M.Sc. (I.T.) Sem. III

ETHICAL HACKING

QUESTION BANK (2014 – 2015)

Unit 1: Introduction to Ethical Hacking	
1.	Explain the following terms with respect to Ethical Hacking a) Hack Value b) Exploit c) Vulnerability d) Target Evaluation e) Zero day attack f) Daisy Chaining
2.	Explain in detail the elements/principles of information security.
3.	Explain the security, functionality and usability triangle
4.	What are the different attack vectors through which the attacker can attack information system? Explain.
5.	Discuss the motives, goal and objectives of information security attack.
6.	Classify the categories of information security threat. Explain each category in detail
7.	What is information warfare? What are its type? Explain.
8.	Discuss the different IPV6 security threats
9.	What is hacking? What is ethical hacking? What are the effects of hacking on business?
10.	Who is an Hacker? What motivates the hacker? Discuss the different classes of hacker
11.	Compare hacking and ethical hacking. What are the effects of hacking on business?
12.	What is Hactivism? Explain.
13.	Enumerate different phases of hacking? Explain each in detail.
14.	What are the different types of attack on a system? Explain each in detail.
15.	Why is ethical hacking necessary? Explain the scope and limitation of ethical hacking
16.	What are the skills that an ethical hacker should possess?
17.	What is defence in depth? Explain.
18.	What is incident management? What is the purpose of incident management process?
19.	What is information security policies? What are its goal?
20.	Classify the information security policies. Explain the structure and contents of security policies.
21.	Explain the different types of security policies.
22.	What are the steps to create and implement security policies? Explain with example.
23.	What is vulnerability research? Why does the administrator need it?
24.	What is penetration testing? Explain. Why is it required?
25.	Explain the penetration testing methodology.
Unit 1: Footprinting and Reconnaissance	
26.	What is footprinting? Explain the following terminologies: a) Open source or passive information gathering b) Anonymous footprinting c) Organizational or private footprinting d) Active information gathering e) Pseudonymous footprinting f) Internet foorprinting
27.	Why do attacker need footprinting? What are the objectives of footprinting?

28.	What are the different types of threats due to footprinting? Explain.
29.	Enumerate the different methodology used for footprinting. Explain the footprinting through search engine.
30.	Explain website footprinting.
31.	Explain email footprinting.
32.	What is competitive intelligence? What are the sources of competitive intelligence? What type of information can be gathered using it?
33.	Explain footprinting using google.
34.	How "Whois" can be used for footprinting?
35.	Explain DNS footprinting.
36.	Explain network footprinting.
37.	How is footprinting done through social engineering? Explain.
38.	How footprinting is done using social networking site?
39.	Explain any 5 footprinting tools.
40.	What countermeasures can be taken against footprinting?
41.	Explain footprinting pentesting.
Unit 1: Scanning Networks	
42.	What is network scanning? What are different types of scanning? What are objectives of network scanning?
43.	What is ICMP scanning? How is it carried out? What is ping sweep explain?
44.	Explain the TCP connection establishment and connection termination process.
45.	What are the different TCP communication flags? How can they may use to create custom packet?
46.	Compare IPV4 and IPV6 network scanning.
47.	Compare Nmap and Hping2/3.
48.	Enumerate different scaling techniques. Explain each.
49.	Explain TCP connect / full open scan.
50.	Explain XMS Scan, Null Scan and IDLE Scan. Also explain FIN Scan, ICMP EchoScan, UDP Scanning?
51.	Explain ACK flag scanning.
52.	What are the counter measures against the port scanning?
53.	Explain the scanning methodology in detail.
54.	What is banner grabbing? What are its types? Explain. What are the uses of banner grabbing?
55.	What are the counter measures against banner grabbing?
56.	What are the uses of hiding file extension from web pages?
57.	What is vulnerability scanning? What can it detect? What is the benefit of drawing network diagrams?
58.	What is a proxy server? How does it work? Why do attackers user proxy servers?
59.	How can proxy server be used for attacks? What is proxy chaining?
60.	What is HTTP tunnelling? Why do attackers need it?
61.	What is SSH tunnelling? How many machines are required for it? How is SSH tunnel created?
62.	What are anonymizers? Why are they used? What are different types of annonymizers?
63.	What is IP spoofing? What are the different techniques to detect IP spoofing? Explain.
64.	What are countermeasures against IP spoofing? Explain.
65.	Explain Scanning Pen Testing.
Unit 1: Enumeration	
66.	What is enumeration? What information can be enumerated by intruders? Explain the

