# Wifi Pineapple MKII

## Summary

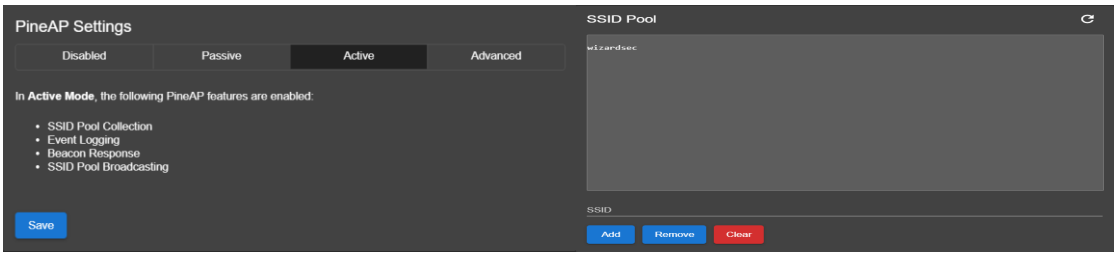
The WiFi Pineapple management GUI can be accessed by connecting to one of the spoofed APs created by the PineAP, thus circumventing the use of a pre-shared key to access the management GUI. The password to access the management GUI can then be easily fuzzed to gain access to the management GUI. The default username used to access the GUI is “root”. Upon further investigation, it was found that the login screen will accept any username supplied, so long as it is paired with the correct password.

## Tools Used

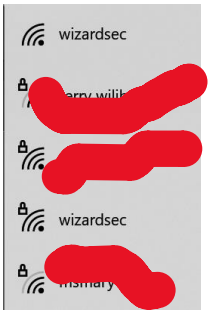
Kali Linux, Bettercap, Nmap, OWASP ZAP

## Process

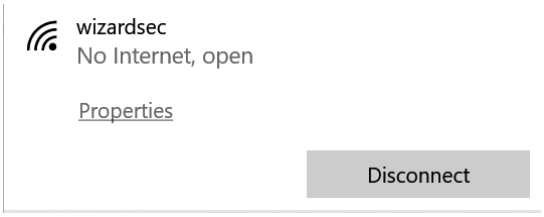
In active mode, the pineapple broadcasts open SSIDs collected in the SSID pool to allow clients to associate. The test AP “wizardsec” was added to the SSID pool and the PineAP was set to active mode.



In Windows 10, both the test AP “wizardsec” and the spoofed open AP “wizardsec” were displayed




The client device, a Windows 10 Laptop, was connected to the open spoofed AP “wizardsec”



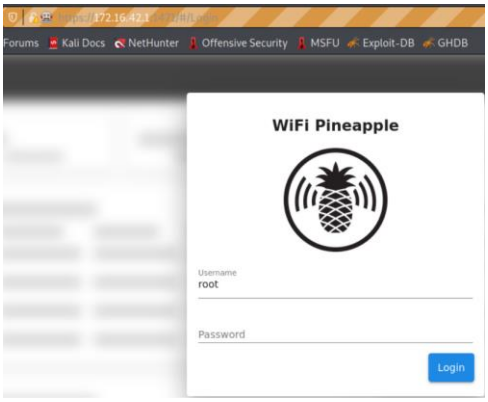

The client device, equipped with a Kali VM with Bettercap and Nmap, was used to enumerate the open AP. The gateway address of the MKVII was found to be 172.16.42.1

| IP | MAC | Hostname | Vendor | Sent | Recvd | Seen | Info |
|---|---|---|---|---|---|---|---|
| 172.16.42.1 | [redacted] | mk7.lan. | Orient Power Home Network Ltd. | 0 | 0 | 09:17:47 | gateway |
| 172.16.42.124 | [redacted] | eth0 | PCS Computer Systems GmbH | 0 | 0 | 09:17:47 | interface |

Upon further enumeration via an Nmap scan of the ip address 172.16.42.1, the open ports 22, 53, 80, and 1471 were found

