

Forum:[Hack Forums](#)

Thread: [How to become a certified Hackerman](#)

V?rt - May 16, 2024, 7:10 pm

RoadMap to Certifications and a Degree.

Certifications in cybersecurity and hacking provide structured learning paths and validate skills, ranging from foundational IT knowledge to advanced penetration testing and defensive strategies. They offer credibility within the industry and demonstrate practical expertise, enhancing job opportunities and earning potential. However, they should be complemented by practical experience and continuous learning to stay updated in this rapidly evolving field.

Certifications:

[CompTIA A+](#)

CompTIA A+ 220-1101 covers mobile devices, networking technology, hardware, virtualization and cloud computing.

CompTIA A+ 220-1102 covers operating systems, security, software and operational procedures.

[CompTIA Linux+](#)

CompTIA Linux+ covers an evolving job role that focuses more on how Linux powers the cloud. The exam includes cutting edge technologies that help automate and orchestrate business processes, including infrastructure as code and containers.

[CompTIA Network+](#)

The CompTIA Network+ certification verifies that the successful candidate has the knowledge and skills required to:

Establish network connectivity by deploying wired and wireless devices. Understand and maintain network documentation.

Understand the purpose of network services.

Understand basic datacenter, cloud and virtual networking concepts.

Monitor network activity, identifying performance and availability issues.

Implement network hardening techniques.

Manage, configure, and troubleshoot network infrastructure.

[CompTIA Security+](#)

The CompTIA Security+ certification exam will verify the successful candidate has the knowledge and skills required to assess the security posture of an enterprise environment and recommend and implement appropriate security solutions; monitor and secure hybrid environments, including cloud, mobile, and IoT; operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance; identify, analyze, and respond to security events and incidents

[CompTIA PenTest+](#)

The CompTIA PenTest+ will certify the successful candidate has the knowledge and skills required to plan and scope a penetration testing engagement including vulnerability scanning, understand legal and compliance requirements, analyze results, and produce a written report with remediation techniques.

[CompTIA CySA+](#)

The CompTIA Cybersecurity Analyst (CySA+) certification verifies that successful candidates have the knowledge and skills required to detect and analyze indicators of malicious activity, understand threat intelligence and threat management, respond to attacks and vulnerabilities, perform incident response, and report and communicate related activity.

[Google IT Support](#) Gain skills required to succeed in an entry-level IT job

Learn to perform day-to-day IT support tasks including computer assembly, wireless networking, installing programs, and customer service

Learn how to provide end-to-end customer support, ranging from identifying problems to troubleshooting and debugging

Learn to use systems including Linux, Domain Name Systems, Command-Line Interface, and Binary Code

[PEN-200: Penetration Testing with Kali Linux](#)

The industry-leading Penetration Testing with Kali Linux (PWK/PEN-200) course introduces penetration testing methodologies, tools, and techniques in a hands-on, self-paced environment. Learners who complete the course and pass the exam will earn the OffSec Certified Professional (OSCP) certification which requires holders to successfully attack and penetrate various live machines in a safe lab environment. The OSCP is considered to be more technical than other ethical hacking

certifications and is one of the few that requires evidence of practical penetration testing skills.

[PEN-300: Advanced Evasion Techniques and Breaching Defenses](#)

Evasion Techniques and Breaching Defenses (PEN-300) is an advanced penetration testing course. Learners who complete the course and pass the exam will earn the OffSec Experienced Pentester (OSEP) certification. This course builds on the knowledge and techniques taught in Penetration Testing with Kali Linux, teaching learners to perform advanced penetration tests against mature organizations with an established security function and focuses on bypassing security mechanisms that are designed to block attacks.

[WEB-200: Foundational Web Application Assessments with Kali Linux](#)

Learn the foundations of web application assessments with Foundational Web Application Assessments with Kali Linux (WEB-200). Learners who complete the course and pass the exam will earn the OffSec Web Assessor (OSWA) certification and will demonstrate their ability to leverage web exploitation techniques on modern applications. This course teaches learners how to discover and exploit common web vulnerabilities and how to exfiltrate sensitive data from target web applications. Learners that complete the course will obtain a wide variety of skill sets and competencies for web app assessments.

[EXP-312: Advanced macOS Control Bypasses](#)

Advanced macOS Control Bypasses (EXP-312) is our first macOS security course. It's an offensive logical exploit development course for macOS, focusing on local privilege escalation and bypassing the operating system's defenses. EXP-312 is an advanced course that teaches the skills necessary to bypass security controls implemented by macOS, and exploit logic vulnerabilities to perform privilege escalation on macOS systems. Learners who complete the course and pass the exam earn the OffSec macOS Researcher (OSMR) certification.