	different enumeration techniques.
67.	Explain the different services with their port numbers to enumerate.
68.	What is NETBIOS? What is NetBIOS enumeration? Explain.
69.	How can systems be enumerated using default passwords? What is SNMP enumeration? Explain.
70.	Explain the different commands used for Unix/Linux enumeration.
71.	What is LDAP? What is LDAP enumeration? Explain.
72.	What is NTP enumeration? What are the commands used for NTP enumeration? Explain.
73.	What is SMTP enumeration? What are the commands used for NTP enumeration?
74.	What is DNS enumeration?? How is DNS zone transfer enumeration done using nslookup?
75.	What are the countermeasures against SNMP and DNS enumeration? Explain.
76.	What are the countermeasures against SMTP, LDAP and SMB enumeration? Explain.
77.	Explain the enumeration Pen Testing.
Unit 2: System Hacking	
78.	What are the pre-requisites for system hacking? What are the steps for hacking a system? Explain.
79.	What are the different techniques to crack passwords? Explain.
80.	What are the different types of password attacks? Explain.
81.	What is Rainbow attack? How is it carried out? Explain.
82.	What is a distributed network attack? What are its features? What are its two modules? Explain.
83.	Explain the different non-electronic attacks.
84.	Write and explain the automatic password cracking algorithm.
85.	How can password be stolen using USB drive? Explain.
86.	How are keyloggers used to steal passwords? Explain
87.	How does Microsoft authentication take place? Explain. How are hash passwords stored in Microsoft security accounts manager?
88.	What is LAN manager hash? How is LAN Manager hash generated?
89.	Explain the NTLM authentication process.
90.	Explain the Kerberos authentication process.
91.	What is salting? Explain.
92.	How can we defend against password cracking? Explain.
93.	What is privilege escalation? What are its types? Explain. How can system be protected against privilege escalation?
94.	What are the malicious programs that an attacker can execute on victim's machine? Explain in brief.
95.	What are keyloggers? What are different types of keyloggers? Explain.
96.	How do attackers use remote keyloggers? Explain.
97.	Explain acoustic and CAM keyloggers.
98.	What is spyware? How can it be propagated? What does it do?
99.	What are different types of spywares? Explain Desktop spyware.
100.	What are different types of spywares? Explain Email and Internet spyware.
101.	What are different types of spywares? Explain child monitoring spyware.
102.	What are different types of spywares? Explain screen capturing spyware.
103.	What are different types of spywares? Explain USB spyware and GPS spyware.
104.	What are different types of spywares? Explain audio and video spyware.
105.	What are different types of spywares? Explain print spyware and telephone/cellphone