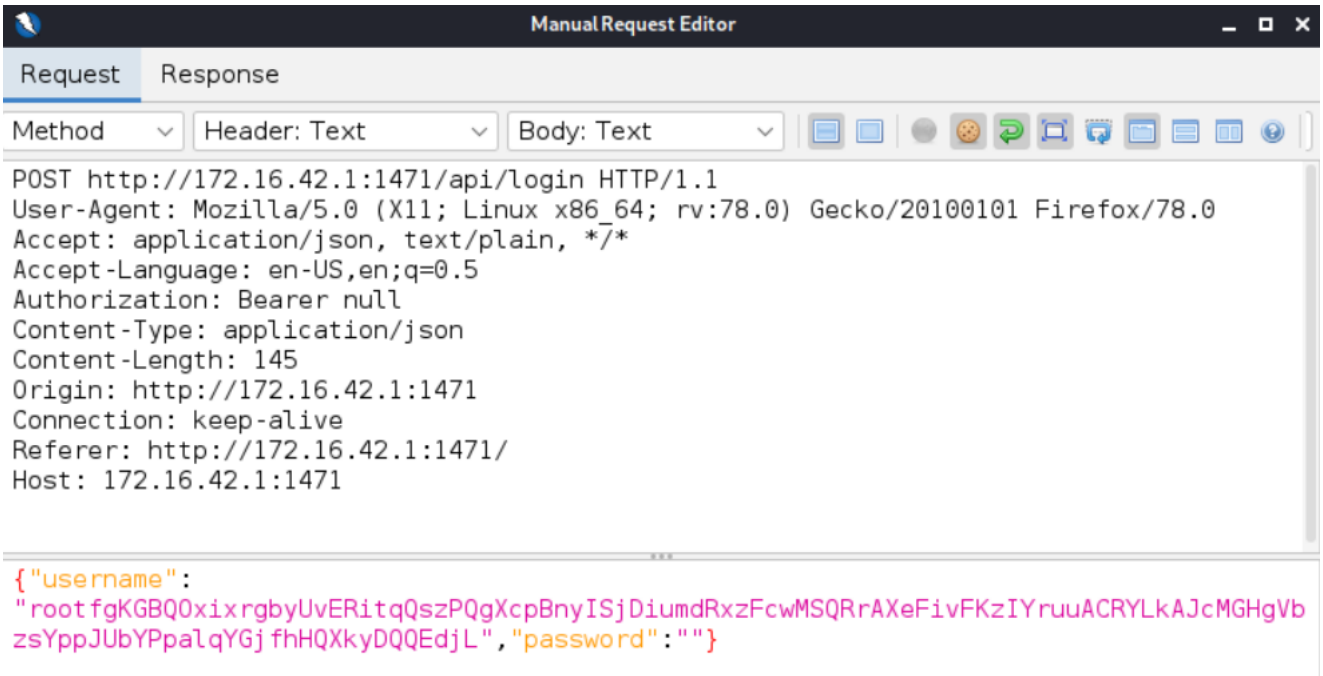
```
PORT     STATE SERVICE   REASON  VERSION
22/tcp   open  ssh       syn-ack OpenSSH 8.0 (protocol 2.0)
53/tcp   open  domain    syn-ack Cloudflare public DNS
80/tcp   open  http      syn-ack nginx 1.17.7
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: nginx/1.17.7
|_http-title: 403 Forbidden
1471/tcp open  csdmbase? syn-ack
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest, HTTPOptions:
```

Firefox ZAP browser was used to navigate to the ip address 172.16.42.1 on port 1471 and the login screen for the management AP was displayed.

