

Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

Student:

Andre Hardy

Email:

ahardy754@email.porterchester.edu

Time on Task:

5 hours, 14 minutes

Progress:

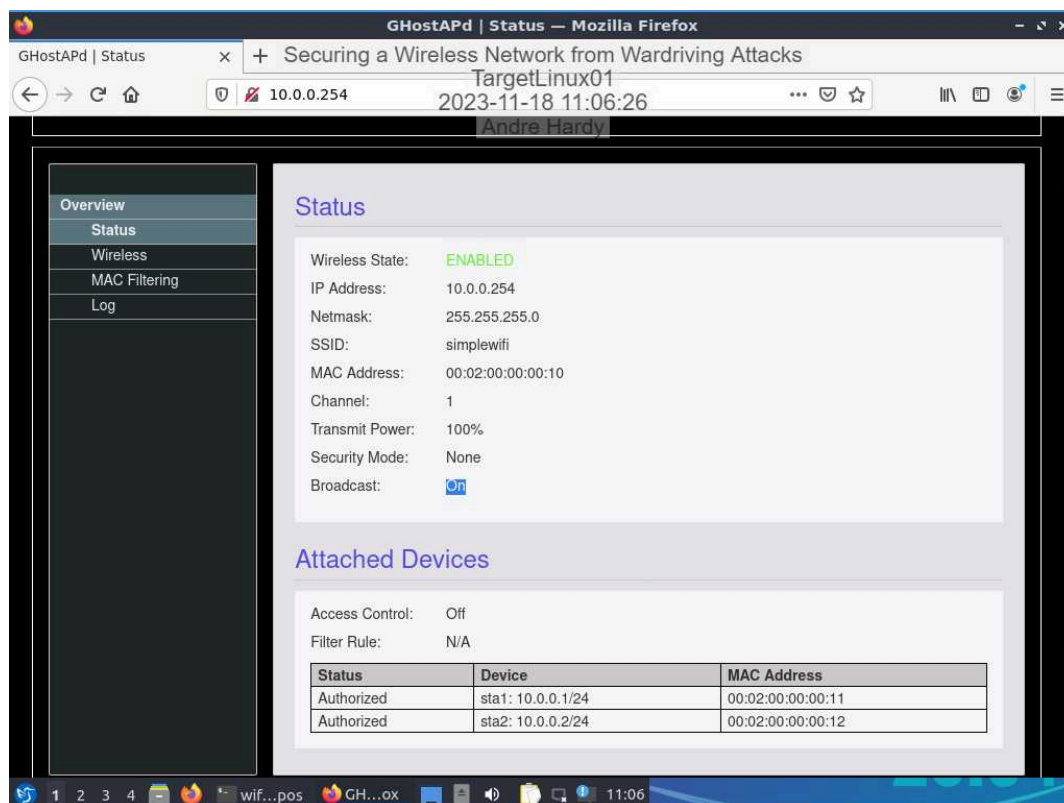
100%

Report Generated: Saturday, November 18, 2023 at 3:24 PM

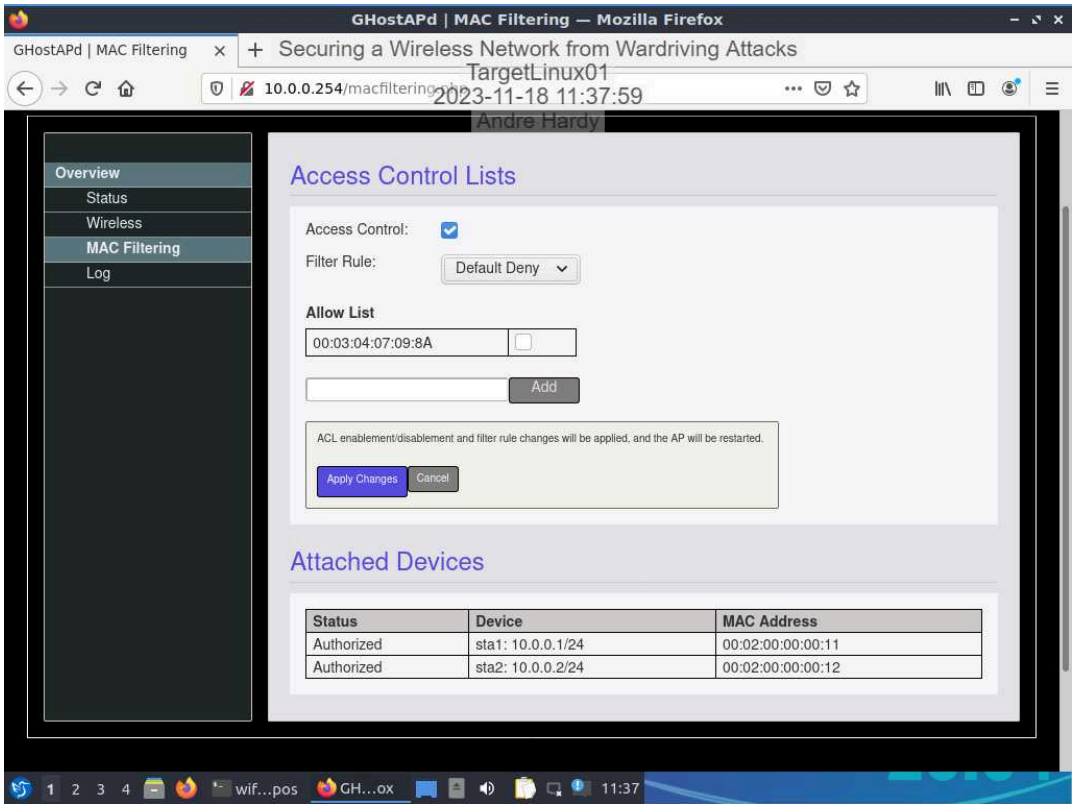
Section 1: Hands-On Demonstration

Part 1: Review a Wi-Fi Access Point Configuration

13. **Make a screen capture** showing the **wireless networking configuration** in GHostAPd **Status** screen.