[EXP-301: Windows User Mode Exploit Development](#)

Windows User Mode Exploit Development (EXP-301) is a course that teaches learners the basics of modern exploit development. Despite being a fundamental course, it is at the 300 level because it relies on substantial knowledge of assembly and low level programming. It begins with basic buffer overflow attacks and builds into learning the skills needed to crack the critical security mitigations protecting enterprises.

[WEB-300: Advanced Web Attacks and Exploitation](#)

Advanced Web Attacks and exploitation (WEB-300) is an advanced web application security course that teaches the skills needed to conduct white box web app penetration tests.

[SOC-200: Foundational Security Operations and Defensive Analysis](#)

Learn the foundations of cybersecurity defense with Foundational Security Operations and Defensive Analysis (SOC-200), a course designed for job roles such as Security Operations Center (SOC) Analysts and Threat Hunters. Learners gain hands-on experience with a SIEM, identifying and assessing a variety of live, end-to-end attacks against a number of different network architectures.

Degree:

Western Governor's University is the all around best option for quick and cheap college. It's important to consider that the most efficient strategy for achieving the degree with minimal cost involves completing the majority of the coursework outside of WGU, obtaining credits from those courses, and then enrolling when you're between 50-65% done. This approach minimizes expenses and is the optimal choice in terms of both time and money.

Bachelor of Science, Cybersecurity and Information Assurance (BSCSIA)

Class Roadmap:

Spoiler ([Click to View](#))

Composition: Successful Self-Expression

Critical Thinking: Reason and Evidence

Intro to Systems Thinking

Intro to Communication: Connecting with Others

Ethics in Technology

American Politics and the US Constitution

Applied Algebra

Applied Probability and Statistics

Health, Fitness and Wellness

Natural Science Lab

Intro to IT

IT Foundations (A+ Core 1)

IT Applications (A+ Core 2)

Data Management - Foundations

Network and Security - Foundations

Scripting and Programming - Foundations

Business of IT - Applications (ITILv4 Foundations)

Data Management - Applications

Fundamentals of Information Security *

Introduction to Python

Linux Foundations (LPI Linux Essentials)

Business of IT - Project Management (Project+)

Cyber Defense and Countermeasures (CySA+)

Digital Forensics in Cybersecurity

Introduction to Cryptography

Managing Cloud Security (CCSP *Optional)

Legal Issues in Information Security

Information Systems Security (SSCP)

Emerging Technologies in Cybersecurity

Managing Information Security

Penetration Testing and Vulnerability Analysis (Pentest+)

Networks (Network+)

Network and Security - Applications (Security+)

IT Capstone Written Project

Certifications included in this program at no extra cost include:

Spoiler ([Click to View](#))

Certified Cloud Security Professional (CCSP) - Associate of (ISC)2 designation

Systems Security Certified Practitioner (SSCP) - Associate of (ISC)2 designation

ITIL® Foundation Certification

CompTIA A+

CompTIA Cybersecurity Analyst Certification (CySA+)

CompTIA IT Operations Specialist

CompTIA Network+

CompTIA Network Vulnerability Assessment Professional

CompTIA Network Security Professional

CompTIA PenTest+

CompTIA Project+

CompTIA Secure Infrastructure Specialist
CompTIA Security+
CompTIA Security Analytics Professional

Skills for your resume that you will learn in this program:

Spoiler ([Click to View](#))

Secure Systems Analysis & Design

Data Management

Web and Cloud Security

Hacking Countermeasures and Techniques

Digital Forensics and Incident Response

M?tt - May 16, 2024, 7:17 pm

If anyone has questions about WGU, feel free to shoot them my way. I actually graduated from there and loved the program for how cheap and flexible it was. I can also answer questions regarding CompTIA, ISC2, and GIAC exams. Great post Vert!

V?rt - May 16, 2024, 7:19 pm

(May 16, 2024 07:17 PM)M?tt Wrote: [\[CITE\]](#) If anyone has questions about WGU, feel free to shoot them my way. I actually graduated from there and loved the program for how cheap and flexible it was. I can also answer questions regarding CompTIA, ISC2, and GIAC exams. Great post Vert! Same, I'm currently in the Software Engineering program and it's an amazing college.

Thank you for the kind words! Hopefully some people gain interest and reach out to you for some answers! Thanks for helping!

Nomad.Null - May 16, 2024, 7:50 pm

Good list of starter certs, but I am skeptical of the Pentest+

So far, nothing I've taken has compared to Offensive Security's OSCP and more advanced pentesting certs. The knowledge to be gained there is just the best, bar none.

Excellent starter tutorial though.