	spyware.
106.	What are the countermeasures against different types of keyloggers?
107.	How can system be protected from spyware? Explain.
108.	What are rootkits? What are its objectives? How does an attacker place rootkit? What are different types of rootkits?
109.	How does rootkit work? Explain. How can the system be protected against rootkit?
110.	What are the different ways to detect rootkits? Enumerate the steps to detect rootkit.
111.	What is NTFS alternate data stream? How are NTFS streams created? How can system be protected against NTFS streams?
112.	What is steganography? How does it work?
113.	Explain the classification of steganography. (or Explain Technical and Linguistic steganography.)
114.	Explain the different steganography techniques.
115.	What are the applications of steganography? Explain.
116.	What are the different types of steganography?
117.	Explain the different issues in Information Hiding.
118.	What is steganalysis? What are its challenges?
119.	What are the different types of steganography attacks?
120.	How can image, text, audio and video steganography be detected? Explain.
121.	Why do attackers cover tracks? What are different ways to cover tracks?
122.	Explain password cracking pen testing.
123.	Explain privilege escalation pen testing and executing applications pen testing.
124.	Explain pen testing for detecting hidden files.
125.	How can pen testing be done to check whether we can cover the tracks of our activity?
Unit 2: Trojans and Backdoors.	
126.	What is a Trojan? What is the purpose of Trojans?
127.	What are the indications of a Trojan attack? What do Trojan creators look for?
128.	How can a system be infected using a Trojan?
129.	What are wrappers? Explain.
130.	What are the different ways a Trojan can get into a system? Explain.
131.	How are Trojans deployed? What are the different techniques used by Trojans to evade antivirus software?
132.	What are different types of Trojans? Explain each in brief.
133.	How can Trojans be detected? What are the countermeasures against Trojans and Backdoors?
134.	Explain the pen testing for Trojans and Backdoors.
Unit 2: Viruses and Worms.	
135.	What is a virus? What are the characteristics of virus? What are the stages in life cycle of a virus? Explain.
136.	Explain the Infection phase and Attack phase in working of viruses.
137.	What are the objectives behind creating viruses? What are the indications of a virus attack?
138.	What are the different ways in which computer gets infected with virus? What are the techniques used for infecting computers with viruses?
139.	What are the different types of viruses? Explain each in brief.
140.	What are computer worms? Why are they created? How do they differ from virus?
141.	What is Sheep Dip computer? What is antivirus system? Explain.
142.	Explain the procedure for Malware analysis.
143.	What are the different methods to detect computer viruses? What are the

	countermeasures against computer viruses?
144.	Explain the penetration testing for virus.
Unit 2: Sniffing	
145.	What is wiretapping? What are different types of wiretapping?
146.	What is packet sniffing? How is it done? What are the threats due to packet sniffing?
147.	How do sniffers work? Explain.
148.	What are different types of sniffing attacks? Explain each in brief.
149.	Explain the two types of sniffing. What protocols are vulnerable to sniffing?
150.	What is content addressable memory table? How does it work? What happens when Content addressable memory table is full? What is mac flooding?
151.	How can we defend against MAC attacks? Explain.
152.	What is DHCP starvation attack? What is rogue DHCP attack? How can we defend against these attacks?
153.	What is APR spoofing attack? How does ARP spoofing work?
154.	What is ARP poisoning? What are the threats due to ARP poisoning? How can we defend against ARP poisoning?
155.	Explain MAC spoofing and IRDP spoofing. How can we defend against them?
156.	What is DNS poisoning? What are the steps to launch DNS poisoning attacks? What are the types of DNS poisoning attacks? Explain.
157.	How can we protect against DNS spoofing? Explain.
158.	How can an attacker hack network using sniffers?
159.	What are the countermeasures against sniffing?
160.	What are the different ways to detect sniffing? Explain.
161.	Explain Sniffing pen testing.
Unit 3: Social Engineering	
162.	What is Social Engineering? What type of behaviours can be vulnerable to social engineering attacks?
163.	Why is social engineering effective? What are the factors that make companies vulnerable to social engineering attacks?
164.	What are the warning signs of social engineering attacks? What are the phases of social engineering attacks?
165.	Explain the impact of social engineering attack on an organization.
166.	Who are the common targets for social engineering attacks?
167.	Explain the different types of social engineering.
168.	Explain Human based social engineering in detail.
169.	Explain computer based social engineering in detail.
170.	Explain Mobile based computer engineering in detail.
171.	What are the reasons for insider attacks? How can these attacks be prevented?
172.	Discuss the common social engineering targets and defence strategies.
173.	Explain social engineering through impersonation on social networking sites.
174.	What are the risks of social networking to corporate networks? Explain.
175.	What is identity theft? What are the different ways to steal an identity?
176.	What are the ways to minimize the risk of identity theft?
177.	What are the countermeasures against social engineering?
178.	How can phishing emails be detected? Explain.
179.	What are the countermeasures against identity theft?
180.	Explain Social Engineering pen testing.
Unit 3: Denial of Service.	
181.	What is denial of service attack? What are distributed denial of service attacks? How do

