



Report Card for Alvin Sarkadi - Your Grade NA

CompTIA PenTest+ Cert Guide (PT0-002)

Final Exam

Result	Correct	Incorrect	Time taken	On Date
95 %	76	4	01 h 24 m	27-NOV-24

Lessons

#	Lessons	Items	Correct
1	Introduction to Ethical Hacking and Penetration Testing	9	9
2	Planning and Scoping a Penetration Testing Assessment	3	3
3	Information Gathering and Vulnerability Scanning	18	18
4	Cloud, Mobile, and IoT Security	3	3
5	Exploiting Wired and Wireless Networks	5	4
6	Social Engineering Attacks	4	4
7	Exploiting Application-Based Vulnerabilities	7	7
8	Performing Post-Exploitation Techniques	5	4
9	Reporting and Communication	13	13
10	Tools and Code Analysis	13	11

Items

#	Items	Correct Answer	Your Answer	Result
1	Ethical hackers and penetration testers adopt _____ practices.	A	A	Correct
2	Which document was created for the pur...nducting information security testing?	C	C	Correct
3	Which of the following is not motivated by money?	D	D	Correct
4	Which of the following documents speci...ring a penetration testing engagement?	D	D	Correct
5	Which of the following options provide...-life attacker tactics and techniques?	C	C	Correct
6	Amazon created which model to address ...nd compliance responsibilities in AWS?	A	A	Correct
7	Which of the following are examples of...odology standard or guidance document?	D	D	Correct
8	Which of the following can ethical hac...ing tools on known vulnerable systems?	B	B	Correct
9	Which state regulation requires the co...ility assessments on an ongoing basis?	B	B	Correct
10	In which environment would the tester ...quo;s organization and infrastructure?	D	D	Correct
11	Which of the following took over the n... the most profitable illegal industry?	C	C	Correct
12	Which security rule focuses on safegua...cessed, or transmitted electronically?	D	D	Correct
13	Which of the following allows certific...d for a given domain and organization?	A	A	Correct
14	_____ allows certificate author...d for a given domain and organization.	A	A	Correct

#	Items	Correct Answer	Your Answer	Result
15	What tools can be used for performing ... reconnaissance using DNS information?	D	D	Correct
16	Which type of vulnerability scan shows...vices that are exposed to the network?	B	B	Correct
17	Which of the following is a standard d...assign identifiers to vulnerabilities?	B	B	Correct
18	Which of the following is not an example of active reconnaissance?	B	B	Correct
19	Conducting Vulnerability Scanning Using Nessus			Correct
20	Which Nmap command scans UDP ports?	A	A	Correct
21	Which of the following tools is highly...terfaces (APIs) to gather information?	C	C	Correct
22	Which type of enumeration is helpful i... being used in the target environment?	C	C	Correct
23	What type of scan is being performed w...ollowing command? nmap -sS 10.1.1.0/24	C	C	Correct
24	Performing Reconnaissance on a Network			Correct
25	Which of the following Nmap options would you use to perform a TCP connect scan?	D	D	Correct
26	Which command could be used to obtain the email servers used by h4cker.org?	B	B	Correct
27	During a penetration testing engagemen...e used to perform this reconnaissance?	A	A	Correct
28	Which type of vulnerability scan requi... have root-level access to the system?	A	A	Correct
29	Using Nmap for Network Enumeration			Correct
30	Which Nmap command is used to enumerate hosts on a network?	B	B	Correct

