1. Why can remote access VPNs not use Main Mode for IKE Phase-1 if the authentication method is pre-shared key?
A. Because remote access servers always use aggressive mode for IKE Phase-1.
B. Because XAUTH is not compatible with IKE Main Mode.
C. Because IKE Main Mode does not support the pre-shared key authentication method.
D. Because pre-shared key authentication with Main Mode requires that the peer's IP is known before the connection is established.
E. Because remote access clients always use aggressive mode for IKE Phase-1.
2. What is the blocksize of the DES encryption cipher?
A. 40 bits
B. 128 bits
C. 64 bits
D. 56 bits
E. 112 bits
3. What is this: 16:23:57.094021 IP 192.168.124.204.137 > 192.168.124.255.137: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
A. A Spanning Tree Protocol broadcast
B. A NetBIOS over TCP/IP name service broadcast
C. An ARP broadcast
D. A NetBIOS over TCP/IP session service broadcast
E. A CDP broadcast
4. Which is the least secure encryption cipher of those listed below?
A. Triple-DES
B. MD5
C. AES
D. DES
E. IDEA
5. 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
6. Which operating system is most likely to be vulnerable to the TTYPROMPT vulnerability in the telnet service?
A. Solaris 9
B. Linux
C. Solaris 10
D. Solaris 8
E. FreeBSD
7. Which of the following algorithms could be used to negotiate a shared encryption key?
A. Triple-DES
B. SHA1
C. DES
D. AES
E. Diffie-Hellman
8. Why might a tester insert the string "<script>alert("it works")</script>" into a web form?
A. To check for a session fixation vulnerability.
B. To check for a SQL Injection vulnerability.
C. To check for a blind SQL Injection vulnerability.
D. To check for a Cross-Site Scripting vulnerability.
E. To check that the form submission works correctly.
9. Which protocols are associated with PPTP?
A. IP protocol 89
B. IP protocol 94
C. TCP port 443
D. TCP port 1723 and IP protocol 47
E. UDP port 500, IP protocol 50 and IP protocol 51.
10. Where are the encrypted passwords stored on a Solaris system?
A. /etc/shadow
B. In the TPM chip
C. /etc/passwd
D. /etc/master.passwd
E. /etc/group
11. Which of the following statements about the rwho protocol is true?
A. The rwho daemon sends regular broadcasts to UDP port 513, and listens to broadcasts from other systems.
B. rwho clients can query the rwho daemon. The protocol uses ONC/RPC.
C. rwho clients can query the rwho daemon using UDP port 513.
D. rwho clients can query the rwho daemon using TCP port 513.
E. The rwho daemon sends regular broadcasts to TCP port 513, and listens to broadcasts from other systems.
12. How would you establish a null session to a windows host from a windows command shell?
A. NET USE \\hostname\c$ "" /u:NULL
B. NET USE \\hostname\c$ "" /u:""
C. NET USE \\hostname\ipc$ "" /u:""
D. NET USE \\hostname\ipc$ "" /u:NULL
E. NET USE \\hostname\ipc$ NULL /u:NULL
13. If the account lockout threshold is set to 5, how many incorrect password attempts will cause the built in administrator account to be locked out on a Windows 2003 system?
A. one attempt
B. six attempts
C. The built in administrator account will never be locked out.
D. It depends on the account lockout duration setting
E. five attempts
14. What effect would an octal umask of 0027 have on the permissions of new files?
A. Remove group write access, and remove all permissions for others.
B. Add SUID, SGID and Sticky bits, add all owner permissions, and add read and execute group access.
C. It has no effect on new files because it only affects existing files.
D. Add group write access, and add all permissions for others.
E. Remove SUID, SGID and Sticky bits, remove all owner permissions, and remove read and execute group access
15. What is the name given to the field concerned with the security implications of electronic eminations from communications equipment?
A. CYCLONE
B. TEMPEST
C. TYPHOON
D. HURRICANE
E. STORM
16. Which of these is not a valid IPv6 address?
A. 2001:0db8:1428:57ab
B. 2001:db8::1428:57ab
C. 2001:0db8:0:0:0:0:1428:57ab
D. 2001:0db8:0000:0000:0000:0000:1428:57ab
E. 2001:0db8:0:0::1428:57ab
17. 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 access any file on the FTP server.
B. Attackers could exploit the vulnerability to upload files to 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 intercept network traffic on the client's internal network.
E. Attackers could exploit the vulnerability to gain administrative access to the FTP server.
18. 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 home directory field in the password file.
B. Users with an empty GCOS field in the password file.
C. Users with UID 0 in the password file.
D. Users with an empty shell field in the password file.
E. Users with an empty password field in the password file.
19. What are the four potential risk treatments?
A. Treat, Ignore, Downplay and Optimise.
B. Avoid, Reduce, Accept and Transfer.
C. Physical, Environmental, Technical and Managerial.
D. Best Practice, Standards Based, Regulation and Compliance.
E. Theoretical, Practical, Logical and Virtual.
20. 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 with integrated key escrow, which allows the NSA to recover the key
D. It is a cipher that is suitable for encrypting information to be sent across national borders
E. It is a stronger version of a cipher, similar to export versions of European lagers
21. Which of these protocols is not vulnerable to address spoofing if implemented correctly?

