Muhammad Izham Bin Norhamadi
B032020039

No: Date:

Part A

a) 1- SQL injection
2- Cross-Site scripting
3- Broken access control
4- Remote command execution

b) 1- White hat hacker
2- Black hat hacker
3- Script Kiddies
4- State-sponsored hacker

c) i. An attack that exploits computer application vulnerabilities before the software developer releases a patch for the vulnerability

ii- Hackers that get away with database theft usually complete their task, then backtrack to cover their tracks

iii. A defined way to breach the security of an IT system through vulnerability

iv. Existence of a weakness, design or implementation error that can lead to an unexpected and undesirable event compromising the security of the system

No: B032020039

Date:

Law	Ethics
Interpreted by courts	Interpreted by each individual
Applicable to everyone	Personal choice
Geared toward preventing unlawful conduct	Geard toward achieving responsible conduct
Those who break the law will be punished	Those who go against ethics will be socially isolated

une

1- Communications and Multimedia Act 1998
2- Computer Crimes Act 1997
3- Copyright Act (Amendment) 1997
4- Digital Signature Act 1997

Shift right 10 key

THEQ UIET ERYO UBEC OMET HEMO REYO
UARE ABLE TOHEAR

The Quieter You Become The More You Are
Able To Hear

1) Scanning
2) Gaining access
3) Privilege escalation
4) Maintaining access
5) Covering Tracks

Muhammad Izham Bin Norhamadi
B032020039

No: .... Date: ....

h) 1) Passive online attack
2) Active online attack
3) Offline attack

i) 1) Gaining access
2) Privilege escalation
3) Covering tracks

j) i. Internal Penetration test
- comes after external pentest to identify what could be accomplished by an attacker in internal network

Advantage - simulate an attack where an attacker can access internal network

Disadvantage - expensive to attack running systems

ii. External Penetration test
- testing vulnerabilities to review the chances of being attacked by remote attacker.

Advantage - simulate a true cyber attack from outsider
Disadvantages - time consuming

Muhammad Izham Bin Norhamadi
B032020039

No: Date:

Part B

Question 1

a) i. use physical media and leaves a malware infected cd or usb drive in a location sure to be found

ii. a form of social engineering to manipulate people into giving attacker what they want by making up a story to gain your trust

iii. a form of social engineering where a hacker promises a good service in exchange for information that can be used to steal money, data, or account

b) i. 192.168.254.172

ii. TCP half-open - because it sends packets with SYN flag set and waits for SYN-ACK from target and does not complete connection

iii. Open : Port 445, Port 80
Close : Port 25, Port 110

iv. - HTTP service
- Microsoft-ds service

v. - Turn on exploit mitigation on Microsoft Endpoint Protection
- Get latest security update from Microsoft

c) 1- SMB Client Infinite Loop
2- MySQL Getname Buffer Overflow
3- FTP Server PASS Overflow

Muhammad Izham Bin Norhamadi
B032020039

No: .... Date ....

Question 2

a) - misconfigured HTTP headers
- insecure default configuration
- unnecessary HTTP methods
- verbose error messages

b) - website defacement
- information theft
- XSRF attack
- malicious script injection

c) - XSS attack
- Directory traversal attack

d) i) Session hijacking attack
ii) Session hijacking attack
iii) Reverse engineering
iv) Web Parameter tampering

e) i. Directory traversal
ii. Segregate documents and sanitize filename parameter

Muhammad Izham Bin Norhamadi
B032020039

No: .... Date: ....

Question 3

a) 1- Security audits
2- Vulnerability assessment
3- Penetration testing

b) - determine most likely attack
- find exploitable weaknesses
- assess vulnerability risks

c) - Network security
- System software security
- Client-side security
- Server-side security

d) - Passive scanning
- Active scanning

e) 1- Set wireless interface to monitor mode
2- Start airodump-ng to collect authentication handshake
3- Use aireplay-ng to deauthenticate wireless client
4- Run aircrack-ng to crack pre-shared key

f) - Properly configure all authorized access points
- Turn on SSID protection
- Change default password
- Restrict access to authorized user