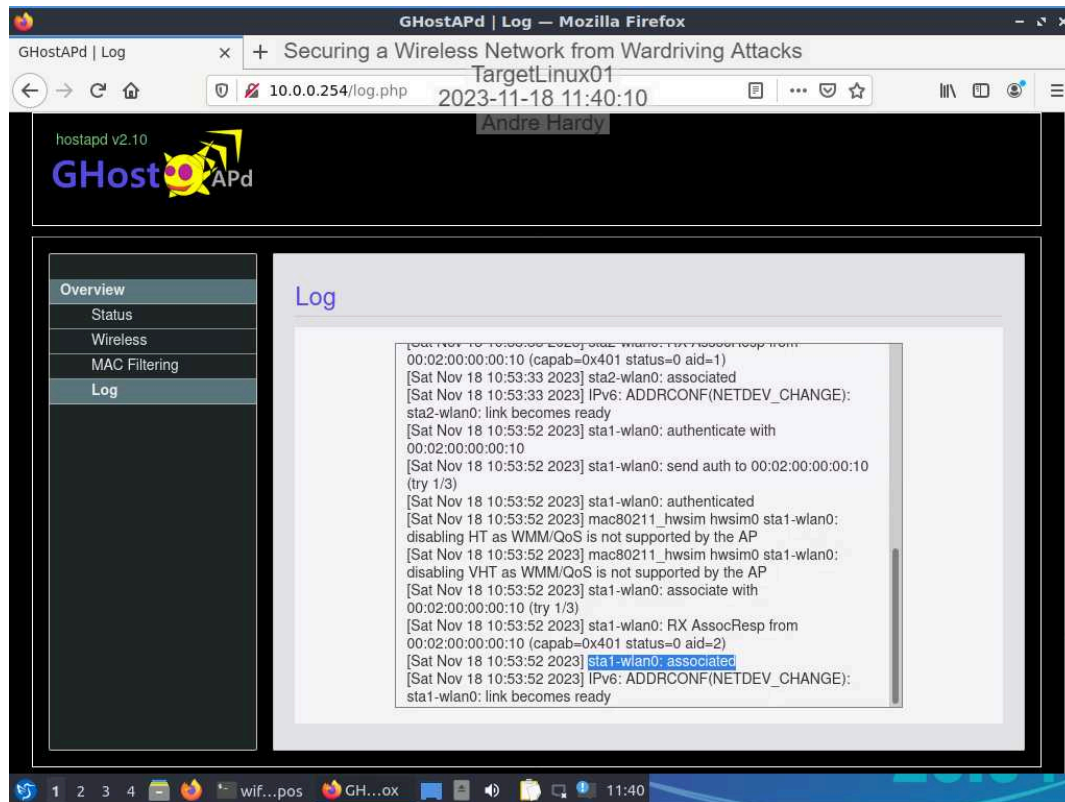
17. Make a screen capture showing the **Allow List** in the **Access Control Lists** section of GHostAPd.



Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

20. Make a screen capture showing the **log** line corresponding to **sta1**'s association with **ap1** in the GHostAPd Log view.

