12-Month Cybersecurity Learning Plan with Projects

Month 1: Foundations of Cybersecurity

Goal: Establish a solid foundation in cybersecurity concepts and networking, with a focus on Python scripting.

Week 1-2: Cybersecurity Overview

Topics: Introduction to Cybersecurity, CIA Triad, Cybersecurity Risks.

Resources: Cisco Networking Academy - Introduction to Cybersecurity (Free certificate)

Python essentials for Cybersecurity (Basic Scripting)

Project: Cybersecurity Awareness Presentation

Develop a slide deck explaining the CIA Triad and common cybersecurity risks.

Python Task: Write a Python script that takes a text file of cybersecurity risks and generates a summary report.

Showcase: Share the presentation and Python script on GitHub or LinkedIn.

Week 3-4: Networking Basics

Topics: OSI Model, TCP/IP, DNS, HTTP/HTTPS.

Resources: Cybrary Introduction to Networking (Free)

Project: Network Configuration using Python

Use Python to automate basic network configuration tasks, like pinging IP addresses or checking open ports.

Showcase: Share the code on GitHub.

Month 2: Network Security

Goal: Learn about securing networks, firewalls, and intrusion detection systems, while leveraging Python.

Week 5-6: Network Security Fundamentals

Topics: Firewalls, VPNs, IDS/IPS systems, Network perimeter security.

Resources: Fortinet Network Security Basics (Free certificate)

Project: Automate Firewall Rules Configuration with Python

Use Python to automate firewall rule configurations on pfSense or similar platforms.

Showcase: GitHub repository with Python script to configure firewall rules.

Week 7-8: Threat Detection and Incident Response

Topics: Incident response, log analysis, SIEM tools.

Resources: Cybrary Incident Response (Free)

Project: Log Analysis with Python

Write a Python script that reads logs from a security device (e.g., firewall) and identifies anomalies or patterns.

Showcase: Share the Python script and analysis report on GitHub.

Month 3: Operating Systems Security

Goal: Learn how to secure Linux and Windows systems with Python tools.

Week 9-10: Linux Security

Topics: File permissions, user management, system hardening.

Resources: Linux Foundation: Introduction to Linux (Free certificate available)

Project: Linux Hardening Script

Create a Python script that automates the hardening of Linux systems (e.g., setting permissions, disabling services).

Showcase: GitHub repository for your hardening script.

Week 11-12: Windows Security

Topics: Securing Windows systems, Active Directory, Group Policies.

Resources: Microsoft Learn: Windows Security (Free)

Project: Windows Security Automation with Python

Automate Windows security tasks like auditing user permissions or checking Active Directory configurations.

Showcase: Document your script and results on GitHub.

Month 4: Cloud Security

Goal: Secure cloud environments, with a focus on AWS, Azure, and Python scripting for automation.

Week 13-14: Introduction to Cloud Security

Topics: Cloud security principles, SaaS, PaaS, IaaS.

Resources: AWS Cloud Practitioner Essentials (Free certificate)

Project: Automate Cloud Security with Python

Use Python and AWS SDK (Boto3) to automate cloud security tasks, such as creating IAM roles and managing EC2 security groups.

Showcase: Upload your Python code and cloud security automation projects to GitHub.

Week 15-16: Google Cloud Security

Topics: Google Cloud Security, IAM.

Resources: Google Cloud Security Fundamentals (Free)

Project: Secure Google Cloud Resources Using Python

Write a Python script to automate Google Cloud security configurations, such as managing IAM roles and securing storage.

Showcase: Publish your Python scripts and documentation on GitHub.

Month 5: Ethical Hacking and Penetration Testing

Goal: Develop ethical hacking skills and integrate Python into penetration testing.

Week 17-18: Introduction to Ethical Hacking

Topics: Ethical hacking principles, penetration testing tools.

Resources: TryHackMe Introduction to Pentesting (Free certificate)

Project: Automate Vulnerability Scanning with Python

Use Python to script vulnerability scanning tools like Nmap and automate vulnerability scanning in a test environment.

Showcase: Share your Python scripts and vulnerability scanning reports on GitHub.

Week 19-20: Penetration Testing Tools

Topics: Nmap, Metasploit, vulnerability scanning.

Resources: Hack The Box Academy (Free basic access)

Project: Python Exploits for Pen Testing

Write Python scripts to automate exploitation tasks using Metasploit or similar tools.

Showcase: Share your scripts and penetration testing results on GitHub.

Month 6: Advanced Penetration Testing and Exploitation

Goal: Master advanced penetration testing techniques and exploit development.

Week 21-22: Advanced Penetration Testing

Topics: Web application security, exploitation techniques.

Resources: Cybrary Penetration Testing and Ethical Hacking (Free)

Project: Exploit Automation with Python

Develop Python scripts to automate exploitation techniques such as SQL injection or XSS (Cross-Site Scripting).

Showcase: Upload scripts and results to GitHub.

Week 23-24: Web Application Security (OWASP)

Topics: OWASP Top 10 vulnerabilities, web application attacks.

Resources: OWASP Web Application Security (Free)

Project: Python Script to Test OWASP Top 10 Vulnerabilities

Write a Python script that tests for common web application vulnerabilities like SQL Injection and XSS.

Showcase: Publish your Python-based security testing tools on GitHub.

Month 7: Security Monitoring and Incident Management

Goal: Learn how to monitor security events and respond effectively.

Week 25-26: Security Operations Center (SOC)

Topics: Security event analysis, SOC tools.

Resources: Cybrary SOC Analyst (Free)

Project: SIEM Integration with Python

Use Python to integrate and automate log data into SIEM systems such as Splunk or Elastic Stack.

