

Wifi Pineapple MKII

Summary

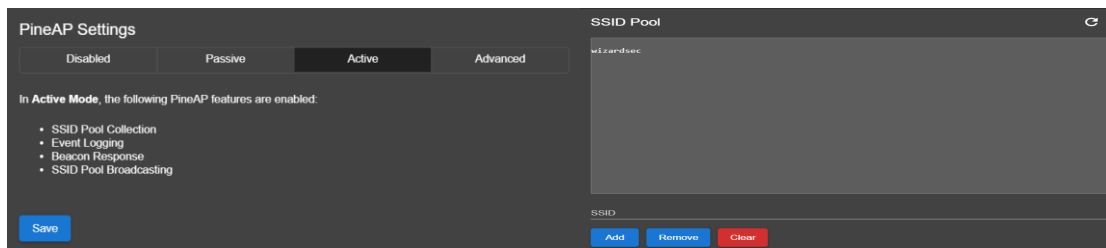
The WiFi Pineapple management GUI can be accessed by connecting to one of the spoofed APs created by the PineAP, thus circumventing the use of a pre-shared key to access the management GUI. The password to access the management GUI can then be easily fuzzed to gain access to the management GUI. The default 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

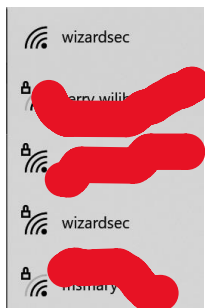
Kali Linux, Bettercap, Nmap, OWASP ZAP

Process

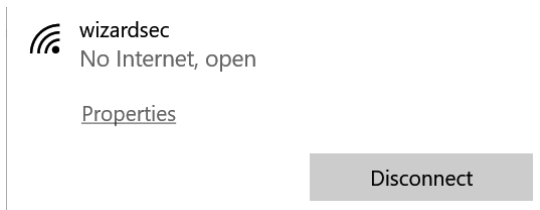
In active mode, the pineapple broadcasts open SSIDs collected in the SSID pool to allow clients to associate. The test AP “wizardsec” was added to the SSID pool and the PineAP was set to active mode.



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 ▾		mk7.lan.	Orient Power Home Network Ltd.	0	0	09:17:47	gateway
172.16.42.124 ▾		eth0	PCS Computer Systems GmbH	0	0	09:17:47	interface

