

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.

The screenshot shows a Mozilla Firefox window displaying the GHostAPd Status page. The URL in the address bar is `http://10.0.0.254`. The page title is "GHostAPd | Status". The main content area is titled "Status" and displays the following wireless networking configuration:

Wireless State:	ENABLED
IP Address:	10.0.0.254
Netmask:	255.255.255.0
SSID:	simplewifi
MAC Address:	00:02:00:00:00:10
Channel:	1
Transmit Power:	100%
Security Mode:	None
Broadcast:	On

Below the status section, there is a "Attached Devices" section with the following details:

Access Control:	Off	
Filter Rule:	N/A	
Status	Device	MAC Address
Authorized	sta1: 10.0.0.1/24	00:02:00:00:00:11
Authorized	sta2: 10.0.0.2/24	00:02:00:00:00:12

Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

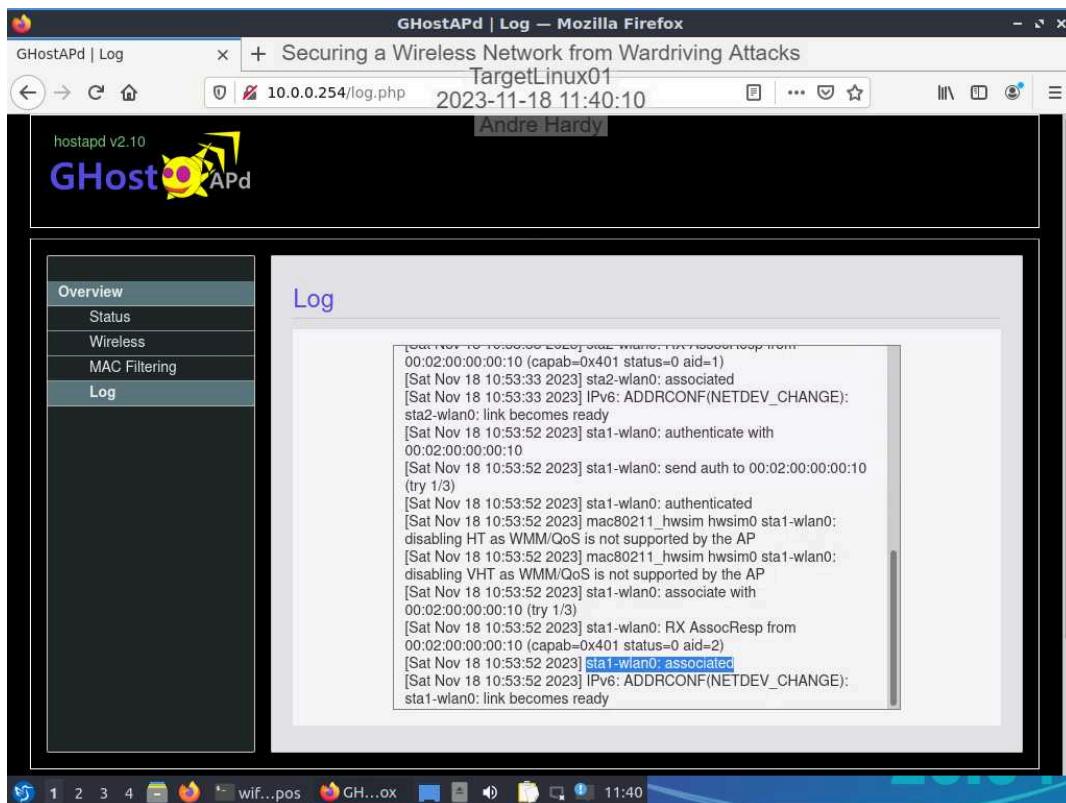
17. Make a screen capture showing the Allow List in the Access Control Lists section of GHostAPd.

The screenshot shows a Mozilla Firefox window titled "GHostAPd | MAC Filtering". The address bar displays "10.0.0.254/macfiltering" and the date and time "2023-11-18 11:37:59". The user is logged in as "Andre Hardy". The main content area is titled "Access Control Lists". Under "Access Control", the checkbox is checked and the dropdown "Filter Rule" is set to "Default Deny". In the "Allow List" section, the MAC address "00:03:04:07:09:8A" is listed in a text input field with an adjacent checkbox. Below this is a "Add" button. A message at the bottom states: "ACL enablement/disablement and filter rule changes will be applied, and the AP will be restarted." with "Apply Changes" and "Cancel" buttons. Below this is a section titled "Attached Devices" which lists two devices: "sta1: 10.0.0.1/24" and "sta2: 10.0.0.2/24", both marked as "Authorized". The MAC addresses for these devices are listed as "00:02:00:00:00:11" and "00:02:00:00:00:12" respectively. The browser's toolbar and taskbar are visible at the bottom.

