Assessment Report

candidate@example.nl

Version 1.0 – April 2024

Powered by:

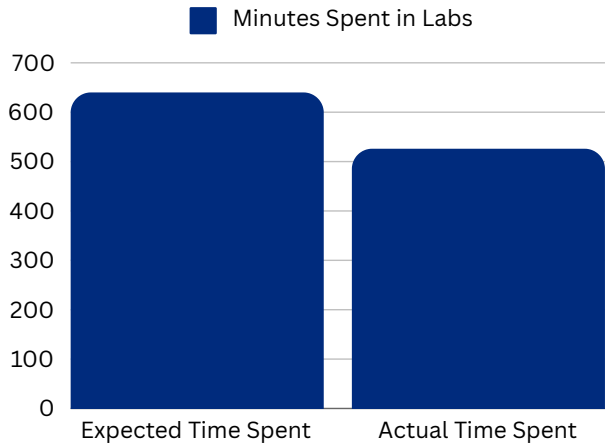
D5 IQ

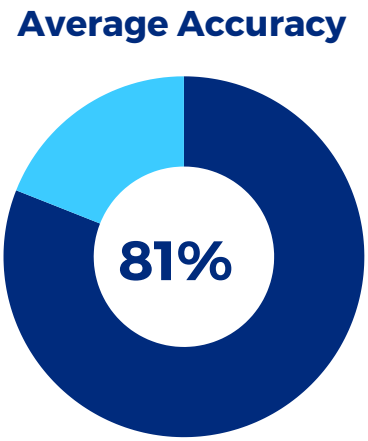
1. Executive Summary

Candidate Name had an average score on the cyber security evaluation:

- Scored **508 points of the 1030 points (49%)** and **completed 14 of the 21 labs**
- Spent **a total time of 8 hours and 46 minutes** in the assessment
- Achieved an **average accuracy of 81%** on finished labs throughout the assessment
- Achieved **an average score on all Knowledge areas** of the NICE framework related to the labs

1.1 Time Spent / Average Accuracy





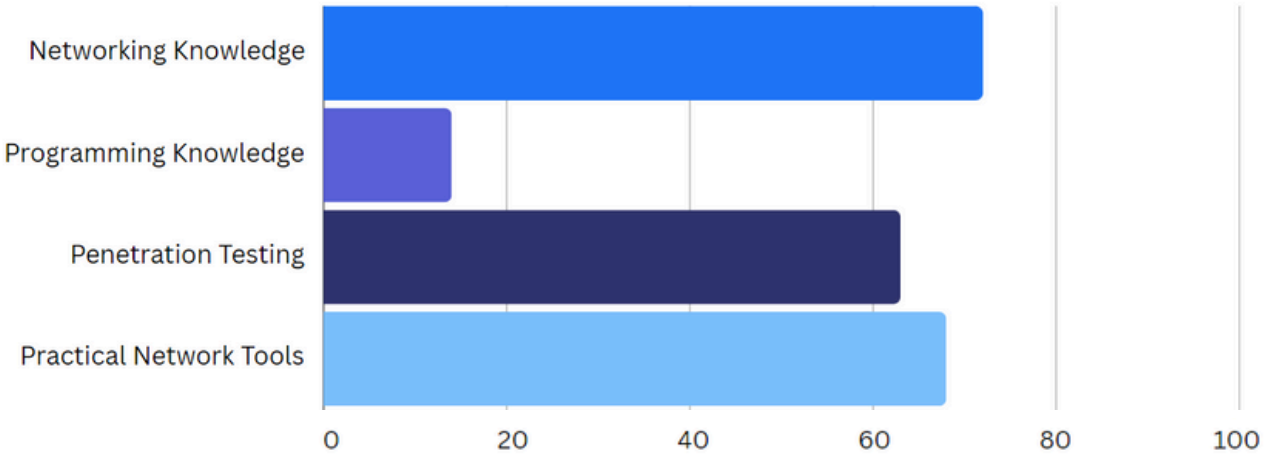
Candidate Score

2. Introduction

This report provides a comprehensive assessment of Candidate Name's performance in the cybersecurity evaluation, encompassing factors such as time spent in practical labs, accuracy in lab exercises, and a benchmark comparison against a candidate with a perfect score. The analysis will reveal candidate's strengths and areas for growth, while also examining the relevant Knowledge areas achieved during the assessment in accordance with the NICE framework.