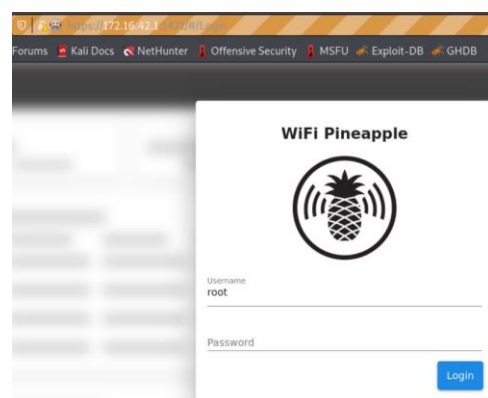
Upon further enumeration via an Nmap scan of the ip address 172.16.42.1, the open ports 22, 53, 80, and 1471 were found

```
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  csdmdbase?  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.

▼  http://172.16.42.1:1471



 GET: /

▼  api

 GET: checkUpdating

 GET: device

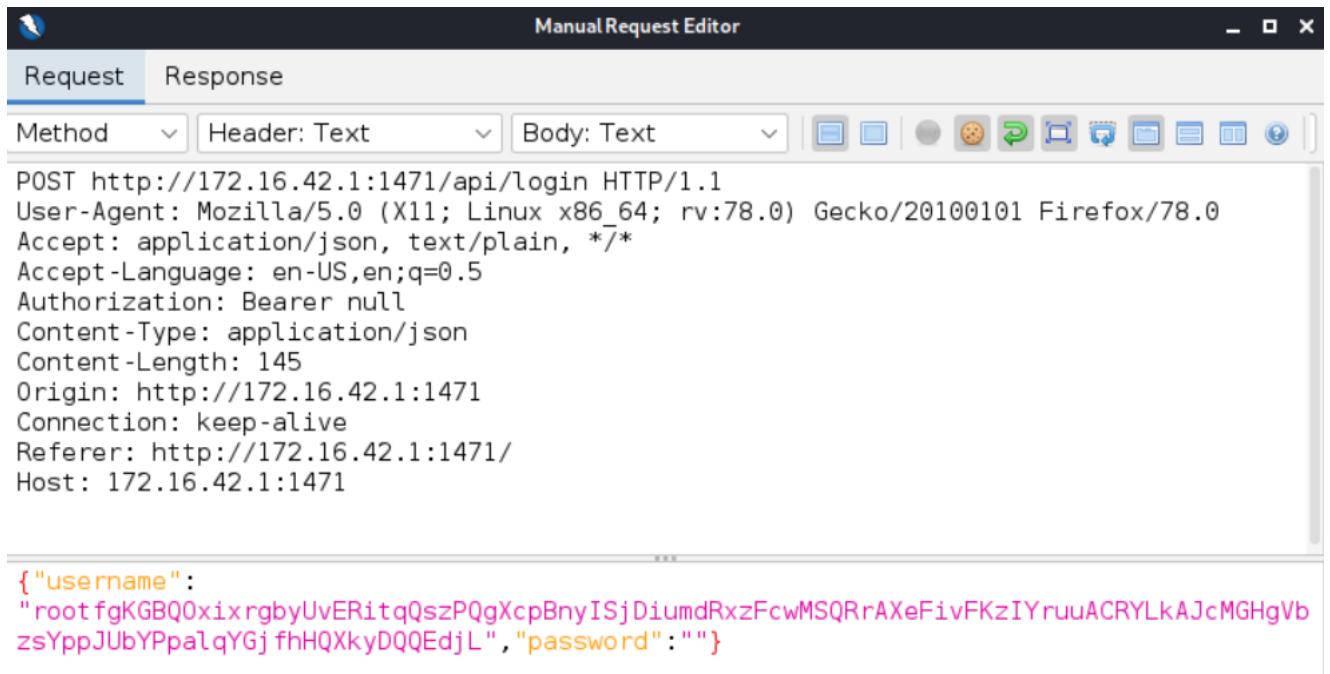
 POST: login()({"username": "root", "password": ""})

  POST: login()({"username": "rootfgKGBQOxixrgbyUvERitqQs...")

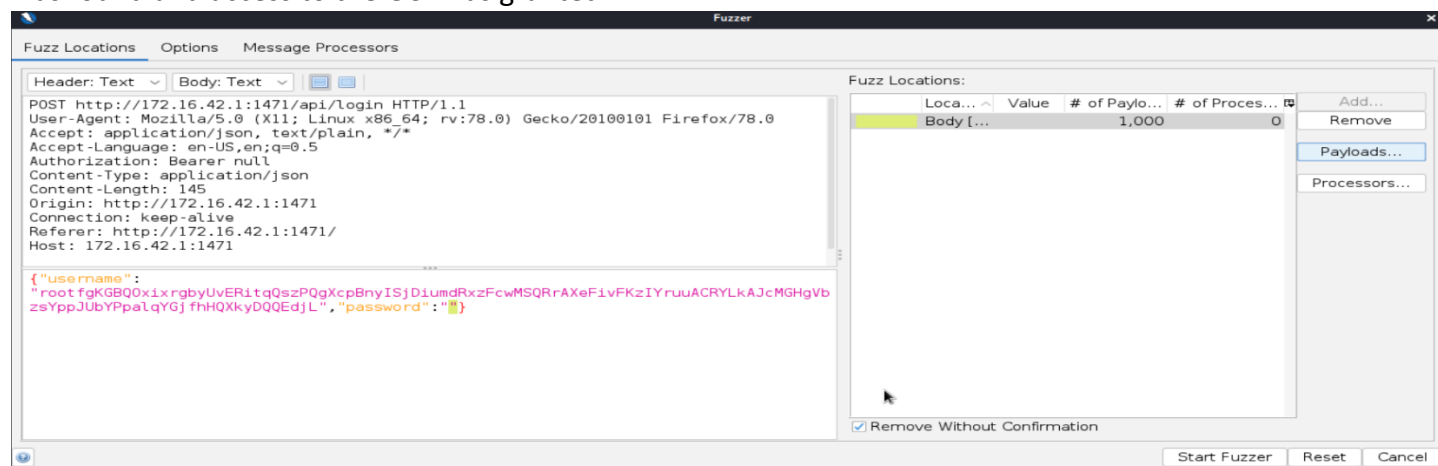
 GET: modules

 GET: setupRequired

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.

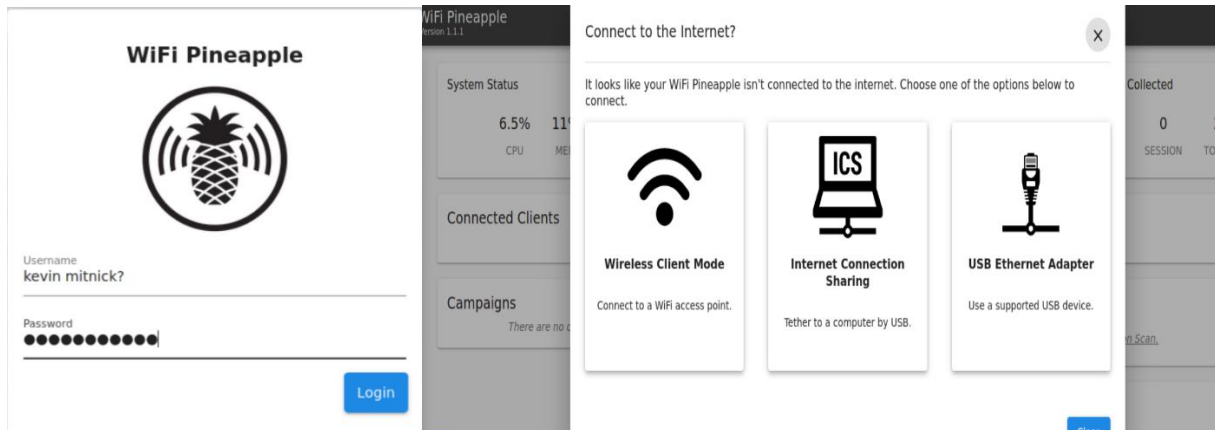


Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
1,086 Fuzzed		200 OK		50 ms	137 bytes	135 bytes			password123
0 Original		400 Bad Request		46 ms	194 bytes	32 bytes			
1 Fuzzed		400 Bad Request		91 ms	194 bytes	32 bytes			123456
2 Fuzzed		400 Bad Request		186 ms	194 bytes	32 bytes			password
3 Fuzzed		400 Bad Request		182 ms	194 bytes	32 bytes			12345678
4 Fuzzed		400 Bad Request		165 ms	194 bytes	32 bytes			qwerty
5 Fuzzed		400 Bad Request		187 ms	194 bytes	32 bytes			123456789

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.

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	St...	Payloads
11 Fuzzed		200 OK		91 ms	137 bytes	135 bytes			kevin mitnick?, password123
22 Fuzzed		200 OK		75 ms	137 bytes	135 bytes			keanu reeves, password123
33 Fuzzed		200 OK		36 ms	137 bytes	135 bytes			bob, password123
44 Fuzzed		200 OK		58 ms	137 bytes	135 bytes			random joe, password123
55 Fuzzed		200 OK		75 ms	137 bytes	135 bytes			root, password123
0 Original		400 Bad Request		46 ms	194 bytes	32 bytes			
1 Fuzzed		400 Bad Request		96 ms	194 bytes	32 bytes			kevin mitnick?, 123456
5 Fuzzed		400 Bad Request		48 ms	194 bytes	32 bytes			kevin mitnick?, 123456789
6 Fuzzed		400 Bad Request		35 ms	194 bytes	32 bytes			kevin mitnick?, 12345

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 😞