Q1. The database used by metaspoilt pro to store host data is

1. Mysql
2. IBMDB2
3. PostgresQL
4. Oracle DB

Answer: C

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

1. They are equal in speed
2. Passive reconnaissance
3. Active reconnaissance

Answer: C

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

1. True
2. False

Answer: True

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

1. USB storage
2. Client-side exploit
3. Phishing
4. Cloud connection

Answer: D

Q5. The \_\_\_\_\_\_\_\_\_\_ uses a compromised system to route network traffic

1. Routing module
2. Meterpreter
3. Botnet
4. VPN Pivot

Answer: D

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

1. Click sniffing
2. Click tracking
3. Click monitoring
4. Click jacking

Answer B

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

1. Asset Tag
2. Host Name
3. Host Tag
4. Hash Tag

Answer: C

Q8. There can be only one Metasploit Administrative user.

1. True
2. False

Answer: False

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

1. True
2. False

Answer: True

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

1. Perform targeted exploitation on known hosts and collect data
2. None of the above
3. Perform common tasks such as scanning, exploiting, collecting and reporting
4. Conduct a phishing campaign against human targets

Answer: C

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

1. True
2. False

Answer: False

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

1. Post-Exploitation macros
2. Task chains
3. Post exploitation modules
4. Meterpreter

Answer: A

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

1. True
2. False

Answer: True

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

1. Exploit Listing
2. Analysis
3. Network Map
4. Target Profile

Answer: D

Q15. Task chains need a minimum of 5 tasks

1. False
2. True

Answer: False

Q16. By Default, Metasploit will always automatically update

1. True
2. False

Answer: False

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

1. Timesheet (csv,xls,xlsx)
2. RAR Archive
3. Zip Workspace
4. Microsoft Word (doc, docx)

Answer: C

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

1. Passive Network Discovery
2. SSH Key Testing
3. Known Credentials instruction
4. Pass The Hash

Answer: B

Q19. SMB is a valid bruteforce target.

1. True
2. False

Answer: True

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

1. True
2. False

Answer: True

Q21. What payloads do exploits use by default?

1. Reverse staged payloads over HTTPS
2. Command shell
3. Reflective DLL injection
4. Meterpreter

Answer: D

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

1. All of the above steps are required to sync the two databases
2. By adding the credentials, IP address, and port for the Nexpose Security Console
3. By adding permission in the Nexpose Security Console to allow connections from Metasploit
4. By imposting a Nexpose XML 2.0 export

Answer: B

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

1. Port number
2. File name
3. Running processes
4. Service name

Answer: B, C

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

1. True
2. False

Answer: False

Q25. Metasploit Pro license details can be viewed:

1. In the software license page
2. On the Home page
3. In the bottom left corner of each page
4. In the user settings page

Answer: D

Q26. A phishing campaign requires these components:

1. Email redirect page, and browser exploit
2. None of the above
3. Email landing page, and redirect page
4. Portable file, landing page, and email

Answer: C

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

1. True
2. False

Answer: False

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

1. True
2. False

Answer: False

Q29. The following is a supported credentials format:

Administrator:501:deq132a2B4642c7423fa06gx35:421a1cb1c0ed74a2ec000c8::

1. False
2. True

Answer: False

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

1. False
2. True

Answer: True

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

1. True
2. False

Answer: False

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

Answer: hots

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

1. True
2. False

Answer: False

Q34. What is the definition of a remote exploit?

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

Answer: B

Q35. Match the Web Application task to its definition:

Web Audit

Web Exploit

Web Scan

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

Web Audit: Performs vulnerability checks for injection flaws

Web Exploit: Takes advantage of known vulnerabilities

Web Scan: Recursively parses websites to find valid URLs

Q36. Match the Metasploit Pro Service to their description

Prosrv

Nginx

Postgres

Tin

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

Prosvc: The Metasploit RPC Server

Nginx: Application Server for Ruby on Rails

Postgres: The database that contains the project data

Tin: The web server that hosts the web interface

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

1. Pid\_list
2. Ps
3. Pid
4. Ps\_list

Answer: B

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

1. OS <==> linux
2. OS<>Linux
3. All hosts @windows true
4. Not=linux

Answer: B

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

1. False
2. True

Answer: False

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

1. Detect all open ports on a target
2. Map a network utilizing a packet Capture
3. Scan a network without sending outbound traffic
4. Capture all secure traffic on the network

