UNIVERSITÀ DEGLI STUDI DI SALERNO

Penetration Testing And Ethical Hacking

Penetration Testing Report

Candidato:
Aniello Giugliano

Professore:
Arcangelo Castiglione

Anno Accademico 2018/19

1.Executive Summary

Per il progetto relativo all'esame di "Penetration Testing and Ethical Hacking" è stata svolta un attività di penetration testing sulla macchina virtuale "Typhoon 1.02", scaricata dal sito http://vulnhub.com. Lo scopo del testing è stato quello di verificare le conoscenze e le capacità acquisite durante il corso. Per effettuare il test, è stato usato un approccio "GreyBox Testing" , poiché si avevano informazioni parziali riguardanti l' hardware della macchina target , ma non si aveva alcuna informazione riguardante i software installati al suo interno.Il test è stato eseguito trovandosi sulla stessa rete locale della macchina da analizzare(rete esame).
Il test è stato portato avanti dal punto di vista di un attaccante con accesso alla rete locale, ma che non abbia alcuna conoscenza delle macchine connesse o dell'infrastruttura. Oltre all'analisi delle varie vulnerabilità si è cercato di affrontare la challange proposta da Vulnhub , la quale richiedeva l'accesso e la lettura di un file text della macchina target chiamato root-flag.
Il testing è stato condotto dal 16 giugno 2019 al 1 luglio 2019.Il test ha evidenziato alcune vulnerabilità all'interno del sistema , le quali se sfruttate nell'opportuno modo, portano al controllo del sistema da parte di utenti malevoli.Questo report, descrive dettagliatamente tutte le vulnerabilità riscontrate sulla macchina target.

2.Engagement Highlights

Nel processo di testing non esiste nessun vincolo tra il penetration tester e l' azienda committente in quanto si tratta di un test finalizzato ad una attività progettuale, quindi è possibile utilizzare tutti gli strumenti e le tecniche , senza restrizione alcuna. Non esiste alcun accordo di non divulgazione.

3.Vulnerability Report

Durante il processo di testing sono state trovate numerose vulnerabilità.Le vulnerabilità principali sono quelle che riguardano i servizi di Apache Tomcat e Drupal. In particolare la versione di Apache Tomcat utilizza username e password di default (“tomcat”) per il login come amministratore, e questo consente agli attaccanti malintenzionati di aumentare i loro privilegi. La versione di Drupal, essendo una versione non aggiornata,è soggetta ad una vulnerabilità , chiamata”Drupalgeddon2”,la quale consente agli aggressori di sfruttare più vettori di attacco sul sito Drupal e questo potrebbe comportare la completa compromissione del sito.

4.Remediation Report

Le indicazioni generali che si possono dare per risolvere i problemi che abbiamo riscontrato sono:

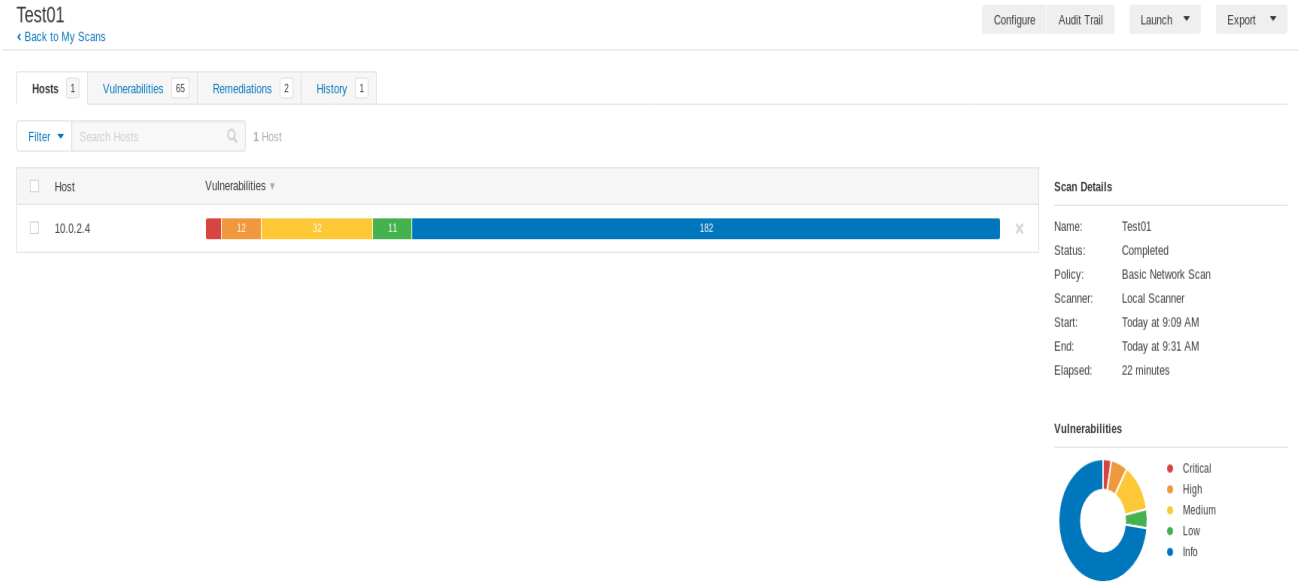
- Aggiornare i servizi di Apache Tomcat e Drupal alle versioni più recenti in modo da risolvere alcune delle vulnerabilità che esistevano con le vecchie versioni.
- Cambiare le credenziali di default di Apache Tomcat, per rendere più difficile l' accesso da parte di utenti malintenzionati.
- Utilizzare per tutti gli utenti all'interno del sistema password più complesse. Per le password dovrebbero essere utilizzate una combinazione di lettere maiuscole, minuscole,numeri e simboli. Inoltre la lunghezza delle password dovrebbe avere un numero minimo di caratteri. Tutto questo viene fatto per rendere più difficile il processo di identificazione da parte di utenti malintenzionati.

5.Findings Summary

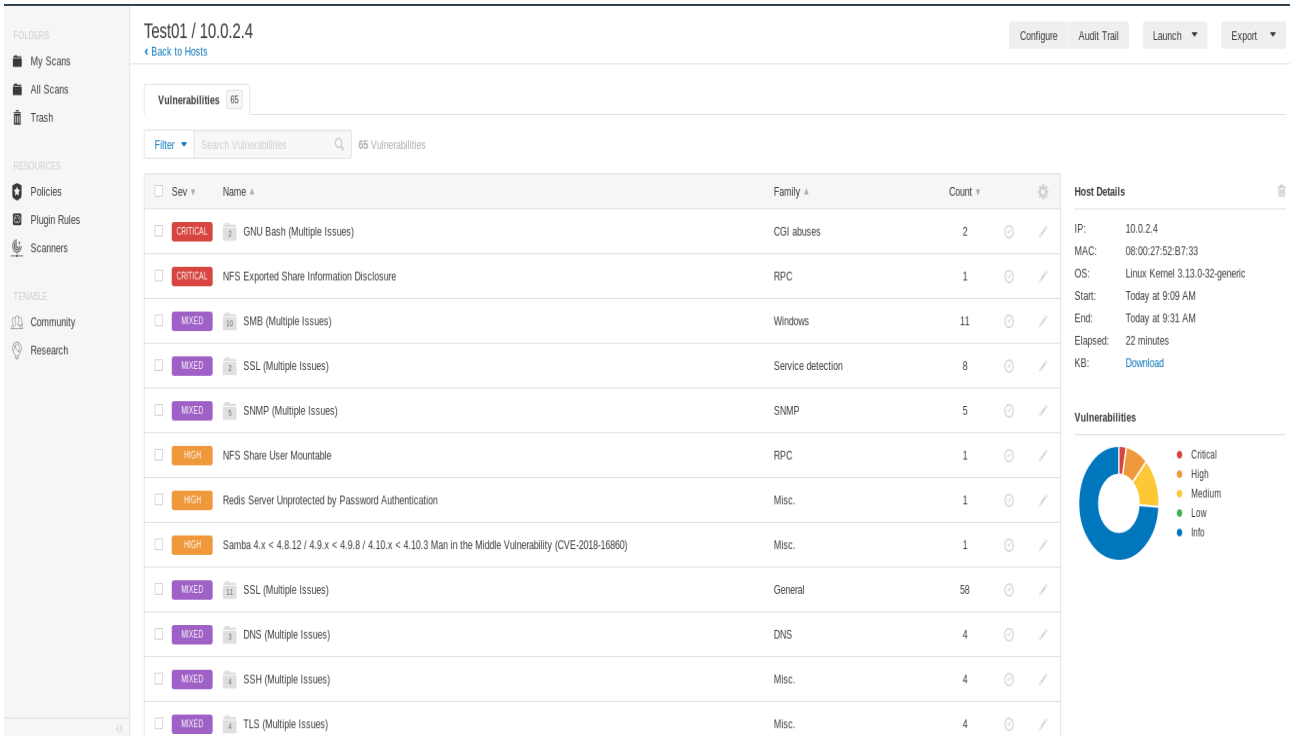
In questo capitolo verranno mostrate le varie criticità riscontrate all'interno della macchina virtuale Typhoon 1.02. Le diverse vulnerabilità sono state riscontrate sia con metodi di scansione automatica che con metodi di scansione manuale, quindi in questo documento verrà fatta una sintesi di tutte le informazioni ottenute. Le varie vulnerabilità che sono state riscontrate verranno valutate con la scala CVSS , con il seguente Rating:

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

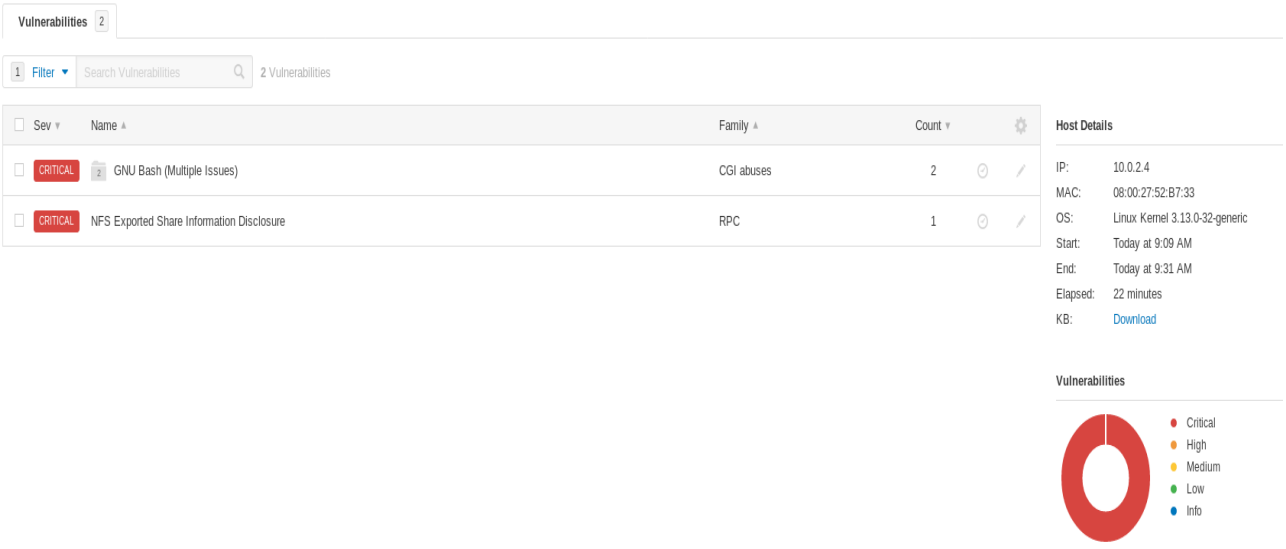
Per la scansione automatica delle vulnerabilità è stato usato Nessus.
I risultati della scansione sono i seguenti:



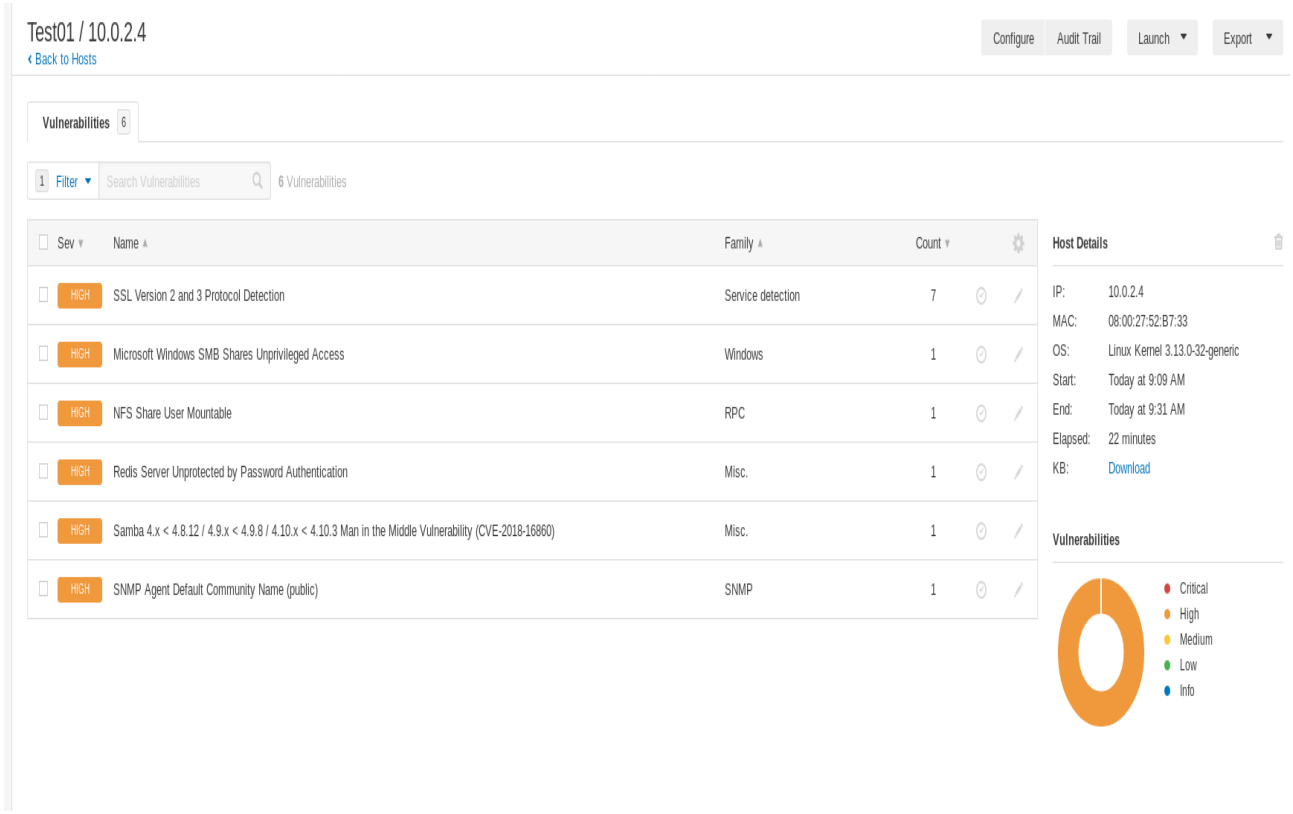
Le vulnerabilità totali che sono state trovate sono 65.



Filtrando i risultati della scansione per Score:Critical si ottengono i seguenti risultati:



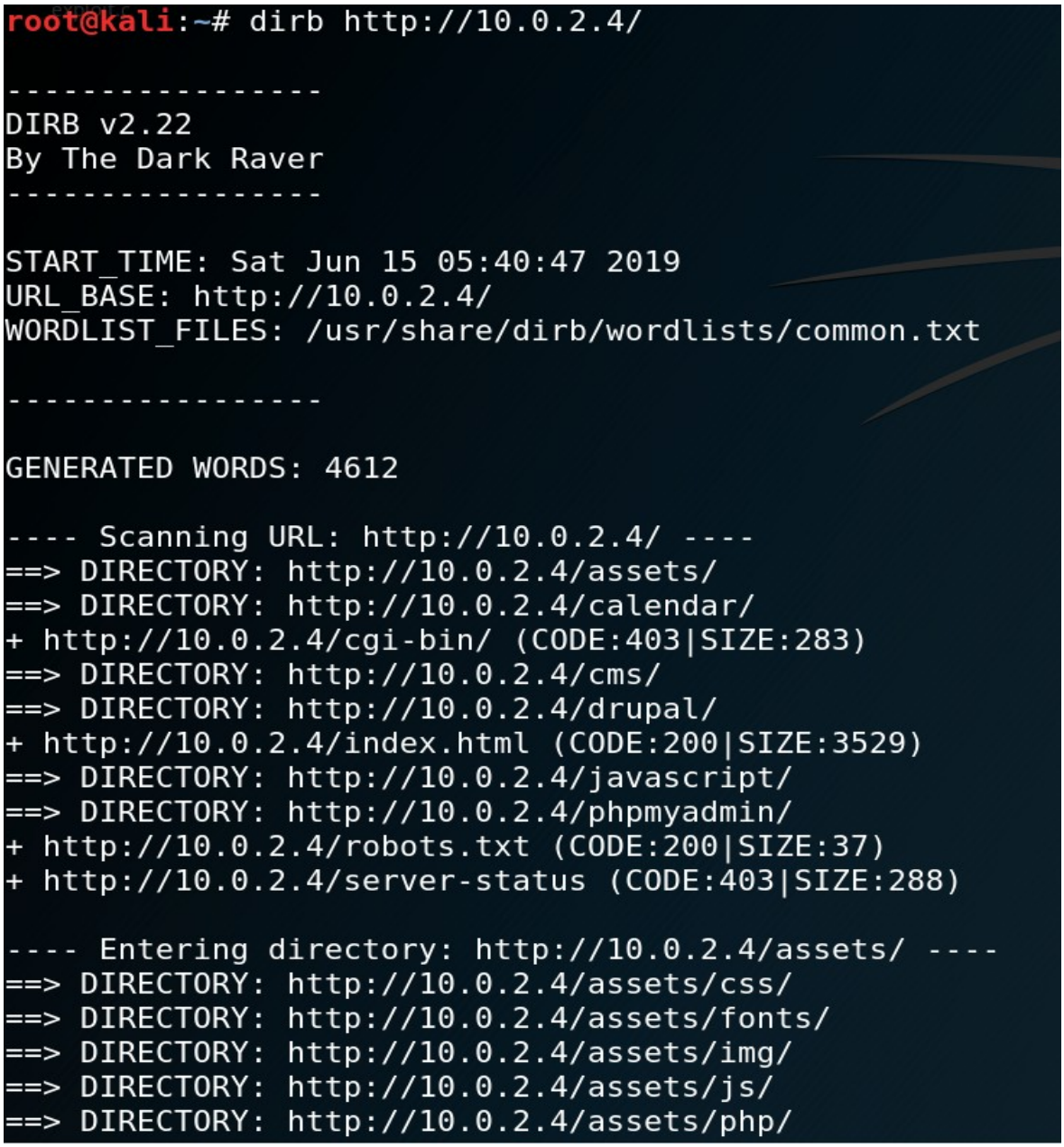
Filtrando i risultati per Score:High , si ottengono i seguenti risultati:



E’ stata effettuata anche una scansione con Nikto2 , per rilevare ed analizzare vulnerabilità di sicurezza causate da errori di configurazione del server e applicazioni web obsolete.

```
root@kali:~# nikto -h http://10.0.2.4
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.0.2.4
+ Target Hostname:    10.0.2.4
+ Target Port:        80
+ Start Time:         2019-06-12 10:59:25 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0xdc9 0x578fef1e684d5
+ 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 MI
ME type
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.26
+ Entry '/mongoadmin/' 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.
+ Uncommon header 'nikto-added-cve-2014-6278' found, with contents: true
+ OSVDB-112004: /cgi-bin/test.sh: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-201
4-6271).
+ OSVDB-112004: /cgi-bin/test.sh: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-201
4-6278).
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Uncommon header 'x-ob_mode' found, with contents: 0
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /cms/: This might be interesting...
+ /phpmyadmin/: phpMyAdmin directory found
+ 8500 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time:           2019-06-12 10:59:57 (GMT-4) (32 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

E’ stata effettuata una scansione con Dirb , per trovare tutte le directory all’interno della macchina target.

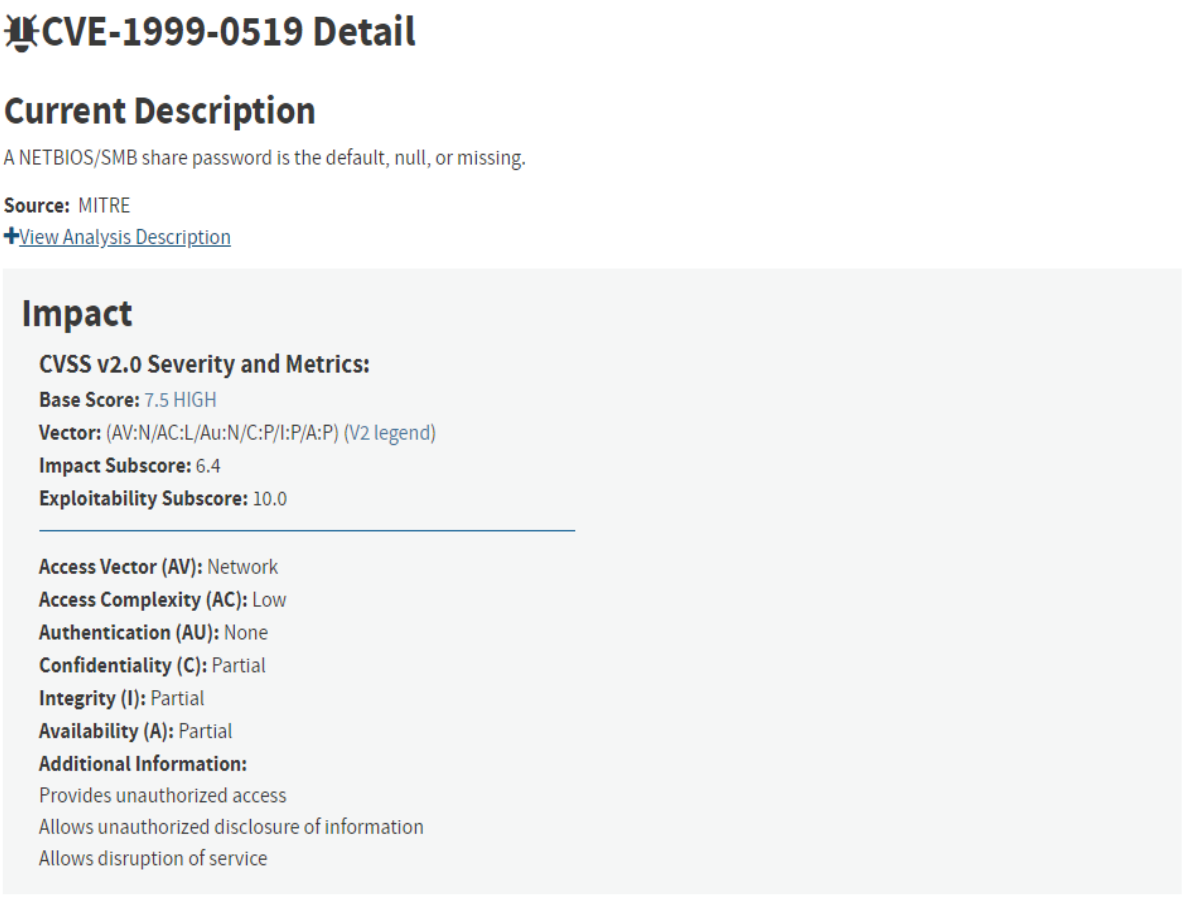


6.Detailed Summary

In questo capitolo verranno descritte le principali vulnerabilità che sono state trovate,e verranno mostrate nel dettaglio queste vulnerabilità. In particolare verrà mostrata una breve descrizione della criticità , ed il rischio ad essa associato.

1. CVE-1999-0519 CVE-1999-0520

Il servizio di Windows SMB ha una o più pagine di Windows a cui è possibile accedere tramite la rete con le credenziali specificate.
A seconda dei diritti di condivisione, può consentire ad un utente malintenzionato di leggere o scrivere dati riservati.



CVE-1999-0520 Detail

Current Description

A system-critical NETBIOS/SMB share has inappropriate access control.

Source: MITRE

+View Analysis Description

Impact

CVSS v2.0 Severity and Metrics:

Base Score: 6.4 MEDIUM

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

Availability (A): None

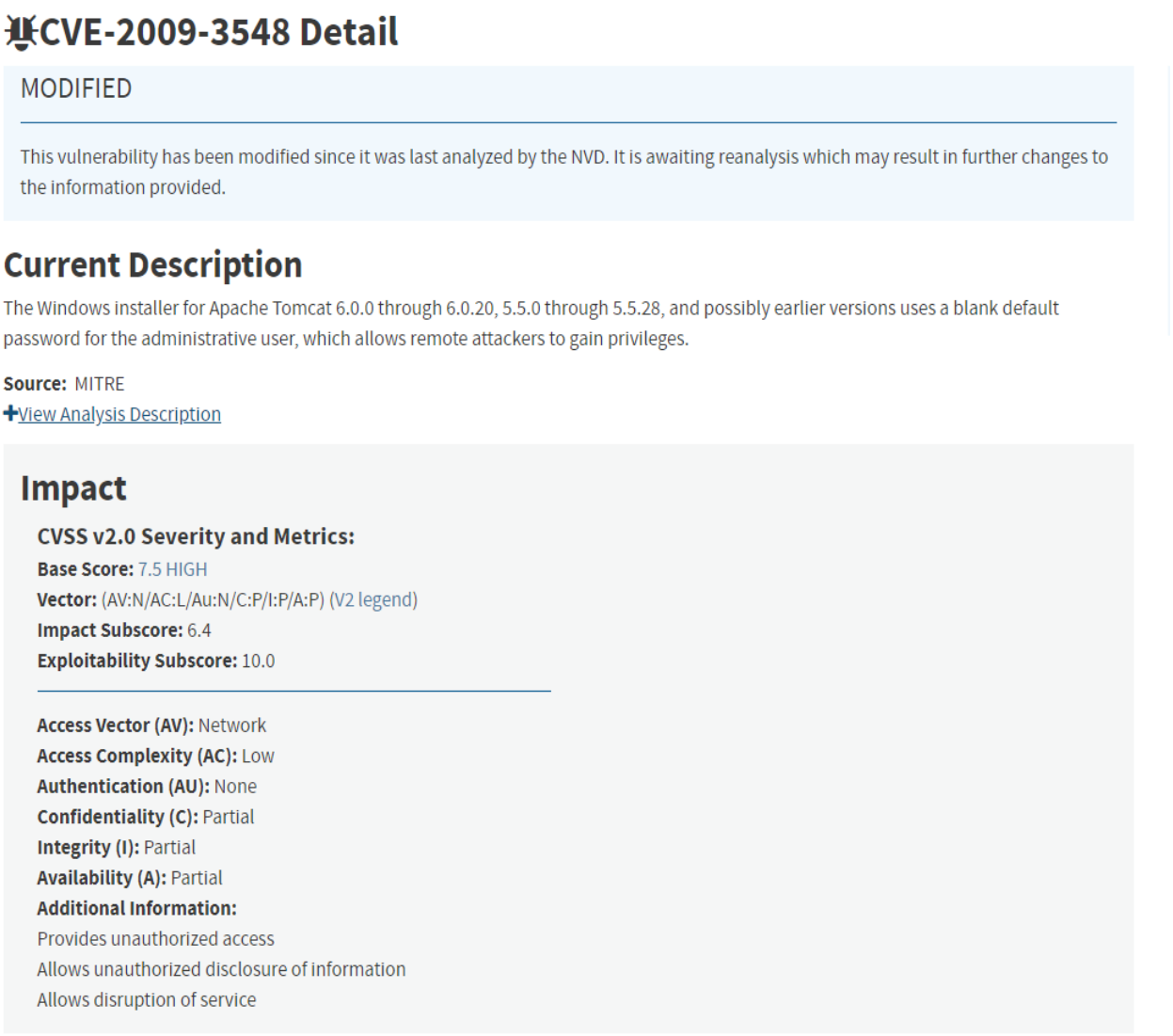
Additional Information:

Allows unauthorized disclosure of information

Allows unauthorized modification

2. CVE-2009-3548

Il servizio di Apache Tomcat utilizza username e password di default per il login dell' amministratore del sistema. Questo consente ad utenti malintenzionati di accedere facilmente al servizio ed aumentare i loro privilegi.