A. UDP
B. TCP
C. IP
D. Ethernet
E. SMTP

22. 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 remove the "everyone" group from the access token for non-authenticated users, preventing most access from null sessions.
C. It does not have any effect, because 1 is not a valid setting on NT and 2000.
D. It does not have any effect, because 1 is the default setting on NT and 2000.
E. It prevents RID cycling.

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

24. Which protocols and ports are used by Telnet, SMTP and Finger?
A. UDP/23, UDP/25 and UDP/79.
B. TCP/23, TCP/25 and TCP/79.
C. TCP/23, TCP/35 and TCP/69.
D. TCP/23, TCP/25 and TCP/69.
E. TCP/22, TCP/25 and TCP/79.

25. 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 load its configuration file from NVRAM
C. Cause the target router to download the configuration file from the TFTP server at 10.0.0.1 from a file called "file".
D. Cause the target router to write its configuration file to NVRAM
E. Cause the target router to upload its configuration file to the TFTP server at 10.0.0.1 as a file called "file".

26. What RPC authentication mechanism does NFS v2 and v3 use?
A. AUTH_SYS, using Unix UID and GID
B. Kerberos
C. AUTH_NONE, no authentication
D. RPCSEC_GSS, Generic security services
E. AUTH_DH, Diffie-Hellman authentication

27. Which of these statements about the Windows built in administrator account is correct?
A. It is always named "Administrator"
B. It is the only member of the "Administrators" group
C. It always has RID 500
D. It cannot be renamed
E. It always has SID 500

28. *What does the "*Root Squash" option on an NFS export do?
A. Makes all users on the NFS client access files as root on the server.
B. Prevents any access by the root user on the NFS client.
C. Allows the root user on the NFS client to access files as root on the server.
D. Makes the root user on the NFS client access files as nobody on the server.
E. Prevents the use of SUID files that are owned by root on the NFS server.

29. With blind SQL injection, the results of the injection are not visible, and no errors are displayed. How can blind SQL injection be detected?
A. By sniffing the packets travelling between the browser and the web server.
B. The results are encoded in the HTTP headers returned by the server.
C. The attacker can only detect blind SQL injection by gaining physical access to the web server.
D. By observing the HTTP response code sent by the server.
E. The web server behaviour changes when a successful injection is performed.