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.

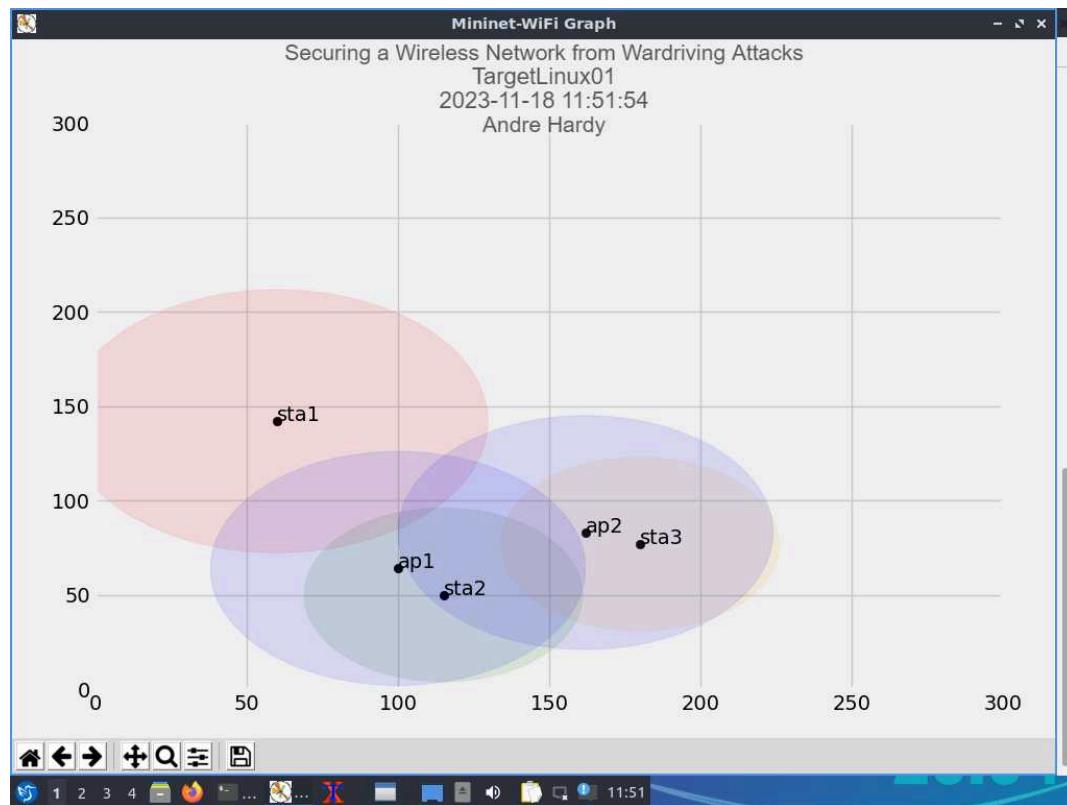


Part 2: Perform a Wardriving Attack with LinSSID

Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

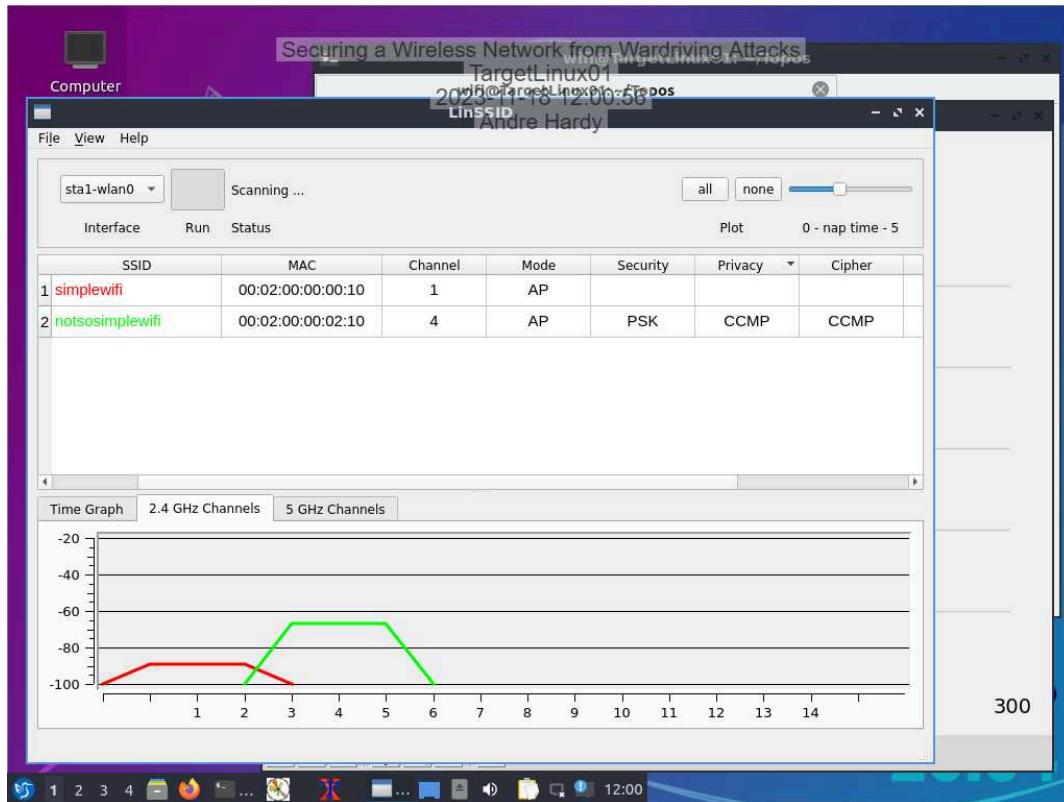
