



## Report Card for Nicholas Rabone - Your Grade A

### CompTIA PenTest+ (PT0-001)

#### Practice Test B

Result	Correct	Incorrect	Time taken	On Date
99 %	82	1	19 m	04-JAN-22

## Lessons

#	Lessons	Items	Correct
1	Performing Post-Exploitation Techniques	5	5
2	Exploiting Application-Based Vulnerabilities	19	19
3	Exploiting Wired and Wireless Networks	23	22
4	Planning and Scoping a Penetration Testing Assessment	8	8
5	Penetration Testing Tools	9	9
6	Exploiting Local Host and Physical Security Vulnerabilities	8	8
7	Understanding How to Finalize a Penetration Test	1	1
8	Information Gathering and Vulnerability Identification	6	6
9	Social Engineering Attacks	4	4

# Items

#	Items	Correct Answer	Your Answer	Result
1	Which of the following is a tool that could be used for command and control?	A	A	Correct
2	Which of the following statements is c...d filtering invalid session ID values?	D	D	Correct
3	Refer to the following script: msf >...found in host 10.1.1.1 in this script?	D	D	Correct
4	Which of the following is a best pract...igation against web session hijacking?	A	A	Correct
5	Which of the following attacks is typi...g the Object Exchange (OBEX) protocol?	C	C	Correct
6	Which of the following is a term used ...ated with a given activity or process?	A	A	Correct
7	Which of the following tools can be used to fuzz a web application?	A	A	Correct
8	In which of the following wireless att... a cloned captive portal or a website?	B	B	Correct
9	In which of the following attacks woul...witting participants in a DDoS attack?	B	B	Correct
10	The _____ is a document that sp...ring a penetration testing engagement.	D	D	Correct
11	Which of the following is a type of as...r agree on a specific goal or outcome?	C	C	Correct
12	An attacker may use a _____ to c...ensitive data (including credentials).	C	C	Correct
13	Which of the following is recommended ...XSS and SQL injection vulnerabilities?	D	D	Correct
14	Which of the following Meterpreter com...s logged in on the compromised system?	B	B	Correct

#	Items	Correct Answer	Your Answer	Result
15	Which of the following is a service provided by NetBIOS?	D	D	Correct
16	Which of the following is the default ...SMTP for non-encrypted communications?	C	C	Correct
17	Refer to the following script: \$ c...king the command shown in this script?	C	C	Correct
18	Which of the following describes an ARP cache poisoning or ARP spoofing attack?	C	C	Correct
19	Which of the following Nmap options pe...rt of the Nmap Scripting Engine (NSE)?	A	A	Correct
20	Which of the following is a community-...e efficiently identify active threats?	C	C	Correct
21	Which of the following involves an una... anything that is protected by a lock?	C	C	Correct
22	Which of the following attacks generat...perform a denial-of-service condition?	A	A	Correct
23	Which of the following HTTP methods co...ection to a transparent TCP/IP tunnel?	A	A	Correct
24	Which of the following is a way that a...acker might perform session hijacking?	A	A	Correct
25	Which of the following is true about scope creep?	A	A	Correct
26	Which of the following is not a useful...plication programming interface (API)?	C	C	Correct
27	Refer to the following exhibit: From: ...ttack technique shown in this exhibit?	D	D	Correct
28	Which of the following tools can be us...tion attack against wireless networks?	D	D	Correct
29	Which of the following is a post-explo...nnection back to the attacking system?	A	A	Correct