Answer: A

Q41. You can reset your metasploit Pro password by:

1. Contacting Technical Support
2. Generating a temporary password through the forgot password link
3. Passwords can not be reset
4. Launching the resetpw script

Answer: D

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

1. All of the above
2. Database pooling
3. Hash tag
4. Host comments

Answer: D

Q43. Match the following host statuses to their descriptions:

Host Credentials have been compromised  
host details have been discovered  
Host has been exploited successfully  
host data has been collected

Cracked

Scanned

Shelled

Looted

Cracked- Host Credentials have been compromised

Scanned- host details have been discovered

Shelled- host data has been collected

Looted- host data has been collected

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

1. Service name
2. Name of file
3. Hostname
4. Size of file

Answer: A

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

1. Exploit chain
2. Task chain
3. Scheduled task
4. All of the above

Answer: B

Q46 Host tags can be used for:

1. All of the above
2. Targeted Reporting
3. Targeted Scanning
4. Targeted Exploiting

Answer: A

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

1. OS language
2. Port/protocol
3. References to databases for vulnerabilities
4. Host
5. OS name

Answer: A, B, E

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

Answer: 3790

Q49. A Metasploit \_\_\_\_\_\_\_\_\_is a container for hosts, reports, and data for penetration test engagements.

Answer: Project

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

1. Obtain domain administrator credentials
2. Knowing your environment
3. Root access
4. Permission and scope of engagement

Answer: D

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

1. Password hashes
2. Desktop screenshots
3. System information
4. Event logs

Answer: D

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

1. Scans firewalls for vulnerabilities
2. Discovers outbound ports on a firewall that an attacked can use to exfiltrate information
3. Scans for all firewall rules
4. All of the anove

Answer: B

Q53. To create a project backup you:

1. Export data from the Exports tab
2. Click the “Start Project Backup” buttons
3. Copy the Metasploit installation directory
4. Stop Metasploit Services

Answer: A

Q54. Metasploit automatically applies weekly updates

1. True
2. False

Answer: False

Q55. View the \_\_\_\_\_\_ file for troubleshooting module issues.

1. Metasploit.log
2. Framework.log
3. Prosrvc.log
4. Production.log

Answer: B

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

1. False
2. True

Answer: False

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

1. True
2. False

Answer: False

Q58. Reports can only be generated as a pdf.

1. True
2. False

Answer: False

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

1. Discovery > Exploitation >Data collection > Cleanup > Reporting
2. Discovery > Exploitation > Reporting> Data collection > Cleanup
3. Exploitation > Discovery >Data collection > Cleanup
4. Reporting > Cleanup> Data collection > Exploitation > Discovery

Answer: A

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

1. True
2. False

Answer: False

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

1. True
2. False

Answer: False

Q62. What is the definition of a payload?

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

Answer: C

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

1. Microsoft Event Viewer EVT
2. Nmap XML
3. Nexpose HTML Report
4. Office Doc

Answer: B

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

1. True
2. False

Answer: False

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

1. Administrator
2. System Administrator
3. Root
4. Global administrator

Answer: A

Q66. A bind payload:

1. None of the above
2. Attaches an open command shell to a listening service on the compromised machines
3. Automatically cracks and reveals passwords
4. Connects back to the attacking machine with an open command shell

Answer: B

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

1. Comprehensive host vulnerability data
2. Confirmed working exploits
3. Additional services to exploit
4. Windows password hashes

Answer: A

Q68. Project data can be exported as XML.

1. True
2. False

Answer: True

Q69. Metasploit Pro can automatically tag targets by OS.

1. False
2. True

Answer: True

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

1. True
2. False

Answer: True

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

1. Netstat
2. Netcat
3. Nmap
4. Nexpose

Answer: C

Maybe D???

Q72. What is the definition of an Exploit?

1. Information returned from a system which aids in identifying potential weaknesses
2. A security flaw or weakness in an application or system that enables an attacked to compromise the target system
3. 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
4. A program that takes advantage of a specific vulnerability and provides an attacked with access to the target system

Answer: D

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

1. All of the above are valid
2. Forward and reverse
3. VPN and proxy
4. SSH and telnet

Answer: C

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

1. Port/protocol
2. IP address
3. Hostname
4. OS

Answer: A

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

1. True
2. False

Answer: False