

0.1 example

0.1.1 Enumeration

Table 1: Service enumeration example

example	
Type	open ports
TCP	1,2,3
UDP	23,42
Linux OS Soft XP	42.42.42.42

0.1.2 Exploitation

Used Vulnerability: CVE-123-42 "Stupid Idiot User"

abc

Vulnerability Explanation:

BLA BLA WRITE SOMETHING HERE

```
1 Kali prep:
3 Modifications in the exploit
5 Running the exploit
7 Escaping the low priv shell:
```

Listing 1: Exploitation of example

Exploit execution

Quote: "The execution of the exploit. This can be a URL that is browsed to, running a python script, executing a Metasploit module, etc. You do not need to screenshot every step, just the last step you took when sending your low privilege exploit."

Figure 1: Exploitation of example

Privilege Escalation

Low Priv Shell "Local"

Quote: "The output of the successful low privilege exploit from #1, the output of "ifconfig/ipconfig", and the contents of the local.txt file. "

Figure 2: Local shell of example

Priv esc exploit

Quote: " The execution of the privilege escalation exploit. This can be a URL that is browsed to, running a Python script, executing a Metasploit module, etc. You do not need to screenshot every step, just the last step you took when sending your privilege escalation exploit."

Figure 3: Priv escalation exploit of example

Proof and Post escalation

1 **Post exploitation commands run:**

Listing 2: Post exploitation of example

Proof

Quote: (for non Priv esc) "The output of the successful exploit from #1, the output of "ifconfig/ipconfig", and the contents of the proof.txt file"

Quote:"The output of the successful privilege escalation exploit from #3, the output of "ifconfig/ipconfig", and the contents of the proof.txt file"

Figure 4: Proof of example

0.1.3 DeepThought

Enumeration

Table 2: Service enumeration DeepThought

DeepThought	
Type	open ports
TCP	1,2,3
UDP	23,42
Earth	42.42.42.23

Exploitation

Used Vulnerability: Vogons

BLA BLA WRITE SOMETHING HERE

Vulnerability Explanation:

BLA BLA WRITE SOMETHING HERE

```
2 Kali prep:
3
4 Modifications in the exploit
5 PANIC PANIC PANIC
6 Running the exploit
7
8 Escaping the low priv shell:
```

