

# **Offensive Security**

## Penetration Test Report for Internal Lab and Exam

John Doe

john@doe.com

OSID: OS-11111

March 28, 2019

# Contents

<b>1</b>	<b>Example</b>	<b>3</b>
1.1	Service Enumeration . . . . .	3
1.2	Remote Access Exploitation . . . . .	3
1.3	Privilege Escalation . . . . .	4
<b>2</b>	<b>DeepThought</b>	<b>7</b>
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:** 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 When performing the penetration test, John Doe noticed an outdated version of Human running from the service enumeration phase.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<sup>1</sup> 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

---

<sup>1</sup><https://www.exploit-db.com/exploits/9623>

# 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

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

**Listing 2:** Post exploitation of Example with low privileges

# 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:** 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<sup>2</sup> 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.

```
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

## 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:** Privilege escalation exploit of Example

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

**Listing 4:** Post exploitation of Example

<sup>2</sup><https://www.exploit-db.com/exploits/9623>

# Proof

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 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

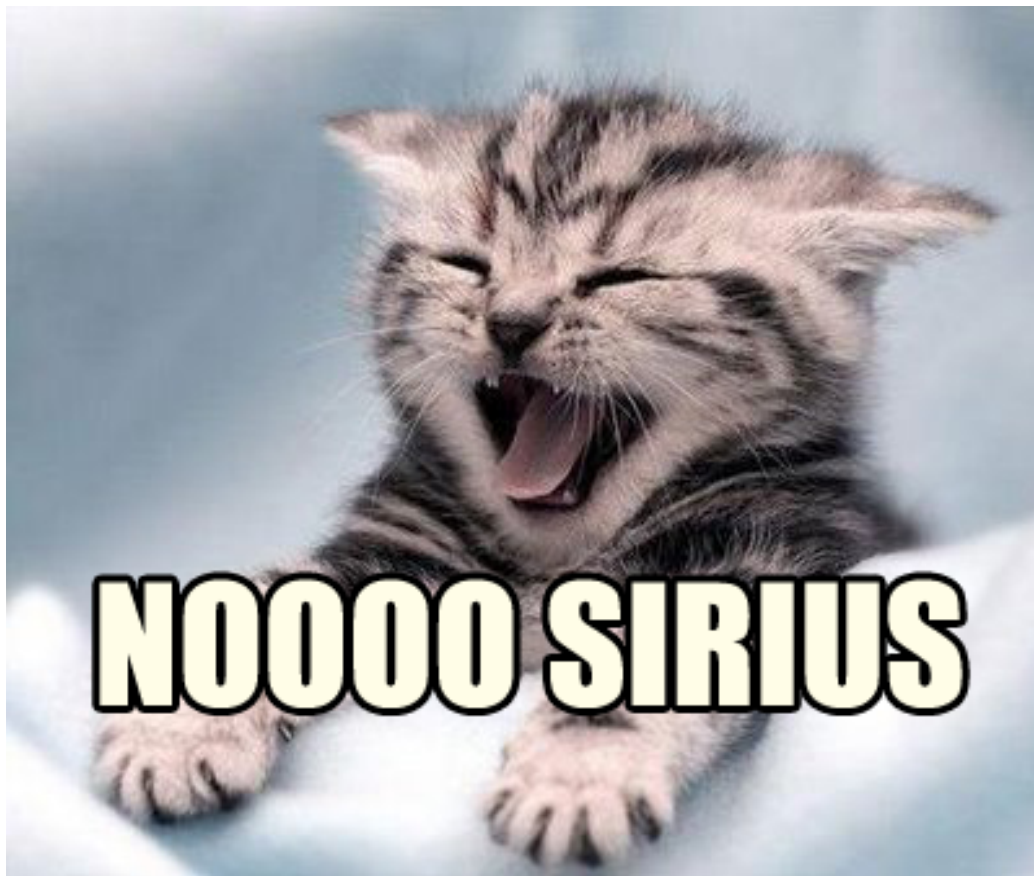
**Vulnerability Exploited:** Vogons

**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

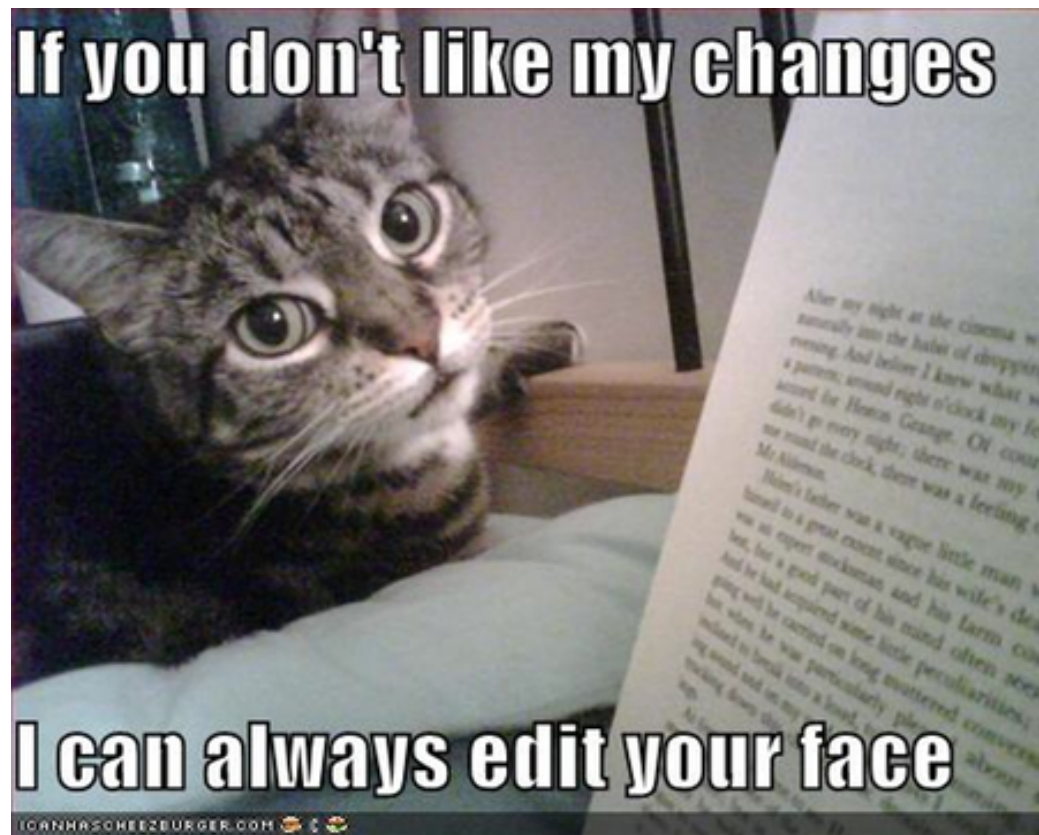


Figure 8: Proof of DeepThought