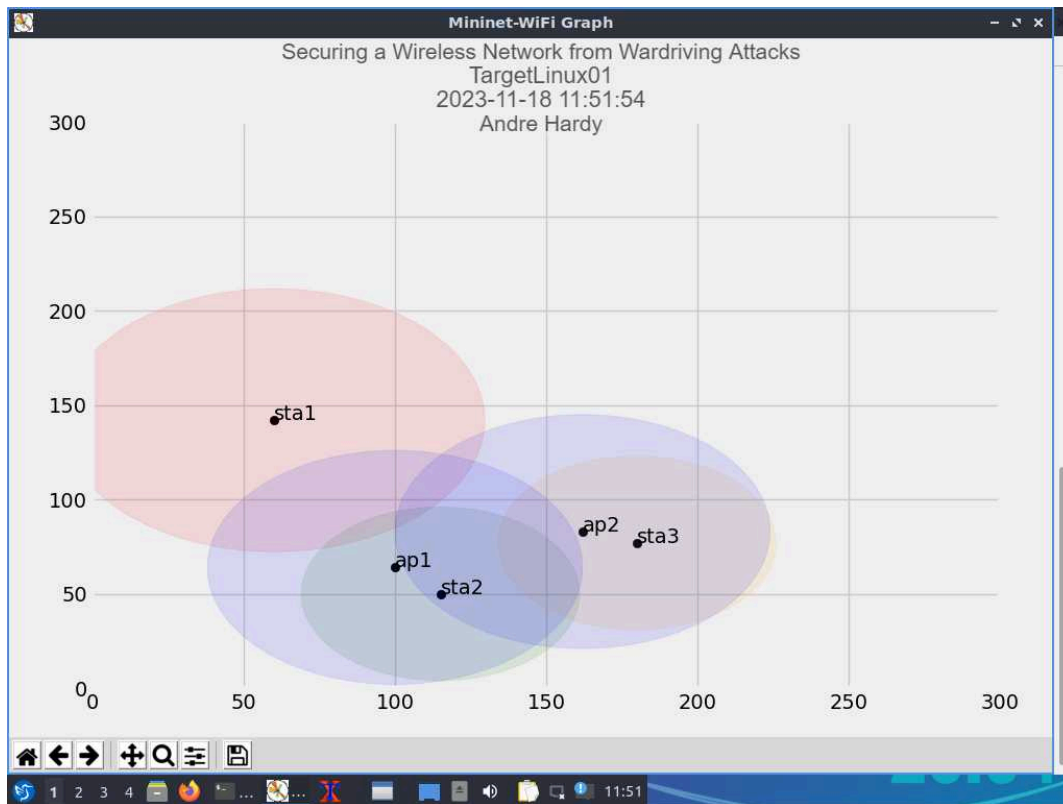


Part 2: Perform a Wardriving Attack with LinSSID

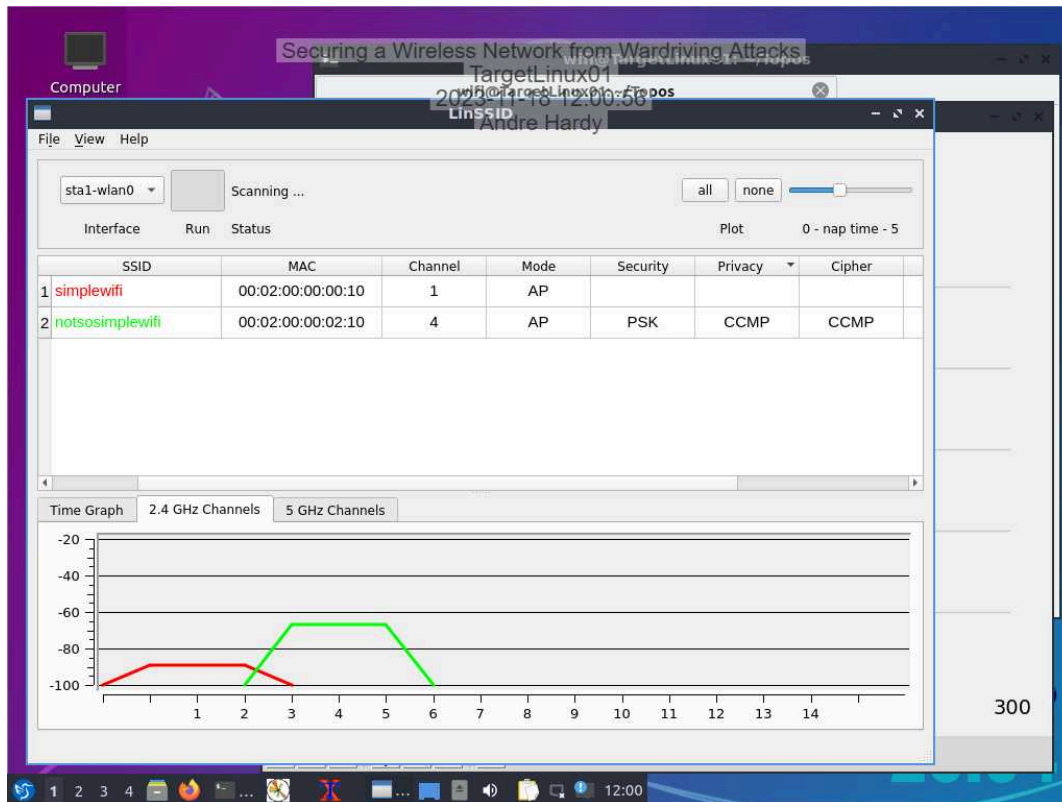
Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

10. **Make a screen capture** showing **sta1's** increased antenna gain as displayed in the **Mininet-WiFi Graph**.



