Offensive Security

Penetration Test Report for Internal Lab and Exam

v.1.1

john@doe.com

OSID: OS-11111

Contents

1 Example

1.1 Service Enumeration

Example	
Type	Open ports
TCP	1,2,3
UDP	23,42
Linux OS Soft XP	**42.42.42.42**

Table 1: Service enumeration Example

1.2 Remote Access Exploitation

Vulnerability Exploited: CVE-123-42 „Stupid Idiot User“

Vulnerability Explanation:

Vulnerability Fix: The publishers of Human have issued a patch to fix this known issue.

Severity: **Critical**

Proof of Concept: Modifications to the existing exploit was needed and is highlighted in red.

```
SELECT * FROM login WHERE id = 1 or 1=1 AND user LIKE "%root%"

if (x = y):
    space indent
    tab indent

In the code section :
Green Text
Red Text
Blue Text
```

Listing 1: Exploitation of Example

./hosts/Example/1-remote-exploit.png

Figure 1: Exploitation of Example

Proof of remote access: The remote access can be proven with the following command:

```
hostname && id && ifconfig && cat local.txt
```

Listing 2: Post exploitation of Example with low privileges

```
./hosts/Example/2-local.png
```

Figure 2: Proof of remote access to Example

1.3 Privilege Escalation

Vulnerability Exploited: CVE-123-43 „Very Stupid Idiot User Again“

Vulnerability Explanation:

Vulnerability Fix: The publishers of Human have issued a patch to fix this known issue.

Severity: Critical

Proof of Concept: Modifications to the existing exploit was needed and is highlighted in red.


```
SELECT * FROM login WHERE id = 1 or 1=1 AND user LIKE "%root%"
In the code section :
Green Text
Red Text
Blue Text
```

Listing 3: Exploitation of Example

./hosts/Example/3-privesc-exploit.png

Figure 3: Privilege escalation exploit of Example

Proof of successful privilege escalation: The successful privilege escalation can be proven with the following command:

```
hostname && id && ifconfig && cat proof.txt
```

