Metasploit Pro Certified Specialist Exam Prep

Q1. The database used by Metaspoilt Pro to store host data is

A. Mysql
B. IBMDB2
C. PostgresQL
D. Oracle DB

Q2. Which is faster: passive reconnaissance or active reconnaissance?

A. They are equal in speed
B. Passive reconnaissance
C. Active reconnaissance

Q3. Module Search results are sorted by Discolsure date descending by default

A. True
B. False

Q4. Metasploit Pro DOES NOT offer the following type of social engineering technique:

A. USB storage
B. Client-side exploit
C. Phishing
D. Cloud connection

Q5. The _____ uses a compromised system to route network traffic

A. Routing module
B. Meterpreter
C. Botnet
D. VPN Pivot

Q6. _____ is a method of client side testing that tracks the number of human targets that click on a link

A. Click sniffing
B. Click tracking
C. Click monitoring
D. Click jacking

Q7. A _____ is an identifier that lets you easily search for hosts, organize assets, create work queues, and track findings for automatic inclusion in reports

A. Asset Tag
B. Host Name
C. Host Tag
D. Hash Tag

Q8. There can be only one Metasploit Administrative user.

A. True
B. False

Q9. VPN Pivot can have an IP set statically when DHCP is not available

A. True
B. False

Q10. The Quick PenTest Wizard is a guided interface to create a new project and:

A. Perform targeted exploitation on known hosts and collect data
B. Conduct a phishing campaign against human targets
C. Perform common tasks such as scanning, exploiting, collecting and reporting
D. None of the above

Q11. The Vulnerabiliuty Validation wizard can validate client-side vulnerabilities.

A. True
B. False

Q12. _____ automatically carry/carries out a series of tasks when a new session is opened.

A. Post-Exploitation macros
B. Task chains
C. Post exploitation modules
D. Meterpreter

Q13. A campaign that you build with the canned phishing campaign can only contain one e-mail and up to two web pages

A. True
B. False

Q14. A(n) _____ uses the host information obtained by the scan to build an attack plan based on the system and device type

A. Exploit Listing
B. Analysis
C. Network Map
D. Target Profile

Q15. Task chains need a minimum of 5 tasks

A. False
B. True

Q16. By default, Metasploit will always automatically update

A. True
B. False

Q17. Metasploit Pro can export project data to which the following common formats?

A. Timesheet (csv,xls,xlsx)
B. RAR Archive
C. Zip Workspace
D. Microsoft Word (doc, docx)

Q18. The ____ MetaModule tries an SSH private key on the specified hosts on the network and reports which hosts were successfully accessed.

A. Passive Network Discovery
B. SSH Key Testing
C. Known Credentials instruction
D. Pass The Hash

Q19. SMB is a valid bruteforce target.

A. True
B. False

Q20. Metasploit Pro does not automatically detect IPv6 addresses during a discovery scan

A. True
B. False

Q21. What payloads do exploits use by default?

A. Reverse staged payloads over HTTPS
B. Command shell
C. Reflective DLL injection
D. Meterpreter

Q22. How does one add a Nexpose Security Console connection to Metasploit?

A. By importing a Nexpose XML 2.0 export
B. By adding the credentials, IP address, and port for the Nexpose Security Console
C. By adding permission in the Nexpose Security Console to allow connections from Metasploit
D. All of the above steps are required to sync the two databases

Q23. What is NOT shown in the services tab? (select all that apply)

A. Port number
B. File name
C. Running processes
D. Service name

Q24. Social Engineering campaigns can only use a local SMTP instance.

A. True
B. False

Q25. Metasploit Pro license details can be viewed:

A. In the software license page
B. On the Home page
C. In the bottom left corner of each page
D. In the user settings page

Q26. A phishing campaign requires these components:

A. Email redirect page, and browser exploit
B. None of the above
C. Email landing page, and redirect page
D. Portable file, landing page, and email

Q27. During a phishing campaign, the Target Addresses are automatically restricted to the network range of the project.

A. True
B. False

Q28. Once a project is made, users cannot be added to a project.

A. True
B. False

Q29. The following is a supported credentials format:

Administrator:501:deq132a2B4642c7423fa06gx35:421a1cb1c0ed74a2ec000c8::

A. False
B. True

Q30. Metasploit Pro's Web Application scanner can use a session cookie for authentication.