	they work?
182.	Explain the different techniques of denial of service attacks. What are the symptoms of denial of service attacks?
183.	What are bandwidth attacks? What are service request floods?
184.	Explain SYN attack and SYN flooding.
185.	Explain ICMP flood attack.
186.	Explain phlashing, sabotage and bricking a system.
187.	What are application level flood attacks? Explain.
188.	Explain Organized Crime Syndicates. Explain their organizational chart.
189.	What is a botnet? What is the purpose of botnet? Explain the botnet propagation technique.
190.	Discuss the botnet ecosystem.
191.	What is activity profiling? Explain wavelet based signal analysis and sequential change point detection.
192.	What are the countermeasures against denial of service and distributed denial of service attacks?
193.	What are the techniques to defend against botnets? Explain.
194.	Explain denial of service penetration testing.
Unit 3: Session Hijacking.	
195.	What is session hijacking? What are the steps to hijack a session? What are the dangers posed by hijacking a session?
196.	Why is session hijacking successful? What are the key session hijacking techniques? Explain.
197.	How can brute force be used for session hijacking? What is referrer attack?
198.	Explain spoofing and hijacking attacks.
199.	Explain the session hijacking process.
200.	Explain active and passive session hijacking techniques.
201.	Explain network level and application level session hijacking.
202.	Explain Man-in-the-middle and man-in-the-browser attacks.
203.	What is cross site scripting attack? How is it done?
204.	What is session fixation? What are the techniques used for session fixation?
205.	What is TCP/IP hijacking? How is it performed?
206.	Explain RST hijacking, blind hijacking and UDP hijacking.
207.	What are the counter measures against session hijacking?
208.	Explain session hijacking pen testing.
Unit 3: Hacking Webservers.	
209.	What is website defacement? Why are webservers compromised? What are the consequences of webserver compromisation?
210.	What is the impact of webserver attacks?
211.	What are the effects of webserver misconfiguration? Explain with example.
212.	Explain directory traversal and web cache poisoning attacks.
213.	Explain HTTP response hijacking attack.
214.	Explain the different techniques to crack webserver passwords.
215.	What are the different ways of web application attacks? Explain.
216.	Explain the webserver attack methodology.
217.	What are the countermeasures against hacking webservers?
218.	How can we defend against HTTP response splitting and web cache poisoning?
219.	What are patches and hotfixes? What is patch management?
220.	Explain Webserver pen testing.

Unit 4: Hacking Web Applications	
221.	What is a web application? What are its components? Explain.
222.	Explain the architecture of web application. How does web application work? Explain.
223.	What is Web 2.0? What are the applications of Web 2.0? Explain.
224.	Explain the web application vulnerability stack.
225.	Give the examples of web attack vectors.
226.	Explain the different threats to web applications. Explain each in brief.
227.	Explain how input validation flaws make web applications vulnerable.
228.	With the help of an example, explain, parameter tampering attack.
229.	What is directory traversal attack? What can an attacker do with directory traversal?
230.	How security misconfiguration can make web applications vulnerable? Explain with examples.
231.	With respect to web applications, what are injection flaws? What are its different types? Explain.
232.	What is LDAP injection? How does it work? Explain.
233.	Explain the hidden field manipulation attack with example.
234.	What are cross site scripting attacks? Explain in detail.
235.	Explain cross site request forgery attack. How does it work?
236.	What is web application denial of service attack? Explain different web application denial of service attacks.
237.	What is cookie poisoning? How does it work?
238.	How session fixation helps attackers to hijack a valid user session? Explain.
239.	How does insufficient transport layer security and improper error handling make web applications vulnerable? Explain.
240.	How do unvalidated redirects and forwards make web applications vulnerable? Explain.
241.	Explain the various attacks that can be done at the various layers of web services stack.
242.	Explain the web services footprinting attack and web service XML poinsoning.
243.	Explain the Web App hacking methodology.
244.	How is footprinting of web infrastructure done? Explain.
245.	Explain the analysis to be carried out to identify attack surfaces that are exposed.
246.	What are the different types of attacks on authentication mechanisms of web applications? Explain.
247.	What are the different types of password attacks? Explain.
248.	Explain the different types of authorization attacks.
249.	Explain session management attack.
250.	What are different ways to attack data connectivity? Explain.
251.	What are the different ways to attack Web App clients?
252.	Explain the different types of attacks on Web services? Explain each.
253.	What is encoding scheme? What are different encoding schemes?
254.	What are the countermeasures against command injection flaws?
255.	How can web applications be defended against cross site scripting attacks?
256.	What are the countermeasures against denial of service attacks on web applications?
257.	What are the counter measures against web application attacks?
258.	Explain in detail, the web application pen testing.
Unit 4: SQL Injection	
259.	What is SQL injection? What are the major threats of SQL injection?
260.	What are the different types of attacks that can be launched with SQL injection?
261.	Explain the following SQL injection attacks with examples:

	a) Code analysis b) Attack Analysis c) Updating a table d) Adding new records e) Identifying table name f) Deleting the table
262.	What are the different ways to detect SQL injection? Explain.
263.	Explain the SQL injection black box pen testing.
264.	What are the different types of SQL injections? Explain.
265.	Explain simple and union SQL injection attacks.
266.	What is blind injection? Explain in detail with examples.
267.	Explain the SQL injection methodology.
268.	How can web site login be bypassed using SQL injection? Explain with example.
269.	How can database, table and column be enumerated using SQL injection? Explain.
270.	Explain password grabbing SQL server hashes grabbing using SQL injection.
271.	How can SQL injection be used for the following: a) Transfer database to attacker's machine. b) Interact with the operating system. c) Interact with the file system. d) Network reconnaissance.
272.	Explain the different types of signature evasion techniques.
273.	Explain sophisticated matches, hex encoding and manipulating white spaces evasion techniques.
274.	Explain in-line comment, char encoding and string concatenation evasion techniques.
275.	Why do attackers obfuscate codes? Explain with example.
276.	What are the countermeasures against SQL injection? Explain.
Unit 4: Hacking Wireless Networks	
277.	What is service set identifier? Explain. Explain the different authentication modes of Wi-Fi.
278.	Explain the Wi-Fi authentication process using centralised authentication server.
279.	What is Wi-Fi chalking? What are different ways of Wi-Fi chalking? What are different symbols used for it?
280.	What are the different wireless encryption algorithms?
281.	What is WEP encryption? How does it work? What are its goals? What are flaws in WEP encryption?
282.	What is WPA? How does it work? What are temporal keys?
283.	What is WPA2? How does it work?
284.	Compare WEP, WPA and WPA2.
285.	What are the issues with WEP?
286.	Enumerate the reasons that make initialization vectors weak.
287.	How can WEP encryption be broken?
288.	How can we defend against WPS cracking?
289.	What are the different wireless access control threats?
290.	How can integrity attacks be launched on wireless networks?
291.	What are the different confidentiality attacks that can be launched on wireless networks? Explain.
292.	What are the different availability attacks that can be launched on wireless networks? Explain.
293.	What are the different authentication attacks that can be launched on wireless networks?