Listing 4: Post exploitation of Example

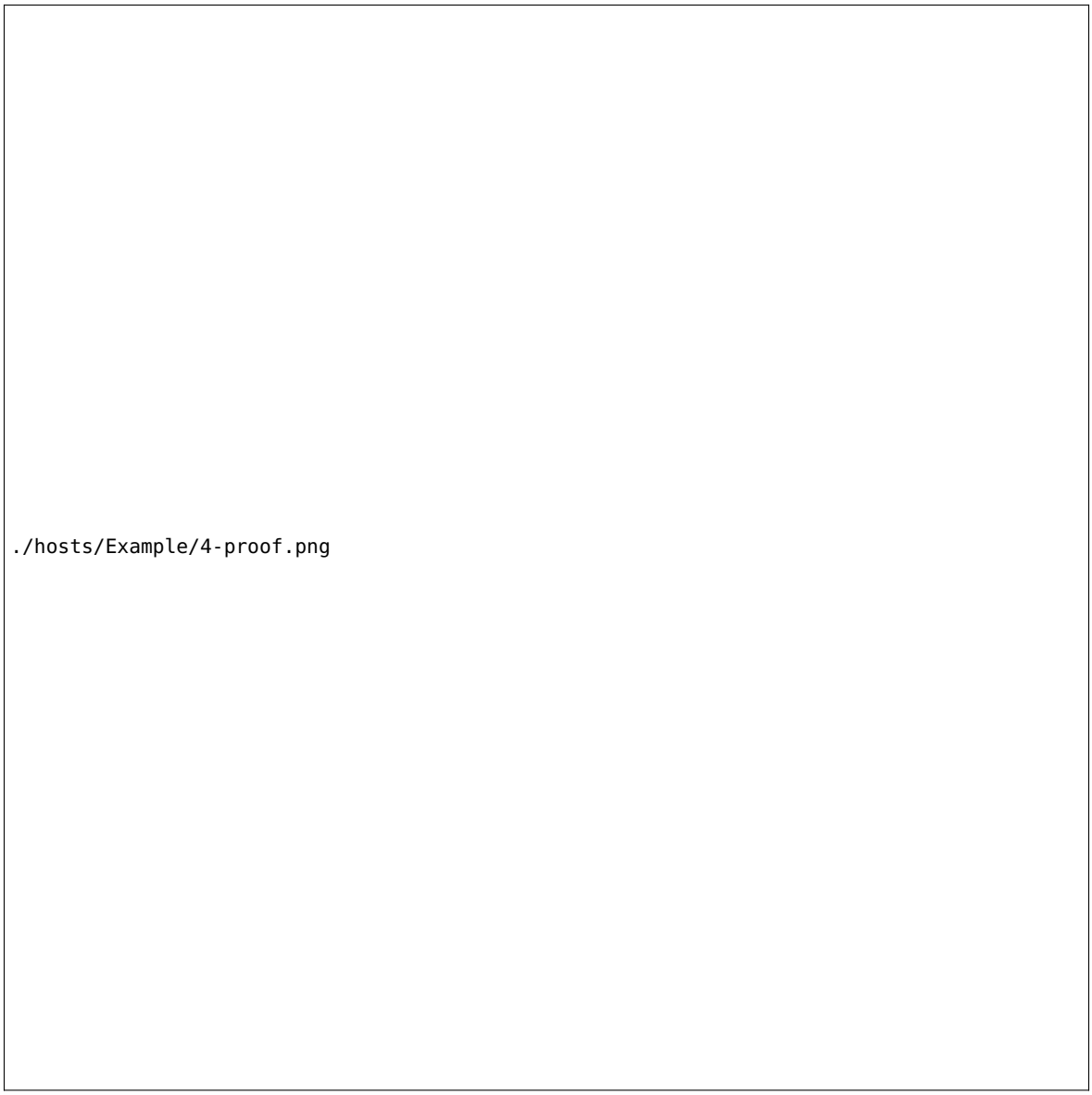

Figure 4: Proof of successful privilege escalation on Example

2 DeepThought

2.1 Service Enumeration

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

Table 2: Service enumeration DeepThought

2.2 Remote Access Exploitation

Vulnerability Exploited: Vogons

Vulnerability Explanation: BLA BLA WRITE SOMETHING HERE

Severity: **Critical**

Proof of Concept: Some text here

```
Kali prep:

Modifications in the exploit
PANIC PANIC PANIC
Running the exploit

Escaping the low priv shell:
```

