NARSIMHA REDDY ENGINEERING COLLEGE
An Autonomous Institution| Affiliated to JNTUH | Approved by AICTE
Accredited by NBA & NAAC with 'A' Grade

## WORK SHEET

# UNIT – 5

## Multiple Choice Questions (MCQs)

1. Client-side exploits primarily target:
   a) Servers
   b) Browsers
   c) Switches
   d) Routers
2. ActiveX was mainly associated with:
   a) Chrome
   b) Firefox
   c) Internet Explorer
   d) Safari
3. DEP stands for:
   a) Data Execution Prevention
   b) Dynamic Execution Process
   c) Data Encryption Policy
   d) Device Execution Platform
4. Heap Spraying targets:
   a) Stack Memory
   b) Heap Memory
   c) ROM
   d) Cache
5. Which browser security feature isolates content?
   a) Sandboxing
   b) Routing
   c) Switching
   d) Bridging
6. A zero-day vulnerability is:
   a) Fully Patched
   b) Publicly Known and Fixed
   c) Unknown and Unpatched
   d) Disabled
7. Malware Analysis helps understand:
   a) Malware Behavior
   b) Network Cabling
   c) Switching
   d) Routing
8. A Honeynet is:
   a) Antivirus
   b) Firewall
   c) Network of Honeypots
   d) IDS

9. Dynamic Malware Analysis involves:
   a) Reading Documentation
   b) Executing Malware in Isolation
   c) Encrypting Files
   d) Network Design
10. Spyware is designed to:
   a) Encrypt Files
   b) Collect Information Secretly
   c) Backup Data
   d) Compress Data

## Fill in the Blanks

1. Client-side exploits commonly target web _____.
2. ActiveX controls were heavily used in _____Explorer.
3. Heap spraying utilizes the _____region of memory.
4. Browser _____helps isolate web content.
5. Zero-day vulnerabilities have no available _____.
6. Malware stands for malicious _____.
7. Honeypots are designed to attract _____.
8. Static analysis examines malware without _____ it.
9. Dynamic analysis observes malware _____.
10. Ransomware typically _____files and demands payment.