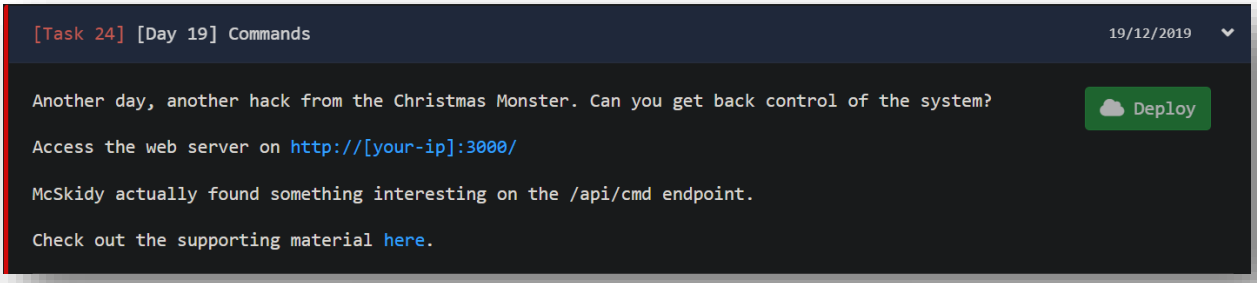
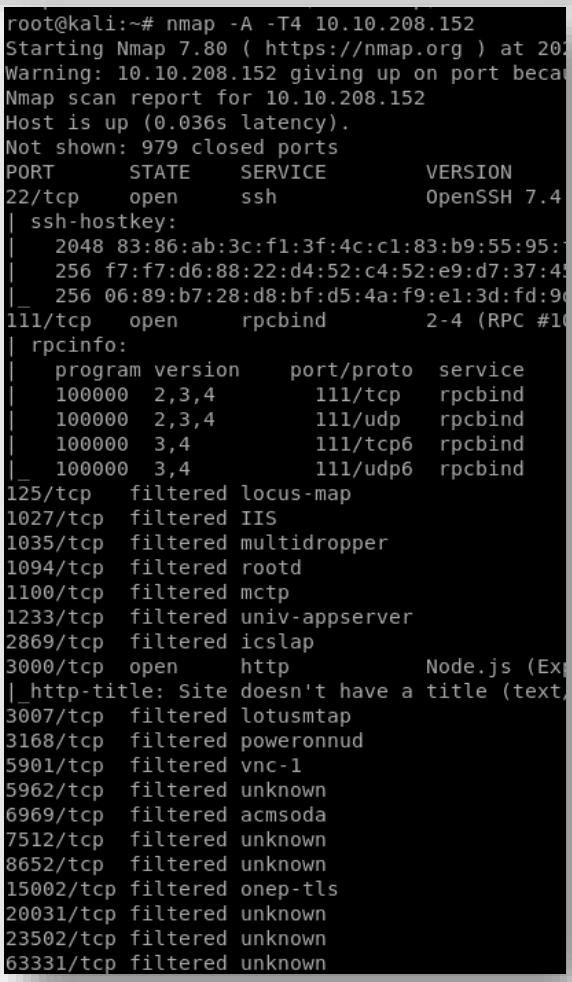
https://docs.google.com/document/d/1W65iKmUMtz-srteErhrGFJkWBXJ4Xk5PYlCZVMlZgs8/edit