10. Make a screen capture showing sta1's increased antenna gain as displayed in the Mininet-WiFi Graph.



Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

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.

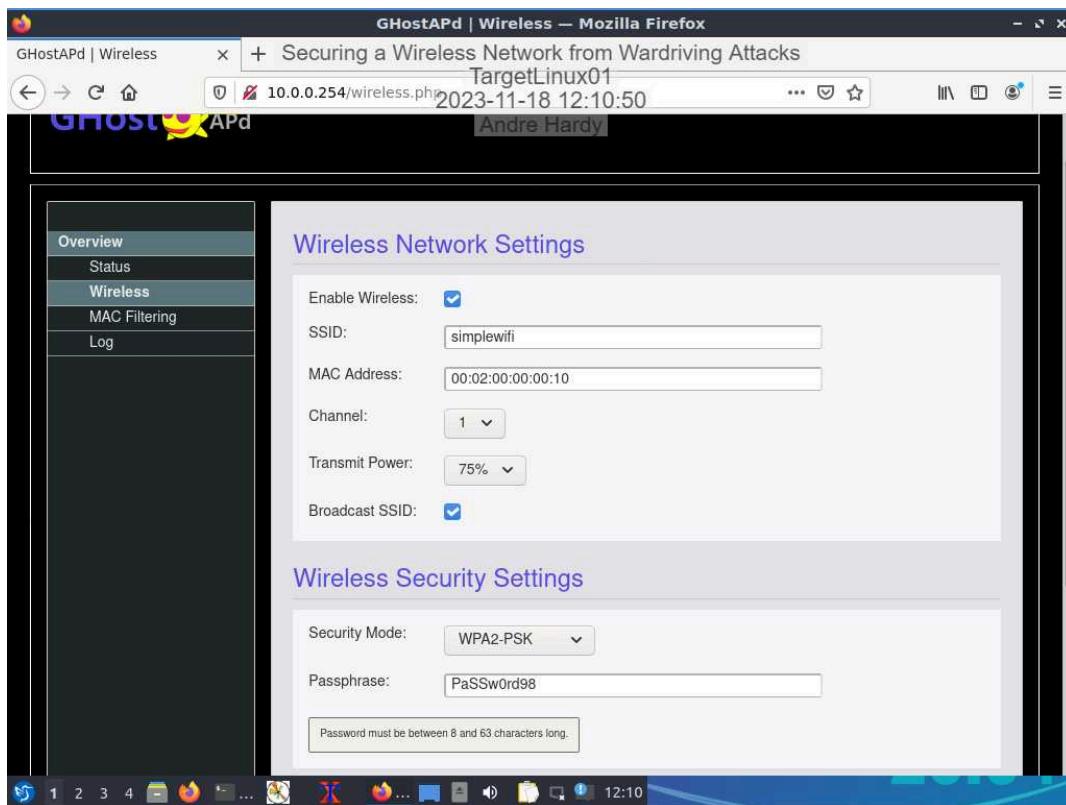
(100.0, 64.0)