3. NICE Knowledge Area Categories

Below, you will find various knowledge area categories that highlight the candidate's strengths and areas for improvement:



Networking Knowledge
This category covers essential aspects of computer networks, including types, protocols, security, and infrastructure, focusing on practical applications and communication methods.

Penetration Testing
This category delves into understanding exploitation tools and techniques, adversarial tactics, and the latest intrusion methods. It includes knowledge of SQL, stages of cyber attacks, hacking methodologies, penetration testing, application security risks, and system vulnerabilities.

Practical Network Tools
This category focuses on the use and application of network analysis tools like ping, traceroute, nslookup, and packet analysis tools such as Wireshark. It includes understanding of network traffic analysis, identifying software communication vulnerabilities, forensics lab design, and secure software deployment.

Programming Knowledge
This category encompasses understanding algorithms, data structures, and complexity analysis. It covers software debugging, both interpreted and compiled languages, secure coding techniques, and general programming concepts including various computer languages, testing, and file types.

4. Candidate Performance Breakdown

Lab Title	Time Spent (min)	Recom Time (min)	Difficulty	Average Accuracy	Final Score
C++: Hardcoded Secrets	15.77	10	3	100	25/30
Introduction to Networking: Ep.7 — Demonstrate...	9.22	15	3	100	30/30
Tactics – Demonstrate your Knowledge	7.32	15	3	100	30/30
Demonstrate Your Skills: Networking	30.22	45	4	58	31/40
Intro to Wireshark	8.32	11	4	80	37/40
Linux CLI: Ep.17 – Demonstrate your Skills	59.66	60	4	85	36/40
Privilege Escalation: Windows – Introduction	29.30	20	4	89	31/40
Python: Hardcoded Secrets*	10.72	10	4	NaN	0/40
SQLi Basics: Basic SQL Injection*	34.4	10	4	55	17/40

C++: Path Traversal*	2.17	20	5	NaN	0/50
Cross-Site Scripting: Ep.2 – Reflected XSS	16.75	30	5	100	50/50
Demonstrate Your Skills: Scanning	40.27	54	5	54	41/50
GDB: Ep. 3 — Memory Inspection and Modification*	31.76	20	5	NaN	0/50
Web Applications: Page Source Review	40.22	10	5	82	24/50
Cross-Site Scripting: Ep.5 – Filter Evasion	10.5	30	6	100	60/60
Demonstrate Your Skills: Wireshark	31.45	44	6	63	47/60
Privilege Escalation: Linux – Demonstrate Your Skills*	1	60	6	NaN	0/60
Privilege Escalation: Windows – Demonstrate Your Skills*	27.42	60	6	NaN	0/60
SQL Injection – File Downloads	58.43	36	6	100	49/60
Python: Unrestricted File Upload*	20	20	7	NaN	0/70
C++: Demonstrate Your Skills (Advanced)*	1	60	8	NaN	0/80

*The candidate started the lab but has not completed it

Difficulty explanation: **1-3** Entry-Level proficiency **4-6** Intermediate proficiency **7-9** Advanced proficiency

Methodology: The scoring methodology for this assessment combined accuracy, time efficiency, and lab difficulty. Higher accuracy and time efficiency were rewarded with more points, while the difficulty of labs influenced the score. The formula first calculates the accuracy score by assigning a maximum of 5 points based on the accuracy per lab. It then assesses time efficiency by comparing "Actual Time Spent" to "Recommended Time"; if more time is spent, it generates a reduced score based on the inverse proportion of recommended to actual time, otherwise, it assigns a maximum of 5 points. These two scores are added to form a preliminary score, which is then multiplied by the lab's "Difficulty" rating to produce the final score.

Accuracy is scored based on a color-coding system: 90 to 100% accuracy is green, 51 to 89% accuracy is yellow, and 0 to 50% (and NaN) accuracy is red. Time efficiency is also scored based on a color-coding system: under or equal to the recommended time is green, less than double the recommended time is yellow, and double or more the recommended time (and NaN) is red. These scores are then combined to determine the final score for each lab.

