



# Università degli Studi di Salerno

Dipartimento di Informatica

*Penetration Testing and Ethical Hacking*

## **Penetration Testing Report**

---

Professore:

Arcangelo Castiglione

Candidato:

Giacomo Coccoziello

Anno Accademico 2018/2019

## **Sommario**

1. *Executive Summary*
2. *Engagement Highlights*
3. *Vulnerability Report*
4. *Remediation Report*
5. *Findings Summary*
6. *Detailed Summary*

## 1. Executive Summary

Per l'esame di "Penetration Testing and Ethical Hacking" è stata svolta un'analisi di Penetration Testing sulla macchina virtuale "Troll 1" scaricata dal sito <http://vulnhub.com>. È stato utilizzato un approccio "Gray Box", in quanto si avevano soltanto poche informazioni riguardanti l'hardware della macchina target ma non si avevano le informazioni relative al software. Inoltre, sia la macchina pentester che la macchina target comunicano utilizzando la stessa rete ("esame"). Si è cercato di analizzare quante più vulnerabilità possibili, molte delle quali non sono servite per accedere alla macchina target poiché essendo la macchina sviluppata nel 2004 alcune sono state corrette, altre rappresentano "false vulnerabilità" in quanto definite per aggirare l'obiettivo del pentester. Oltre all'analisi delle vulnerabilità, si è cercato di affrontare la sfida proposta dal sito Vulnhub, la quale richiedeva l'accesso alla macchina target come utente privilegiato (root) e la lettura del file proof.txt.

In questo report andremo a descrivere dettagliatamente tutte le vulnerabilità riscontrate sulla macchina target.

## **2. Engagement Highlights**

Come illustrato nel documento di testing non esistono particolari vincoli tra il pentester e l'utente e/o azienda , in quanto l'attività progettuale prevedeva l'analisi di una macchina virtuale scaricabile dal sito Vulnhub. Infatti, si è cercato di stressare quanto più la macchina virtuale per ottenere l'obiettivo desiderato. In riferimento alle norme legali, non è stato redatto alcun contratto "(Non-Disclosure Agreement – NDA) poiché il progetto è puramente didattico. Le uniche risorse impiegate nel processo di testing sono esclusivamente le ore di lavoro eseguite dal pentester e le risorse del PC. La durata del processo di testing è di circa 20 giorni.

### **3. Vulnerability Report**

Durante il processo di testing sono state trovate numerose vulnerabilità. Tali vulnerabilità sono state ottenute utilizzando sia la scansione manuale eseguita sulle informazioni ricevute da *nmap* (strumento utilizzato in questo caso per effettuare il port scanning) sia la scansione automatica per avere un quadro più raffinato delle vulnerabilità all'interno della macchina target. In questo caso è stato utilizzato OpenVas e Nikto 2 (per rilevare ed analizzare le vulnerabilità di sicurezza causate da errori di configurazione del server e applicazioni server obsolete).

## 4. Remediation Report

In questa sezione andremo a definire i rimedi da apportare nell'analisi di testing:

- Aggiornare la versione di Apache, in modo da risolvere il problema di alcune vulnerabilità note per le vecchie versioni.
- Evitare di attribuire ai file nomi che corrispondono alle informazioni memorizzate all'interno (es: Pass.txt)
- I dati privati e/o fondamentali che vengono scambiati tra due macchine devono essere cifrati, in modo da rendere la trasmissione incomprensibile oppure inviare pacchetti falsi insieme a quelli reali per ingannare un eventuale osservatore.
- Utilizzare per tutti gli utenti password più complesse, impiegando combinazioni di lettere maiuscole, minuscole, numeri e simboli.

## 5. Findings Summary

In questa sezione vengono mostrate le criticità definite nel documento di testing. Per ogni vulnerabilità andremo a spiegare:

- I punti di forza e di debolezza che sono stati rilevati
- Sommario della valutazione dei rischi

Le varie vulnerabilità riscontrate verranno valutate con la scala CVSS v2.0 Ratings.

