives ▪ Differentiate between system software, programming software, application software, and embedded software and provide examples of languages and platforms used to create each. ▪ Demonstrates basic application computing and architectural concepts such as layered architecture types vs. Service Oriented Architectures (SOA) and Microservice environments and how they have evolved over time. ▪ Demonstrates understanding of consumer applications vs. enterprise application environments. ▪ Identify software tools used most to develop apps on Windows, Android, iOS, macOS, and Linux platforms and compare and contrast the advantages and disadvantages. ▪ Describe the role of linkers, compilers, code editors, GUI designers, assemblers, debuggers, IDEs, static code analysis, code coverage tools, and performance analysis tools in developing software. ▪ Compare and contrast commonly used software development tools such as application lifecycle management (ALM), Integrated Development Environments (IDE), Source Code Management (SCM), Test Management, Application Performance Monitoring (APM), Test Automation, Static Analysis, and other application development and delivery toolsets. ▪ Explain how software developers ascertain and document client, end user, or other stakeholder specifications or standards that software must meet. ▪ Discuss ways in which data can be migrated to use or update software from existing applications or data sources. ▪ Explain the purpose of relational vs. nonrelational database technologies. ▪ Describe the use of Relational Database Management Systems in creating database objects and tables, and demonstrate the ability to create a basic database in MySQL, SQL Server, MS Access, Oracle, Sybase, Informix, PostgreSQL or other database systems.

Introduction to Penetration Testing
Hours: 30–45
Sample learning objectives ▪ Explain the purpose of penetration testing ▪ Discuss the importance of ethics in using penetrating testing methods for authorized purposes ▪ List and describe the key stages of effective penetrating testing, including preengagement and planning, intelligence gathering, vulnerability analysis and exploitation, postexploitation (remediation), and reporting and certification. ▪ Develop a penetrating testing framework for different aspects of testing: discovery, proving reconnaissance, enumeration, and vulnerability assessments. ▪ Define and demonstrate the ability to use an Open-Source Security Testing Methodology Manual. ▪ Explain the purpose of and demonstrate the ability to use the Open Web Application Security Project to identify critical threats. ▪ Explain the purpose of and demonstrate the ability to use NIST penetration testing methodologies.

- Demonstrate the ability to follow Penetrating Testing Execution Standards to conduct penetrating testing.
- Demonstrate the ability to use the Information System Security Assessment Framework to conduct penetration testing and explain the utility of the Information Systems Security Assessment Framework (ISSAF) in the future, since it is no longer being updated.

Advanced Penetration Testing

Hours: 30–45

Sample learning objectives

- List and explain the advantages and disadvantages of using automated or software-driven penetration testing tools.
- Perform intelligence gathering on a variety of systems or software products using automated and manual tools to identify potential vulnerabilities or entry points.
- Demonstrate the ability to use various testing tools for intelligence gathering (i.e., Recon-Ng, Spiderfoot, Metasploit, Wireshark, etc.).
- Demonstrate the ability to enter a system based on the potential vulnerabilities identified during intelligence gathering.
- Prepare a complete and accurate vulnerability assessment report to identify the steps, tools used, location, and methods of entry for a particular issue.
- Demonstrate the ability to use the CVSS to rank the severity of vulnerabilities.
- Rank security concerns based on their ease of exploitation and the damage they can cause
- Propose solutions to fix vulnerabilities.
- Explain the key components of a penetration test report and strategies for writing effective and informative reports.
- Create accurate and thorough penetrating testing reports that can be used by technical and nontechnical personnel (e.g., executives, compliance teams, advertising and marketing personnel, etc.) to improve security and user confidence.
- Issue certificates upon completion of a penetrating testing audit.

Programming Languages (Optional)

Hours: 30–50

Sample learning objectives

- Describe the uses and functionalities of various programming languages, such as Python, Java, JavaScript, Golang, C#, C++, R, Swift, Kotlin, Ruby, etc.
- Describe the use of JavaScript in programming for the Web and demonstrate the ability to write basic code in JavaScript.
- Demonstrate the ability to write simple code in one or more languages.
- Demonstrate the ability to identify code errors in one or more languages.
- Explain the sources of vulnerability associated with different programming languages.
- Describe the various strategies a penetration tester would use based on the programming language used to create the software or application being tested.