Scoring Formula:

$$\left[\left(\frac{\text{Accuracy}}{100} \times 5\right) + \left(\text{if}\left(\text{Time Spent} > \text{Recommended Time}\right)\text{then}\left(\frac{\text{RecomTime}}{\text{TimeSpent}} \times 5\right)\text{else } 5\right)\right] \times \text{Difficulty}$$

5. Appendix

5.1 Knowledge Area Categories

In the following section, knowledge areas are organized into categories based on their similarities. This classification helps us accurately evaluate each candidate's skills and knowledge in these areas, providing a clear picture of their strengths and areas for improvement.

Networking Knowledge

K-ID	Description	Total Points	Comparison to max
K0113	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).	30	100%
K0202	Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).	110	100%
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	61	87%
K0300	Knowledge of network mapping and recreating network topologies.	41	82%
K0388	Knowledge of collection searching/analyzing techniques and tools for chat/buddy list, emerging technologies, VOIP, Media Over IP, VPN, VSAT/wireless, web mail and cookies.	41	82%
K0010	Knowledge of communication methods, principles, and concepts that support the network infrastructure.	31	78%
K0034	Knowledge of network services and protocols interactions that provide network communications.	31	78%
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	31	78%
K0174	Knowledge of networking protocols.	31	78%
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	31	78%
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	31	78%
K0471	Knowledge of Internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).	31	78%

K0491	Knowledge of networking and Internet communications fundamentals (i.e. devices, device configuration, hardware, software, applications, ports/protocols, addressing, network architecture and infrastructure, routing, operating systems, etc.).	31	78%
K0555	Knowledge of TCP/IP networking protocols.	31	78%
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.	31	78%
K0398	Knowledge of concepts related to websites (e.g., web servers/pages, hosting, DNS, registration, web languages such as HTML).	159	57%
K0192	Knowledge of Windows/Unix ports and services.	0	0%
K0444	Knowledge of how Internet applications work (SMTP email, web-based email, chat clients, VOIP).	0	0%

Penetration Testing

K-ID	Description	Total Points	Comparison to max
K0119	Knowledge of hacking methodologies.	198	90%
K0310	Knowledge of hacking methodologies.	198	90%
K0110	Knowledge of adversarial tactics, techniques, and procedures.	77	86%
K0342	Knowledge of penetration testing principles, tools, and techniques.	177	84%
K0367	Knowledge of penetration testing.	177	84%
K0536	Knowledge of structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).	84	84%
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.	41	82%
K0630	Knowledge of the latest intrusion techniques, methods and documented intrusions external to the organization.	47	78%
K0634	Knowledge of exploitation techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).	47	78%
K0069	Knowledge of query languages such as SQL (structured query language).	67	67%
K0206	Knowledge of ethical hacking principles and techniques.	159	57%

K0624	Knowledge of Application Security Risks (e.g. OWASP Top 10 list).	177	55%
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	225	49%
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	119	44%
K0009	Knowledge of application vulnerabilities.	159	37%
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	0	0%
K0629	Knowledge of white/black listing	0	0%

Practical Network Tools

K-ID	Description	Total Points	Comparison to max
K0011	Knowledge of capabilities and applications of network analysis tools (e.g., ping, traceroute, nslookup).	30	100%
K0185	Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark).	37	92%
K0129	Knowledge of command-line tools (e.g., mkdir, mv, ls, passwd, grep).	36	90%
K0318	Knowledge of operating system command-line tools.	36	90%
K0058	Knowledge of network traffic analysis methods.	68	85%
K0272	Knowledge of network analysis tools used to identify software communications vulnerabilities.	68	85%
K0334	Knowledge of network traffic analysis (tools, methodologies, processes).	68	85%
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.	68	85%
K0062	Knowledge of packet-level analysis.	84	84%
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	115	82%
K0111	Knowledge of network tools (e.g., ping, traceroute, nslookup)	31	78%
K0194	Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.	17	42%

K0373	Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.	115	24%
K0178	Knowledge of secure software deployment methodologies, tools, and practices.	0	0%
K0186	Knowledge of debugging procedures and tools.	0	0%

