1. Which operating system is most likely to be vulnerable to the TTYPROMPT vulnerability in the telnet service?
   A. Solaris 10
   B. Solaris 8
   C. Solaris 9
   D. Linux
   E. FreeBSD
2. You connect to TCP port 22 on a target system and receive the banner "SSH-1.99-OpenSSH_3.9p1". Which of the following statements about this system are true?
   A. It is an SSH server, and supports SSH version 1 only.
   B. It is an SSH server, and supports SSH version 2 only.
   C. It is an SSH server, and supports SSH version 1 and version 2.
   D. It is an SSH server, and only allows connections from an OpenSSH client.
   E. It is an SSH server, and supports SSH version 1.99.
3. What are the three main pieces of legislation that are relevant to penetration testing in the UK?
   A. The Freedom of Information Act, The Data Protection Act and The Terrorism Act.
   B. The Terrorism Act, The Freedom of Information Act and The Computer Misuse Act.
   C. The Food Standards Act, The Misuse of Drugs Act and The Breeding and Sale of Dogs Act.
   D. The Computer Misuse Act, The Human Rights Act and The Data Protection Act.
   E. The Rehabilitation of Offenders Act, The Employment Relations Act and The Human Rights Act.
4. What is the primary legal reason for obtaining written permission before starting a test?
   A. There are no legal reasons, only commercial reasons.
   B. Because otherwise the client might not pay for the work.
   C. Because otherwise the penetration test might breach the Human Rights Act.
   D. Because otherwise the penetration test might breach the Computer Misuse Act.
   E. Because otherwise the penetration test might breach the Data Protection Act.
5. Which of the following cipher modes use a block cipher to generate a key stream that can be used as a stream cipher?
   A. CBC
   B. CFB
   C. ECB
   D. EDE
   E. ABC
6. Which nmap flag enables OS TCP/IP stack fingerprinting?
   A. -sS
   B. -n
   C. -v
   D. -O
   E. -P0
7. What is the OUI part of the Ethernet MAC address 00:0B:46:48:29:80?
   A. 00:0B
   B. 00:0b:46:48:29
   C. 00:0B:46
   D. 00:0b:46:48
   E. 00
8. You discover a vulnerability on an Internet accessible web server which allows you to execute commands as a non-privileged user. The web server is behind a firewall that allows only TCP port 80 inbound and permits all outbound traffic. What technique could be used to get shell access to the webserver?
   A. It is not possible to obtain shell access in these circumstances.
   B. Run a shell on the webserver with its control channel listening on a high TCP port.
   C. Run a shell on the webserver with its control channel listening on TCP port 80.
   D. Run a shell on the webserver and connect its control channel back to a TCP port on your local system.
   E. Run a shell on the webserver with its control channel listening on TCP port 81.
9. What is the name of the database administrator account on Microsoft SQL server?
   A. sa
   B. dbo
   C. root
   D. administrator
   E. admin
10. When was the Apache chunked encoding vulnerability fixed in version 2.0?
   A. 2.0.36
   B. 2.0.39
   C. 2.0.30
   D. 2.0.1
   E. 2.0.64
11. What is the name given to the field concerned with the security implications of electronic eminations from communications equipment?
   A. TYPHOON
   B. TEMPEST
   C. STORM
   D. CYCLONE
   E. HURRICANE
12. You find a system that is offering the NFS RPC service. What is the logical next step?
   A. Try to find a buffer overflow vulnerability in the NFS service.
   B. Run "showmount -e" to list the NFS exports.
   C. Try to mount an exported filesystem.
   D. Report it as a vulnerability.
   E. Leave it and move on because there are no known vulnerabilities in NFS.
13. Which of these is not an ICMP message type?
   A. Source Quench
   B. Echo reply
   C. Echo request
   D. Host unreachable
   E. Router Solicitation
14. What is this: 17:58:01.396446 CDPv2, ttl: 180s, Device-ID 'chestnut.nta-monitor.com', length 404
   A. A NetBIOS over TCP/IP name service broadcast
   B. An ARP broadcast
   C. A Spanning Tree Protocol broadcast
   D. A NetBIOS over TCP/IP session service broadcast
   E. A CDP broadcast
15. Which of the following algorithms could be used to negotiate a shared encryption key?
   A. Diffie-Hellman
   B. DES
   C. SHA1
   D. AES
   E. Triple-DES
16. What would you expect the command "finger 0@hostname" (that is a zero) against a Solaris 8 system to display?
   A. Users with an empty password field in the password file.
   B. Users with UID 0 in the password file.
   C. Users with an empty shell field in the password file.
   D. Users with an empty home directory field in the password file.
   E. Users with an empty GCOS field in the password file.
17. The register_globals setting in php.ini is
   A. A security risk if enabled, and should never be used.
   B. Nothing to do with security, and the setting depends on the developers preference.
   C. Nothing to do with security, but can improve the performance of PHP scripts.
   D. Nothing to do with security, but can reduce the memory usage of PHP scripts.
   E. A security benefit and should always be enabled.
18. What command might you use to obtain a list of systems from a master browser, together with details about the version and available services.
   A. amap
   B. nbtstat
   C. lservers
   D. nbtquery
   E. hping3
19. What password hashes are stored by default on a Windows 2003 system?
   A. Salted MD5
   B. Unix crypt
   C. DES
   D. LM Hash and NTLM Hash
   E. MD4
20. Which protocol and port does a normal DNS lookup use?
   A. UDP port 53
   B. UDP port 43
   C. TCP port 45
   D. TCP port 53
   E. TCP port 43

