Date:	
Sun Mon Tue Wed Thu Fri Sat	
Activity #5	
Information Security	
Information Security	
212-5614	
2/C-36/9	
Tunes The time of malware involved in it	
19th of 110000	
is the backdoor In backdoor	
the include is able to bypass the tradition	
Security system and can access the	
system.	
Evades	
High priveleges: Operate with elevated	
access to bypass security	11
Concealment: Hide unouthorized access	
points and actions	
Exploitation: Use system vulnerabilities	
to avoid detection	. 4
Modification: Alter system files to prevent being spotted by	
prevent being spotted by	
security tools	
	4
Recommended Security Measures,	
-) Conduct regular security assessments to idealify vulnerabilities and suspicion activities.	-
to identify vulnerabilities and suspicion	
activities.	
	-

	Date,
1	Sun Mon Tue Wed Thu Fri Sat
TB	> Implement kernel protection
79	-> Implement kernel protection -> Aware staff about phishing attacks.
	3. 17 000000 12.0000
<b>*</b>	(2) In heatPoverflow attacks the data is
	writerile al librate correspting the
0	written beyond buffer limits, corrupting the adjacent memory Attackers can after
9	action memory tructors can auch
0	pointers/ control overflow to run malicious
7	l'etrain blode i roup setting and in will.
-	Consequences
-	Heap overflow attacks can lead to
9	unauthorized access allowing attackers.
9	to gain control of the system and
-9	data corruption, causing system crashes or
-	data corruption, causing system crashes or
	unpredictable behavious Additionally
	affackers may exploit this vulnerability
	for privilege Jescalation, gaining higher
-	levels of access within the sixtem
-	Preventions Rivers 100
-	-) Input Validation
	-) lie functions like etrocky to limit
-	Copying.
4	-) Detect heap overflow
-3	- 9 dentify issues early in development
	the state of the s
	a territorio de la terr
-	
-	
-	
-	

Sun Mon Tue Wed Thu Fri Sat	-
(3) Common Techniques for SQL injection	
Tantology - Based Attacks: Injecting a toutology into a query to by-pass authorize	
into a guery to be one	rations
chocks!	all G
-> Union-Based, Using Union-SELECT. As combine results from multiple quesies and entract date from tables	6
occupit of the state of the combine	
gram muliple quesier and entract dat	a
	1
3 Blind SQL Injection, Where attackers deduce	9
information based on the application's responses	0
to crafted queries even without seeing direct	0
output.	
Security Measures:	0
	-
-> Deploye While a Only A: P. 1001	0
> Deploy Web application Firewalls. > Limit Database permissions > Employ Amed most live to	0
Employ ist	
SQL statements that encapsulate	
SCE statements	0
- > Use prepared statements with bound	9
-> Use prepared statements with bound parameters to seperate SQL code from data	5
	9
(4) Data Inference and Encryption:	•
전화 (1984) : 1984 - 1985	-
These attacks occur when attackers analyses	3
multiple publicly available datasets to deduce	-9
sensitive information and a identify a divided	-
multiple publicly grailable datasets to deduce sensitive information, such as identifying individuals	1
	3

M	:
-	Sun Mon Tue Wed Thu Fri Sat
<b>M</b>	This can result in risks like identity disclosure,
-	Teputational damage, and lead reporturious To provet
-	Teputational damage, and legal repercussions. To prevent such breaches, data encryption techniques like data-at-rest and det dayla-in-Iransit encryption. are esseptial, while homomorphic encryption enables computation on encrypted dayla. Howover querying encrypted data presents aboltoned in the little encrypted dayla.
<b>*</b>	data-at-rest and de dayla is transfer
<u> </u>	are essential milite homes d'in la mayonon.
	Computation on encryption enables
	encrupted data provide de la
	performance may lead to the things including
	limitations in the time of the sure of the sures and
*	hindring dade will like apabilities, potentially
	encrypted data presents challenges, including performance overhead, complexity in queries and limitations in analytic capabilities, potentially hindering data usability.
4	
4	
*	
*	
-	1
1	
4	
della .	
-	
4	
9	
<b>A</b>	