Offensive Security

Penetration Test Report for

Internal Lab and Exam

John Doe

john@doe.com

OSID: OS-11111

March 28, 2019

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: Human is vulnerable to a remote code execution. Attackers can use this vulnerability to access the system from a remote location. When performing the penetration test, John Doe noticed an outdated version of Human running from the service enumeration phase. A public exploit[1] was available and could be used without modification. A targeted attack was performed on the system, which gave John Doe low privilege access to the system.

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.

```
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

[1] https://www.exploit-db.com/exploits/9623

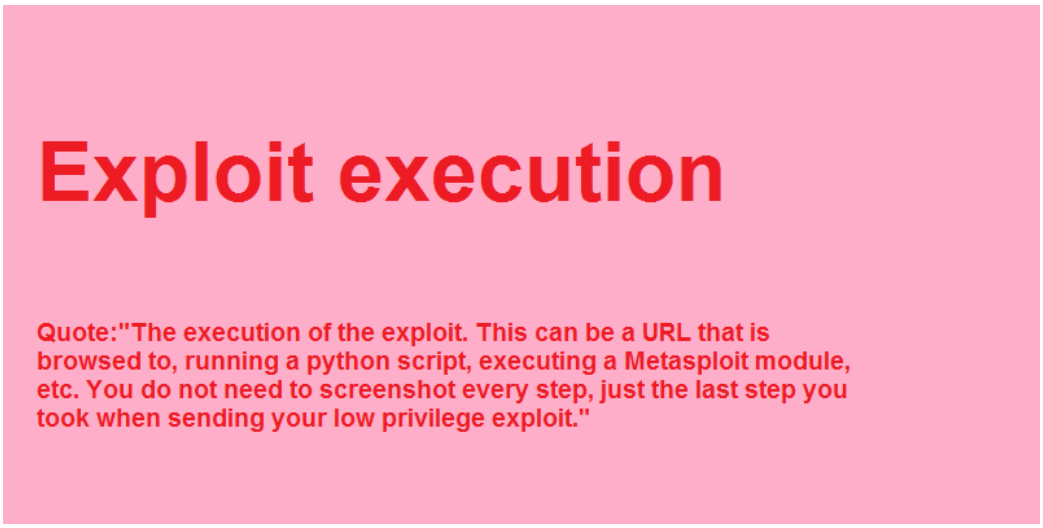

Figure 1: Exploitation of Example

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

Listing 2: Post exploitation of Example with low privileges

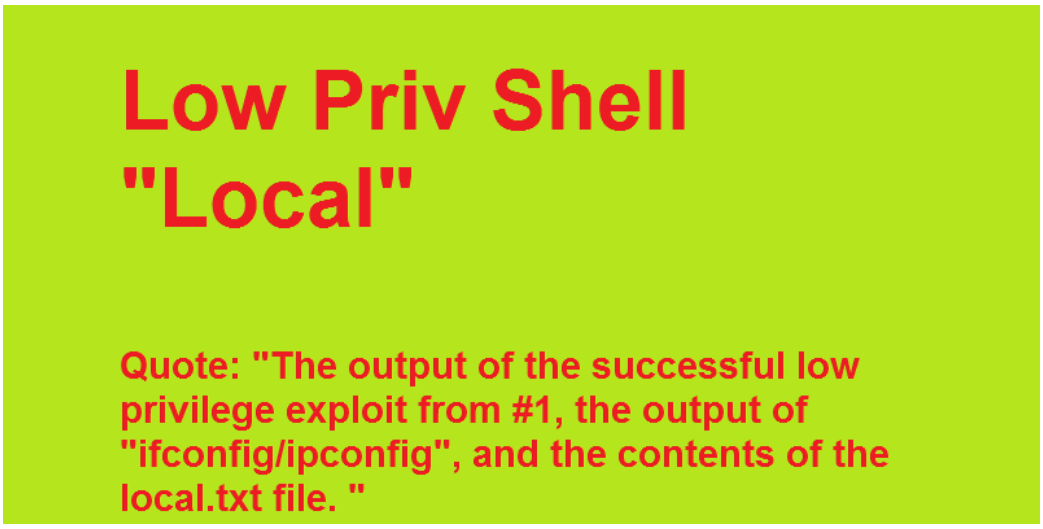