Introduction to Cloud-Based Computing (Optional)

Hours: 20–30

Sample learning objectives

- Explain the fundamentals of Cloud computing and describe the challenges clients may face when transitioning to the Cloud environment.
- Differentiate between Amazon Web Services (AWS), Azure, Microsoft 365, and Google Cloud Platform services, explaining the optimal uses and challenges.
- Describe the different forms of cloud computing, such as infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), and serverless.
- Explain the ways in which cloud computing services can be used to support web, app, database, mobile, analytics, networking, blockchain, development, and security services.

Cloud Penetration Testing (Optional)

(These learning objectives align with the Global Information Assurance Certification—GIAC Penetration Tester Practitioner Certification Exam, https://www.giac.org/certifications/cloud-penetration-tester-gcpn**)**

Hours: 30–50

Sample learning objectives

- Demonstrate an understanding of the AWS authentication methods as well as privilege escalation in the AWS environment.
- Demonstrate an understanding of Azure Functions capability and code execution in the Azure environment.
- Demonstrate an understanding of AWS and Azure Command-line Interface (CLI) structure and application mapping through Application Program Interface (API)s and HTTP requests.
- Demonstrate an understanding of examples of cloud-native applications and CI/CD pipelines and finding vulnerabilities in them.
- Demonstrate an understanding of the fundamentals of penetration testing applied to cloud applications, including recon, assessment, discovery, and restrictions of cloud environments.
- Demonstrate an understanding of the structure and configurations of public cloud infrastructures.
- Discover and identify sources of exposure in cloud environments, including exposed ports, services, databases, secrets, and developer tools and repositories.
- Explain Microsoft Azure cloud services web identity management and authentication standards and attacks against Azure users and services.
- Demonstrate an understanding of username harvesting and password attack methodologies and tools.
- Demonstrate understanding of Red Team penetration testing processes, including exploitation and payload development.
- Demonstrate an understanding of the process of obfuscation of commands and attack structure through domain fronting and other tools and pivoting using the proxies and other methods.
- Demonstrate an understanding of common web application attacks and how they impact cloud-native applications and serverless functions.

Relevant military experience
Army: MOS 17C—Cybersecurity **Air Force:** Cyber Intelligence Specialties **Navy:** Naval Sea Systems Command (NAVSEA) cybersecurity positions

Diversity, equity, and inclusion
Penetration testers are generally included in the labor category of cyber security analysts. Among cyber security analysts, nearly 80 percent are men, 66 percent are white, followed by Asian (9.6 percent), African American (9.2 percent) and Hispanic/Latino (9 percent). Organizations such as the Washington Center sponsor a Cybersecurity Accelerator Program to provide internships in cybersecurity to encourage women and underrepresented minorities to pursue cybersecurity careers.

Works Consulted

"Penetration Tester," Career One Stop, accessed January 2024, https://www.careeronestop.org/Toolkit/Careers/Occupations/occupation-prolife.aspx?keyword=Penetration%20Testers&onetcode=15129904&location+UNITED%20STATES.

"Penetration Testers," O*NET OnLine, accessed January 2024, https://www.onetonline.org/link/summary/15-1299.04.

"Penetration Testers," Apprenticeship USA, accessed January 2024, https://www.apprenticeship.gov/apprenticeship-occupations/listings?occupationCode=15-1299.04.

"Exploitation Analysis," National Initiative for Cybersecurity Careers and Studies (NICCS), accessed February 2024, https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/expoitation-analysis.

"CompTIA PenTest+ Certification Exam Objectives," CompTIA PenTest+, accessed February 2024, https://partners.comptia.org/docs/default-source/resources/comptia-pentest-pt0-002-exam-objectives-(4-0).

STATEMENT OF INDEPENDENCE

The Urban Institute strives to meet the highest standards of integrity and quality in its research and analyses and in the evidence-based policy recommendations offered by its researchers and experts. We believe that operating consistent with the values of independence, rigor, and transparency is essential to maintaining those standards. As an organization, the Urban Institute does not take positions on issues, but it does empower and support its experts in sharing their own evidence-based views and policy recommendations that have been shaped by scholarship. Funders do not determine our research findings or the insights and recommendations of our experts. Urban scholars and experts are expected to be objective and follow the evidence wherever it may lead.

URBAN
INSTITUTE · ELEVATE · THE · DEBATE

500 L'Enfant Plaza SW
Washington, DC 20024

www.urban.org