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

31. Which of the following cipher modes use a block cipher to generate a key stream that can be used as a stream cipher?
A. CFB
B. ECB
C. CBC
D. EDE
E. ABC

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

33. What is the default password for the DBSNMP user on Oracle 9i?
A. blank
B. DBSNMP
C. MANAGER
D. SYSADM
E. CHANGE_ON_INSTALL

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

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

36. Which nmap flag enables OS TCP/IP stack fingerprinting?
A. -sS
B. -v
C. -n
D. -P0
E. -O

37. Which of the following is NOT an EAP method?
A. EAP-PSK
B. EAP-TTLS
C. EAP-TLS
D. EAP-MD5
E. EAP-RSA

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

39. Which of these is an IP option?
A. Timestamp
B. Maximum Segment Size
C. Window Scale
D. Record Route
E. SACK

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

41. When was the Apache chunked encoding vulnerability fixed in version 1.3?
A. 1.3.1

B. 1.3.42
C. 1.3.24
D. 1.3.20
E. 1.3.26

42. An accepted limitation of Diffie-Hellman key agreement protocol is
A. It is vital to keep the shared prime secret
B. It is possible for one of the peers to control the generated secret
C. It can only generate encryption keys up to 128 bits
D. An attacker who can monitor the exchange can determine the shared secret
E. It is vulnerable to a man-in-the-middle attack

43. What are the privileged TCP and UDP ports, which only a privileged user can listen on?
A. 1024 - 65535 inclusive.
B. 0 - 1024 inclusive.
C. 32768 - 65535 inclusive.
D. 0 - 65535 inclusive.
E. 0 - 1023 inclusive.

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

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

46. 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. select version();
C. display version;
D. get version;
E. show version;

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

48. Some older TCP implementations are vulnerable to a DoS attack that exploits the small queue for connections in progress?
A. Predictable Initial Sequence Numbers
B. SYN flood.
C. SMURF Attack.
D. Teardrop Attack.
E. LAND Attack.

49. What is the function of the /etc/ftpusers file on a Unix FTP server?
A. It is not used for anything.
B. It lists IP addresses that users can connect to the FTP server from.
C. It lists the users that are permitted to use the FTP server.
D. It lists the users that are NOT permitted to use the FTP server.
E. It selects the authentication mechanism for the FTP server.

50. In active directory, what does FSMO (pronounced "Fizz-Mo") stand for?
A. Fixed Single Master Operations
B. Flexible Security Master Operations
C. Flexible Single Master Operations
D. Forest Single Master Operations
E. Forest Security Master Operations

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

52. During a penetration test, you gain access to a database containing personal details of staff. What is the best course of action?
A. Publish the information in a case study.
B. Change the database settings to address the vulnerability.
C. Drop the database so hackers cannot access this data.
D. Note the issue but do not store any of the personal data on your system.
E. Take a copy of the database so you can use it in your report.

53. When should the scope of work be defined?
A. After testing is completed, but before the report is written.
B. As soon as possible after testing is started.
C. During testing, based on the results from the port scan.
D. Before testing is started.
E. The scoping is optional, and may be omitted if the client agrees.

54. Which of these techniques is commonly implemented in modern C compilers to prevent buffer overflow exploitation?
A. Loop unrolling
B. Register optimisation
C. Canary values
D. Stack alignment
E. Inline functions

55. Which of the following encryption algorithms is an asymmetric cipher?
A. DES
B. 3DES
C. AES
D. RSA
E. RC5

56. What are the valid key lengths for the AES encryption cipher?
A. 128 and 256
B. 56, 112 and 168
C. 64, 128 and 256
D. 128, 192 and 256
E. 128, 160 and 256

57. Which are the six base SIP methods?
A. REGISTER, UNREGISTER, ACK, NAK, HELLO, BYE
B. REGISTER, ASSOCIATE, DISASSOCIATE, CANCEL, BYE, OPTIONS
C. REGISTER, INVITE, ACK, HELLO, BYE, OPTIONS
D. REGISTER, INVITE, ACK, CANCEL, BYE, OPTIONS
E. GET, POST, HEAD, OPTIONS, TRACE, CONNECT

58. Which scan would be most likely to discover a firewall that blocks all traffic to itself from the interface connected to the network you are scanning from?
A. UDP port scan
B. Ping sweep
C. ARP scan
D. SNMP query
E. TCP port scan

59. You find a system that is offering the NFS RPC service. What is the logical next step?
A. Report it as a vulnerability.
B. Try to find a buffer overflow vulnerability in the NFS service.
C. Leave it and move on because there are no known vulnerabilities in NFS.
D. Run "showmount -e" to list the NFS exports.
E. Try to mount an exported filesystem.