21. Which of these protocols is not vulnerable to address spoofing if implemented correctly?
    A. UDP
    B. Ethernet
    C. SMTP
    D. TCP
    E. IP
22. What does "export" signify for an SSL cipher
    A. It is a weak cipher that was acceptable for export under the old US cryptography export regulations
    B. It is the strongest cipher that is currently permitted to be exported from the US
    C. It is a cipher that is suitable for encrypting information to be sent across national borders
    D. It is a cipher with integrated key escrow, which allows the NSA to recover the key
    E. It is a stronger version of a cipher, similar to export versions of European lagers
23. What is the length of the IV for a WEP key?
    A. 128 bits
    B. 64 bits
    C. 40 bits
    D. 24 bits
    E. 56 bits
24. Which of the following is NOT an EAP method?
    A. EAP-RSA
    B. EAP-TLS
    C. EAP-MD5
    D. EAP-PSK
    E. EAP-TTLS
25. What RPC authentication mechanism does NFS v2 and v3 use?
    A. AUTH_DH, Diffie-Hellman authentication
    B. AUTH_SYS, using Unix UID and GID
    C. RPCSEC_GSS, Generic security services
    D. Kerberos
    E. AUTH_NONE, no authentication
26. What is this: password 7 052D131D33556C081D021200
    A. A password with the literal value "052D131D33556C081D021200"
    B. A password encoded with salted MD5
    C. A password encoded with unsalted DES
    D. A password encoded with the reversible Cisco vigenere algorithm
    E. A password encoded with Unix crypt
27. On a Unix system, what is the effect of the execute bit on a directory?
    A. It allows the directory to be traversed.
    B. It allows all files in the directory to be executed.
    C. It allows the directory to be executed.
    D. It has no effect.
    E. It depends on the version of Unix that is being used.
28. What is the normal sequence of events in a penetration test?
    A. Testing, Scoping, Report Writing, Debrief.
    B. Scoping, Testing, Report Writing, Debrief.
    C. Debrief, Testing, Scoping, Report Writing.
    D. Testing, Scoping, Debrief, Report Writing.
    E. Scoping, Report Writing, Testing, Debrief.
29. What is the default VLAN on most switches?
    A. VLAN 4096
    B. VLAN 1000
    C. VLAN 0
    D. VLAN 4095
    E. VLAN 1
30. Which Act amended the Computer Misuse Act 1990?
    A. The Police and Justice Act 2006.
    B. The Police and Criminal Evidence Act.
    C. The Regulation of Investigatory Powers Act 2000.
    D. The Terrorism Act 2006.
    E. The Terrorism Act 2000.
31. Should users be informed that a penetration test is being carried out?
    A. Yes, they have a right to know when their privacy may be breached unless the system's AUP says otherwise.
    B. No, they don't have any need to know.
    C. Yes, because it is always polite to keep people informed.
    D. Yes, they might want to observe the penetration testing process.
    E. No. It is vital that they are not aware or they may interfere with the testing process.
32. AJAX is
    A. A household cleaner