18. Make a screen capture showing the multiple WLANs discovered in LinSSID.

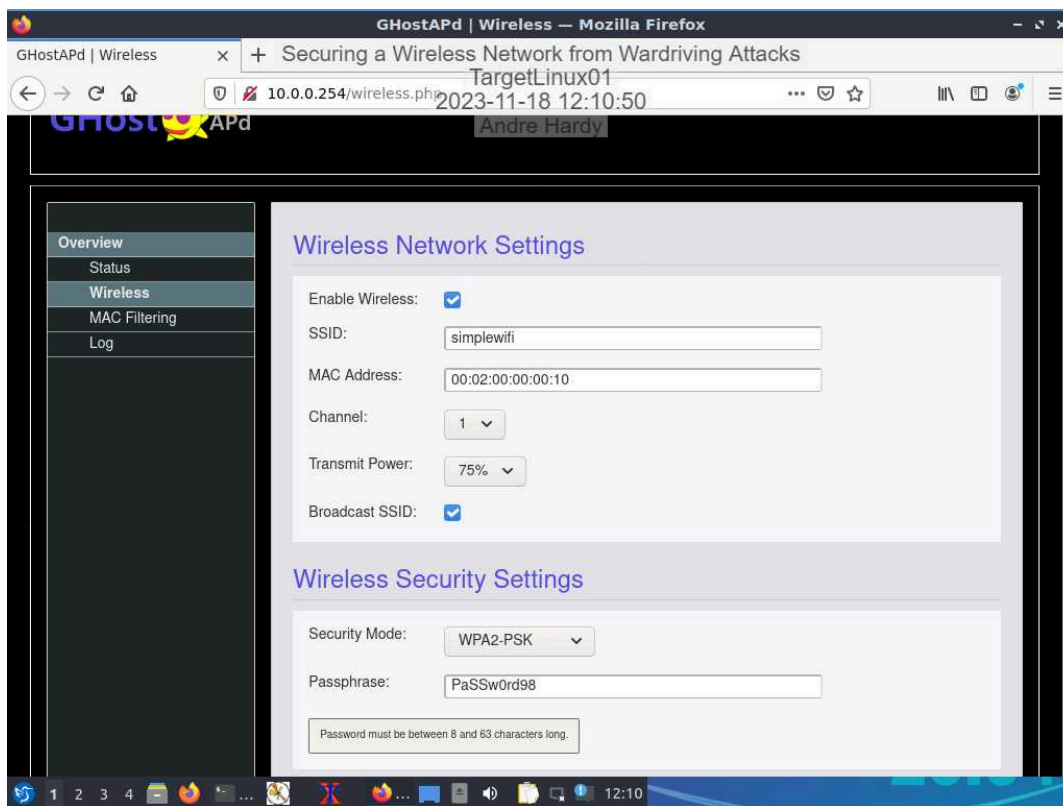


23. Record the GPS (x and y graph) coordinates of the ap1 access point.

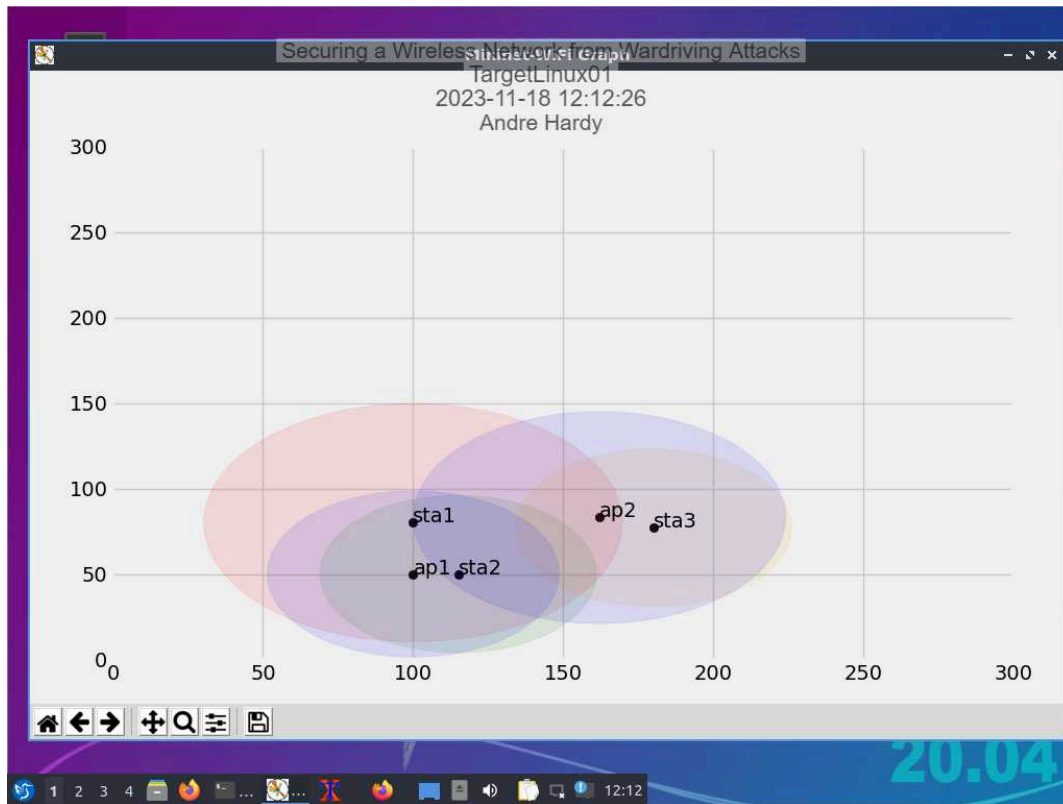
(100.0, 64.0)

Part 3: Secure the Access Point

11. **Make a screen capture** showing the **new security mode** and **transmit power values** for *simplewifi* on the **GHostAPd Status** page.



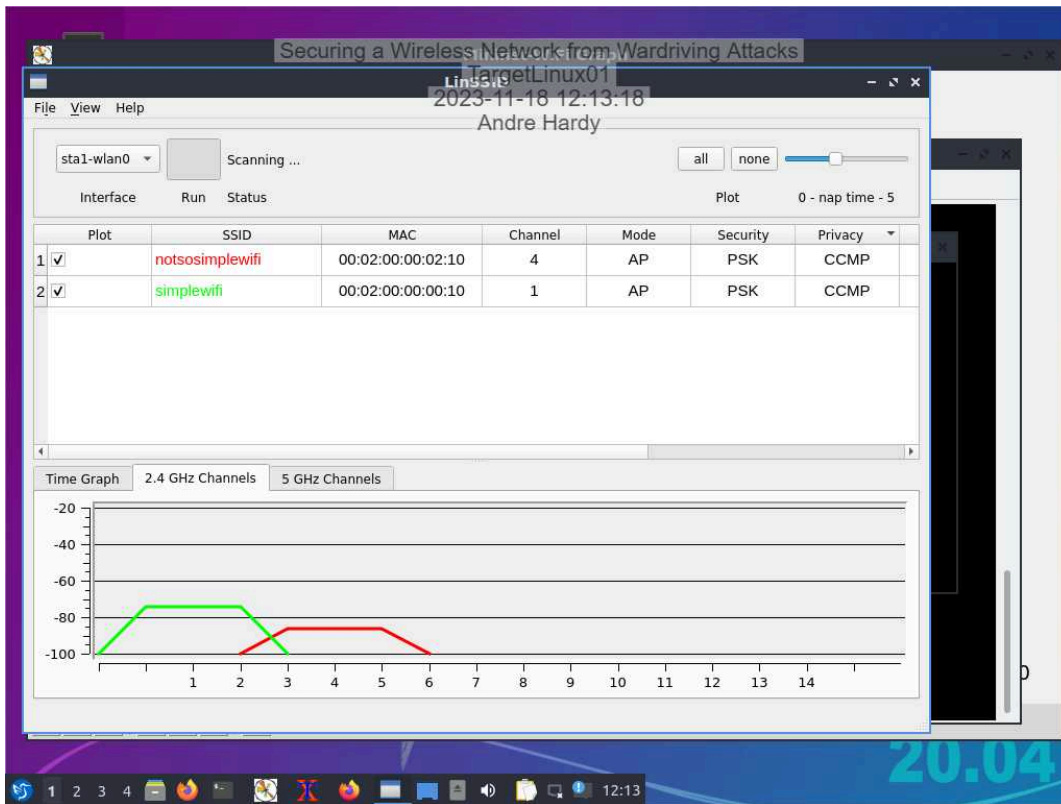
15. **Make a screen capture** showing the **relocated ap1** with **75% transmission power** in the **Mininet-WiFi Graph**.



Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

19. Make a screen capture showing both WPA2-PSK networks in LinSSID.



Section 2: Applied Learning

Part 1: Perform a Wardriving Attack with Kismet

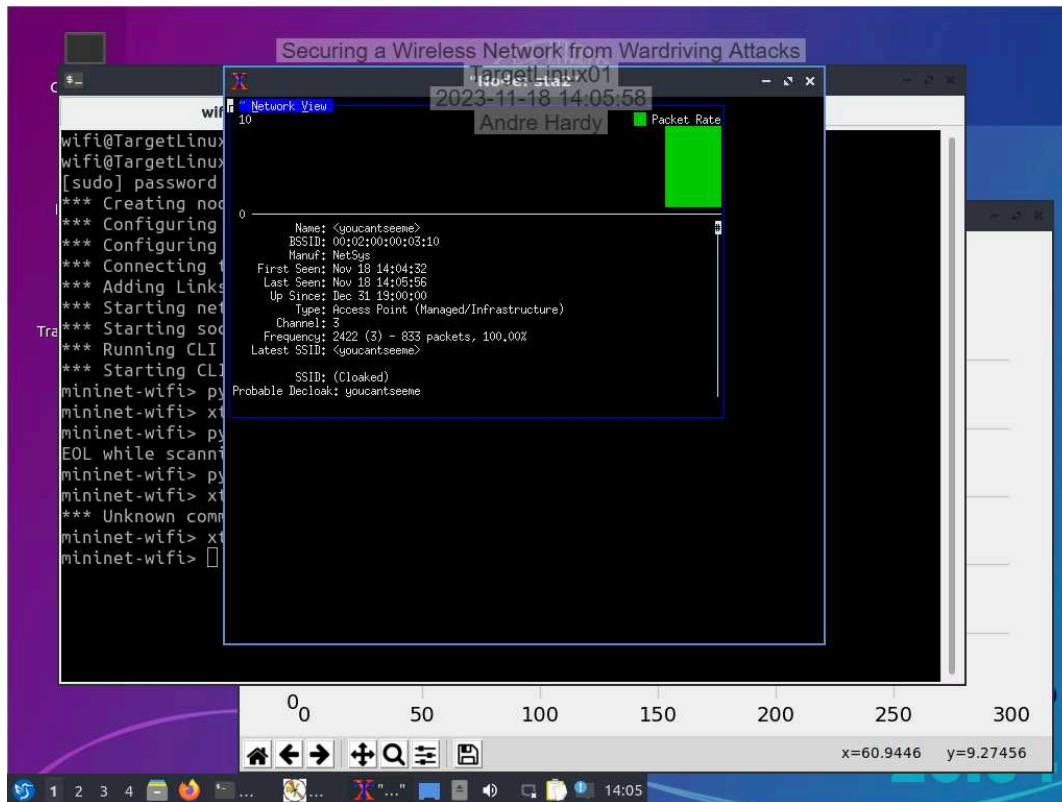
11. Make a screen capture showing the list of five networks detected by Kismet.