<u>Severity</u>	<u>Base Score Range</u>
Low	0.0 – 3.9
Medium	4.0 – 6.9
High	7.0 – 10.0

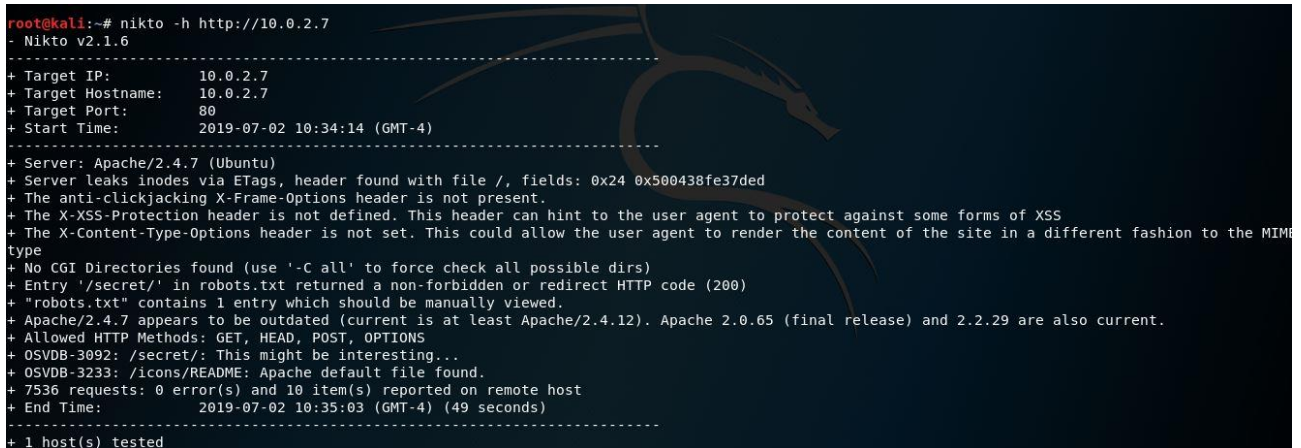
Per ottenere le vulnerabilità sono stati utilizzati vari strumenti tra cui:

- Openvas

Vulnerability	Severity	QoD	Host	Location
CVE-2017-7679	7.5		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2014-0226	6.8		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2017-15715	6.8		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2018-1312	6.8		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2017-9788	6.8		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2013-6438	5.0		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2014-0098	5.0		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2014-0231	5.0		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2014-3523	5.0		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2016-0736	5.0		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2016-2161	5.0		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2016-8743	5.0		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2017-15710	5.0		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2017-9798	5.0		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2018-17199	5.0		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2015-1419	5.0		10.0.2.7	cpe:/a:beasts:vsftpd:3.0.2
CVE-2014-0117	4.3		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2014-0118	4.3		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2014-8109	4.3		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2015-3185	4.3		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2016-4975	4.3		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2018-1283	3.5		10.0.2.7	cpe:/a:apache:http_server:2.4.7
CVE-2016-8612	3.3		10.0.2.7	cpe:/a:apache:http_server:2.4.7

e le vulnerabilità totali riscontrate con OpenVas sono 23.

- Nikto 2: per rilevare ed analizzare le vulnerabilità di sicurezza causate da errori di configurazione del server e applicazioni server obsolete.

A terminal window showing the output of a Nikto v2.1.6 scan on the target IP 10.0.2.7. The scan identifies several security issues, including missing security headers (X-Frame-Options, X-XSS-Protection, X-Content-Type-Options), outdated Apache version (2.4.7), and directory listings. The scan completed with 7536 requests and 10 items reported on the remote host.

```
root@kali:~# nikto -h http://10.0.2.7
- Nikto v2.1.6
-----
+ Target IP:      10.0.2.7
+ Target Hostname: 10.0.2.7
+ Target Port:    80
+ Start Time:     2019-07-02 10:34:14 (GMT-4)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x24 0x500438fe37ded
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME
type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/secret/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3092: /secret/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7536 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:      2019-07-02 10:35:03 (GMT-4) (49 seconds)
-----
+ 1 host(s) tested
```

- Dirb: per ottenere informazioni aggiuntive sulle directory della macchina target.



```
root@kali:~# dirb http://10.0.2.7
-----
DIRB v2.22
By The Dark Raver
-----
New Folder: 37292.c
START_TIME: Sat Jul 13 04:21:34 2019
URL_BASE: http://10.0.2.7/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
phpmeter.php
GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.7/ ----
+ http://10.0.2.7/index.html (CODE:200|SIZE:36)
+ http://10.0.2.7/robots.txt (CODE:200|SIZE:31)
==> DIRECTORY: http://10.0.2.7/secret/
+ http://10.0.2.7/server-status (CODE:403|SIZE:288)

---- Entering directory: http://10.0.2.7/secret/ ----
+ http://10.0.2.7/secret/index.html (CODE:200|SIZE:37)

-----
END_TIME: Sat Jul 13 04:21:51 2019
DOWNLOADED: 9224 - FOUND: 4
```