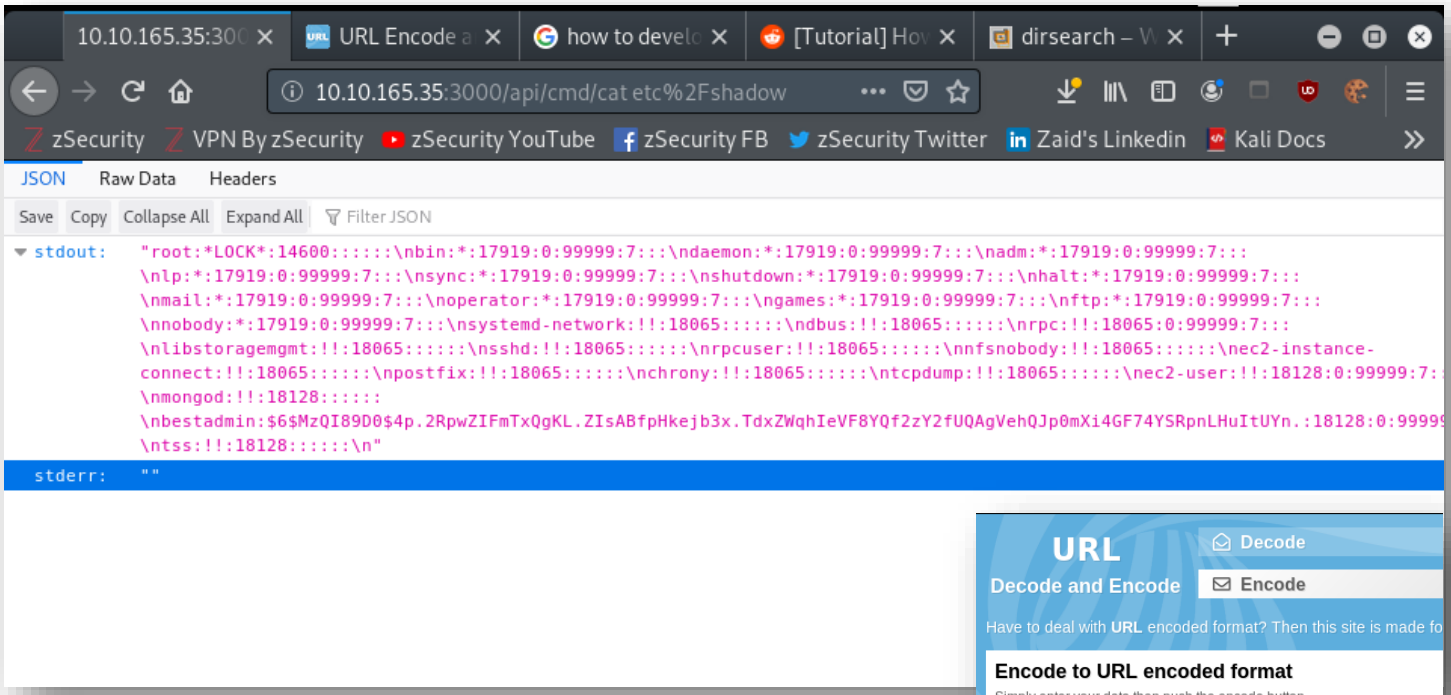


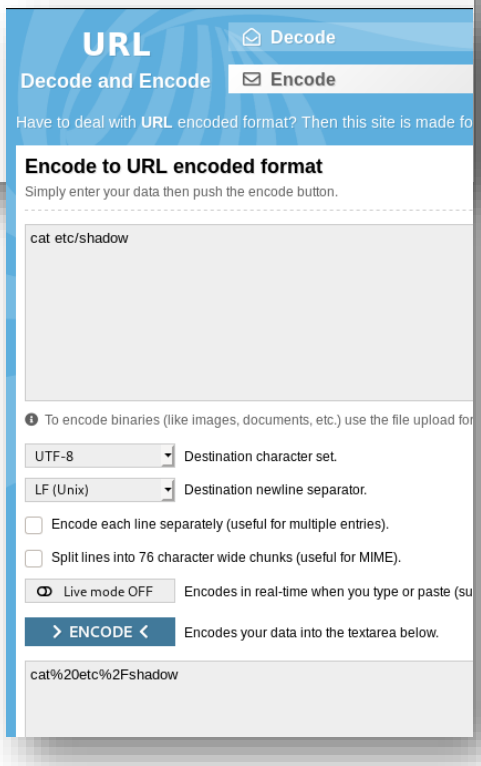


- Nmap shows available ports and services on the machine

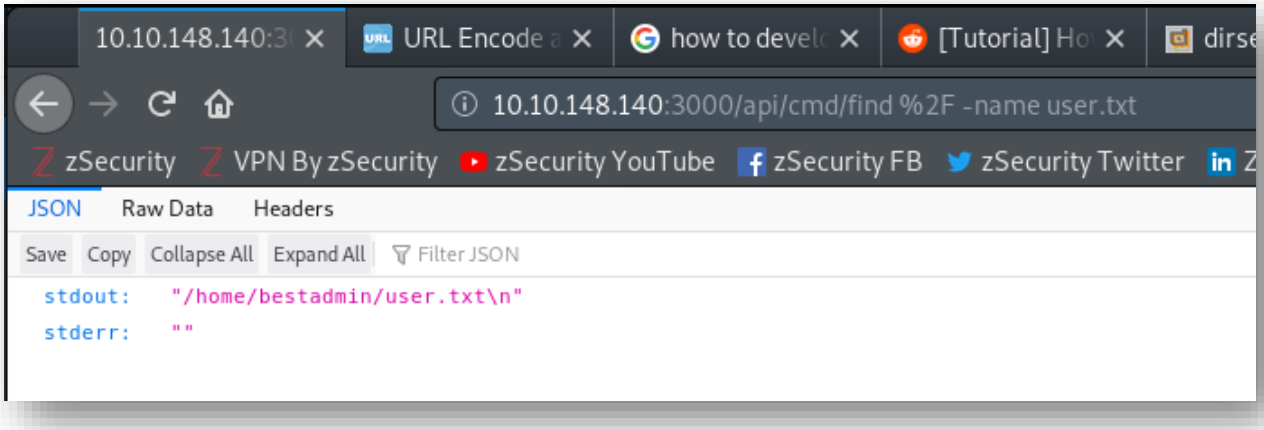
Objective

1. **What are the contents of the user.txt file?**
   - I just spent an hour vuln-scanning and brute forcing directories before I re-read the instructions. /api/cmd/…
   - So a quick test of <machine_ip>:3000/api/cmd/ls returns the contents of the working directory of the web server
   - Lets test if we have root access and able to view the /etc/shadow file





- Use a URL encoder to convert ‘cat etc/shadow’ to correct format that server expects
- Boom, we get the password hash for the bestadmin account!
- ==========
- So I spent a while with hashcat, trying to perform dictionary attack with various wordlists but cannot crack the password. Must not be in a wordlist(that I can find).
- Lets try and find the file with find command
    - Find / -name user.txt
    - URL encoded: find%20%2F%20-name%20user.txt



- Then we can inject the command `cat /home/bestadmin/user.txt` to get the flag
- 5W7WkjxBWwhe3RNsWJ3Q