18. Make a screen capture showing the **SSID: youcantseeme** probe request in your **Node: sta1** Kismet window.

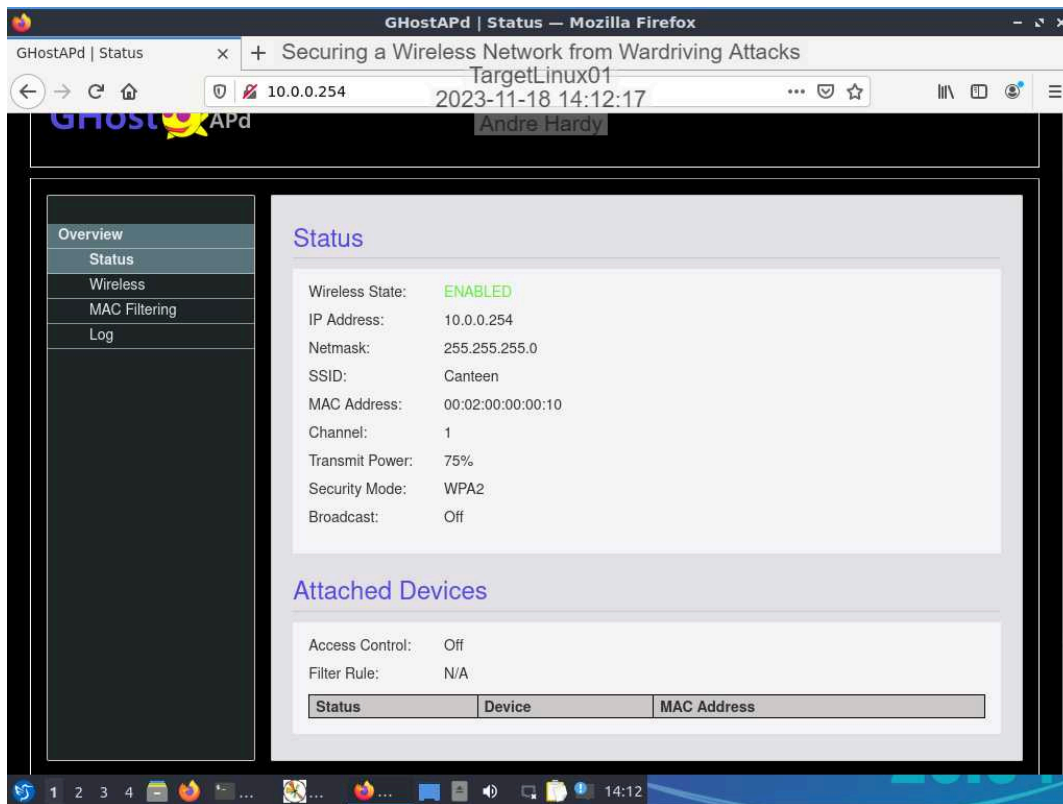


31. Make a screen capture showing the <youcantseeme> network details in your Node: sta2 Kismet window.



Part 2: Harden the Access Point

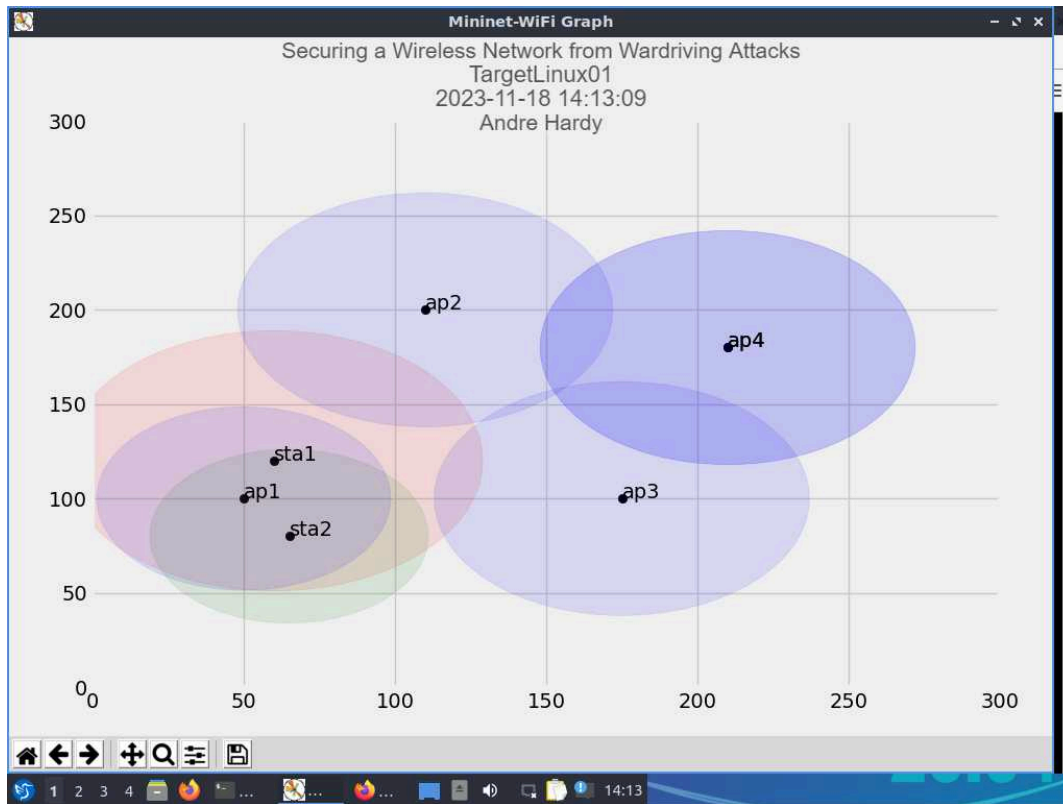
6. Make a screen capture showing the **WPA2-enabled Canteen** network as reported by the **Status** page.



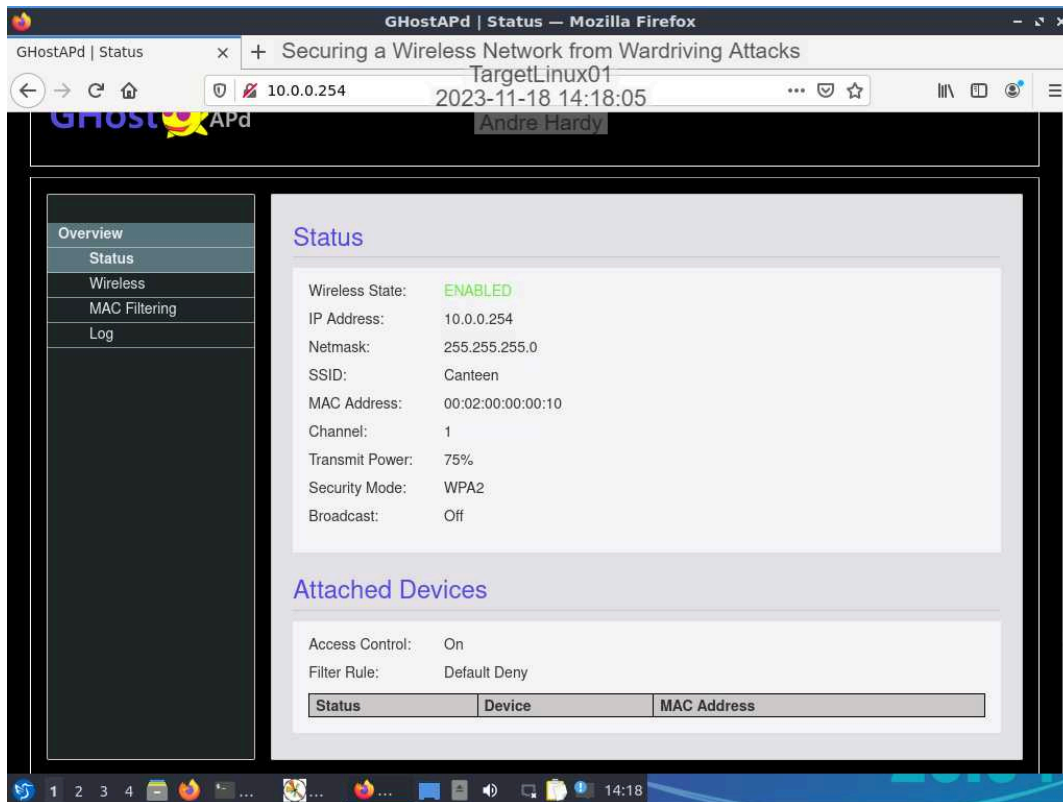
Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