CVE-2009-3548 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 Windows installer for Apache Tomcat 6.0.0 through 6.0.20, 5.5.0 through 5.5.28, and possibly earlier versions uses a blank default password for the administrative user, which allows remote attackers to gain privileges.

Source: MITRE

+View Analysis Description

Impact

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): Low

Authentication (AU): None

Confidentiality (C): Partial

Integrity (I): Partial

Availability (A): Partial

Additional Information:

Provides unauthorized access

Allows unauthorized disclosure of information

Allows disruption of service

3. CVE-2014-7910

Essendo la versione di Google Chrome installata sulla macchina target una versione datata, presenta varie vulnerabilità che se sfruttate consentono all' attaccante di effettuare attacchi di tipo DOS.

CVE-2014-7910 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

Multiple unspecified vulnerabilities in Google Chrome before 39.0.2171.65 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.

Source: MITRE

+View Analysis Description

Impact

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

4.CVE-2017-14387

Il servizio NFS presente all'interno di EMC Isilon One FS mantiene le impostazioni di esportazione NFS predefinite ,consentendo ad un utente malintenzionato di sfruttare tale vulnerabilità.

CVE-2017-14387 Detail

Current Description

The NFS service in EMC Isilon OneFS 8.1.0.0, 8.0.1.0 - 8.0.1.1, and 8.0.0.0 - 8.0.0.4 maintains default NFS export settings (including the NFS export security flavor for authentication) that can be leveraged by current and future NFS exports. This NFS service contained a flaw that did not properly propagate changes made to the default security flavor to all new and existing NFS exports that are configured to use default NFS export settings and that are mounted after those changes are made. This flaw may potentially allow NFS clients to access affected NFS exports using the default and potentially weaker security flavor even if a more secure one was selected to be used by the OneFS administrator, aka an "NFS Export Security Setting Fallback Vulnerability."

Source: MITRE

+View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 6.5 MEDIUM
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N (V3 legend)
Impact Score: 2.5
Exploitability Score: 3.9

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): Low
Integrity (I): Low
Availability (A): None

CVSS v2.0 Severity and Metrics:

Base Score: 6.4 MEDIUM
Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:N) (V2 legend)
Impact Subscore: 4.9
Exploitability Subscore: 10.0

Access Vector (AV): Network
Access Complexity (AC): Insufficient_Info
Authentication (AU): None
Confidentiality (C): Partial
Integrity (I): Partial
Availability (A): None
Additional Information:
Allows unauthorized disclosure of information
Allows unauthorized modification

5.CVE-2018-7600

