

[Task 24] [Day 19] Commands

19/12/2019

Another day, another hack from the Christmas Monster. Can you get back control of the system?

Access the web server on [http://\[your-ip\]:3000/](http://[your-ip]:3000/)

McSkidy actually found something interesting on the /api/cmd endpoint.

Check out the supporting material [here](#).

Deploy

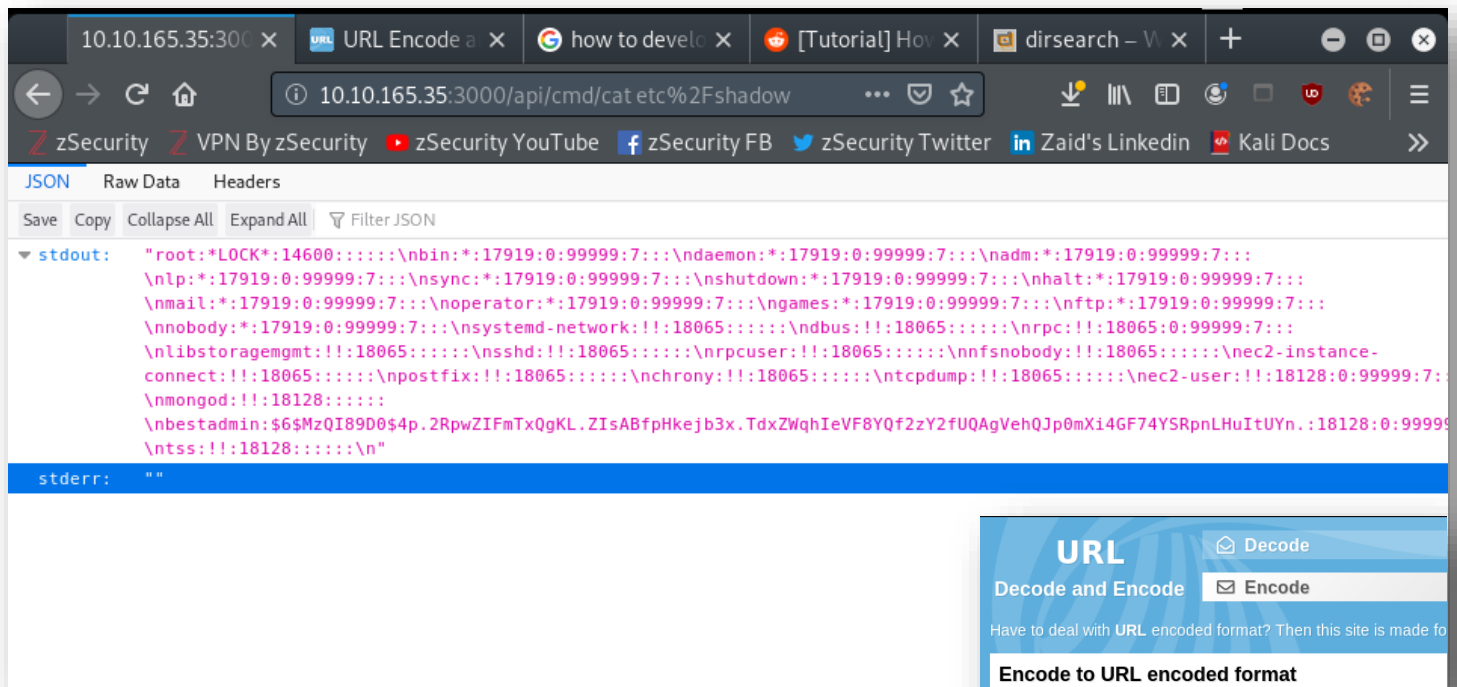
```
root@kali:~# nmap -A -T4 10.10.208.152
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-19 19:12:00
Warning: 10.10.208.152 giving up on port because no response after 10s
Nmap scan report for 10.10.208.152
Host is up (0.036s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.4p1 Ubuntu
| ssh-hostkey:
|   2048 83:86:ab:3c:f1:3f:4c:c1:83:b9:55:95:71:0d:00:00:00
|   256 f7:f7:d6:88:22:d4:52:c4:52:e9:d7:37:45:14:00:00:00
|_  256 06:89:b7:28:d8:bf:d5:4a:f9:e1:3d:fd:90:00:00:00
111/tcp   open  rpcbind      2-4 (RPC #100)
| rpcinfo:
|   program version    port/proto  service
|   100000   2,3,4      111/tcp     rpcbind
|   100000   2,3,4      111/udp     rpcbind
|   100000   3,4        111/tcp6    rpcbind
|   100000   3,4        111/udp6    rpcbind
|_
125/tcp   filtered locus-map
1027/tcp   filtered IIS
1035/tcp   filtered multidropper
1094/tcp   filtered rootd
1100/tcp   filtered mctp
1233/tcp   filtered univ-appserver
2869/tcp   filtered icslap
3000/tcp   open  http         Node.js (Express)
|_ http-title: Site doesn't have a title (text/html)
3007/tcp   filtered lotusmtap
3168/tcp   filtered poweronnud
5901/tcp   filtered vnc-1
5962/tcp   filtered unknown
6969/tcp   filtered acmsoda
7512/tcp   filtered unknown
8652/tcp   filtered unknown
15002/tcp  filtered onep-tls
20031/tcp  filtered unknown
23502/tcp  filtered unknown
63331/tcp  filtered unknown
```