	Explain.
294.	How is rogue access point attack done?
295.	Explain the following attacks on wireless networks: a) Client Mis-association. b) Mis-configured access point c) Unauthorized association d) Ad-hoc connection attack e) HoneySpot Access point f) Access point MAC spoofing
296.	Explain Jamming signal attack.
297.	Explain the wireless hacking methodology.
298.	What are the different ways of footprinting wireless networks? Explain.
299.	What is GPS mapping? How does and attacker use it?
300.	What do attackers gain by wireless traffic analysis?
301.	What is spectrum analysis? Explain.
302.	What is Aircrack-ng suite? What are the different programs it contains?
303.	How can the following attacks be launched using Aircrack-ng suite? a) Revealing hidden SSID b) Fragmentation attack c) MAC spoofing attack d) De-authentication and disassociation e) Man in the middle attack
304.	Explain wireless ARP poisoning attack.
305.	What is Evil Twin? Explain.
306.	What is Bluetooth hacking? Explain the different Bluetooth device attacks?
307.	What are the different threats to Bluetooth devices?
308.	How to bluejack a victim? Explain.
309.	What are the countermeasures against Bluetooth hacking?
310.	How can rogue access point be detected and blocked? Explain.
311.	Explain the different wireless security layers.
312.	What are the countermeasures against wireless attacks?
313.	What are wireless intrusion prevention systems? How are they deployed?
314.	What is wireless penetration testing? What is its purpose?
315.	Explain the wireless penetration testing framework.
316.	Explain pen testing of LEAP encrypted wireless LAN.
317.	Explain pen testing of WPA/WPA2 encrypted WLAN.
318.	Explain pen testing of WEP encrypted WLAN.
319.	Explain pen testing unencrypted WLAN.
Unit 4: Hacking Mobile Platform	
320.	i. Explain the following terminologies related to hacking mobile platforms: Stock ROM, CyanogenMod, Bricking the Mobile Device, Bring your own Device. ii. Explain the different mobile attack vectors.
321.	What are the different mobile platform vulnerabilities and risks? Explain each in brief.
322.	Discuss the security issues arising from App Stores. What are the threats of mobile malware?
323.	What are the issues with App Sandboxing? Explain.
324.	What are the features of Android OS? Explain the architecture of Android OS.
325.	What is Android Device Administration API? What are the policies it supports?

326.	What is rooting? What is its use? What are the risks associated with rooting?
327.	How can Android devices be secured?
328.	What is iOS? Explain core framework of iOS.
329.	Explain jailbreaking with respect to iOS. What are its types? What are jailbreaking techniques?
330.	How can the devices using iOS be secured?
331.	Enumerate the features of Windows Phone 8.
332.	Explain Windows phone secure boot process.
333.	How can Windows OS devices be secured? Explain.
334.	What is Blackberry OS? What are the features of Blackberry devices? Explain the Blackberry Enterprise solution architecture.
335.	Explain the blackberry attack vectors. Explain each in brief.
336.	What are the different ways in which attacker can exploit SMS on Blackberry devices?
337.	How can Blackberry devices be secured?
338.	What is mobile device management? Explain the logical architecture of mobile device management.
339.	Enumerate the general security guidelines for Mobile devices.
340.	List the guidelines for mobile device security for administrators.
341.	Explain Android phone pen testing.
342.	Explain iPhone pen testing.
343.	Explain Windows phone pen testing.
344.	Explain Blackberry phone pen testing.
Unit 5: Invading IDS, Firewalls and Honeypots	
345.	What is intrusion detection system? How does it work?
346.	What are the different ways to detect intrusion?
347.	What are the different types of intrusion detection systems?
348.	What are the general indications of intrusions?
349.	What is a firewall? How does it work? Explain the architecture of firewall.
350.	What are demilitarized zones?
351.	What are different types of firewalls? Explain in detail.
352.	Explain packet filtering firewall.
353.	Explain circuit-level gateway firewall.
354.	Explain application-level firewall.
355.	Explain stateful multilayer firewall.
356.	Explain the following techniques of firewall identification: a) Port scanning b) Banner grabbing c) Firewalking
357.	What is Honeypot? How does it work? What are different types of Honeypots?
358.	How is Honeypot setup?
359.	What is insertion attack?
360.	What types of denial of service attacks can be launched against intrusion detection systems? Explain.
361.	What is obfuscation? How can it be used to evade intrusion detection systems?
362.	What is false positive generation attack against intrusion detection systems?
363.	What is session splicing? What is its use in attacking intrusion detection systems?
364.	Explain Unicode evasion technique to evade intrusion detection systems.
365.	Explain in detail fragmentation attacks on intrusion detection systems.
366.	Explain in detail time-to-live attacks on intrusion detection systems.

