**List of Experiments**

Subject: Information Security (CE348) (6th Sem)

|  |  |  |
| --- | --- | --- |
| **Exp.**  **No** | **Name of Experiment** | **Hours** |
| 1 | Apply attacks for cryptanalysis to decrypt the original message from a given cipher text using Play fair cipher.  Key = charusat |  |
| 2 | Implement RSA algorithm.  Reference :[**RSA**](https://www.youtube.com/watch?v=VF3AHG0T9ec) |  |
| 3 | Demonstrate DNS based phishing attack. |  |
| 4. | The transmission of information need to be secure over the communication channel and the data has to be confidential. Study and implement the practical approach for Steganography.  -Using DOS commands  -Using OpenPuff Tool | 02 |
| 5. | In computers, Footprinting is the process of accumulating data regarding a specific network environment, usually for the purpose of finding ways to intrude into the environment. Footprinting can reveal system vulnerabilities and improve the ease with which they can be exploited. Study practical approach to implement Footprinting: Gathering Target Information making use of following tools: Dmitry – Deepmagic  Reference : <https://www.youtube.com/watch?v=_zd3goGLM7Q> UA Tester  Reference : <https://www.youtube.com/watch?v=WsTupi32ZYE> Whatweb  Reference : <https://www.youtube.com/watch?v=Fx9sIgxcNwU> | 02 |
| 6. | Port scanning involves connecting with TCP and UDP ports on a system, once you have found the IP addresses of a target organization by Footprinting technique. You have to map the network of this organization. Nmap is a network mapper and a power full, flexible, freely available and easy to use tool. It is available for both Linux and Windows based operating system. Study practical approach to implement Scanning and Enumeration Techniques using Nmap.  Reference :[**Demo**](https://www.youtube.com/watch?v=fp1042XK4A8) | 02 |

|  |  |  |
| --- | --- | --- |
|  | [**S-DES**](https://www.youtube.com/watch?v=QcKHfMgcnbw) |  |
| 6. | System hacking is the way hackers get access to individual computers on a network. Ethical hackers learn system hacking to detect, prevent, and counter these types of attacks. Study practical approach to implement System Hacking and learn different ways to crack password.  Reference:  [**Demo**](https://www.youtube.com/watch?v=Jaq7w4iqInY) | 02 |
| 8. | Attacking Web Application: SQL injection and Cross Site Scripting Attack  Reference:  [**Demo**](https://www.youtube.com/watch?v=6GJi86Q_pK8) | 04 |
| 9. | Practical approach to study Wireshark. Reference:  [**Wireshark**](https://www.youtube.com/watch?v=yC0e0bSSleo) | 02 |
| 10. | Write a program to generate Digital Signature. Reference:  [**Code**](https://docs.oracle.com/javase/tutorial/security/apisign/gensig.html) | 02 |
| 11. | Case study on security. | 04 |

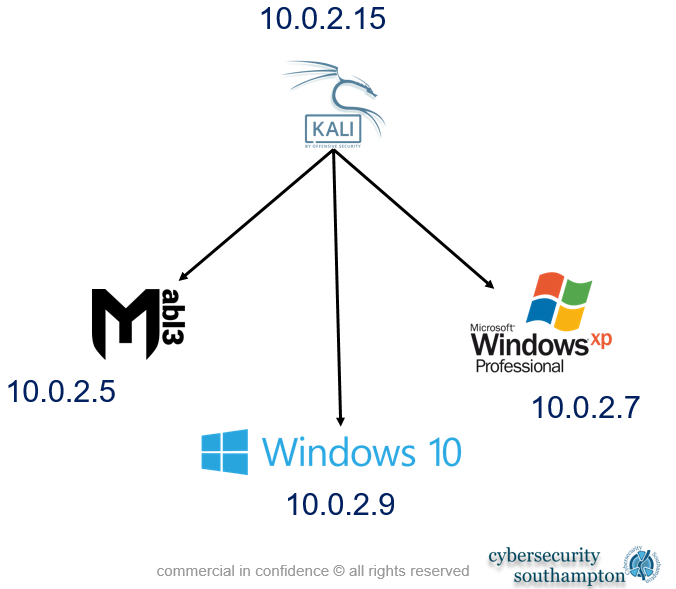
**Name of Faculty:**

1. Martin Parmar

2. Sneha Padhiar

**1. Practical Scenario with Lab Set up**

Study and implement penetration testing and ethical hacking with the **Metasploit** framework. Set up a simple virtual lab based on Virtual Box with a Kali Linux Virtual Machine (VM) acting as attacker, and a Metasploitable Linux VM, a Windows XP SP3 and a Windows 10 VM as victims to target.



**2.** Study and implement Nmap to scan network and discover not only everything connected to it, but also a wide variety of information about what's connected, what services each host is operating, and so on. It allows a large number of scanning techniques, such as UDP, TCP connect (), TCP SYN (half-open), and FTP. It also offers a wide variety of scan types, including Proxy (bounce attack), Reverse-ident, ICMP (ping sweep), FIN, ACK sweep, Xmas, SYN sweep, IP Protocol, and Null scan. See the man page's Scan Techniques section for more details.

**Lab set up:**