Figure 2: Proof of remote access to Example

1.3 Privilege Escalation

Proof of remote access:

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

Vulnerability Explanation: Human is subject to a bug in XYZ. Attackers can use this vulnerability to perform a privilege escalation and take completely control over the system. When performing the penetration test, John Doe noticed an outdated version of Human. A public exploit[2] was available and could be used without modification. A targeted attack was performed on the system, which gave John Doe full administrative access over the system.

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

Figure 3: Privilege escalation exploit of Example

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

Listing 4: Post exploitation of Example

[2] https://www.exploit-db.com/exploits/9623

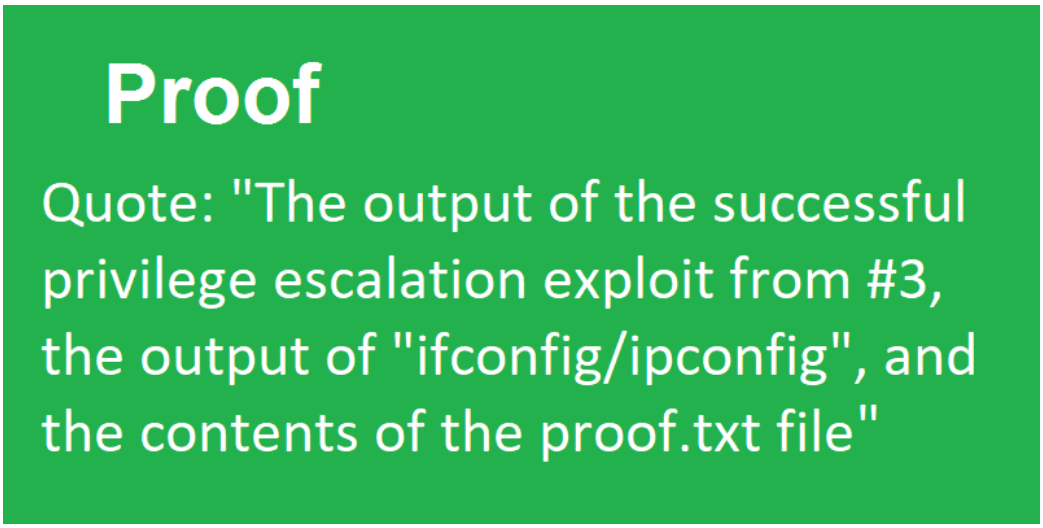

Figure 4: Proof of successful privilege escalation on Example

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**