Programming Knowledge

K-ID	Description	Total Points	Comparison to max
K0024	Knowledge of algorithms, data structures, and complexity analysis.	49	82%
K0079	Knowledge of software debugging principles.	0	0%
K0139	Knowledge of interpreted and compiled computer languages.	0	0%
K0140	Knowledge of secure coding techniques.	0	0%
K0396	Knowledge of computer programming concepts, including computer languages, programming, testing, debugging, and file types.	0	0%
K0545	Knowledge of target language(s).	0	0%

Ranking	Knowledge Area Category	Average Benchmark Score
1	**Networking Knowledge**	**72%**
2	**Practical Network Tools**	**68%**
3	**Penetration Testing**	**63%**
4	**Programming Knowledge**	**14%**

To quantify each candidate's achievements in alignment with the NICE framework's Knowledge (K) areas, a systematic process is employed. Candidate points for each individual lab exercise are directly assigned to the relevant K values. This method allows for the creation of a cumulative score for each K value, reflecting both the frequency and level of achievement across the assessment. The ranked K values then provide insights into the candidate's areas of highest proficiency after taking the assignment but also the areas of improvement. For a comprehensive list of these relevant K values, please refer to the appendix.

Note that the K values have not been grouped (e.g. similar K-values) and that the analysis for Skills or Tasks for the NICE framework have not been created

5.2 Knowledge Areas Assigned to Labs

C++: Demonstrate Your Skills (Advanced)

Knowledge ID	Description
K0009	Knowledge of application vulnerabilities.
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language (PL/SQL) and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0373	Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.

C++: Hardcoded Secrets

Knowledge ID	Description
K0009	Knowledge of application vulnerabilities.
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language (PL/SQL) and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0373	Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.

C++: Path Traversal

Knowledge ID	Description
K0009	Knowledge of application vulnerabilities.
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language (PL/SQL) and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0373	Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.

Cross-Site Scripting (XSS): Reflected

Knowledge ID	Description
K0009	Knowledge of application vulnerabilities.
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language (PL/SQL) and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0119	Knowledge of hacking methodologies.

K0202	Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).
K0206	Knowledge of common adversary tactics, techniques, and procedures.
K0310	Knowledge of hacking methodologies.
K0342	Knowledge of penetration testing principles, tools, and techniques.
K0367	Knowledge of penetration testing.
K0398	Knowledge of security event correlation tools.
K0624	Knowledge of Application Security Risks (e.g., OWASP Top 10 list).

Cross-Site Scripting: Ep.5 – Filter Evasion

Knowledge ID	Description
K0009	Knowledge of application vulnerabilities.
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language (PL/SQL) and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0119	Knowledge of capabilities and limitations of network systems.
K0202	Knowledge of the structure and content of a network packet.
K0206	Knowledge of common adversary tactics, techniques, and procedures.
K0310	Knowledge of computer network defense (CND) policies, procedures, and regulations.
K0342	Knowledge of penetration testing principles, tools, and techniques.
K0367	Knowledge of penetration testing.
K0624	Knowledge of security event correlation tools.
K0398	Knowledge of Application Security Risks (e.g., OWASP Top 10 list).

Demonstrate Your Skills: Networking

Knowledge ID	Description
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.
K0010	Knowledge of communication methods, principles, and concepts that support the network infrastructure.
K0034	Knowledge of network services and protocols interactions that provide network communications.
K0058	Knowledge of network traffic analysis methods.

K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).
K0111	Knowledge of network tools (e.g., ping, traceroute, nslookup)
K0174	Knowledge of networking protocols.
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
K0272	Knowledge of network analysis tools used to identify software communications vulnerabilities.
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
K0334	Knowledge of network traffic analysis (tools, methodologies, processes).
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.
K0471	Knowledge of Internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).
K0491	Knowledge of networking and Internet communications fundamentals (i.e. devices, device configuration, hardware, software, applications, ports/protocols, addressing, network architecture and infrastructure, routing, operating systems, etc.).
K0555	Knowledge of TCP/IP networking protocols.
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.

Demonstrate Your Skills: Scanning

Knowledge ID	Description
K0119	Knowledge of hacking methodologies.
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
K0224	Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.
K0300	Knowledge of network mapping and recreating network topologies.
K0310	Knowledge of hacking methodologies.
K0388	Knowledge of collection searching/analyzing techniques and tools for chat/buddy list, emerging technologies, VOIP, Media Over IP, VPN, VSAT/wireless, web mail and cookies.