Showcase: Share the integration script and documentation on GitHub.

Week 27-28: Log Management and SIEM

Topics: SIEM basics, log analysis, event correlation.

Resources: Splunk Fundamentals 1 (Free)

Project: Log Correlation with Python

Automate log correlation and analysis tasks using Python to detect security incidents.

Showcase: Upload your Python script for log management to GitHub.

Month 8: Security Automation and Scripting

Goal: Automate security tasks using Python and PowerShell.

Week 29-30: Automating Security with Python

Topics: Python for security automation.

Resources: Cybrary Python for Security Professionals (Free)

Project: Python Security Automation for Incident Response

Write a Python script that automates the response to security incidents, such as blocking IPs after detecting a brute force attack.

Showcase: Publish scripts and automation tools on GitHub.

Week 31-32: PowerShell for Security Automation

Topics: Automating security tasks using PowerShell.

Resources: PowerShell for Security Professionals (Free)

Project: Automate Security Tasks with PowerShell

Automate tasks like updating security patches or auditing security configurations using PowerShell.

Showcase: Share PowerShell scripts on GitHub.

Month 9: Cyber Threat Intelligence and Threat Hunting

Goal: Learn how to gather and analyze threat intelligence and hunt for threats in systems.

Week 33-34: Threat Intelligence

Topics: Threat intelligence gathering, IoCs (Indicators of Compromise).

Resources: Coursera Cyber Threat Intelligence (Free audit)

Project: Threat Intelligence Automation with Python

Use Python to automate the collection of IoCs and correlate them with known threats.

Showcase: Share your Python scripts for threat intelligence automation on GitHub.

Week 35-36: Threat Hunting

Topics: Threat hunting, anomaly detection.

Resources: TryHackMe Threat Hunting (Free certificate)

Project: Python Threat Hunting Script

Create a Python script that analyzes system logs for signs of potential threats or abnormal behavior.

Showcase: Upload your Python threat hunting scripts on GitHub.

Month 10: Cybersecurity Policy, Governance, and Risk Management (cont'd)

Goal: Understand policy frameworks and risk management in cybersecurity.

Week 37-38: Cybersecurity Policies and Frameworks

Topics: NIST Cybersecurity Framework, ISO/IEC 27001, Risk Management.

Resources: NIST Cybersecurity Framework (Free)

Project: Risk Assessment Framework

Develop a Python-based tool to automate risk assessments by evaluating common security metrics.

Showcase: Publish your risk assessment framework and documentation on GitHub.

Week 39-40: Risk Management and Governance

Topics: Identifying and managing cyber risks, Governance, and Compliance.

Resources: Coursera Cybersecurity Risk Management (Free audit)

Project: Governance Policy Template

Create a security governance policy template for a hypothetical company, covering risk management and compliance requirements.

Showcase: Share your policy template and risk management strategies on LinkedIn or GitHub.

Month 11: Advanced Threats and Penetration Testing

Goal: Dive deeper into complex penetration testing techniques and advanced exploitation methods.

Week 41-42: Advanced Penetration Testing Techniques

Topics: Advanced exploitation methods, buffer overflow, reverse engineering.

Resources: Offensive Security (OSCP) or TryHackMe Advanced Pentesting (Free certificate)

Project: Develop Exploits and Write Up

Perform an advanced penetration test on a vulnerable machine and document the findings, including the development of custom exploits.

Showcase: Share your penetration test findings and exploitation techniques on GitHub.

Week 43-44: Reverse Engineering Malware

Topics: Malware analysis, reverse engineering.

Resources: Cybrary Reverse Engineering Malware (Free)

Project: Python Script for Malware Analysis

Create a Python script that helps automate the process of analyzing malware behavior, such as extracting and analyzing code.

Showcase: Share the malware analysis scripts and findings on GitHub.

Month 12: Final Project and Certification Preparation

Goal: Complete a capstone project that demonstrates your expertise and prepare for cybersecurity certifications.

Week 45-46: Final Capstone Project

Topics: Integrating your knowledge into a comprehensive security solution.

Project: Full Security Assessment and Penetration Testing Report

Conduct a full security assessment, including network, system, and application vulnerabilities, followed by penetration testing, and document the findings in a comprehensive report.

Showcase: Create a detailed GitHub repository with your final capstone project, including reports, scripts, and configurations.

Week 47-48: Certification Exam Preparation

Topics: Review for certifications such as CompTIA Security+, Certified Ethical Hacker (CEH), or CySA+.

Resources: Use practice exams and official study materials.

Project: Take a certification exam

Complete the practice exams and schedule for your chosen certification.

Showcase: Share your certification results and prepare a LinkedIn post to showcase your accomplishments.

Certification Recommendations

Months 1-4: Focus on foundational certifications such as CompTIA Security+ or Cisco Networking Academy courses.

Months 5-8: Dive into ethical hacking and penetration testing, working toward certifications like Certified Ethical Hacker (CEH) or CySA+.

Months 9-12: Focus on advanced certifications, such as Certified Information Systems Security Professional (CISSP), CompTIA Security+, or Offensive Security Certified Professional (OSCP).

Project and Certification Portfolio Showcase:

Maintain a GitHub portfolio for all scripts, automation tools, reports, and projects.

Share your journey and projects on LinkedIn to demonstrate your skills and progression.

Document each project with clear explanations, code comments, and a professional-looking presentation of results.

Conclusion

By following this comprehensive plan, you will gain hands-on experience with cybersecurity tools, Python scripting, network security, ethical hacking, and incident response, while continuously building a portfolio of projects. You'll also be prepared to take relevant cybersecurity certifications and be ready to pursue a career as a cybersecurity analyst.

Let me know if you'd like adjustments or additional recommendations!