    B. A Dutch football team
    C. Automatic Java and XML
    D. Apache Javascript and XML
    E. Asynchronous Javascript and XML
33. Which protocols and ports are used by Telnet, SMTP and Finger?
    A. TCP/23, TCP/25 and TCP/69.
    B. UDP/23, UDP/25 and UDP/79.
    C. TCP/23, TCP/35 and TCP/69.
    D. TCP/23, TCP/25 and TCP/79.
    E. TCP/22, TCP/25 and TCP/79.
34. The UK Government protective marking levels are, from lowest to highest protection:
    A. NPM, PROTECT, RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET.
    B. CLASSIFIED, INTERNAL USE ONLY, SECRET, TOP SECRET.
    C. CONFIDENTIAL, SECRET, TOP SECRET.
    D. TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED.
    E. NPM, RESTRICTED, PROTECT, CONFIDENTIAL, SECRET, TOP SECRET.
35. What effect does setting the RestrictAnonymous registry setting to 1 have on a Windows NT or 2000 system?
    A. It prevents enumeration of SAM accounts and names.
    B. It does not have any effect, because 1 is the default setting on NT and 2000.
    C. It does not have any effect, because 1 is not a valid setting on NT and 2000.
    D. It remove the "everyone" group from the access token for non-authenticated users, preventing most access from null sessions.
    E. It prevents RID cycling.
36. Which tool is commonly used for passive TCP/IP fingerprinting?
    A. nmap
    B. hping2
    C. scapy
    D. p0f
    E. nbtstat
37. During a penetration test, you gain access to a database containing personal details of staff. What is the best course of action?
    A. Note the issue but do not store any of the personal data on your system.
    B. Change the database settings to address the vulnerability.
    C. Take a copy of the database so you can use it in your report.
    D. Drop the database so hackers cannot access this data.
    E. Publish the information in a case study.
38. An accepted limitation of Diffie-Hellman key agreement protocol is
    A. It is vital to keep the shared prime secret
    B. It can only generate encryption keys up to 128 bits
    C. It is vulnerable to a man-in-the-middle attack
    D. An attacker who can monitor the exchange can determine the shared secret
    E. It is possible for one of the peers to control the generated secret
39. Which of these is not a valid IPv6 address?
    A. 2001:0db8:0:0:0:0:1428:57ab
    B. 2001:db8::1428:57ab
    C. 2001:0db8:0:0::1428:57ab
    D. 2001:0db8:1428:57ab
    E. 2001:0db8:0000:0000:0000:0000:1428:57ab
40. What are the four mandatory transform attributes for an IKE Phase-1 SA?
    A. Encryption Algorithm, Hash Algorithm, Authentication Method, Diffie Hellman Group
    B. Encryption Algorithm, Key Length, Authentication Method, SA Lifetime
    C. SA Lifetime, Key length, PRF, Field Size
    D. SA Lifetime, Hash Algorithm, Authentication Method, PRF
    E. Protocol ID, Transform ID, IPsec Mode, Authentication Algorithm
41. what technique forwards traffic to an attacker's system by associating the attacker's MAC address with the IP address of the target system?