Listing 3: Exploitation of DeepThought

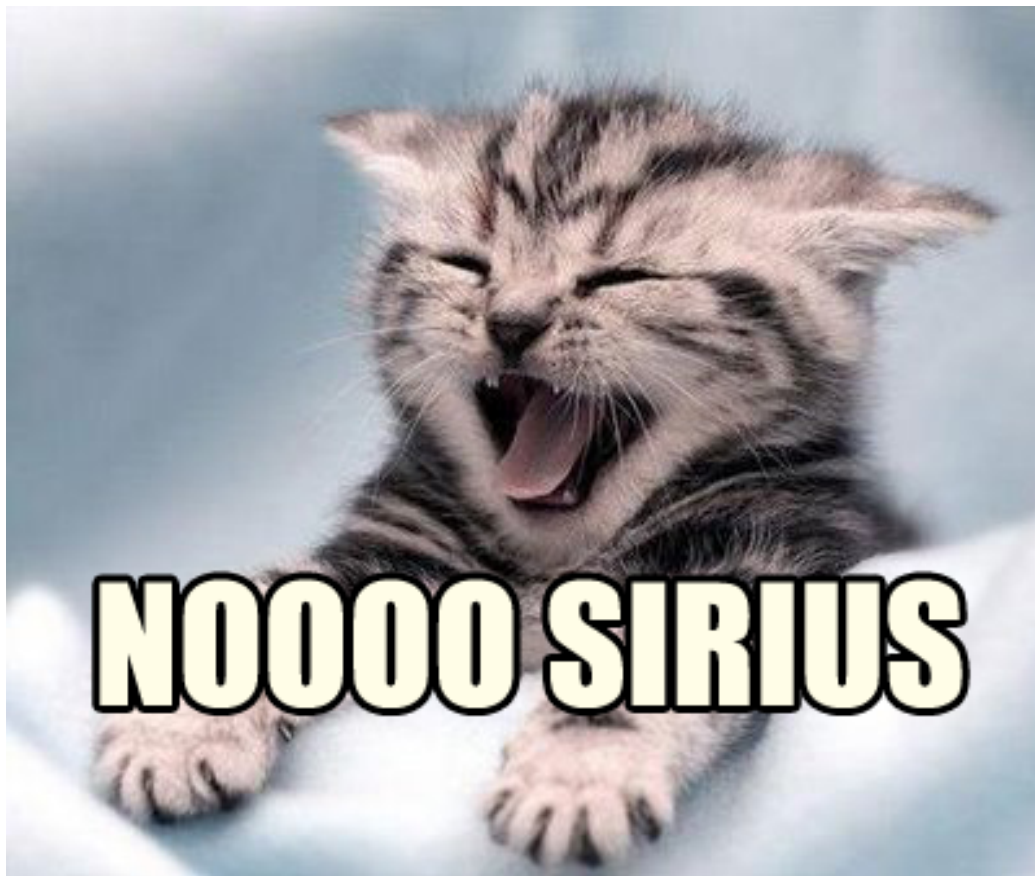


Figure 5: Exploitation of DeepThought

Privilege Escalation



Figure 6: Local shell of DeepThought



Figure 7: Priv escalation exploit of DeepThought

Proof and Post escalation

1 Post exploitation commands run:

Listing 4: Post exploitation of DeepThought

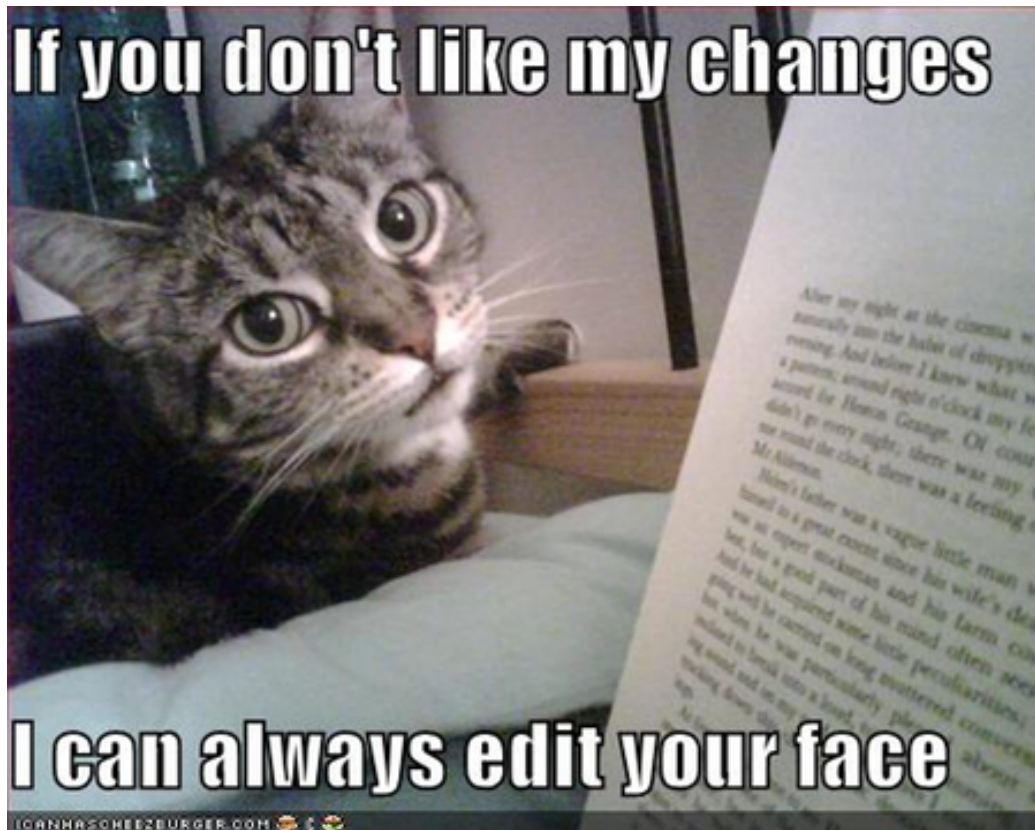


Figure 8: Proof of DeepThought