Demonstrate Your Skills: Wireshark

Knowledge ID	Description
K0062	Knowledge of packet-level analysis.
K0110	Knowledge of adversarial tactics, techniques, and procedures.
K0119	Knowledge of hacking methodologies.
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
K0310	Knowledge of hacking methodologies.
K0536	Knowledge of structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).
K0630	Knowledge of the latest intrusion techniques, methods and documented intrusions external to the organization.
K0634	Knowledge of exploitation techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).

GDB: Memory Inspection and Modification

Knowledge ID	Description
K0079	Knowledge of software debugging principles.
K0186	Knowledge of debugging procedures and tools.
K0396	Knowledge of computer programming concepts, including computer languages, programming, testing, debugging, and file types.

Intro to Wireshark

Knowledge ID	Description
K0058	Knowledge of network traffic analysis methods.
K0062	Knowledge of packet-level analysis.
K0185	Knowledge of forensics lab design configuration and support applications (e.g., VMWare, Wireshark).
K0272	Knowledge of network analysis tools used to identify software communications vulnerabilities.
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).

K0334	Knowledge of network traffic analysis (tools, methodologies, processes).
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.
K0536	Knowledge of structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).

Introduction to Networking: Ep.7 – Demonstrate Your Knowledge

Knowledge ID	Description
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.
K0011	Knowledge of capabilities and applications of network analysis tools (e.g., ping, traceroute, nslookup).
K0113	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).

Linux CLI: Ep.17 – Demonstrate your Skills

Knowledge ID	Description
K0318	Knowledge of operating system command-line tools.
K0129	Knowledge of command-line tools (e.g., mkdir, mv, ls, passwd, grep).

Privilege Escalation: Linux

Knowledge ID	Description
K0079	Knowledge of software debugging principles.

Privilege Escalation: Windows

Knowledge ID	Description
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
K0192	Knowledge of Windows/Unix ports and services.

Privilege Escalation: Windows – Introduction

Knowledge ID	Description
K0177	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).

Python: Hardcoded Secrets / Unrestricted File Upload

Knowledge ID	Description
K0009	Knowledge of application vulnerabilities.
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0139	Knowledge of interpreted and compiled computer languages.
K0140	Knowledge of secure coding techniques.
K0178	Knowledge of secure software deployment methodologies, tools, and practices.
K0206	Knowledge of ethical hacking principles and techniques.
K0373	Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.
K0396	Knowledge of computer programming concepts, including computer languages, programming, testing, debugging, and file types.
K0398	Knowledge of concepts related to websites (e.g., web servers/pages, hosting, DNS, registration, web languages such as HTML).
K0444	Knowledge of how Internet applications work (SMTP email, web-based email, chat clients, VOIP).
K0545	Knowledge of target language(s).
K0624	Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
K0629	Knowledge of white/black listing

SQL Injection: File Download

Knowledge ID	Description
K0024	Knowledge of algorithms, data structures, and complexity analysis.
K0069	Knowledge of query languages such as SQL (structured query language).

K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0206	Knowledge of ethical hacking principles and techniques.
K0342	Knowledge of penetration testing principles, tools, and techniques.
K0367	Knowledge of penetration testing.
K0373	Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.
K0398	Knowledge of concepts related to websites (e.g., web servers/pages, hosting, DNS, registration, web languages such as HTML).
K0624	Knowledge of Application Security Risks (e.g., OWASP Top 10 list).

SQLi Basics: Basic SQL Injection

Knowledge ID	Description
K0069	Knowledge of query languages such as SQL (structured query language).
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0194	Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.
K0342	Knowledge of penetration testing principles, tools, and techniques.
K0367	Knowledge of penetration testing.
K0373	Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.
K0624	Knowledge of Application Security Risks (e.g. OWASP Top 10 list).

Tactics – Demonstrate your Knowledge

Knowledge ID	Description
K0110	Knowledge of adversarial tactics, techniques, and procedures

Web Applications: Page Source Review

Knowledge ID	Description
K0009	Knowledge of application vulnerabilities.

K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
K0373	Knowledge of basic software applications (e.g., Outlook, Word, Excel).