Part 3: Secure the Access Point

Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

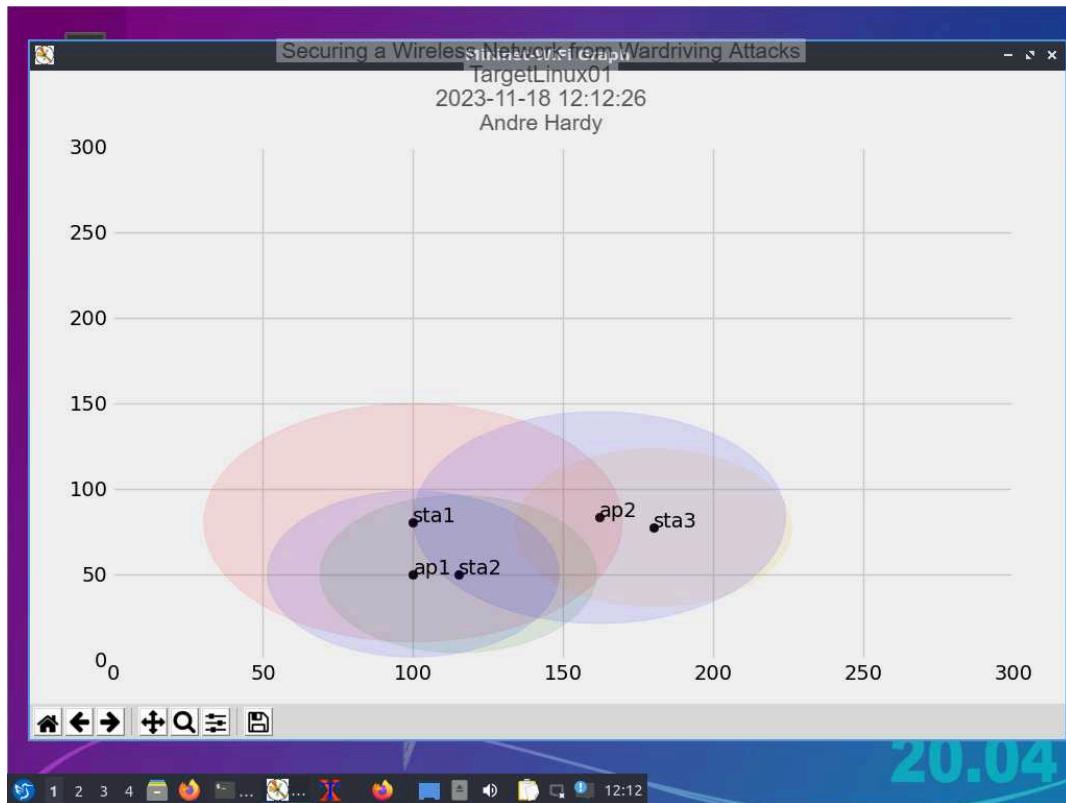
11. Make a screen capture showing the new security mode and transmit power values for **simplewifi** on the GHostAPd Status page.



Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

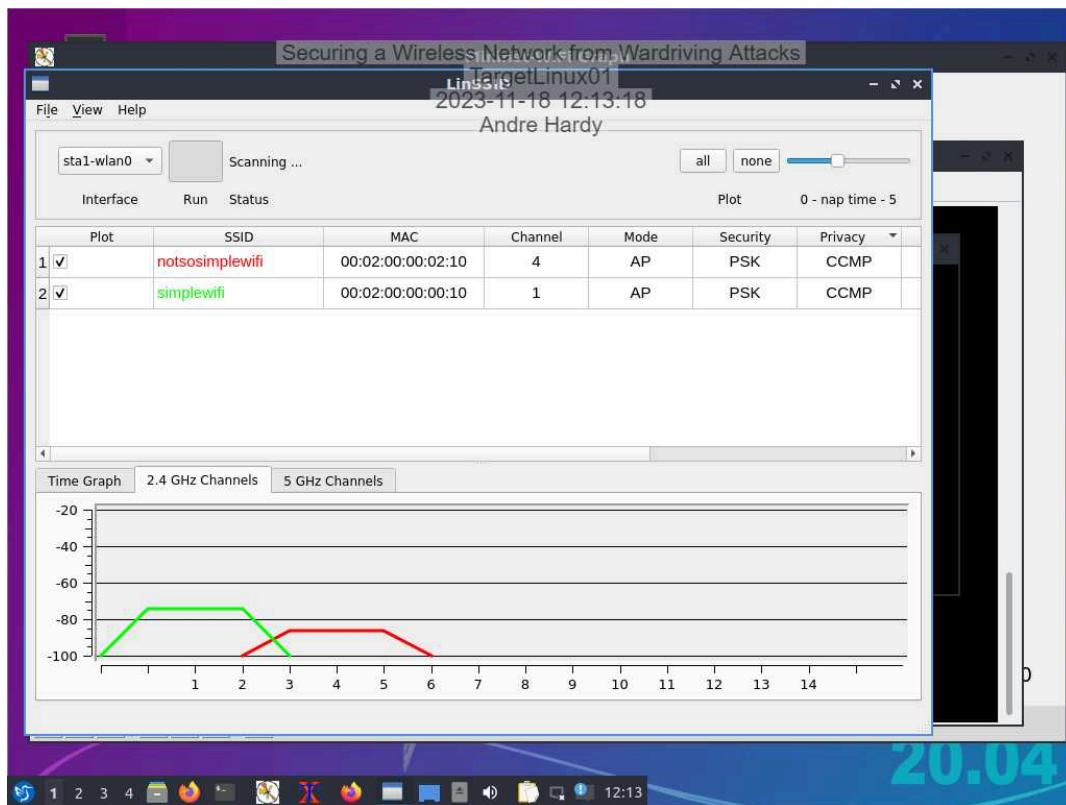
15. Make a screen capture showing the relocated ap1 with 75% transmission power in the Mininet-WiFi Graph.