60. What is this: password 7 052D131D33556C081D021200
A. A password encoded with Unix crypt
B. A password encoded with unsalted DES
C. A password encoded with salted MD5
D. A password encoded with the reversible Cisco vigenere algorithm
E. A password with the literal value "052D131D33556C081D021200"

61. What identifies the superuser on a Unix or Linux system?
A. Any user with UID 65535 in the password file.
B. Anyone who logs on at the system console.

C. Any user that belongs to the "root" group in the group file.
D. The user with the username "root" in the password file.
E. Any user with UID 0 (zero) in the password file.

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

63. The UK Government protective marking levels are, from lowest to highest protection:
A. TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED.
B. CONFIDENTIAL, SECRET, TOP SECRET.
C. NPM, RESTRICTED, PROTECT, CONFIDENTIAL, SECRET, TOP SECRET.
D. NPM, PROTECT, RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET.
E. CLASSIFIED, INTERNAL USE ONLY, SECRET, TOP SECRET.

64. What are the SIP and RTP protocols used for in VoIP?
A. SIP and RTP are competing protocols that are both used for setting up and tearing down calls.
B. SIP is used for setting up and closing down calls, and RTP 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. RTP is used for setting up and closing down calls, and SIP is used for audio data transmission.
E. SIP and RTP are competing protocols that are both used for audio data transmission.

65. What is the primary legal reason for obtaining written permission before starting a test?
A. Because otherwise the penetration test might breach the Human Rights Act.
B. Because otherwise the penetration test might breach the Data Protection Act.
C. Because otherwise the penetration test might breach the Computer Misuse Act.
D. There are no legal reasons, only commercial reasons.
E. Because otherwise the client might not pay for the work.

66. Which of the following statements about the time protocols "time", "daytime" and "NTP" are correct?
A. "time" represents the time as a 32-bit value, "daytime" uses a 64-bit value, and "NTP" uses an ASCII string.
B. "time" represents the time as a 64-bit value, "daytime" uses an ASCII string, and "NTP" uses a 32-bit value.
C. "time" represents the time as a 32-bit value, "daytime" uses an ASCII string, and "NTP" uses a 64-bit value.
D. "time" represents the time as an ASCII string, "daytime" uses a 32-bit value, and "NTP" uses a 64-bit value.
E. "time" represents the time as an ASCII string, "daytime" uses a 64-bit value, and "NTP" uses a 32-bit value.

67. Which of these is not a valid IP address?
A. 192.168.300.1
B. 10.0.0.1
C. 172.16.3.7
D. 195.32.67.14
E. 192.168.0.1

68. What command would you use to list the installed patches on a Solaris system?
A. patchlist or pkglist
B. cat /etc/patchlist
C. pkginfo
D. pkg_info
E. showrev -a or showrev -p

69. On a Unix system, what is the effect of the execute bit on a directory?
A. It allows all files in the directory to be executed.
B. It allows the directory to be executed.
C. It allows the directory to be traversed.
D. It depends on the version of Unix that is being used.
E. It has no effect.

