Renato Campos

Cybersecurity Prework

Monday August 31, 2020

CompTIA Activity

Each header below is a document that I have downloaded for the CompTIA activity. Enumerated beneath each header is a list of topics that I am already familiar with, but have not mastered to my liking.

Certified Ethical Hacker

1. ANSI / CNSS
2. Vulnerability Analysis
3. IoT Hacking
4. Malware
5. Windows 10 / Server 2016
6. MacOS / Unix / Linux
7. Network Scanning
8. Packet Sniffing
9. Social Engineering
10. DoS/DDoS
11. Public Key Infrastructure

CompTIA Pentest

1. Scanning Enumeration
2. Packet Crafting
3. Packet Inspection
4. Eavesdropping
5. Consideration of Vulnerability Scanning
6. Phishing
7. Man-in-the-middle
8. Injections
9. Authentication
10. OS Vulnerabilities
11. Privilege Escalation
12. Persistance
13. Password Cracking
14. Logic

15. I/O

CompTIA Cybersecurity Analyst

1. Intelligence Sources
2. Internet of Things
3. Cloud Service Models
4. Cloud Deployment Models
5. Network Architecture
6. Honeypot
7. Platforms
8. Secure Coding Best Practices
9. Permissions
10. Whitelisting
11. Blacklisting
12. Firewall
13. Port Security
14. Scripting
15. Network
16. Cloud
17. Privacy vs Security
18. Non-technical Controls
19. Technical Controls
20. Policies and Procedures

CompTIA Security+

1. Phishing
2. Smishing
3. Vishing
4. Spam
5. Malware
6. Password Attacks
7. Privilege Escalation
8. Wireless
9. Man-in-the-middle
10. Layer 2 Attacks
11. Malicious Code or Script Execution
12. Zero-day
13. Configuration Management
14. Secure Sockets Layer
15. Deception and Disruption
16. Cloud Models

17. Cloud Service Providers
18. Microservices/API
19. Secure Coding Techniques
20. Emdedded Systems
21. Internet of Things
22. Protocols
23. DNS
24. Network Access Control
25. Port Security
26. Network Appliances
27. Cloud Security Controls

CompTIA Linux+

1. Bootloaders
2. Boot Options
3. File Locations
4. Boot Modules and Files
5. Kernel Panic (Sadly, I am familiar with this.)
6. Commands
7. Locations
8. Diagnostic Tools
9. Configuration Files
10. Basic Partitions
11. File System Hierarchy
12. Device Mapper
13. Tools
14. File System Types
15. Templates
16. Bootstrapping
17. Storage
18. Enviroment Variables
19. Character Sets
20. Package Types
21. Installation Tools
22. Build Tools
23. Repositories
24. Aquisition Commands
25. Creation
26. Modification
27. Deletion
28. Queries
29. Profiles

30. Important Files and File Contents
31. Text Editors
32. File Readers
33. Output Redirection
34. Text Processings
35. File and Directory Operations
36. Systemd Management
37. SSH
38. VPN
39. Cron
40. At
41. Crontab
42. fg
43. bg
44. &
45. kill
46. Ctrl+c
47. Ctrl+z
48. Nohup
49. Types of Devices
50. Monitoring and Configuration Tools
51. File Locations
52. Hot Pluggable Devices
53. GUI
54. Remote Desktop
55. Console Redirection
56. Accessibility
57. File and Directory Permissions
58. Privilege Escalation
59. User Types
60. Boot Security
61. Archive and Restore Utilities
62. Compression
63. Backup Types
64. CPU Monitoring and Configuration
65. Memory Monitoring and Configuration
66. Process Management
67. Permissions
68. Acess
69. File Creation
70. Storage
71. Permission
72. Dependencies

73. Troubleshooting Additional Hardware Issues
74. Shell Enviroments and Shell Variables
75. #!/bin/bash
76. Sourcing Scripts
77. Directory and File Permissions
78. Extensions
79. Commenting
80. Exit Codes
81. Looping Constructs
82. Conditional Statements
83. Escaping Characters
84. Arguments
85. Files

IT Certification Roadmap

1. CompTIA A+ / Network+ / Security+ / Pentest+ / CASP+
2. CCNA / CCNP / CCIE