A. False
B. True

Q31. It is okay to use the Passive Recon MecaModule outside scheduled scanning periods.

A. True
B. False

Q32. From the _____ tab, you can view hosts, nodes, services, vulnerabilities, captured data, and network topology at the project level

Q33. Once a project is created, the owner cannot be changed: the owner of the project must be the original creator.

A. True
B. False

Q34. What is the definition of a remote exploit?

A. An exploit that always provides administrative or root level access
B. An exploit that takes advantage of active services on a network connected device
C. An exploit embedded in a document that takes advantage of a vulnerable document viewer or editor
D. An exploit that cannot be used against a workstation target under any circumstances

Q35. Match the Web Application task to its definition:

1 - Web Audit

2 - Web Exploit

3 - Web Scan

A - Performs vulnerability checks for injection flaws
B - Takes advantage of known vulnerabilities
C - Recursively parses websites to find valid URLs

Q36. Match the Metasploit Pro Service to their description

1 - Prosrv

2 - Nginx

3 - Postgres

4 - Tin

A - The Metasploit RPC Server
B - Application server for the Ruby on Rails Web Browser
C - The web server that hosts the web interface|
D - The database that contains project data

Q37. What command lists the processes when interacting with a Meterpreter shell directly?

A. Pid_list
B. Ps
C. Pid
D. Ps_list

Q38. To Search for hosts that are not Linux, use the following advanced search query:

A. OS <==> linux
B. OS<>Linux
C. All hosts @windows true
D. Not=linux

Q39. The network topology is a logical map of the network: you can also launch attacks and scans from here.

A. False
B. True

Q40. Passive Network Discovery does NOT allow you to do the following:

A. Detect all open ports on a target
B. Map a network utilizing a packet Capture
C. Scan a network without sending outbound traffic
D. Capture all secure traffic on the network

Q41. You can reset your Metasploit Pro password by:

A. Contacting Technical Support
B. Generating a temporary password through the forgot password link
C. Passwords cannot be reset
D. Launching the resetpw script

Q42. _____ allow/allows you to share found information with other project users.

A. All of the above
B. Database pooling
C. Hash tag
D. Host comments

Q43. Match the following host statuses to their descriptions:

1 - Host Credentials have been compromised
2 - Host details have been discovered
3 - Host has been exploited successfully
4 - Host data has been collected

A - Cracked

B - Scanned

C - Shelled

D – Looted

Q44. What is NOT shown in the captured data tab?

A. Service name
B. Name of file
C. Hostname
D. Size of file

Q45. A _____ is a series of tasks that you can automate to run at a specific time and date.

A. Exploit chain
B. Task chain
C. Scheduled task
D. All of the above

Q46 Host tags can be used for:

A. All of the above
B. Targeted Reporting
C. Targeted Scanning
D. Targeted Exploiting

Q47. What information is shown in the Note tab? (select all that apply)

A. OS language
B. Port/protocol
C. References to databases for vulnerabilities
D. Host
E. OS name

Q48. The default port for the Metasploit Pro web interface is _____.

Q49. A Metasploit _____is a container for hosts, reports, and data for penetration test engagements.

Q50. What do you need to obtain from the owner of the network before starting a penetration test?

A. Obtain domain administrator credentials
B. Knowing your environment
C. Root access
D. Permission and scope of engagement

Q51. Which of the following are NOT typically collected evidence?

A. Password hashes
B. Desktop screenshots
C. System information
D. Event logs

Q52. What is the purpose of the firewall Egress Testing MetaModule?

A. Scans firewalls for vulnerabilities
B. Discovers outbound ports on a firewall that an attacked can use to exfiltrate information
C. Scans for all firewall rules
D. All of the above

Q53. To create a project backup you:

A. Export data from the Exports tab
B. Click the “Start Project Backup” buttons
C. Copy the Metasploit installation directory
D. Stop Metasploit Services

Q54. Metasploit automatically applies weekly updates

A. True
B. False

Q55. View the _____ file for troubleshooting module issues.

A. Metasploit.log
B. Framework.log
C. Prosrvc.log
D. Production.log

Q56. Only one user can access an instance of Metaploit Pro.