70. What is this: 17:58:01.396446 CDPv2, ttl: 180s, Device-ID 'chestnut.nta-monitor.com', length 404
A. A NetBIOS over TCP/IP session service broadcast
B. A NetBIOS over TCP/IP name service broadcast
C. A CDP broadcast
D. An ARP broadcast
E. A Spanning Tree Protocol broadcast

71. What are the four mandatory transform attributes for an IKE Phase-1 SA?
A. Protocol ID, Transform ID, IPsec Mode, Authentication Algorithm
B. Encryption Algorithm, Hash Algorithm, Authentication Method, Diffie Hellman Group
C. SA Lifetime, Hash Algorithm, Authentication Method, PRF
D. Encryption Algorithm, Key Length, Authentication Method, SA Lifetime
E. SA Lifetime, Key length, PRF, Field Size

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

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

74. 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. Run a shell on the webserver and connect its control channel back to a TCP port on your local system.
B. It is not possible to obtain shell access in these circumstances.
C. Run a shell on the webserver with its control channel listening on a high TCP port.
D. Run a shell on the webserver with its control channel listening on TCP port 81.
E. Run a shell on the webserver with its control channel listening on TCP port 80.

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

76. Which protocol and port does a normal DNS lookup use?
A. UDP port 43
B. TCP port 45
C. TCP port 43
D. UDP port 53
E. TCP port 53

77. Which of the following web application technologies would you expect to be most secure?
A. A PHP4 application
B. A pure Java application.
C. A Perl application running under MOD-Perl
D. A Perl application running as CGI scripts.
E. A PHP3 application

78. Which nmap command performs a half-open or "SYN" TCP portscan?
A. nmap -n -P0 -v -sN -p1-1024 hostname
B. nmap -n -P0 -v -sF -p1-1024 hostname
C. nmap -n -P0 -v -sS -p1-1024 hostname
D. nmap -n -P0 -v -sA -p1-1024 hostname
E. nmap -n -P0 -v -sT -p1-1024 hostname

79. Which command will perform a DNS zone transfer of the domain "company.com" from the nameserver at 10.0.0.1?
A. dig @10.0.0.1 company.com zone-transfer
B. dig @10.0.0.1 company.com.zone
C. dig @10.0.0.1 company.com ls
D. dig @10.0.0.1 company.com any
E. dig @10.0.0.1 company.com axfr

80. What is this: 17:57:57.850175 802.1d config 8064.00:0c:85:f1:3f:80.8010 root 8064.00:0b:46:48:29:80 pathcost 19 age 1 max 20 hello 2 fdelay 15
A. A Spanning Tree Protocol broadcast
B. A NetBIOS over TCP/IP name service broadcast
C. A NetBIOS over TCP/IP session service broadcast
D. An ARP broadcast
E. A CDP broadcast

81. Which of these is not an ICMP message type?
A. Host unreachable
B. Router Solicitation

C. Echo request
D. Echo reply
E. Source Quench

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

83. The DNS entries for www.customer.com and www.example.com both point to the same IP address. How does the web server know which domain is being requested by the browser?
A. It inspects the cookies sent by the client.
B. It uses the HTTP Host: header.
C. Both websites must have the same content.
D. It inspects the client's SSL certificate.
E. It uses a reverse DNS lookup of the client's IP address.

84. If an attacker gained access to a Microsoft SQL server using the "sa" account, which stored procedure would he use to add a user account?
A. xp_adduser
B. xp_commandshell
C. xp_cmdshell
D. sp_cmdshell
E. sp_commandshell

85. Which of these is an Ethernet multicast MAC address?
A. 01:00:0c:cc:cc:cc
B. 00-10-db-74-d0-52
C. 000b.dbb2.fa60
D. 00:10:db:74:d0:52
E. 00:10:DB:74:D0:52

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

87. Which of these methods is the best way to determine if a remote host is running an X Window server that allows remote connections from the local host?
A. Check to see if UDP port 177 is open
B. Run "xdpyinfo -display remotehost:0.0"
C. Check to see if TCP port 6000 is open
D. Check to see if TCP port 6001 is open
E. Run "xterm -display remotehost:0.0"

88. What is the default password for the SYS user on Oracle 10g?
A. DBSNMP
B. There is no default
C. SYSADM
D. CHANGE_ON_INSTALL
E. MANAGER

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

90. AJAX is
A. Asynchronous Javascript and XML
B. Automatic Java and XML
C. Apache Javascript and XML
D. A household cleaner
E. A Dutch football team