- Nmap shows available ports and services on the machine

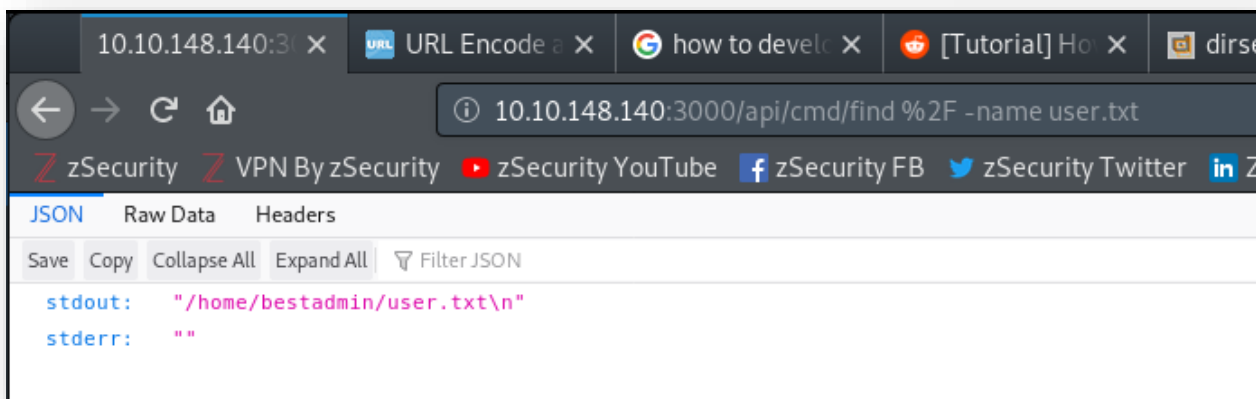
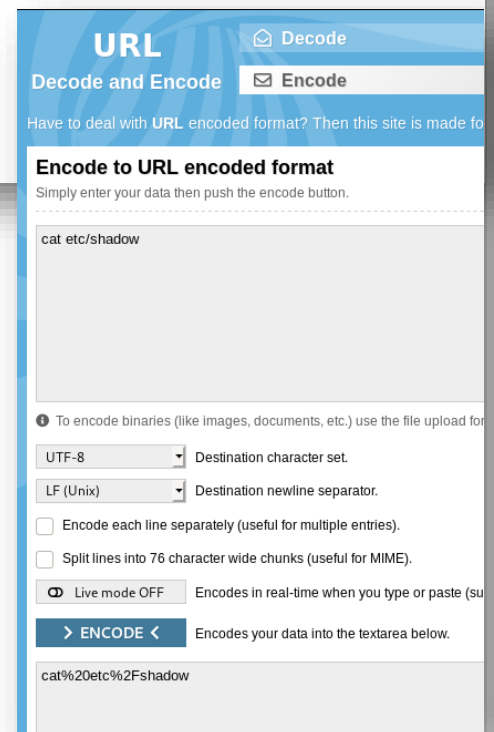
Objective

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/lis 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
- **5W7WkxjBWwhe3RNsWJ3Q**