A. False
B. True

Q57. Listeners do not require a unique address an d port: you can have multiple listeners on a single port/host.

A. True
B. False

Q58. Reports can only be generated as a pdf.

A. True
B. False

Q59. The suggested workflow in a Metasploit Pro project is:

A. Discovery > Exploitation >Data collection > Cleanup > Reporting
B. Discovery > Exploitation > Reporting> Data collection > Cleanup
C. Exploitation > Discovery >Data collection > Cleanup
D. Reporting > Cleanup> Data collection > Exploitation > Discovery

Q60. Meterpreter injects into multiple parts of the filesystem, and runs on the hard drive of the victim's machine.

A. True
B. False

Q61. The Metasploit Pro Console and Metasploit Framework have the same feature set.

A. True
B. False

Q62. What is the definition of a payload?

A. Executable code that gains root or administrator privileges on a vulnerable target
B. Executable code that strictly runs vulnerability checks
C. Executable code that performs a malicious action such as executing a remote shell
D. Executable code that exploits a vulnerability on the target system, to gain access as an attacker

Q63. Which of these formats can be imported into Metasploit?

A. Microsoft Event Viewer EVT
B. Nmap XML
C. Nexpose HTML Report
D. Office Doc

Q64. There is no way to reset your password for Metasploit Pro, if this is forgotten, you must reinstall.

A. True
B. False

Q65. Only members with the _____ role can manage user accounts, install updates, and configure global settings in Metasploit Pro.

A. Administrator
B. System Administrator
C. Root
D. Global administrator

Q66. A bind payload:

A. None of the above
B. Attaches an open command shell to a listening service on the compromised machines
C. Automatically cracks and reveals passwords
D. Connects back to the attacking machine with an open command shell

Q67. Nexpose scan data imported into Metasploit Pro can provide:

A. Comprehensive host vulnerability data
B. Confirmed working exploits
C. Additional services to exploit
D. Windows password hashes

Q68. Project data can be exported as XML.

A. True
B. False

Q69. Metasploit Pro can automatically tag targets by OS.

A. False
B. True

Q70. Sessions are always automatically opened with guessed credentials during a Brute force.

A. True
B. False

Q71. The primary network tool Metasploit Pro uses for discovery:

A. Netstat
B. Netcat
C. Nmap
D. Nexpose

Q72. What is the definition of an Exploit?

A. Information returned from a system which aids in identifying potential weaknesses
B. A security flaw or weakness in an application or system that enables an attacked to compromise the target system
C. Code that is executed on a compromised system, usually to increase access such as through a shell or creation of an account, or to retrieve sensitive information
D. A program that takes advantage of a specific vulnerability and provides an attacked with access to the target system

Q73. What are the two Pivot types in Metasploit Pro?

A. SSH and telnet
B. Forward and reverse
C. VPN and proxy
D. All of the above

Q74. What can NOT be shown in the Hosts tab?

A. Port/protocol
B. IP address
C. Hostname
D. OS

Q75. By default, Nexpose scans run from Metasploit Pro are always purged in Nexpose upon completion

A. True
B. False

Answer Key

1	C	26	C	51	D
2	C	27	FALSE	52	B
3	TRUE	28	FALSE	53	A
4	D	29	FALSE	54	FALSE
5	D	30	TRUE	55	B
6	B	31	FALSE	56	FALSE
7	C	32	HOTS	57	FALSE
8	FALSE	33	FALSE	58	FALSE
9	TRUE	34	B	59	A
10	C	35	1A-2B-3C	60	FALSE
11	FALSE	36	1A-2B-3D-4C	61	FALSE
12	A	37	B	62	C
13	TRUE	38	B	63	B
14	D	39	FALSE	64	FALSE
15	FALSE	40	A	65	A
16	FALSE	41	D	66	B
17	C	42	D	67	A
18	B	43	1A-EB-3C-4D	68	TRUE
19	TRUE	44	A	69	TRUE
20	TRUE	45	B	70	TRUE
21	D	46	A	71	C
22	B	47	ABE	72	D
23	BC	48	3790	73	C
24	FALSE	49	PROJECT	74	A
25	D	50	D	75	FALSE