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.



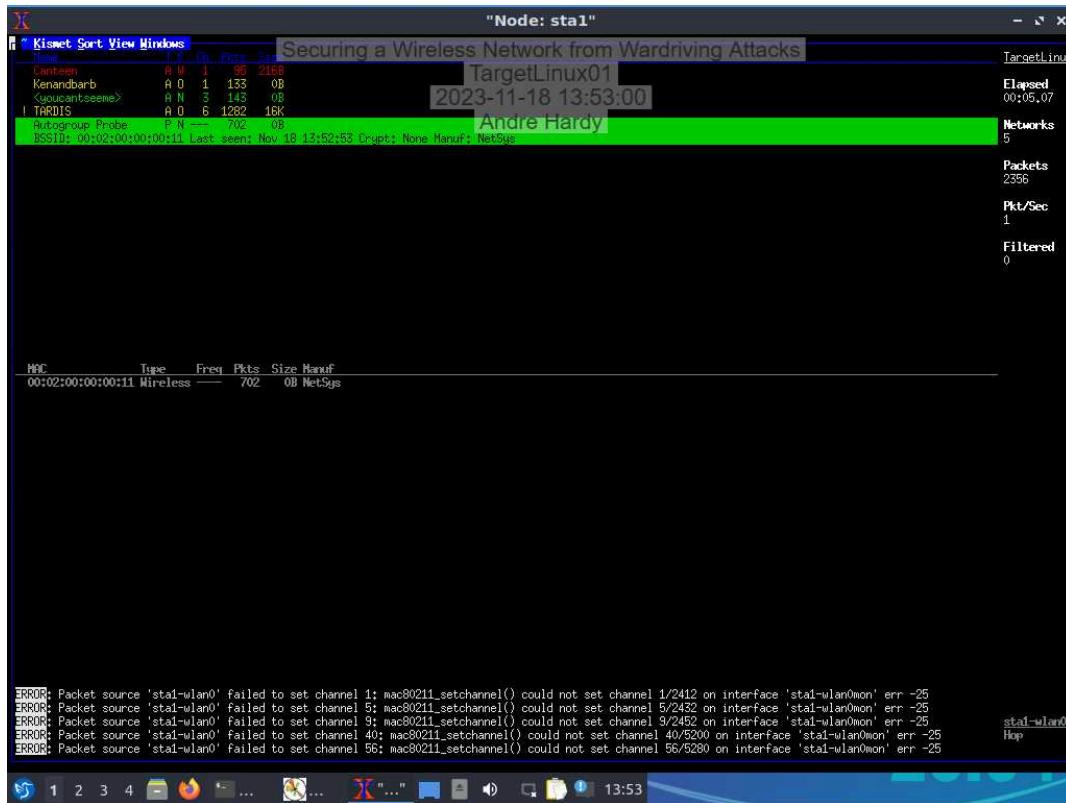
Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

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.



Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

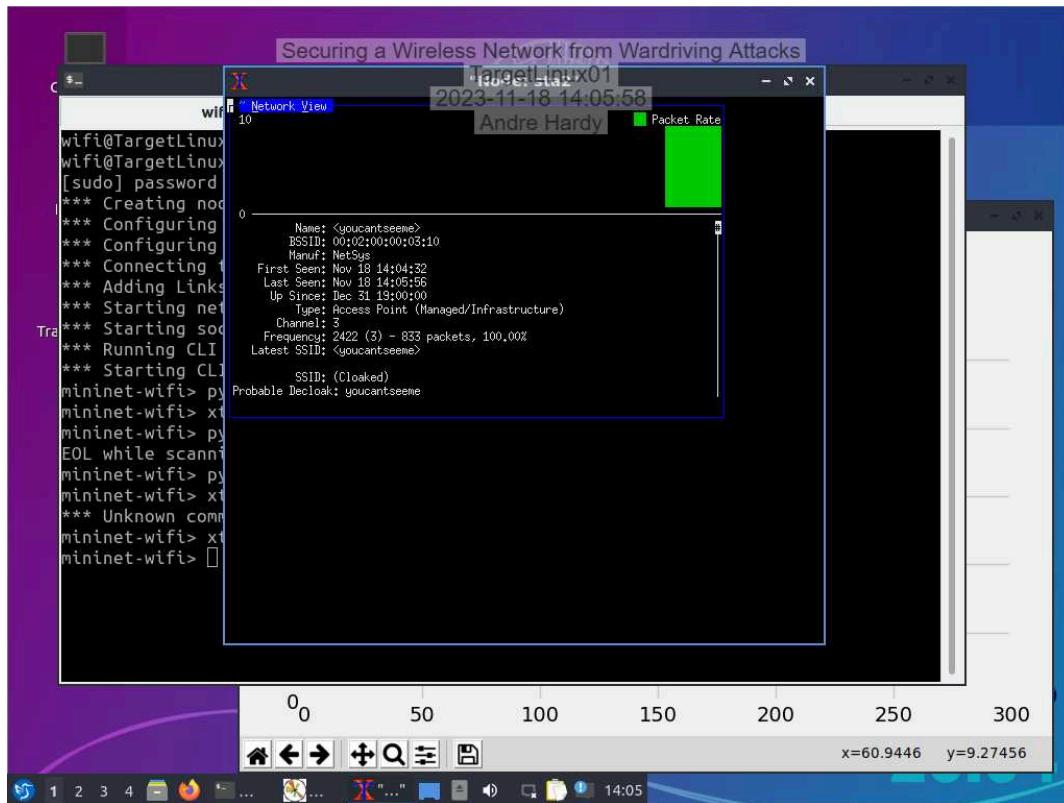
18. Make a screen capture showing the SSID: youcantseeme probe request in your Node: sta1 Kismet window.



Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

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



Part 2: Harden the Access Point

Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

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

The screenshot shows a Mozilla Firefox browser window displaying the 'Status' page of the GHostAPD web interface. The title bar reads 'GHostAPD | Status — Mozilla Firefox'. The address bar shows '10.0.0.254 TargetLinux01' and the date/time '2023-11-18 14:12:17'. The user 'Andre Hardy' is logged in. The main content area is titled 'Status' and contains the following information:

Wireless State:	ENABLED
IP Address:	10.0.0.254
Netmask:	255.255.255.0
SSID:	Canteen
MAC Address:	00:02:00:00:00:10
Channel:	1
Transmit Power:	75%
Security Mode:	WPA2
Broadcast:	Off

Below this, there is a section titled 'Attached Devices' with the following settings:

Access Control:	Off
Filter Rule:	N/A

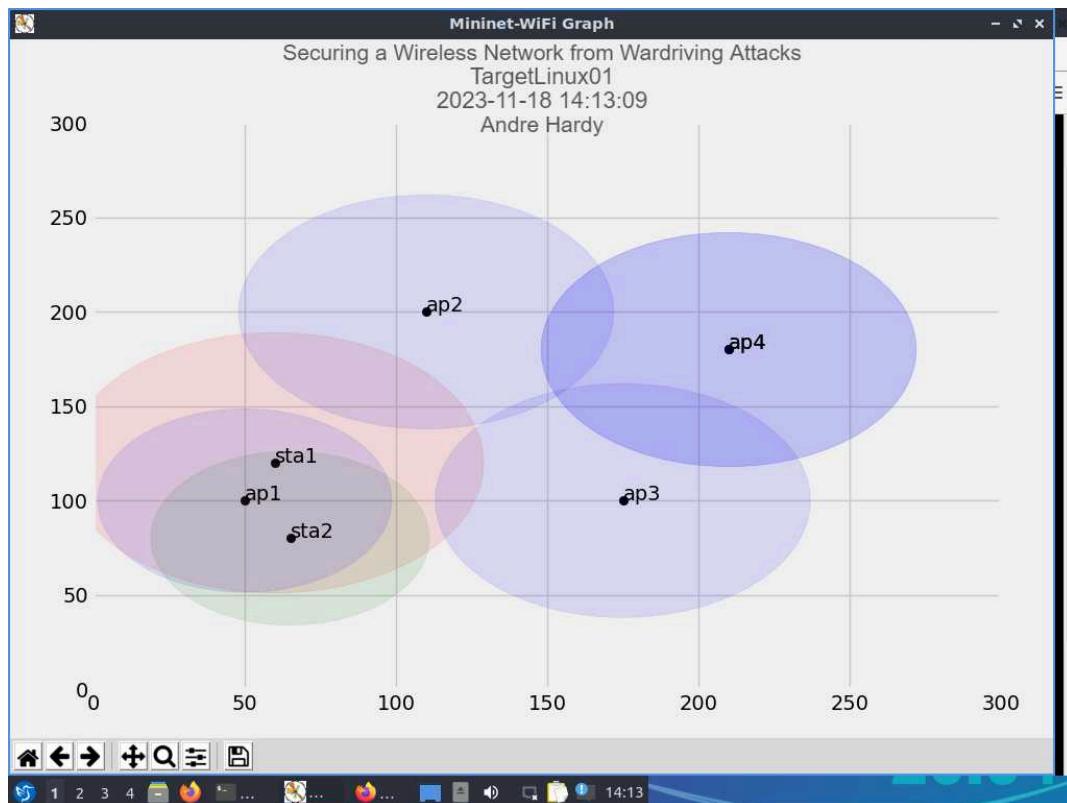
A table header for 'Attached Devices' is visible but empty:

Status	Device	MAC Address
--------	--------	-------------

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.



Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

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

The screenshot shows a Mozilla Firefox window displaying the GHostAPd Status page. The URL in the address bar is `10.0.0.254`. The page title is "GHostAPd | Status — Mozilla Firefox". The main content area is titled "Status" and contains the following configuration details:

Wireless State:	ENABLED
IP Address:	10.0.0.254
Netmask:	255.255.255.0
SSID:	Canteen
MAC Address:	00:02:00:00:00:10
Channel:	1
Transmit Power:	75%
Security Mode:	WPA2
Broadcast:	Off

Below the status section is a "Attached Devices" panel, which currently displays the following settings:

Access Control:	On
Filter Rule:	Default Deny

At the bottom of the Firefox window, the toolbar and status bar are visible, showing icons for file operations, a search bar, and the time "14:18".

Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

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

The screenshot shows a Mozilla Firefox browser window with the title "GHostAPd | MAC Filtering — Mozilla Firefox". The address bar displays "10.0.0.254/macfiltering" and the date/time "2023-11-18 14:25:41". The user "Andre Hardy" is logged in. The main content area is titled "Access Control Lists" and shows the following configuration:

- Access Control:
- Filter Rule: Default Deny

The "Allow List" contains two entries:

00:03:04:07:09:8A	<input type="checkbox"/>
00:02:00:00:00:11	<input type="checkbox"/>

A "Add" button is located below the allow list table.

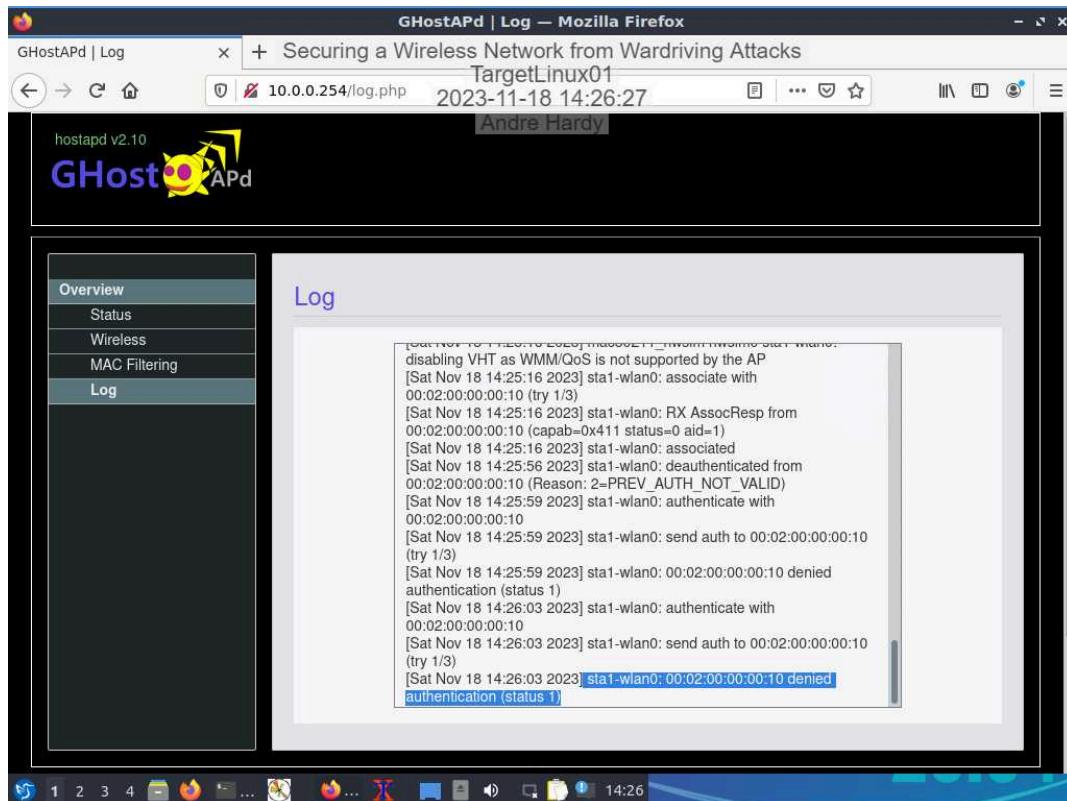
Below the access control section is another titled "Attached Devices" which lists:

Status	Device	MAC Address
Authorized	sta1: 10.0.0.1/24	00:02:00:00:00:11

Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

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



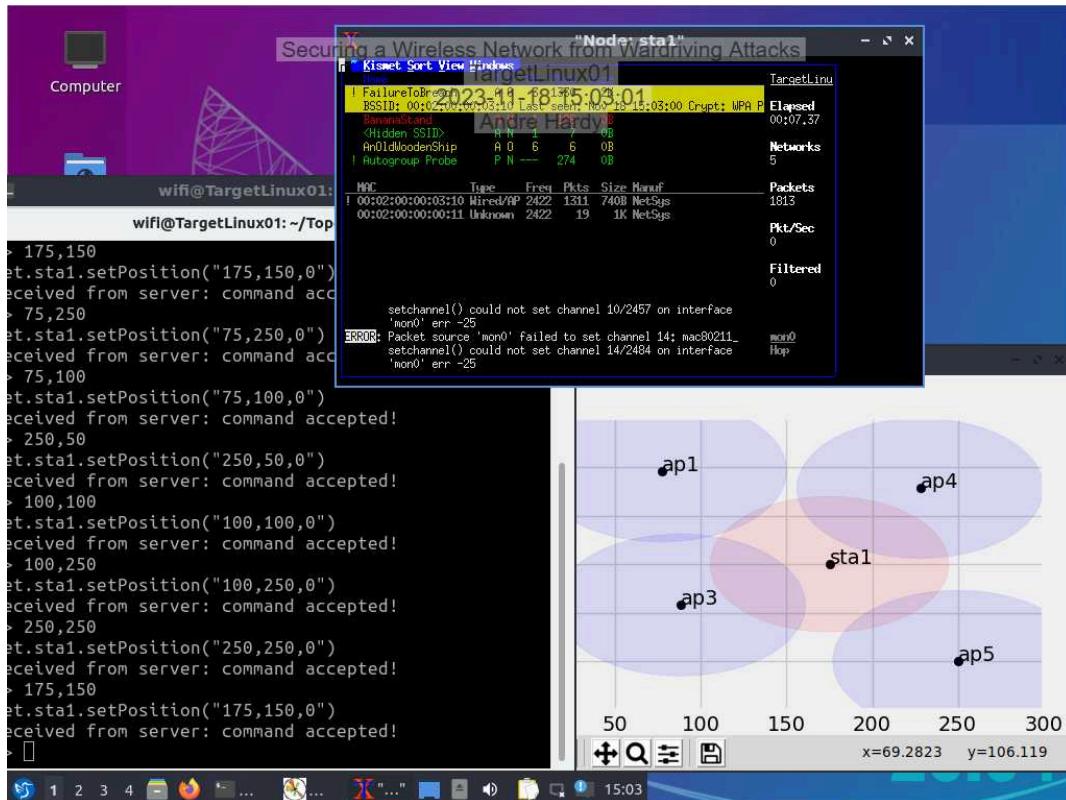
Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

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

Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

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

Part 3: Connect to Hidden WPA2 Access Points

Securing a Wireless Network from Wardriving Attacks

Wireless and Mobile Device Security, Second Edition - Lab 01

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