```
1 Kali prep:

3 Modifications in the exploit
  PANIC PANIC PANIC
5 Running the exploit

7 Escaping the low priv shell:
```

Listing 5: Exploitation of DeepThought

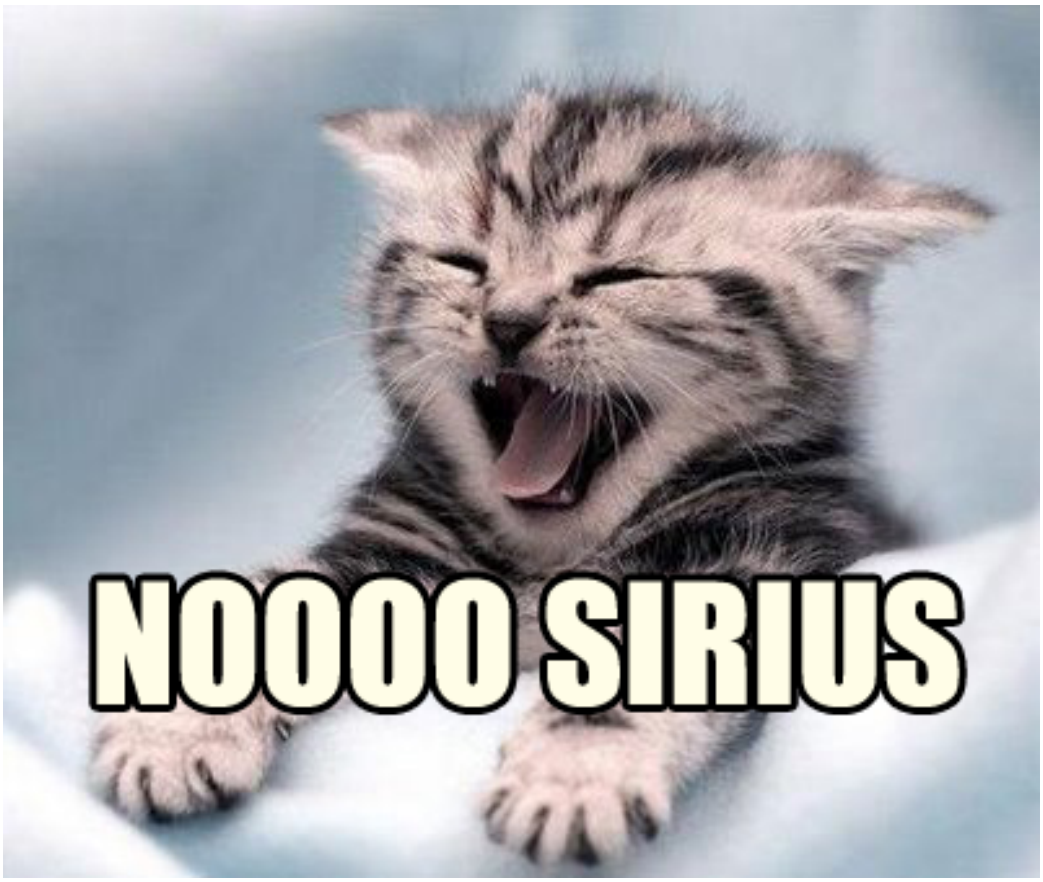

Figure 5: Exploitation of DeepThought

2.2.1 Privilege Escalation

Figure 6: Local shell of DeepThought

Figure 7: Priv escalation exploit of DeepThought

Proof of Concept:

2.2.2 Proof and Post escalation

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

Listing 6: Post exploitation of DeepThought

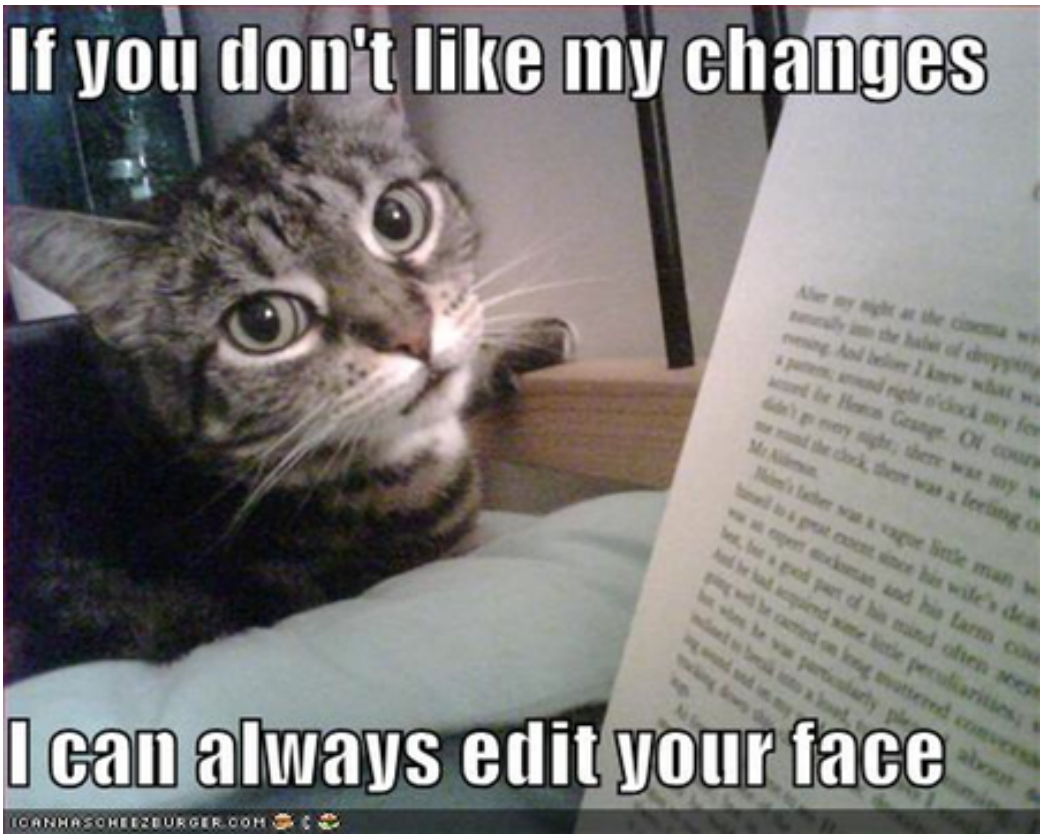

Figure 8: Proof of DeepThought