367.	How can RST and URG packets be used to attack intrusion detection systems?
368.	What are polymorphic and ASCII shellcodes? How can they be used to bypass intrusion detection systems?
369.	Explain application layer attacks on intrusion detection systems.
370.	Explain Desynchronization – Pre connection SYN and Post connection SYN attacks on intrusion detection systems.
371.	How can firewalls be evaded using IP address spoofing?
372.	How source routing can be used to evade firewall restrictions?
373.	What are tiny fragments? How can attacker use them to bypass firewall restrictions?
374.	What are the different techniques to bypass blocked sites? Explain.
375.	What are the different ways to bypass firewalls? Explain.
376.	How are Honeypots detected? Explain.
377.	What are the countermeasures that provide protection against intrusion detection systems, Honeypots and firewalls?
378.	Explain firewall penetration testing.
379.	Explain intrusion detection system penetration testing.
Unit 5: Buffer Overflows	
380.	What is buffer overflow? Explain with example.
381.	Why are programs and applications vulnerable to buffer overflows?
382.	Explain the stack segment and stack based buffer overflows.
383.	Explain the different stack operations.
384.	What is heap? Explain heap based buffer overflow.
385.	What are No Operations? How do attackers use NOP?
386.	What knowledge is required to program buffer overflows? What are the steps to create buffer overflows?
387.	How do attackers attack real programs for buffer overflows and segmentation fault?
388.	What is format string problem? How buffer overflow is caused using format string?
389.	What is stack smashing? What happens once the stack is smashed?
390.	Explain simple buffer overflow in C.
391.	How can buffer overflow exploit be mutated? Explain.
392.	How can we identify and detect buffer overflows?
393.	What are the defences against buffer overflows? How can buffer overflows be prevented?
394.	What are programming countermeasures against buffer overflows?
395.	What is data execution prevention? Explain.
396.	Explain in detail, the buffer overflow pen testing.
Unit 5: Cryptography	
397.	What is cryptography? Why is it used? What are the objectives of cryptography? Explain the cryptography process.
398.	What are the different types of cryptography? Explain.
399.	Write a short note on government access to keys.
400.	What are ciphers? How are they classified?
401.	Explain data encryption standard and advanced encryption standard.
402.	Explain in brief about RC4, RC5 and RC6 algorithms.
403.	Explain digital signature algorithm and related signature schemes.
404.	Explain Rivest Shamir Adleman algorithm with example..
405.	Explain the RSA signature scheme.
406.	What are message digest functions? Explain MD5.How can MD5 be brute forced?

407.	Explain secure hashing algorithm. Compare SHA0, SHA1 and SHA2 functions.
408.	What are digital signatures? How do they work?
409.	What is secured shell? What are its features? What does it protect against?
410.	What is public key infrastructure? Explain in detail.
411.	Who are certifying authorities? List three certifying authorities with the types of certificates they provide.
412.	What is secured sockets layer? What is session identifier? Explain the SSL handshake protocol flow.
413.	Explain transport layer security in detail.
414.	What is disk encryption? What is its use?
415.	What are cryptographic attacks? What are its different categories?
416.	What are the different code breaking techniques? Explain.
417.	Explain Man-in-the-middle attack on digital signature schemes.
Unit 5: Penetration Testing	
418.	What is security assessment? What are the categories of security assessment? Explain each category.
419.	What is vulnerability assessment? What are its limitations?
420.	What is penetration testing? Why is it required?
421.	Compare security audit, vulnerability assessment and penetration testing.
422.	What makes a good penetration test? Explain.
423.	What are the penetration testing points and locations? Explain.
424.	Explain internal and external penetration testing.
425.	Explain black box, grey box and white box penetration testing.
426.	Explain announced, unannounced, automated and manual penetration testing.
427.	Explain the common penetration testing techniques.
428.	How can DNS domain names, IP address information and enumerating information about hosts on publicly available networks be used for penetration testing?
429.	Explain the phases of penetration techniques.
430.	Explain in detail the pre attack phase of penetration testing.
431.	Explain in detail the attack phase of penetration testing.
432.	Explain in detail the post attack phase of penetration testing.
433.	Explain the pen testing methodology.
434.	What is application security assessment? Explain.
435.	Explain the Web application testing
436.	What is network security assessment?
437.	Explain wireless assessment and testing.
438.	Explain penetration testing of network filtering devices.
439.	How is denial of service simulated?
440.	Write a short note on outsourcing penetration testing.
441.	Explain the penetration testing service level agreements.