#	Items	Correct Answer	Your Answer	Result
30	Refer to the following script:Paul' or...shown in the script trying to exploit?	C	C	Correct
31	Which of the following is an attack in...t domain (Layer 2 network) to another?	C	C	Correct
32	Which of the following is not a scorin...n Vulnerability Scoring System (CVSS)?	A	A	Correct
33	Refer to the following script:Paramete... script, and for why is it being used?	D	D	Correct
34	Which of the following can be used as ...nt the timeline of a penetration test?	A,C	A,C	Correct
35	In which of the following SQL injectio...l that is used to inject the SQL code?	B	B	Correct
36	Which of the following is a tool that can be used for credential attacks?	A	A	Correct
37	Suppose you are performing reconnaissa...se to extract information from images?	B	B	Correct
38	Which of the following SMTP commands i...o authenticate a client to the server?	A	C	Incorrect
39	Refer to the following script:bash-3.2....sions of the file shown in the script?	D	D	Correct
40	_____ gathering is a method of...nd analyze information about a target.	C	C	Correct
41	Refer to the following script:medusa -... is the attacker doing in this script?	C	C	Correct
42	_____ is a threat in which a... appear as the valid site to the user.	B	B	Correct
43	Which of the following statements is true regarding RFID tags and devices?	A	A	Correct
44	Which of the following legitimate Wind...used for post-exploitation activities?	A	A	Correct

#	Items	Correct Answer	Your Answer	Result
45	Which of the following scan types typically scanning option in the scan policy?	C	C	Correct
46	Which of the following describes a downgrade attack?	A	A	Correct
47	Refer to the following script: root@ka... type of scan is shown in this script?	D	D	Correct
48	Refer to the following script:https://...niques is demonstrated in this script?	C	C	Correct
49	Which of the following is a tool that ...and other types of credential attacks?	A	A	Correct
50	A _____ is a sequence of HTTP control, and session finalization.	A	A	Correct
51	Which of the following attacks can be done against Windows systems running NTLM?	C	C	Correct
52	Which of the following files contains ... permissions in Android-based systems?	B	B	Correct
53	Which of the following tools can be used at the organization may have in place?	C	C	Correct
54	An attacker may feed to an attacking server passwords or associated credentials.	D	D	Correct
55	Converting & to & mitigates what type of vulnerability?	D	D	Correct
56	Refer to the following script:Host scan... launch the scan shown in this script?	A	A	Correct
57	Which of the following is an attack through the injection of corrupted DNS data?	B	B	Correct
58	What is a critical component of a DHCP spoofing attack?	C	C	Correct
59	Which of the following is not an SQL injection technique?	A,B,C	A,B,C	Correct

#	Items	Correct Answer	Your Answer	Result
60	Refer to the following exhibit: .....ting language is used in this exhibit?	C	C	Correct
61	Which of the following tools can be us...the LSASS process from memory to disk?	C	C	Correct
62	Which of the following statements is true about clickjacking attacks?	B	B	Correct
63	Often a PIN that is used to provision ...mise a wireless infrastructure device?	A	A	Correct
64	Which of the following is an example of passive reconnaissance?	C	C	Correct
65	Successful exploitation of _____ vu...isclosure of a user's session cookies.	C	C	Correct
66	In SNMP implementations, the managed d...atabase called the _____.	C	C	Correct
67	Refer to the following script: Server ...rror message displayed in this script?	D	D	Correct
68	What type of attack is pharming?	A	A	Correct
69	Which of the following statements is true about DOM-based XSS attacks?	A	A	Correct
70	_____ are forged Kerberos servic... given service on a particular server.	C	C	Correct
71	The _____ document is a type o...ly negotiate the work to be performed.	D	D	Correct
72	Refer to the following script: root@ka...attack is demonstrated in this script?	A	A	Correct
73	Refer to the following script:http://t...he URL parameters shown in the script?	C	C	Correct
74	In which type of attack is the respons...by the attacker (spoofing the victim)?	A	A	Correct

#	Items	Correct Answer	Your Answer	Result
75	Which of the following is not true about whaling?	D	D	Correct
76	Which of the following is a social eng... urgency in a decision-making context?	C	C	Correct
77	Which of the following is a suite of t...ased computers from a remote terminal?	B	B	Correct
78	Which of these statements is correct?	C	C	Correct
79	Which of the following protocols is considered weak and should be avoided?	A	A	Correct
80	Which of the following vulnerabilities...le HTTP parameters have the same name?	C	C	Correct
81	Where can you typically find XSS vulnerabilities?	D	D	Correct
82	Which of the following is the term use...accepts and sends email from any user?	B	B	Correct
83	Refer to the following script:select *...lowing is demonstrated in this script?	B	B	Correct