A. Teardrop attack.
B. ARP flooding
C. LAND attack.
D. ARP spoofing or ARP poisoning.
E. SMURF attack.

42. What are the SIP and RTP protocols used for in VoIP?
A. SIP and RTP are competing protocols that are both used for audio data transmission.
B. RTP is used for setting up and closing down calls, and SIP is used for audio data transmission.
C. SIP is used for setting up and closing down calls, but RTP is nothing to do with VoIP.
D. SIP and RTP are competing protocols that are both used for setting up and tearing down calls.
E. SIP is used for setting up and closing down calls, and RTP is used for audio data transmission.

43. What amount of disruption to the client's systems is acceptable during a penetration test?
A. None, and the client should report any anomalous behaviour immediately.
B. Quite a lot. Disruption is to be expected during a full penetration test.
C. It depends, but the client should be asked not to bother the testers as they have enough to deal with.
D. There should be no disruption if the systems are secure, but the client should expect disruption if there are vulnerabilities.
E. An few spontaneous reboots and occasional data corruption, but nothing really bad.

44. What effect would an octal umask of 0027 have on the permissions of new files?
A. It has no effect on new files because it only affects existing files.
B. Remove SUID, SGID and Sticky bits, remove all owner permissions, and remove read and execute group access.
C. Add SUID, SGID and Sticky bits, add all owner permissions, and add read and execute group access.
D. Add group write access, and add all permissions for others.
E. Remove group write access, and remove all permissions for others.

45. Which protocols are associated with IPsec?
A. IP protocol 89
B. UDP port 500, IP protocol 50 and IP protocol 51.
C. TCP port 1723 and IP protocol 47
D. IP protocol 94
E. TCP port 443

46. What is TCP and UDP port number 111 typically used for on a Unix system?
A. The network time protocol (NTP).
B. Nothing. Port 111 is not assigned.
C. The Simple Network Management Protocol (SNMP).
D. The DCE/RPC location service.
E. The ONC/RPC portmapper.

47. What command would you use to display the version number of a Microsoft SQL Server database if you are connected with a command line client?
A. select @@version;
B. get version;
C. display version;
D. select version();
E. show version;

48. What is the maximum length of an SSID?
A. 32 Bytes
B. 48 Bytes
C. 64 Bytes
D. 16 Bytes
E. 24 Bytes

49. The active directory database file is:
A. NTDS.DIT
B. MSAD.DIT
C. NTDS.DAT
D. MDAD.MDB
E. NTDS.MDB

50. Which is the least secure encryption cipher of those listed below?
A. MD5
B. Triple-DES
C. DES
D. AES
E. IDEA

51. What is the primary objective of risk management?
A. To determine what budget should be assigned to information security.
B. To reduce the risk to an acceptable level.
C. To assign responsibility for the various issues that have been discovered.
D. To understand the level of risk.
E. To remove all risk.

52. Which file in a user's home directory controls the trust relationships for Berkeley R services?
A. hosts.equiv
B. rhosts
C. rhosts.allow
D. .rhosts
E. hosts.allow

53. What is the blocksize of the AES encryption cipher?
A. 64 bits
B. 40 bits
C. 56 bits
D. 256 bits
E. 128 bits

54. What is the security model that limits Java applications to a restricted set of functions?
A. chroot jail
B. firewall
C. IDS
D. Object oriented coding
E. Sandbox

55. What does EAP stand for?
A. Extensible Authentication Protocol
B. Extensible Accounting Protocol
C. Enhanced Authentication Protocol
D. Extended Authentication Protocol
E. Extensible Authorization Protocol

56. What does LAMP stand for?
A. Linux Apache MySQL PHP
B. Lightweight Automated MySQL or Postgres
C. Linux Ajax MySQL Perl
D. It's just a name, it doesn't stand for anything.
E. Linux ASP Multi-User Processing

57. Which of these groups of tools are commonly used for packet crafting?
A. wireshark, tcpdump and dsniff
B. john, cain & able and l0phtcrack
C. nmap, superscan and angry IP scanner
D. hping2, hping3 and scapy
E. kismet, netstumbler and aircrack

58. Which protocol and port does a DNS zone transfer use?
A. TCP port 43
B. TCP port 53
C. UDP port 43
D. TCP port 45
E. UDP port 53

59. What command would you use to list the installed packages on a Solaris system?
A. pkg_info
B. pkginfo
C. dpkg -l
D. rpm -qa
E. cat /proc/sys/packages

60. On which web server would you expect to find ISAPI filters and extensions?
A. Apache
B. Sun ONE Web server
C. Microsoft IIS
D. IBM Websphere
E. iPlanet Web Server