Listing 5: Exploitation of DeepThought

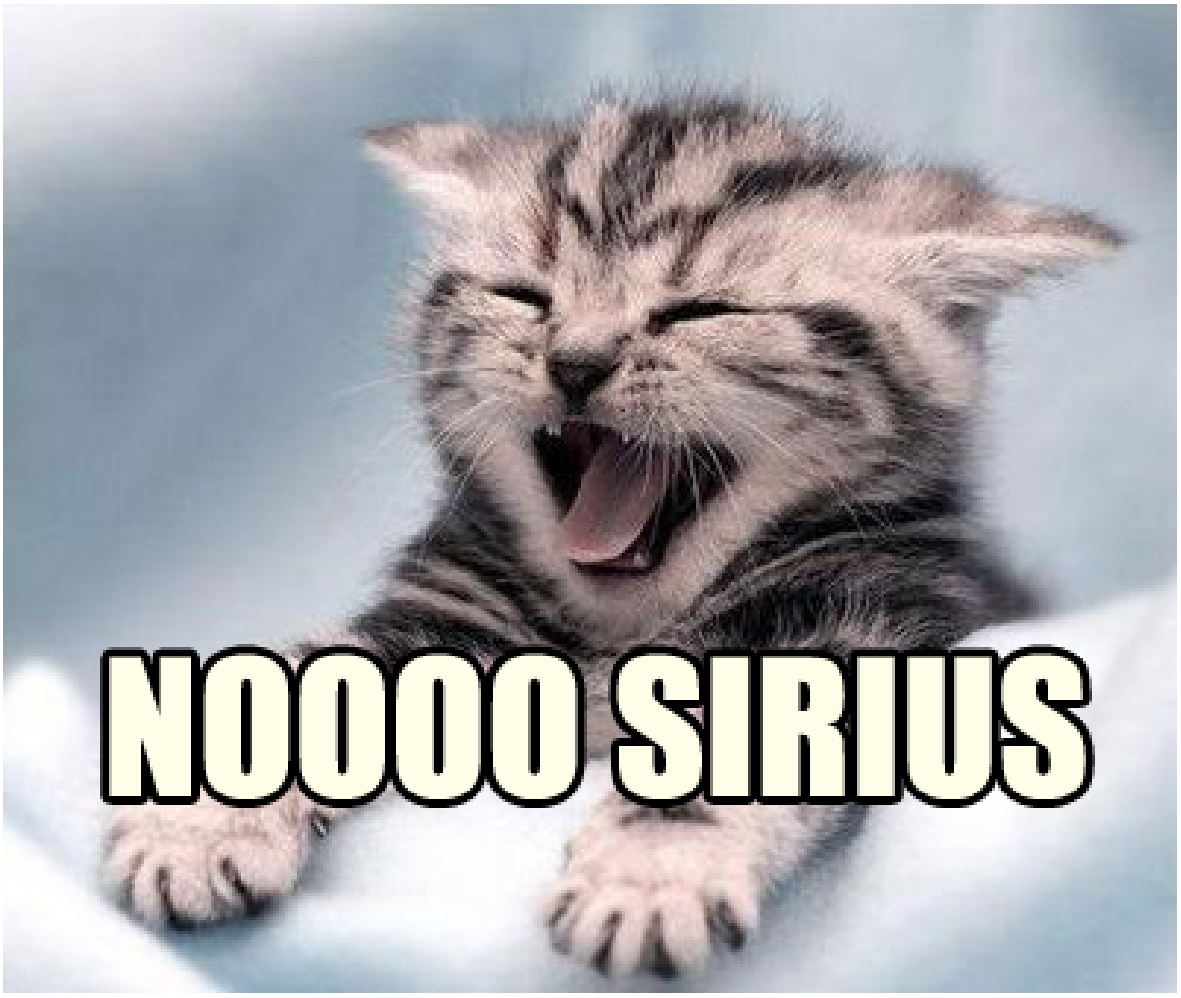

Figure 5: Exploitation of DeepThought

2.2.1 Privilege Escalation

Figure 6: Local shell of DeepThought

Figure 7: Priv escalation exploit of DeepThought

2.2.2 Proof and Post escalation

```
Post exploitation commands run:
```

Listing 6: Post exploitation of DeepThought

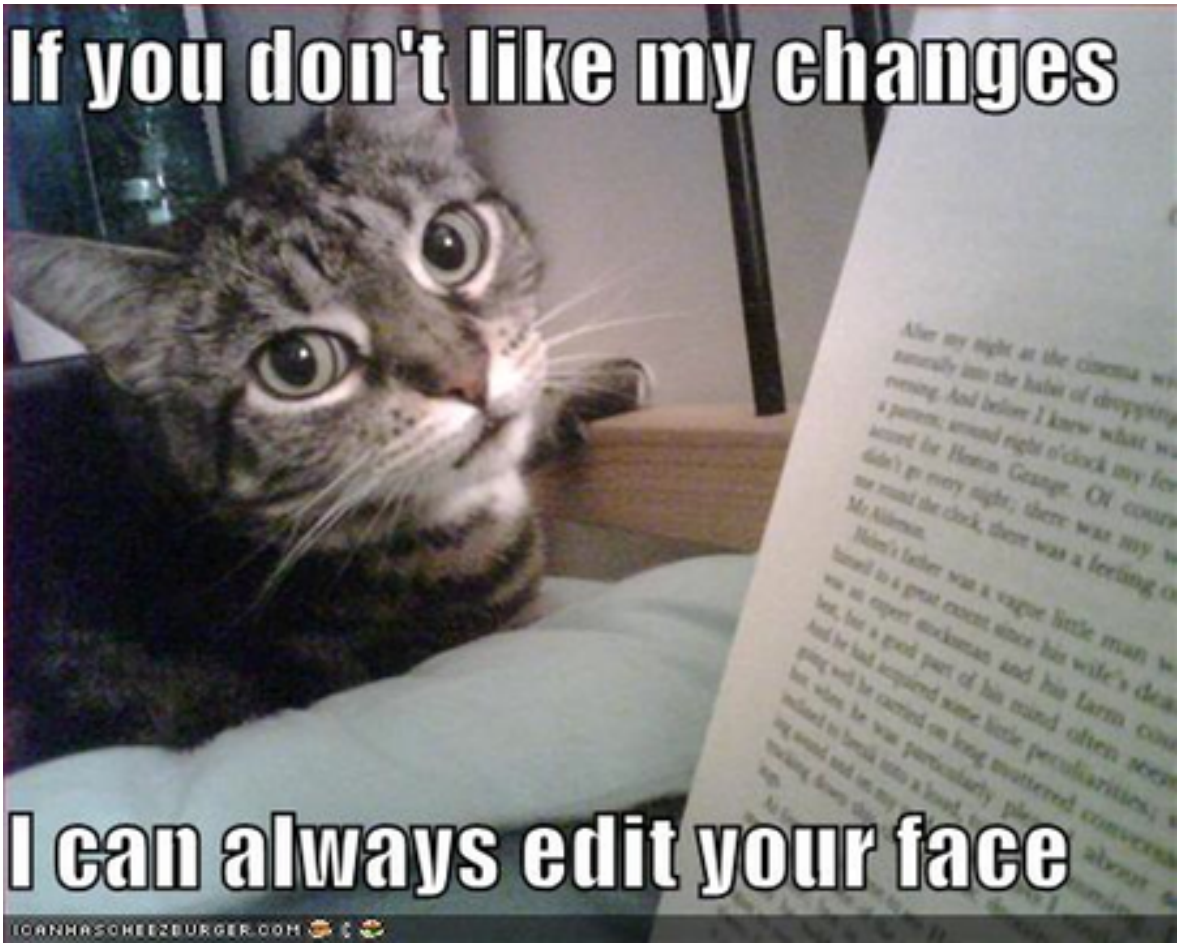

Figure 8: Proof of DeepThought