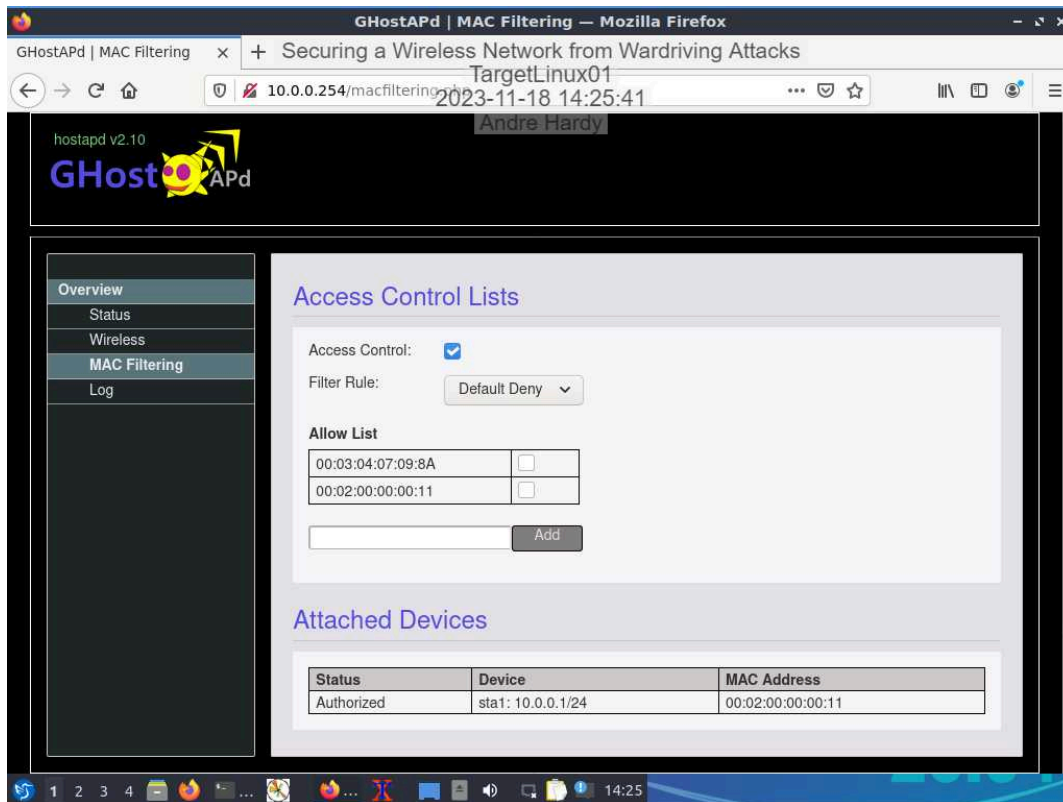
9. Make a screen capture showing ap1's new location and signal range in the Mininet-Wifi Graph window.



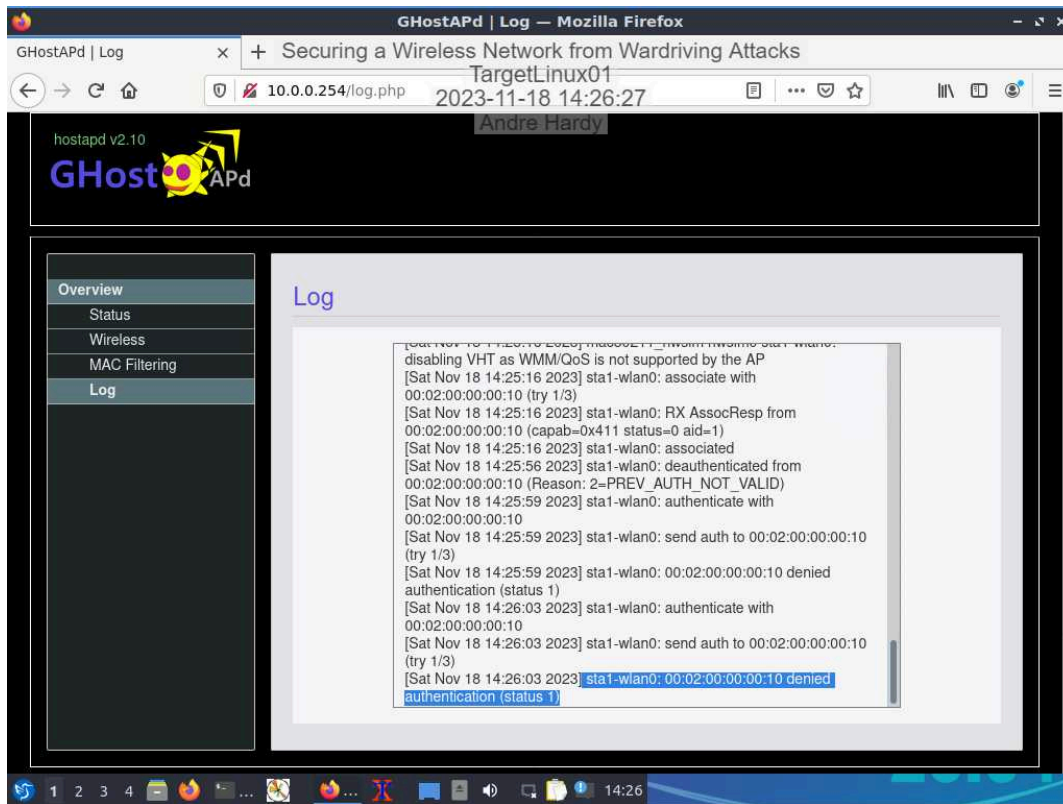
17. Make a screen capture showing the new configuration values for the Canteen network on the Status page.



