

ASSIGNMENT-1 QUESTIONS

Q.No		Question	Course Outcome	BTL
1	a	Some of the most common types of penetration tests are external, which is usually done off-site against an external network, internal where the assessment is conducted from within the target network, web application tests which objective is to find security vulnerabilities in web-based applications through both manual and automated tests, social engineering which tries to exploit to weak link in most organisation i.e. its employees, through phishing, vishing, tailgating, physical testing, media drops etc. What types of penetration testing assessments are there?	CO1	Analyze
	b	What are the phases in the penetration testing lifecycle?	CO1	Understand
2	A *	Briefly explain about working of ARP and mention the 2 types of attacks involved in ARP with the help of a neat diagram.	CO1	Remember
	b	Define sniffing. Explain in detail about the types of sniffing.	CO1	Evaluate
3	A *	Methodologies are not rigid and should not be applied to a penetration test in a rigid manner. It is often necessary to expand on any process beyond documented best practices; penetration testing is no exception. Explain in detail among the OSSTMM and the NIST, which methodology is the best?	CO1	Analyze
	B *	Discuss in detail about OWASP and justify how we use OWASP for all “application penetration tests” we do here at the RHA InfoSEC.	CO1	Understand
4	A *	When the scope of the penetration test is defined, the category/type of the penetration test engagement is also defined along with it. The entire penetration test can be Black Box, White Box, or Gray Box depending upon what the organization wants to test and how it wants the security paradigm to be tested. Explain in detail about the categories of penetration tests.	CO1	Analyze

	B *	Explain in detail about types of penetration tests	CO1	Remember
5	a	Write short notes on categories of hackers.	CO1	Understand
	b	There are several types of penetration tests performed, Explain in detail about the types of penetration tests and which type of penetration test can be used for testing a network environment for potential security vulnerabilities and threats.	CO1	Apply