## Muhammad Izham Bin Norhamed: B032020039

	8032020059
	No: Date.
	Part A
	Carried Brown Ca
a)	1- SQL injection
	2- Cracs-Site scripting
	3- Broken acces control
	4- Remote command execution
(ط	1- White hat hadeer
	2- Block hat hacker
	3- Script Kiddies
	4- State-sponsored backer
	i. An attack that exploits computer application vulnerabilities before
	ii- Hackers that get away with database theft usually complete their task, then backtack to cover their tracks
	their tack, then backtack to cover their tracks
	iii. A defined way to breach the security of an IT eystem through vulnerability
	(Mood)
	iv. Existence of a weakness, design or implementation error that
	iv. Existence of a weakness, design or implementation error the
	can lead to an unexpected and undesirable event
	iv. Existence of a weakness, design or implementation error the can lead to an unexpected and undestrable event compromising the security of the system
	can lead to an unexpected and undesirable event
	can lead to an unexpected and undesirable event
	can lead to an unexpected and undesirable event
	can lead to an unexpected and undesirable event
	can lead to an unexpected and undesirable event

Law	Ethics	
Interpreted by courts	Interpreted by each individual	ď,
Applicable to everyone	Personal choice	
Genred toward preventing	Geard toward achieving	
unlawful conduct	responsible conduct	
Those who break the law	Those who go against	and the second s
will be punished	ethics will be socially	1 (18)
	isolated	
	esile 4 gains	-
	Andrew Sharp - 16/5 - 4	une
1- Communications and Multime	edia Act 1998	

2- Computer Crimes Act 1997 3- Copyright Act (Amendment) 1997 4- Digital Signature Act 1997

Shift right 10 key

UIET ERYO UBEC THEQ OMET HEMO REYO ABLE TOHEAR UARE

The Quieter You Become The More You Are Hear Able To

- 1) Sconning
- 2) Gaining occass
- 3) Privilege escalation
- Meintaining 41
- 5) Covering Fracks

CS CamScanner

## Muhammad Izham Bin Norhamadi B032020039

	No:
	A Prof.
h)	1) Passive online attack
	2) Active online attack
	3) Offline affacle.
V .	The state of the s
$\langle i \rangle$	1) Gaining access
	2) Privilege escalation
	2) Privilege escalation 3) Covering tracks
	The state of the s
ا (ز	i. Internal Penetration test
	- comes after external pentest to identify what could
	- comes after external pentest to identify what could be accomplished by an attacker in internal network
o i	and of all the statements of the statements of the statement of the statem
	Advantage - simulate on attack where an attacker can access internel
	network
	Disadvantage - expensive to attack running systems
4 = 1 1	of the there is have to move a converted to
	Sin I a like the
	ii. External Penetration test
	- testing vulnurabilities to review the chances of being attacked
	by remote attacker.
	Advantage - simulate a true cyber attack from outsider
	Advantage - simulate à line consumina
	Disadvantages - time consuming
	Franks & Halas & as nothing day to have an and the
- V	The state of the s
The state of the state of the state of	
	XIa (
	The same was the same of the s

**CS** CamScanner

	103707003d
	No:
Note that for the part of the selection in the particular	Part B
	in the minimum to the second of the second o
	Question 1
a)	i- use physical media and leaves a malware infected cd or usb drive in a location sure to be found
homelock and production for the second of the second of the second of	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
	to gain your trust
	and the second of the second o
	isi. a form of social engineering where a hacker promises a good service in exchange for information that can be used to
	a good serice in exchange for information that can be used to
1.01.0957	steal money, data, or account
	100700000
(d	1. 192.168.254.172
	ii. TCP half-open - because it sends packets with SYN flag
	set and waits for SYN-ACK from terget and does
	not complete connection
	production of the second of th
6	iii. Open: Port 445, Port 80 Close: Port 25, Port 110
-	Close: Port 25, Port 110
	News and the same and the state of the same and the same
	iv HTTP service
	- Microsoft-ds service
	M. Of Elland Protection
	v Turn on exploit mitigation on Microsoft Endpoint Protection
	- Get latest security update from Microsoft
c)	1- SMB Client Infinite Loop
and the same of th	2- MySOL Getnome Buffer Overflow 3- FTP Server PASS Overflow
	3- FIP SOUR FASS CVATION

STANDARD

	Not manage and an arrange and a second and a	Date
And the state of t		
	Question 2	
a)	- misconfigured HTTP headers	
and the state of t	- insecure default configuration	
The same is the signature.	- unnecessary HTTP methods	
	- verbose error necesages	
(ط	- website defocement	
	- information theft	
	- XSRF attock	
	- malicious script injection	14 12
	V (	
()	- XSS attack	
upper land to the second section of the	- Directory traversal attack	
4)	i) Session hijocking attack	
Total Technique	ii) Session hijacking attack	
0.1	(iii) Reverse engineering	
	iv) Web Parameter tampering	especial material residents and country and the enterprise the property of the enterprise and the enterprise and
6		
e)	i. Directory traversal	
	i. Directory traversal ii. Segregate documents and sonitice	filename parameter
	The second secon	
and the second s	The state of the s	
and the second s		mendenten en 'mende i lan og det i likilarings vid variante folk semen fler om en to sig mend sin et la men
and the second second second second second		

## Muhammod Leham Bin Norhamadi 18032020391

	No: Date:
	Quation 3
and distinction of the state of	
(۵	1- Security audits
	2- Vulnerability assessment
	3- Penetration testing
6	- determine most likely attack
	- find exploitable weaknesses
	- assess unlnerability risks
c)	
	- System software security
tion of the state	- Client-side security
	- Server-cide security
13	
7)	- (agave stand)
	- Active sconning
e)	1- Set winless interface to monitor mode
0)	2- Start airodump-ng to collect authentication handshake
and the second s	3- Use a, replay-ng to deanthent: cate wireless client
	4- Run aircrack-ng to crack pre-shared key
and the second s	
()	- Properly configure all authorized access points
	- Turn on SSID protection
	- Change default password - Restrict access to authorized user
	- Restrict access to authorized user