## 6. Detailed Summary

In questa sezione andremo a descrivere nel dettaglio le principali vulnerabilità che abbiamo ottenuto durante il processo di testing mostrando una breve descrizione ed il rischio ad essa associato. Le informazioni legate alle vulnerabilità che andremo a definire sono reperibili sul sito: <https://nvd.nist.gov/vuln/>

In primis, andremo a definire la vulnerabilità ottenuta con OpenVas con rischio “High”

### ➤ CVE-2017-7679

In Apache httpd 2.2 < 2.2.33 e 2.4 < 2.4.26, mod\_mime può leggere soltanto un byte dopo che il buffer è terminato quando si invia una risposta Content-type dannosa.

#### CVE-2017-7679 Detail


##### MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

#### Current Description

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod\_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

**Source:** MITRE

 [Hide Analysis Description](#)

### CVSS v2.0 Severity and Metrics:

**Base Score:** 7.5 HIGH

**Vector:** (AV:N/AC:L/Au:N/C:P/I:P/A:P) (V2 legend)

**Impact Subscore:** 6.4

**Exploitability Subscore:** 10.0

**Access Vector (AV):** Network

**Access Complexity (AC):** Insufficient\_Info

**Authentication (AU):** None

**Confidentiality (C):** Partial

**Integrity (I):** Partial

**Availability (A):** Partial

**Additional Information:**

Allows unauthorized disclosure of information

Allows unauthorized modification

Allows disruption of service

## ➤ CVE-2014-0226

La race condition nel modulo Apache http server prima delle versione 2.4.10, consentono ai malintenzionati attacchi denial of service oppure di ottenere credenziali sensibili, eseguire codice arbitrario, tramite una richiesta predisposta che genera errori all'interno della funzione status\_handler in modulus/generators/mod\_statuc.c e lua\_ap\_scoreboard\_worker in modules/lua/lua\_request.c

## 🚩 CVE-2014-0226 Detail

### MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

### Current Description

Race condition in the mod\_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status\_handler function in modules/generators/mod\_status.c and the lua\_ap\_scoreboard\_worker function in modules/lua/lua\_request.c.

**Source:** MITRE

[+View Analysis Description](#)

## Impact

### CVSS v2.0 Severity and Metrics:

**Base Score:** 6.8 MEDIUM

**Vector:** (AV:N/AC:M/Au:N/C:P/I:P/A:P) (V2 legend)

**Impact Subscore:** 6.4

**Exploitability Subscore:** 8.6

---

**Access Vector (AV):** Network

**Access Complexity (AC):** Medium

**Authentication (AU):** None

**Confidentiality (C):** Partial

**Integrity (I):** Partial

**Availability (A):** Partial

**Additional Information:**

Allows unauthorized disclosure of information

Allows unauthorized modification

Allows disruption of service

## ➤ CVE-2015-1419

La vulnerabilità non specificata in vsftpd 3.0.2 e versioni precedenti consente ai malintenzionati di aggirare le restrizioni di accesso attraverso vettori sconosciuti, relativi all'analisi del file deny\_file.

## 🚩 CVE-2015-1419 Detail

### MODIFIED

---

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

## Current Description

Unspecified vulnerability in vsftpd 3.0.2 and earlier allows remote attackers to bypass access restrictions via unknown vectors, related to deny\_file parsing.

**Source:** MITRE

[+View Analysis Description](#)

## Impact

### CVSS v2.0 Severity and Metrics:

**Base Score:** 5.0 MEDIUM

**Vector:** (AV:N/AC:L/Au:N/C:N/I:P/A:N) (V2 legend)

**Impact Subscore:** 2.9

**Exploitability Subscore:** 10.0

---

**Access Vector (AV):** Network

**Access Complexity (AC):** Low

**Authentication (AU):** None

**Confidentiality (C):** None

**Integrity (I):** Partial

**Availability (A):** None

**Additional Information:**

Allows unauthorized modification

## ➤ CVE-2013-6438

La funzione `dav_xml_get_cdata` in `main/util.c` nel modulo `mod_dav` in Apache http prima della versione 2.4.8 non rimuove correttamente i caratteri di spaziatura dalle sezioni CDATA, la quale consente ai malintenzionati attacchi denial of service (DoS) tramite una richiesta di scrittura.