La versione di Drupal installata,poichè è datata,consente agli utenti malintenzionati di eseguire codice arbitrario a causa di un problema che interessa più sottosistemi del servizio con configurazioni di modulo predefinite o comuni.

CVE-2018-7600 Detail

Current Description

Drupal before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1 allows remote attackers to execute arbitrary code because of an issue affecting multiple subsystems with default or common module configurations.

Source: MITRE

+View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 9.8 CRITICAL
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 3.9

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

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): Low
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

6. CVE-2011-0518

Vulnerabilità trasversale della directory all'interno di core/lib/router.php in LotusCMS 3.0, quando magic_quotes_gpc è disabilitato, consente agli aggressori remoti di includere ed eseguire file locali arbitrari tramite il parametro di sistema su index.php.

CVE-2011-0518 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

Directory traversal vulnerability in core/lib/router.php in LotusCMS Fraise 3.0, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via the system parameter to index.php.

Source: MITRE

+View Analysis Description

Impact

CVSS v2.0 Severity and Metrics:

Base Score: 5.1 MEDIUM

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

Impact Subscore: 6.4

Exploitability Subscore: 4.9

Access Vector (AV): Network

Access Complexity (AC): High

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

7.CVE-2014-3566

Il protocollo SSL 3.0, utilizzato in OpenSSL , utilizza il padding CBC non deterministico, che permette ad un attaccante di effettuare un attacco di man in the middle ed ottenere dati in chiaro tramite un attacco padding-oracle.

CVE-2014-3566 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 SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.

Source: MITRE

+View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 6.8 MEDIUM

Vector: AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N (V3 legend)

Impact Score: 4.0

Exploitability Score: 2.2

Attack Vector (AV): Network

Attack Complexity (AC): High

Privileges Required (PR): None

User Interaction (UI): None

Scope (S): Changed

Confidentiality (C): High

Integrity (I): None

Availability (A): None

CVSS v2.0 Severity and Metrics:

Base Score: 4.3 MEDIUM

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

Impact Subscore: 2.9

Exploitability Subscore: 8.6

Access Vector (AV): Network

Access Complexity (AC): Medium

Authentication (AU): None

Confidentiality (C): Partial

Integrity (I): None

Availability (A): None

Additional Information:

Victim must voluntarily interact with attack mechanism

Allows unauthorized disclosure of information