Offensive Security

Penetration Test Report for
Internal Lab and Exam

John Doe

john@doe.com

OSID: OS-11111

February 7, 2019

Contents

1 Example **3**
1.1 Service Enumeration 3
1.2 Remote Access Exploitation 3
1.3 Privilege Escalation 5

2 DeepThought **7**
2.1 Service Enumeration 7
2.2 Remote Access Exploitation 7
2.2.1 Privilege Escalation 9
2.2.2 Proof and Post escalation 10

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: BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA

Severity: Critical

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

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

Listing 1: Exploitation of Example

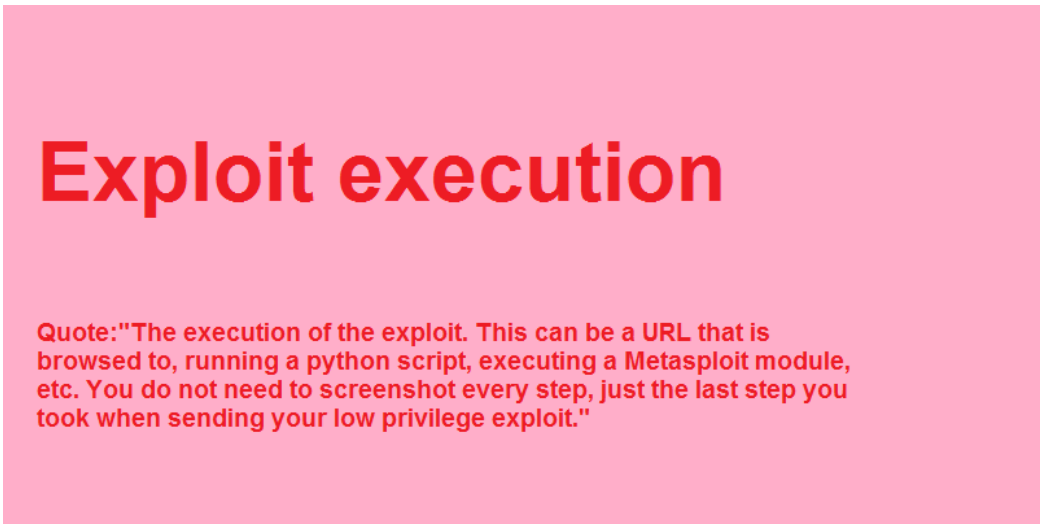

Figure 1: Exploitation of Example

Screenshot:

Proof:

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

Listing 2: Proof of local shell on Example

Figure 2: Local shell of Example

1.3 Privilege Escalation

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

Vulnerability Explanation: BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA BLA WRITE SOMETHING HERE BLA

Severity: Critical

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

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

Listing 3: Exploitation of Example

Figure 3: Priv escalation exploit of Example

Screenshot:

Proof:

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

Listing 4: Post exploitation of Example

Figure 4: Proof of 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:

```
Kali prep:

Modifications in the exploit
PANIC PANIC PANIC
Running the exploit

Escaping the low priv shell:
```