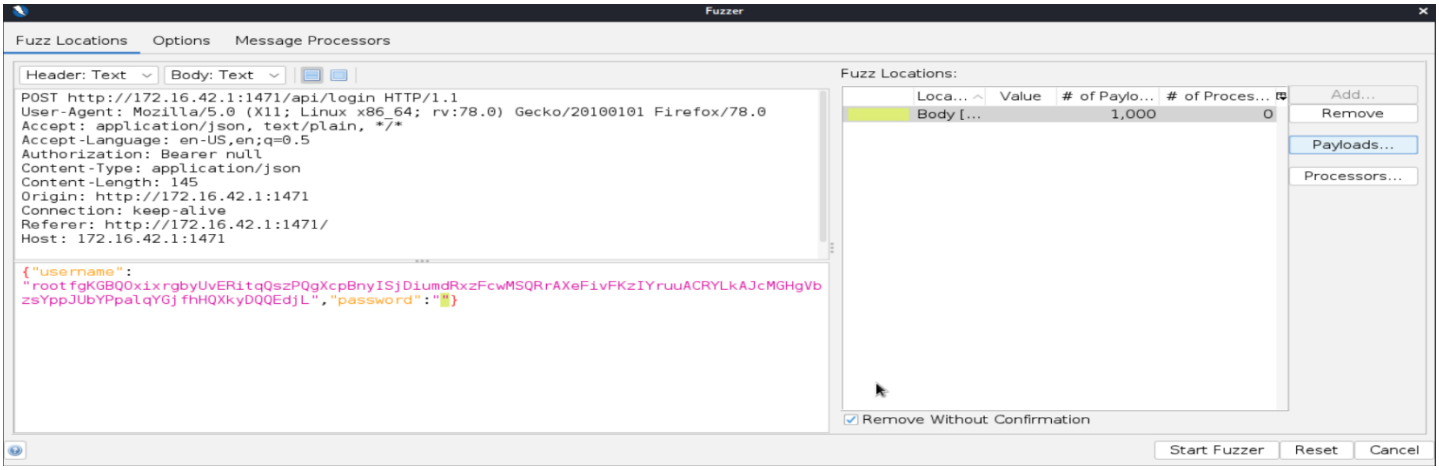


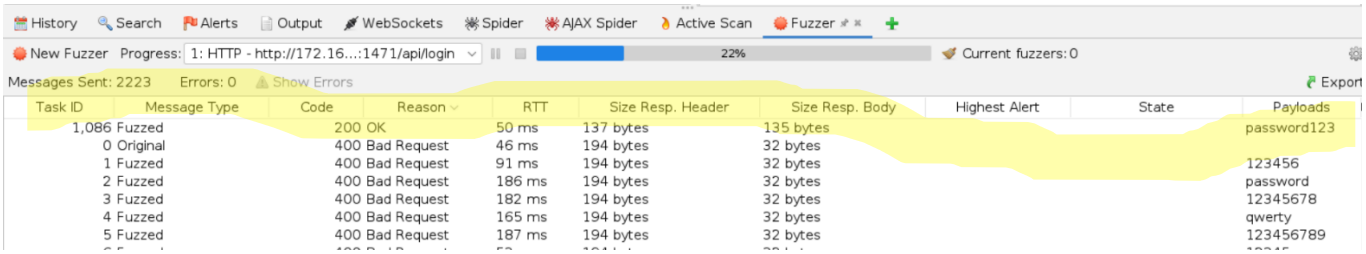
Further Enumeration of the MKVII web app was performed, resulting in the discovery of the MKVII web app's login post data.


The post data was sent to the manual request editor in ZAP, username and password fields were discovered.

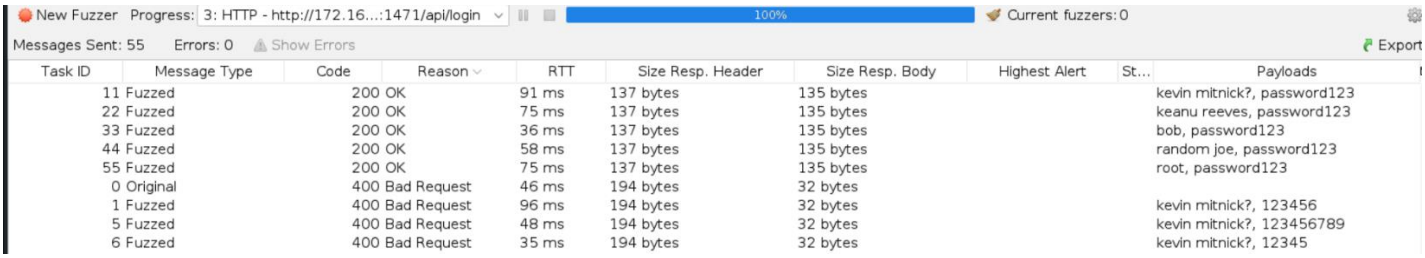


Fuzzing of the password field was executed with a password list. The password for the GUI login was found and access to the GUI was granted.

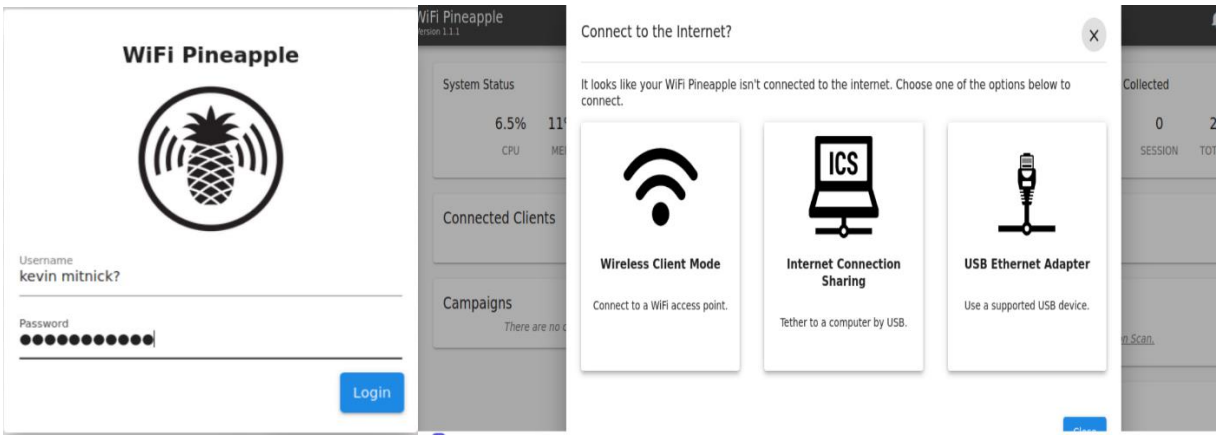



Upon further fuzzing of both username and password fields, it was found that **ANY** username in combination with the correct password allows access to the MKII's management GUI.



A login was attempted with “kevin mitnick?” as the user with the correct password “password123”. Access to the management GUI was granted.




Now Kevin Mitnick has gained access to a Pineapple ☹️