INSE 6190 Wireless Network Security

Security of WLAN

Submitted to:

Professor Dr. Ayda Basyouni

Submitted By:

Student Name	Student ID
Raghu Pavan Annam	40303699
Hariharan Duraisingh	40303001
Vaishnavi Kalathur	40292270

Team Member Contributions:

Student Name	Contribution
Vaishnavi Kalathur (De auth& password recovery)	Executed a deauthentication attack and password recovery on a personal WLAN network. First, monitor mode was enabled using airmon-ng and verified with ifconfig. Using airodump-ng, nearby Wi-Fi networks were scanned, and the target network named “Vaishnavi” was identified along with key details such as BSSID and channel. Then, aireplay-ng was used to send deauthentication packets, triggering a WPA handshake. The captured handshake packets were stored in a WPA folder. For password recovery, the air-crack-ng command was used with a wordlist, successfully retrieving the Wi-Fi password and completing the attack recovery cycle.
Hariharan Duraisingh (DNS Spoofing through MITM)	Configured a DNS spoofing environment using dnsspoof to redirect victim traffic to a locally hosted fake website. Virtual hosts were created in Apache for domains like google.com, serving cloned login pages. Resolved default site issues by properly setting ServerName and DocumentRoot. Verified spoofed DNS responses and successful redirection. Demonstrated how ARP and DNS spoofing can facilitate phishing attacks within local networks.
Raghu Pavan Annam (Creating fake access point)	Responsible for setting up a fake access point using Kali Linux. Monitor mode was enabled with airmon-ng and conflicting services were disabled. Essential tools like dnsmasq for DHCP/DNS and hostapd for simulating the access point were configured. The dnsmasq.conf file was edited to assign IPs (10.0.0.10–10.0.0.250) and route traffic via 10.0.0.1. Using airbase-ng, the rogue AP was launched, routing was configured by assigning a static IP to at0, IP forwarding was enabled, and iptables was used for NAT. A custom fakehosts.conf enabled DNS spoofing, allowing client activity to be logged within a controlled lab environment for analysis.