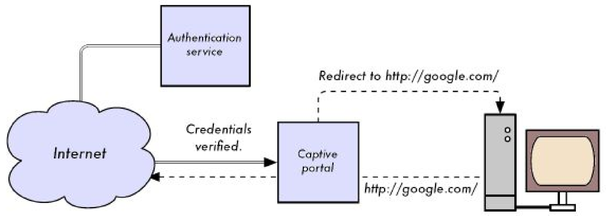
SECURITY ANALYSIS OF A CAPTIVE PORTAL

Omkar Parkhe, Nida Safia Syed, Sri Sai Bhargav Tiruveedhula

Takeaway:

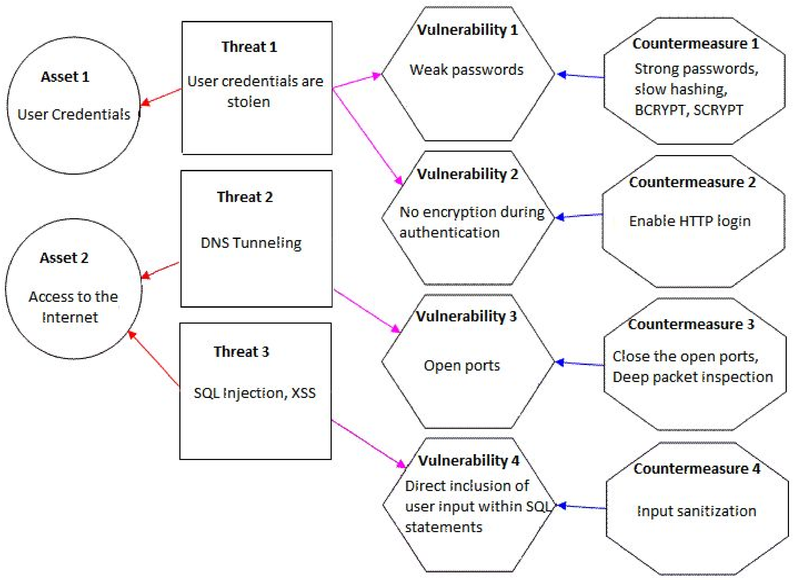
1. Never use captive portals with default settings/configuration.
2. Close all the unecessary ports.
3. Perform input sanitization.
4. Use strong passwords/passphrases.

INTRODUCTION



Captive portals serve the purpose of authenticating users who log into public Wi-Fi networks. They are commonly used to present a landing or log-in page which may require authentication, payment, or the acceptance of policies, that both the host and user agree to adhere by.

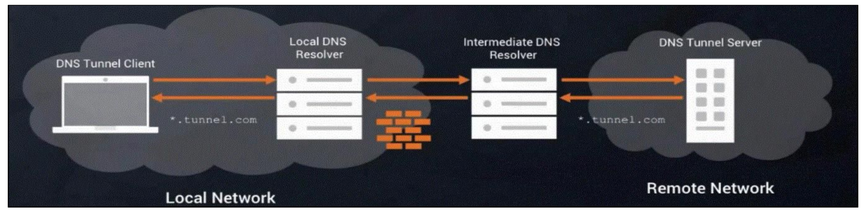
THREAT MODEL



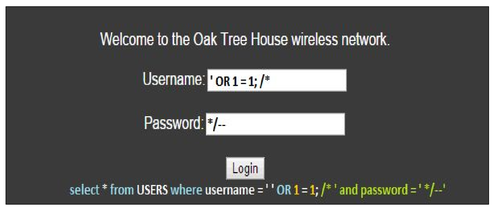
POSSIBLE ATTACKS

1. **Password Guessing:** Malicious users can recover passwords of authenticated users by performing dictionary attacks.

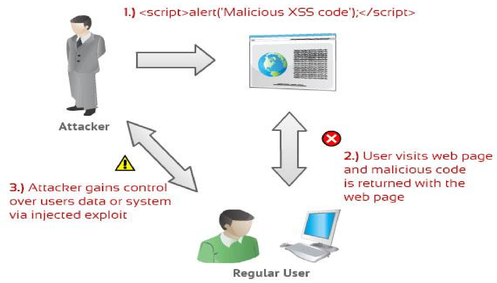
2. **DNS Tunneling Attack:** An adversary can bypass the captive portal by encoding TCP data in DNS queries and responses.



3. **SQL Injection**: Malicious users can inject nefarious SQL statements into the portal's entry field(s) which will unknowingly run on the authentication database.



4. **XSS**: Cross-Site Scripting attacks are a type of injection, in which malicious scripts are injected into the trusted captive portal.



5. **MAC Spoofing:** An attacker can sniff the network traffic and spoof MAC and IP addresses of authenticated users to gain unauthorized access to the network.

RESULTS

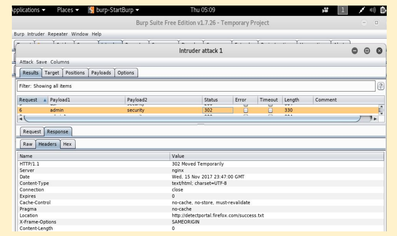
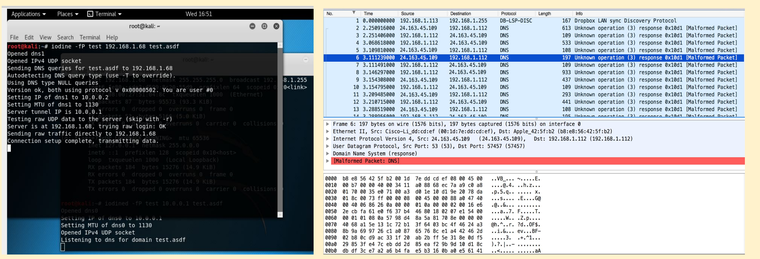


Figure 1.Successful Password Guessing using Burp Suite



Figures 2&3. Successful DNS Tunneling using Iodine Server

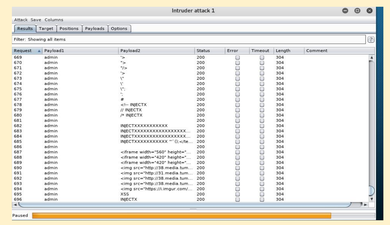


Figure 4. Cross-Site Scripting on the Captive Portal

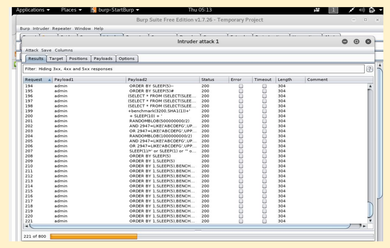


Figure 5. SQL Injection on the Captive Portal

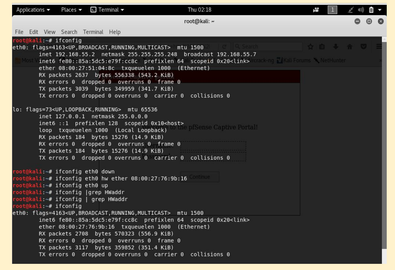


Figure 6: MAC Spoofing