## CVE-2013-6438 Detail

### MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

## Current Description

The `dav_xml_get_cdata` function in `main/util.c` in the `mod_dav` module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

Source: MITRE

[+View Analysis Description](#)

## Impact

### CVSS v2.0 Severity and Metrics:

Base Score: 5.0 MEDIUM

Vector: (AV:N/AC:L/Au:N/C:N/I:N/A:P) (V2 legend)

Impact Subscore: 2.9

Exploitability Subscore: 10.0

Access Vector (AV): Network

Access Complexity (AC): Low

Authentication (AU): None

Confidentiality (C): None

Integrity (I): None

Availability (A): Partial

### Additional Information:

Allows disruption of service

## ➤ CVE-2014-0117

Il modulo `mod_proxy` in Apache Server 2.4 < 2.4.10, quando un reverse proxy è abilitato consente ai malintenzionati di provocare una negoziazione del servizio (arresto del processo figlio) tramite una connessione creata http.

Inoltre, è stato trovato un difetto in `mod_proxy` nelle versioni dalla 2.4.6 alla 2.4.9.

## CVE-2014-0117 Detail

### Current Description

The mod\_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

Source: MITRE

[+View Analysis Description](#)

### Evaluator Description

Per vendor advisory [http://httpd.apache.org/security/vulnerabilities\\_24.html](http://httpd.apache.org/security/vulnerabilities_24.html) "A flaw was found in mod\_proxy in httpd versions 2.4.6 to 2.4.9."

#### Impact

##### CVSS v2.0 Severity and Metrics:

Base Score: 4.3 MEDIUM

Vector: (AV:N/AC:M/Au:N/C:N/I:N/A:P) (V2 legend)

Impact Subscore: 2.9

Exploitability Subscore: 8.6

---

Access Vector (AV): Network

Access Complexity (AC): Medium

Authentication (AU): None

Confidentiality (C): None

Integrity (I): None

Availability (A): Partial

Additional Information:

Allows disruption of service

## ➤ CVE-2017-9788

Nelle versioni di Apache 2.2.34 e 2.4 < 2.4.7 il tipo "Digest" non viene inizializzato o ripristinato prima delle successive assegnazioni di chiave=valore alla funzione mod\_auth\_digest. Fornire una chiave iniziale senza averla assegnata potrebbe rilasciare informazioni potenzialmente riservate ed in altri casi con conseguente negazione del servizio.

## CVE-2017-9788 Detail

### Current Description

In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod\_auth\_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

Source: MITRE

[+View Analysis Description](#)

#### CVSS v2.0 Severity and Metrics:

Base Score: 6.4 MEDIUM

Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:P) (V2 legend)

Impact Subscore: 4.9

Exploitability Subscore: 10.0

Access Vector (AV): Network

Access Complexity (AC): Low

Authentication (AU): None

Confidentiality (C): Partial

Integrity (I): None

Availability (A): Partial

#### Additional Information:

Allows unauthorized disclosure of information

Allows disruption of service

## ➤ CVE-2015-1328

L'implementazione di overlayfs nel kernel linux versione inferiore alla 3.19 < 3.21.21, in Ubuntu fino alla versione 15.04, non controlla in maniera approfondita i permessi per la creazione di file nelle directory superiori del sistema, il che consente a utenti locali di ottenere accesso root facendo leva su una configurazione in cui overlayfs è consentito in un punto di mount arbitrario.

Questa vulnerabilità è stata individuata dopo aver effettuato l'accesso via SSH con le credenziali di accesso ottenuto da Hydra.



## CVE-2015-1328 Detail

### MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

## Current Description

The overlays implementation in the linux (aka Linux kernel) package before 3.19.0-21.21 in Ubuntu through 15.04 does not properly check permissions for file creation in the upper filesystem directory, which allows local users to obtain root access by leveraging a configuration in which overlays is permitted in an arbitrary mount namespace.

Source: MITRE

[+View Analysis Description](#)

### CVSS v2.0 Severity and Metrics:

Base Score: 7.2 HIGH

Vector: (AV:L/AC:L/Au:N/C:C/I:C/A:C) (V2 legend)

Impact Subscore: 10.0

Exploitability Subscore: 3.9

Access Vector (AV): Local

Access Complexity (AC): Low

Authentication (AU): None

Confidentiality (C): Complete

Integrity (I): Complete

Availability (A): Complete

#### Additional Information:

Allows unauthorized disclosure of information

Allows unauthorized modification

Allows disruption of service