29. Make a screen capture showing the **configured ACL parameters**, and any **Attached Devices**, as shown in the **MAC Filtering** page.



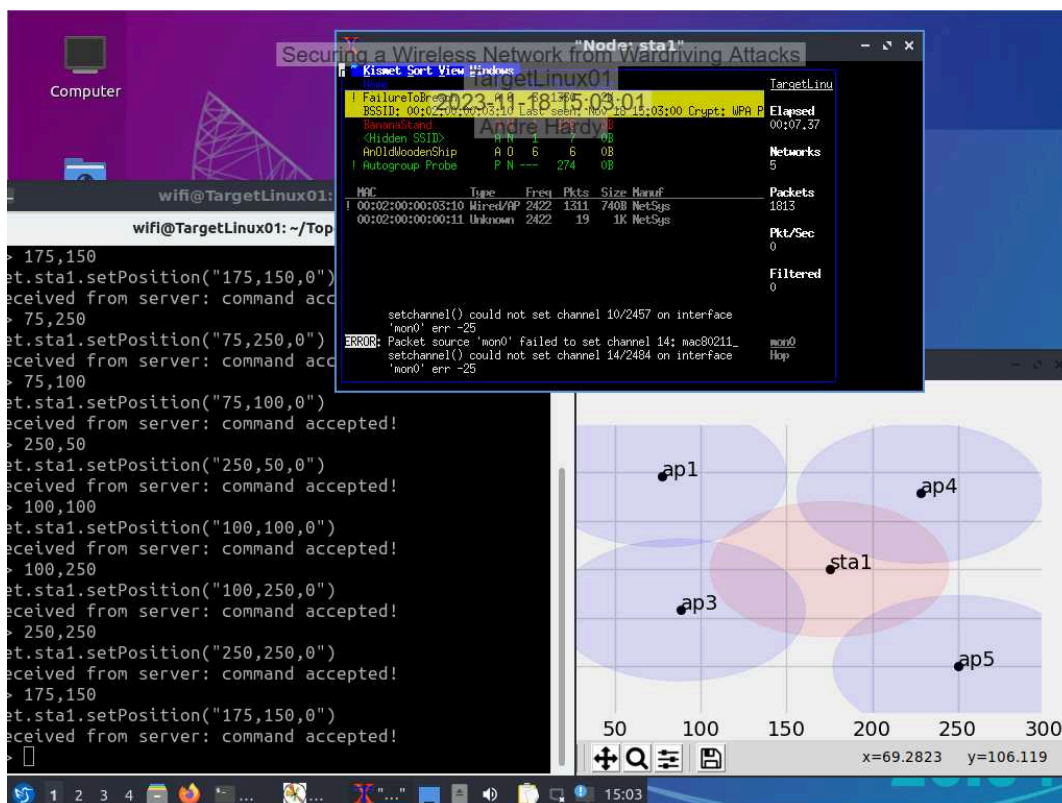
33. Make a screen capture showing **sta1-wlan0** interface being denied authentication in the GHostAPd Log.



Section 3: Challenge and Analysis

Part 1: Perform Data Gathering and Analysis with Wardriving

4. Make a screen capture showing the four discovered networks in Kismet.



5. Document the SSID of the open hidden network you discovered.

GEToutofmyyard8080

6. Document the SSID of the WEP-encrypted network you discovered.

BananaStand

Part 2: Investigate Potential Rogue Access Points

7. Make a screen capture showing the response to your curl/GET request.

```
"Node: stal"
[rook@TargetLinux01]~/home/wifi/stal
[rook@TargetLinux01]~/home/wifi/stal
[rook@TargetLinux01]~/home/wifi/stal
stal-wlan0 IEEE 802.11 ESSID:"GEToutofmyyard8080"
Mode:Managed Frequency:2.412 GHz Access Point: 00:02:00:00:04:15
Bit Rates:1 Mb/s Tx-Power=14 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:
Link Quality=29/70 Signal level=-71 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:2 Missed beacon:0

[rook@TargetLinux01]~/home/wifi/stal
[rook@TargetLinux01]~/home/wifi/stal
curl 10.50.0.254:8080
orig: jgs modified: gd

  ____  _
 / ___|| | | |
| |___| |_| |
 \___ \|  _/
      |_|_|

Outta my yard punk, or I'm releasing Cerby!!
Just kidding, welcome to Heck. Well, to Heck Proxy. The entrance to Heck is off
the grid (heh), but I can tell you where to find it.

Try plugging 450,260 into your GPS, that should park you right at the 'TheGateso
fHeck'. You will need the password, too: 'tedfoottwo'.

Off you go now!
...((mumbling)... now about tend to those troublesome Daemons...((mnnnnnnnnnn)).. c
ome now CB.

[rook@TargetLinux01]~/home/wifi/stal
[rook@TargetLinux01]~/home/wifi/stal
```

Part 3: Connect to Hidden WPA2 Access Points

8. Make a screen capture showing the **decloaked** *TheGatesofHeck* network in Kismet.

