Program: BE Information Technology Engineering

Curriculum Scheme: Revised 2012

Examination: Third Year Semester VI

Course Code: TEITC603 and Course Name: SYSTEM AND WEB SECURITY

Time: 1hour Max. Marks: 50

==========

==========

Note to the students:- All the Questions are compulsory and carry equal marks .

Q1.	Which of the following is often one of the most overlooked areas of security?
Option A:	Operational
Option B:	Technical
Option C:	Internet
Option D:	Physical
Q2.	Which area of security usually receives the least amount of attention during a penetration test?
Option A:	Operational
Option B:	Technical
Option C:	Internet
Option D:	Physical
Q3.	Which of the following attacks can be perpetrated by a hacker against an organization with weak physical security controls?
Option A:	Denial of service
Option B:	Radio frequency jamming
Option C:	Hardware keylogger
Option D:	Banner grabbing
Q4.	Which of the following is an example of a physical security breach?
Option A:	Capturing a credit card number from a web server application
Option B:	Hacking a SQL server in order to locate a credit card number
Option C:	Stealing a laptop to acquire credit card numbers
Option D:	Sniffing a credit card number from packets sent on a wireless hotspot
Q5.	What does LKM stand for?
Option A:	Linux Kernel Module
Option B:	Linux Kernel Mode
Option C:	Linked Kernel Module

Option D:	Last Kernel Mode
Q6.	Of the following, which are common commercial Linux distributions?
Option A:	SUSE, Knark, and Red Hat
Option B:	SUSE, Adore, Debian, and Mandrake
Option C:	SUSE, Debian, and Red Hat
Option D:	SUSE, Adore, and Red Hat
Q7.	What type of attack can be disguised as an LKM?
Option A:	DoS
Option B:	Trojan
Option C:	Spam virus
Option D:	Rootkit
Q8.	Which of the following is a feature of Kerberos?
Option A:	It does not require time synchronization
Option B:	It uses tickets
Option C:	It provides centralized authentication for remote access servers
Option D:	It uses SAML for SSO
Q9.	What are characteristics of Network based IDS?
Option A:	Encryption
Option B:	Hash They look for attack signatures in network traffic
Option C:	Decryption
Option D:	Snorting
Q10.	Firewalls are often categorized as:
Option A:	Network Firewalls
Option B:	Either Network firewalls or Host based firewalls
Option C:	Host Based Firewalls
Option D:	Hardware Firewalls
Q11.	A firewall is a network security system _____based that controls incoming and outgoing network traffic based on a set of rules:
Option A:	Hardware
Option B:	Software
Option C:	Hardware Software
Option D:	Network
Q12.	A firewall is a _____security system:
Option A:	File
Option B:	Network
Option C:	Program
Option D:	Hardware Software

Q13.	What is a reverse WWW shell?
Option A:	A web server making a reverse connection to a firewall
Option B:	A web client making a connection to a hacker through the firewall
Option C:	A web server connecting to a web client through the firewall
Option D:	A hacker connecting to a web server through a firewall
Q14.	Which of the following is a tool used to modify an attack script to bypass an IDS's signature detection?
Option A:	ADMutate
Option B:	Script mutate
Option C:	Snort
Option D:	Specter
Q15.	Which of the following is a system designed to attract and identify hackers?
Option A:	Honeypot
Option B:	Firewall
Option C:	Honeytrap
Option D:	IDS
Q16.	Which of the following is a honeypot-detection tool?
Option A:	Honeyd
Option B:	Specter
Option C:	KFSensor
Option D:	Sobek
Q17.	Which of the following is a reason to use Linux?
Option A:	Linux has no security holes.
Option B:	Linux is always up to date on security patches.
Option C:	No rootkits can infect a Linux system.
Option D:	Linux is flexible and can be modified.
Q18.	Which of the following is not a way to harden Linux?
Option A:	Physically secure the system.
Option B:	Maintain a current patch level.
Option C:	Change the default passwords.
Option D:	Install all available services.
Q19.	Why is it important to use a known good distribution of Linux?
Option A:	Source files can become corrupt if not downloaded properly.
Option B:	Only certain distributions can be patched.
Option C:	Source files can be modified, and a Trojan or backdoor may be included in the source binaries of some less-known or free distributions of Linux.
Option D:	Only some versions of Linux are available to the public.

Q20.	Which of the following tools bypasses a firewall by sending one byte at a time in the IP header?
Option A:	Honeyd
Option B:	Nessus
Option C:	Covert_TCP
Option D:	007 shell