University of Mumbai

Examination 2020 under cluster 4 (PCE)

Program: BE Computer Engineering

Curriculum Scheme: Rev 2012

Examination: Final Year Semester VIII

Course Code: CPE8034 and Course Name: DF

Time: 1 hour Max. Marks: 50

Q=QUESTION	question_description	question_type
A=ANSWER	answer_description	answer_isright
Q1	**_____ has now evolved to be one of the most popular automated tools for unethical hacking.**	M
A	Automated apps	0
A	Database software	0
A	Malware	1
A	Worms	0
Q2	**The first step in applying the scientific method to a digital investigation is to**	M
A	Form a theory on what may have occurred	0
A	Experiment or test the available evidence to confirm or refute your prediction	0
A	Make one or more observations based on events that occurred	1
A	Form a conclusion based on the results of your findings	0
Q3	**What is the ethics behind training how to hack a system?**	M
A	To think like hackers and know how to defend such attacks	1
A	To hack a system without the permission	0
A	To hack a network that is vulnerable	0
A	To corrupt software or service using malware	0
Q4	**Following is considered as one of the ethics in digital forensics.**	M
A	Maintaining privary of evidences	1
A	Sharing evidences with all who are interested to see it.	0
A	Modifying the data based on investigation tools available	0
A	Allow all investigators to see the findings in the investigation case	0
Q5	**What is the first phase of hacking?**	M
A	Attack	0

A	Maintaining access	0
A	Reconnaissance	1
A	Scanning	0
Q6	**Which type of forensics is used to find evidences from laptops, computer and storage media?**	M
A	Mobile forensics	0
A	Network forensics	0
A	Computer forensics	1
A	Memory forensics	0
Q7	**What is not digital Evidence from following?**	M
A	Video and sound files	0
A	E-mail	0
A	Activity logs	0
A	Fignerprints	1
Q8	**Cryptographic checksum can be recorded using**	M
A	md6sum	0
A	mdsum	0
A	addsum	0
A	md5sum	1
Q9	**Which is not the variations of live response**	M
A	Initial live response	0
A	Pre-initial live response	1
A	In-depth response	0
A	Full live response	0
Q10	**_____includes reviewing all the data collected during investigation**	M
A	Forensic analysis	1
A	Forensic checking	0
A	Error Finding	0
A	Review	0
Q11	**Which command is used to display current running process**	M
A	psloogedon	0
A	plist	0
A	ps	1
A	pslog	0
Q12	**Which of the following is not a part of CSIRT team:**	M

A	Security analysts	0
A	Lead investigator	0
A	Information Lead	1
A	HR/legal representation	0
Q13	**Tool for capturing, filtering, and analyzing traffic is _____**	M
A	Routers	0
A	TCP	0
A	NIDS/NIPS	0
A	Tcpdump	1
Q14	**Digital forensics is all of them except**	M
A	Extraction of computer data	0
A	Preservation of computer data	0
A	Interpretation of computer data	0
A	Manipulation of computer data	1
Q15	**Most widely used command for listing open ports on unix system is**	M
A	Netstat	1
A	w-command	0
A	ls command	0
A	ps command	0
Q16	**Which of this Nmap do not check?**	M
A	Services different hosts are offering	0
A	On what OS they are running	0
A	What kind of firewall is in use	0
A	What type of antivirus is in use	1
Q17	**The intent of a _____ is to overkill the targeted server's bandwidth and other resources of the t**	M
A	Phishing attack	0
A	DoS attack	1
A	Website attack	0
A	MiTM attack	0
Q18	**Which of the following is not a sniffing tool?**	M
A	Wireshark	0
A	Dude Sniffer	0
A	Maltego	1
A	Look@LAN	0

Q19	**What are the different ways to classify an IDS?**	M
A	Zone based	0
A	Host & Network based	1
A	Network & Zone based	0
A	Level based	0
Q20	**When does a criminal investigation usually begin?**	M
A	When someone finds evidence of or witnesses a crime	0
A	When witness or victim makes an allegation to the police	1
A	When criminal informs to organisation about crime	0
A	When all proofs are collected against criminal	0
Q21	**Why is it important to hide your identity when conducting an online investigation?**	M
A	To reduce the risk of alerting the offender	1
A	To get yourself in the mindset of covert web investigating	0
A	To make it easier for you to determine the offender's location	0
A	To Search the Web using distinctive aspects	0
Q22	**What port number does HTTPS use?**	M
A	80	0
A	23	0
A	25	0
A	443	1
Q23	**What are the three types of scanning?**	M
A	Port, network, and vulnerability	1
A	Port, network, and services	0
A	Grey, black, and white hat	0
A	Server, client, and network	0
Q24	**Which term describe Organizing report correctly**	M
A	macro to micro	1
A	micro to micro	0
A	micro to macro	0
A	macro to macro	0
Q25	**which is not a goal of report writting in digital forensic**	M
A	Accuretely describe report	0
A	Understandable to decision making	0
A	Voilating legal scrutiny	1

A	Offer a valid conclusion	0