61. Which of the following protocols provides confidentiality and integrity, and is not vulnerable to a man-in-the-middle attack?
A. IPsec using AH

B. Telnet
C. SSH v3
D. SSH v1
E. SSH v2

62. What TCP port does Microsoft SQL Server listen on in hidden mode?
A. 1521
B. 1433
C. 2433
D. 3306
E. 1434

63. During an audit of a Unix system, you find that the file "/etc/crontab" is owned by root and has mode 0666. What is the most serious risk associated with this?
A. Informational: /etc/crontab is not used on modern Unix systems, but it does not represent a risk.
B. Information leakage: any user may view the crontab file.
C. Privilege escalation: this indicates that the "cron" daemon is running, and it might be vulnerable to a buffer overflow.
D. Privilege escalation: any user could create a cron job which would run as root.
E. Informational: This indicates that the "crontab" package is installed, but it does not represent a risk.

64. If you find TCP port 111 open on a Unix system, what is the next logical step to take?
A. Telnet to the port, send "GET / HTTP/1.0" and gather information from the response.
B. Report it as a vulnerability.
C. Telnet to the port to look for a banner.
D. Run amap against it to determine what service is running on that port.
E. Run "rpcinfo -p" to enumerate the RPC services.

65. What attack can be used to force some switches to forward frames to all ports?
A. MAC flooding
B. VLAN hopping
C. ARP spoofing or ARP poisoning
D. IP fragmentation
E. LAND attack

66. Which string in a NetBIOS name indicates that the specified host is a Master Browser?
A. MASTER-BROWSER
B. MSBROWSE
C. MASTERBROWSER
D. MS-BROWSER
E. MS-BROWSE

67. Which of the following are all ONC/RPC services?
A. rusersd, rstatd, sprayd, rexec.
B. ntp, nfs, netbios, nntp.
C. cmsd, kcms_server, sadmind, snmpXdmid.
D. rexec, rlogin, rsh, rsync.
E. telnet, ssh, ftp, http.

68. What is the underlying cause of the WEP vulnerability?
A. Weak hash algorithm.
B. Insufficient key length.
C. Weak encryption algorithm.
D. Lack of authentication between the client and AP.
E. Weak initialisation vector.

69. TCP port 1433 is commonly used by which database?
A. DB2
B. Postgres
C. Microsoft SQL Server
D. MySQL
E. Oracle 9i

70. What is the digest length for the SHA1 hash function?
A. 128 bits
B. 192 bits
C. 56 bits
D. 160 bits
E. 256 bits

71. On a Solaris system, what controls if the superuser is allowed to login over Telnet?
A. There is no control, the superuser is always allowed to login over Telnet.
B. The CONSOLE setting in /etc/default/login
C. It depends on the version of Solaris.
D. The SUID bit on /usr/bin/in.telnetd.
E. There is no control, the superuser is never allowed to login over Telnet.

72. What is the significance of the string "SEP" in the configuration filename of a Cisco IP phone?
A. It stands for Cisco Ethernet Phone, but someone misspelled it and the name stuck.
B. It stands for Selsius Ethernet Phone, which was the original name of the Cisco IP phone.
C. It stands for Skinny Enchanced Phone.
D. It stands for SIP Enhanced Phone.
E. No one knows.

73. Where are the encrypted passwords stored on a FreeBSD system?
A. In the TPM chip
B. /etc/passwd
C. /etc/group
D. /etc/shadow
E. /etc/master.passwd

74. Which command will retrieve the version number from default installations of the BIND nameserver software?
A. dig @nameserver bind.version txt chaos
B. dig @nameserver bind-version txt chaos
C. dig @nameserver version.bind txt chaos
D. dig @nameserver nameserver.version txt chaos
E. dig @nameserver version.bind hinfo chaos

75. What does the phrase "Inherent Risk" mean in risk management?
A. A risk that doesn't really matter.
B. A very serious risk.
C. A risk that is implicitly associated with an activity or location.
D. A risk that no one knows what to do about.
E. A material misstatement relating to an assertion.