#	Items	Correct Answer	Your Answer	Result
31	Which of the following is an example o...IoT devices and cloud-based solutions?	C	C	Correct
32	Which of the following is a cloud-base...t of web services in a cloud provider?	B	B	Correct
33	Understanding the Pass-the-hash Attack			Correct
34	Which social engineering motivation te... urgency in a decision-making context?	B	B	Correct
35	ARP spoofing can be used to do which of the following?	C	C	Correct
36	Simulating the DDoS Attack			Correct
37	Conducting a Cross Site Scripting (XSS) attack			Correct
38	Which type of attack is often based on...e implemented technology or algorithm?	C	C	Correct
39	Which of the following PowerSploit scr...ly inject a DLL into a remote process?	A	A	Correct
40	Which of the following is an attack th...ooth with vulnerable devices in range?	B	A	Incorrect
41	Which term describes the act of gaining knowledge or information from people?	A	A	Correct
42	What is the term for a sequence of transmitted and executed commands?	C	C	Correct
43	Which of the following activities shou...a penetration test to avoid detection?	C	C	Correct
44	What type of vulnerability can be expl...ord_conf=newpasswd &Change=Change#	A	A	Correct
45	Which of the following is a best pract...post-penetration test cleanup process?	C	C	Correct
46	Which character in normal SQL queries ...d and what follows is a new statement?	B	B	Correct

#	Items	Correct Answer	Your Answer	Result
47	Which attack can allow an attacker to ...lete, or modify records in a database?	D	D	Correct
48	Which of the following actions can an ...n persistence in a compromised system?	A,C,D	A,C	Incorrect
49	Which social engineering motivation te...ther legal, organizational, or social?	C	C	Correct
50	Which type of attack is typically desi...ofile users of specific organizations?	A	A	Correct
51	Which of the following is not a name-t...ess resolution technology or protocol?	D	D	Correct
52	What is the term for a sequence of HTT...ons between a web client and a server?	C	C	Correct
53	Which of the following is used to mana...erations on Windows operating systems?	A	A	Correct
54	In which type of attack does the attac...l that is used to inject the SQL code?	B	B	Correct
55	Which of the following might be a reco...gital certificates in a secure manner?	B	B	Correct
56	Which of the following documents the t...loited using each vulnerability found?	D	D	Correct
57	Which operational control focuses on m... take vacations during specific times?	D	D	Correct
58	Which operational control focuses on a...r or from one role to a different one?	A	A	Correct
59	Which of the following involves applyi...ies found in systems and applications?	B	B	Correct
60	Which part of a report documents any r...f the report may not be familiar with?	C	C	Correct
61	Which of the following is the process ...alling, and applying software updates?	C	C	Correct

#	Items	Correct Answer	Your Answer	Result
62	Which of the following metrics lists u...ntegrity impact, availability impact)?	B	B	Correct
63	With which type of control are access permissions based on a specific function?	C	C	Correct
64	You have completed a vulnerability sca...clude in your report for the customer?	B	B	Correct
65	Which of the following are important c...n triggers during penetration testing?	D	D	Correct
66	Which of the following metrics lists i...ediation level, and report confidence?	A	A	Correct
67	As a penetration tester, it is extreme...els with which of the following?	D	D	Correct
68	Which of the following is a popular to...e file format information from images?	D	D	Correct
69	Which of the following is a command sh...uch as Linux, macOS, and even Windows?	C	C	Correct
70	Viewing the Effects of Hostile JavaScript in the Browser			Incorrect
71	Which encoding does malware typically ...load of DNS packets to cybercriminals?	B	B	Correct
72	Which of the following is very popular...re, and reverse engineer binary files?	B	B	Correct
73	Which of the following is a compilatio...known passwords, and stolen passwords?	B	B	Correct
74	Which Objdump command is used to displ...mation about one or more object files?	B	D	Incorrect
75	Cracking a Linux Password Using John the Ripper			Correct
76	Which of the following can be used to ...acks, and using many other techniques?	B	B	Correct

#	Items	Correct Answer	Your Answer	Result
77	Which of the following is a special variable that holds more than one value at a time?	C	C	Correct
78	Whitelisting an IP Address in the Windows Firewall			Correct
79	Which of the following is a collection of resources that can be reused by programs?	C	C	Correct
80	Which of the following tools can be used to automate information gathering in OSINT?	D	D	Correct