Listing 5: Exploitation of DeepThought

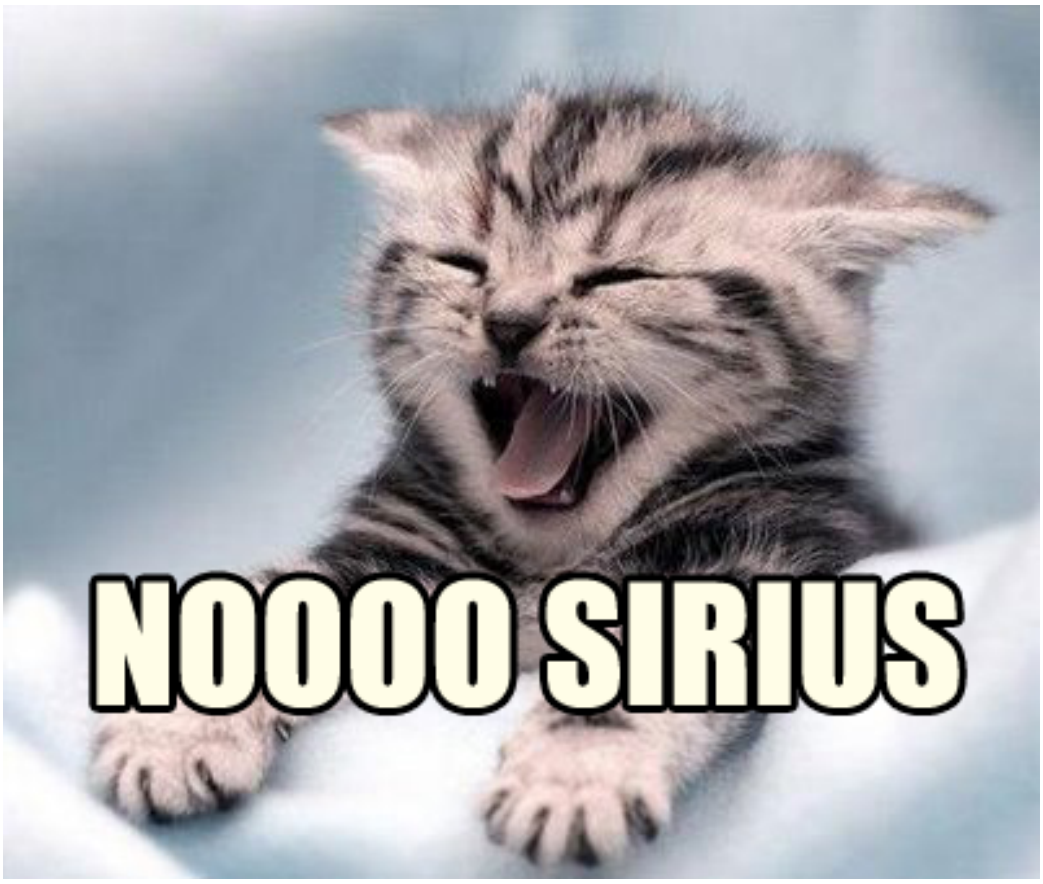

Figure 5: Exploitation of DeepThought

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

```
1 Post exploitation commands run:
```

Listing 6: Post exploitation of DeepThought

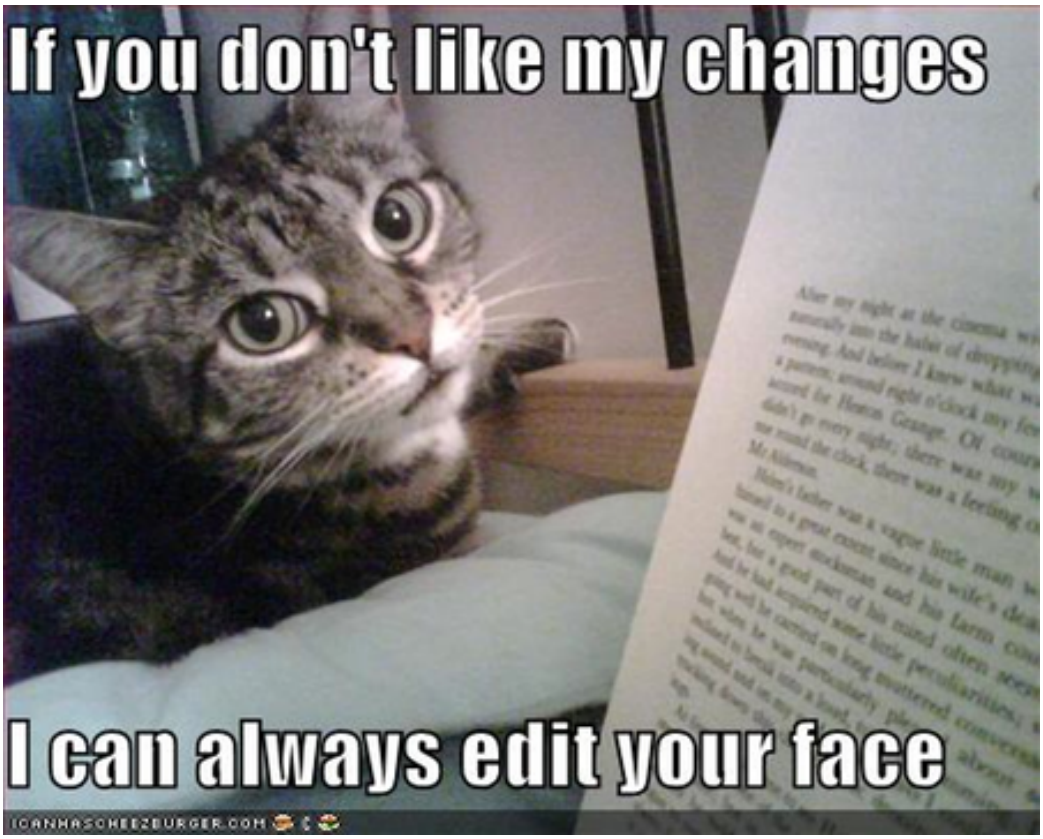

Figure 8: Proof of DeepThought