76. Why might a tester insert the string "<script>alert("it works")</script>" into a web form?
A. To check for a blind SQL Injection vulnerability.
B. To check for a Cross-Site Scripting vulnerability.
C. To check for a SQL Injection vulnerability.
D. To check that the form submission works correctly.
E. To check for a session fixation vulnerability.

77. What is the function of the ARP protocol?
A. It caches frequently used host names.
B. It assigns an IP address to a host.
C. It maps host names to IP addresses.
D. It determines the OUI for layer-2 hardware addresses.
E. It maps IP addresses to layer-2 hardware addresses.

78. Which of these standards defines the structure of a digital certificate?
A. X.400
B. X.500
C. X.509
D. X.25
E. X.21

79. A client asks what effect the penetration test is likely to have on the systems being tested. What would be the best response?
A. There will probably be a large number of log entries, and some accounts may be locked out by password guessing.
B. I don't know, they are your systems not mine.
C. None at all.
D. All sorts of things can happen, it's pretty random and there is no way to predict it.
E. If they are secure, then they will be alright.

80. What is the most secure method to use if you need to run an X Window client on a remote system and display it on your local X server?
A. Use the Sun-DES authentication method.
B. Establish an SSH connection to the remote system and tunnel the X Window connection back to your X Server.
C. Use the XDM-Authorization authentication method.
D. Use the MIT-Magic-Cookie authentication method.
E. Use "xhost +" to allow any system to connect to the X server.

81. What is the default password for the SYS user on Oracle 9i?
A. DBSNMP
B. blank

C. CHANGE_ON_INSTALL
D. MANAGER
E. SYSADM

82. What version of NFS includes strong security, including strong authentication and encryption?
A. version 3
B. version 2
C. version 1
D. version 4
E. version 5

83. What are the seven OSI layers, from lowest to highest?
A. Physical, Data Link, Transport, Network, Session, Presentation, Application
B. Physical, Data Link, Network, Transport, Session, Presentation, Application
C. Physical, Data Link, Network, Transport, Presentation, Session, Application
D. Physical, Network, Data Link, Transport, Session, Presentation, Application
E. Data Link, Physical, Network, Transport, Session, Presentation, Application

84. What is the blocksize of the DES encryption cipher?
A. 128 bits
B. 112 bits
C. 56 bits
D. 64 bits
E. 40 bits

85. You discover an Internet accessible anonymous FTP server on a client's internal network, which is vulnerable to the FTP bounce attack. What is the impact of this vulnerability?
A. Attackers could exploit the vulnerability to intercept network traffic on the client's internal network.
B. Attackers could exploit the vulnerability to access any file on the FTP server.
C. Attackers could exploit the vulnerability to port scan other systems on the client's internal network.
D. Attackers could exploit the vulnerability to gain administrative access to the FTP server.
E. Attackers could exploit the vulnerability to upload files to the FTP server.

86. What command would you use to list the installed packages on a Redhat or Fedora system?
A. pkginfo
B. dpkg -l
C. rpm -qa
D. cat /proc/sys/packages
E. pkg_info

87. Which of the following protocols is the most secure?
A. WEPplus
B. WPA with CCMP (AES)
C. WPA with TKIP (RC4)
D. WEP2
E. WEP

88. What would an SNMP request to set OID 1.3.6.1.4.1.9.2.1.55.10.0.0.1 to "file" on a Cisco router using a community string with read/write access do?
A. Cause the router at IP address 10.0.0.1 to display its configuration file
B. Cause the target router to upload its configuration file to the TFTP server at 10.0.0.1 as a file called "file".
C. Cause the target router to load its configuration file from NVRAM
D. Cause the target router to download the configuration file from the TFTP server at 10.0.0.1 from a file called "file".
E. Cause the target router to write its configuration file to NVRAM

89. UDP port 1434 is commonly used by which database?
A. MySQL
B. Microsoft SQL Server
C. Postgres
D. Oracle 9i
E. DB2

90. A web server returns "Server: Microsoft-IIS/5.0" in the HTTP headers. What operating system is it probably using?
A. Windows XP
B. Windows 2003 Server
C. Windows NT4 Server
D. Windows 2000 Server
E. Windows 2008 Server