V?rt - May 16, 2024, 7:53 pm

(May 16, 2024 07:50 PM)Nomad.Null Wrote: [\[CITE\]](#) Good list of starter certs, but I am skeptical of the Pentest+

So far, nothing I've taken has compared to Offensive Security's OSCP and more advanced pentesting certs. The knowledge to be gained there is just the best, bar none.

Excellent starter tutorial though.

Great addition! I'll add that to the list!

Thank you for the kind words.

Evolution Zero - May 16, 2024, 8:03 pm

I don't like to boast my credentials usually but here is a background and advice: I am Security+ certified here. CEH next on top of my degree. Super fun course. Highly recommend it. They just

came out with the SY0-701 which was a huge overhaul of the exam objectives so for those reading this whom have studied for the Security+, make sure you use the right exam objectives. Furthermore, I recommend study groups every single day for 2-3 months because the way that these exams are written can be very tricky and are meant to trip you up in the exam room.

Great post and I was not expecting this. I read the title and was like lemme skip to the bottom here and explain what to actually do, but you, my friend, covered it perfectly.

Stay safe.

~Xplicit

(May 16, 2024 07:50 PM)Nomad.Null Wrote: [\[CITE\]](#) Good list of starter certs, but I am skeptical of the Pentest+

So far, nothing I've taken has compared to Offensive Security's OSCP and more advanced pentesting certs. The knowledge to be gained there is just the best, bar none.

Excellent starter tutorial though.

Also, I second this. Usually what you want to do is get the triad (A+, N+, S+) then go for the PenTest+. However, I do not see many jobs for SOC analysts and stuff that require the PenTest+. It is more of a specialized certification intended for those who are attempting to become licensed penetration testers.

"SOC-200: Foundational Security Operations and Defensive Analysis"

This, now, on the other hand, sounds freaking sick. The OSCP is my dream to get one day but it is one of the hardest exams you will ever encounter imho.

Nomad.Null - May 16, 2024, 8:38 pm

(May 16, 2024 08:03 PM)Xplicit Wrote: [\[CITE\]](#) The OSCP is my dream to get one day but it is one of the hardest exams you will ever encounter imho.

No joke. It was one of my toughest. The pay off led me to a 6-figure salary within a year of earning it.

It is not only a dream, it fulfills them too.

Evolution Zero - May 16, 2024, 8:47 pm

(May 16, 2024 08:38 PM)Nomad.Null Wrote: [\[CITE\]](#) No joke. It was one of my toughest. The pay off led me to a 6-figure salary within a year of earning it.

It is not only a dream, it fulfills them too.

Jealous man.? That is definitely one of my goals. The problem is the job market right now (unless you're a SOC analyst or have one of the hardest certs to obtain like yourself, for example) is very competitive for cybersecurity. Unless you have your bachelors, the CompTIA triad, and more its basically you against every other joe, smith, and Mary who have the same credentials.

Building connections is extremely important to land those 6 figure a year jobs and I know they pay a lot for people with OSCP but that's straight bank right there, lol.

Bastille - May 16, 2024, 11:54 pm

Great thread, I didn't know the SOC-200 cert and I'm actually looking for a SOC cert to get.

I saw the CSA (Certified SOC Analyst) from Ec-Council but I didn't hear a lot of good things regarding Ec-Council certs in general (especially about the CEH which is not that much appreciated by recruiters).

Good job [V?rt](#) :)

Hackers - May 17, 2024, 7:54 am

Very interesting, this is a great list of certs that people can go for. It helps to see them all in one place. I can really see how having a number of these or similar on a resume can really help support someone's growth as a cybersecurity analyst, researcher, developer, etc.

nofaze - May 17, 2024, 10:28 am

This is a great post i havent been on here in almost 10 years I wanted to get back in to things and its amazing how much its all changed

Stanley - May 19, 2024, 6:21 pm

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

Brill - May 20, 2024, 6:19 am

(May 16, 2024 11:54 PM)Yseurk Wrote: [\[CITE\]](#) Great thread, I didn't know the SOC-200 cert and I'm actually looking for a SOC cert to get.

I saw the CSA (Certified SOC Analyst) from Ec-Council but I didn't hear a lot of good things regarding Ec-Council certs in general (especially about the CEH which is not that much appreciated by recruiters).

Good job [V?rt](#) :)

i don't think you need a course to understand how to stare at a siem all day. if you're unfamiliar with the responsibilities of a soc analyst, google has a course on coursera that'll break down compliance shit & get your feet wet on how to use a siem

LTC - May 20, 2024, 6:39 am

Good Thread but dont forget [censored] Academy they also teach alot and also got a Certificate

Camocody - May 23, 2024, 10:01 pm

This is what i am trying to do :P