Technische Hochschule
Brandenburg
University of
Applied Sciences

# Penetrationstest des Servers „Valentine“

## - Abschlussbericht -

**Hausarbeit**
im Wahlpflichtmodul
Penetration Testing

Sommersemester 2018

**Dozenten**
Wilhelm Dolle
Arkadij Enders
Steven Koleczko

**Hendrik Müller**
hendrik.mueller@th-brandenburg.de
Matr.-Nr. 20202183

**Hannes Fichtel**
hannes.fichtel@th-brandenburg.de
Matr.-Nr. 20202457

Brandenburg an der Havel, den 20. Juli 2018



# Dokumenteninformation

## Abstrakt

In diesem Abschlussbericht finden sich die Resultate des Penetrationstests des Servers „Valentine“.

## Klassifizierung

Vertraulich

## Autoren und Freigabe

| Tester & Ersteller | | Freigegeben von |
|---|---|---|
| Hendrik Müller<br>*THB Chief Testing Officer & Linux Expert* | Hannes Fichtel<br>*THB Testing Counsellor & QM Consultant* | |

## Bearbeitungshistorie

| Version | Autor | Datum | Revision |
|---|---|---|---|
| 0.1 | Hannes Fichtel | 10.07.2018 | Erste Version |
| 0.2 | Hendrik Müller | 14.07.2018 | Ergänzungen |
| 0.3 | Hannes Fichtel | 18.07.2018 | Qualitätssicherung |
| 1.0 | Hannes Fichtel / Hendrik Müller | 19.07.2018 | Finale Version |

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# Tabellenverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| **CBC** | Cipher Block Chaining |
| **CVSS** | Common Vulnerability Scoring System |
| **EoP** | Elevation of Privilege<br>(dt. Privilegien-Eskalation, Rechteausweitung) |
| **HSTS** | HTTP Strict Transport Security |
| **HTTP** | Hypertext Transfer Protocol |
| **HTTPS** | Hypertext Transfer Protocol Secure |
| **MitM** | Man-in-the-Middle |
| **N/A** | not available (dt.: nicht verfügbar) |
| **OWASP** | Open Web Application Security Project |
| **RSA** | Abkürzung (Akronym) für ein asymmetrisches kryptographisches Verfahren benannt nach Rivest, Shamir und Adleman |
| **SSL** | Secure Sockets Layer |
| **TLS** | Transport Layer Security |

# 0 Management Summary

Die Überprüfung des Webservers „Valentine“ brachte mehrere kritische Sicherheitslücken zum Vorschein.
Auf der Internetseite befinden sich öffentlich einsehbare Informationen, die vertraulich und nicht für Außenstehende bestimmt sind. Darunter ist auch ein geheimer (privater) kryptographischer Schlüssel für die Authentifikation mit dem Server. Der Schlüssel ermöglicht, zusammen mit einem Passwort, den Zugang zum Server per Kommandozeile. Ein Angreifer ist in der Lage, beide Credentials in Erfahrung zu bringen.
Der Webserver selbst verfügt über ein SSL/TLS-Zertifikat zur verschlüsselten Kommunikation. Die zur Implementierung des Zertifikats auf dem Webserver genutzte Bibliothek ist jedoch veraltet und weist eine schwerwiegende Verwundbarkeit auf. Ein entfernter Angreifer ist in der Lage, über diese Schwachstelle an sensible Informationen auf dem Server zu gelangen. Unter anderem ermöglicht der Angriff das Auslesen eines Passworts.
Unter Ausnutzung der beiden vorgenannten Schwachstellen ist es einem Angreifer letztlich möglich, sich Zugang zum Server zu verschaffen. Der Angreifer ist darüber hinaus in der Lage, durch eine Rechteausweitung die vollständige Kontrolle über den Server zu übernehmen. Die Erlangung umfassender Rechte auf dem Server wird wiederum durch die Verwendung veralteter Software begünstigt.

Der Betrieb des Webservers stellt nach derzeitigem Stand ein sehr hohes Risiko für die Vertraulichkeit und Integrität der darauf gespeicherten Daten dar. Auch das Risiko für die Verfügbarkeit des Servers und der darauf laufenden Dienste ist außerordentlich hoch. Es besteht dringender Handlungsbedarf.

Die wesentlichen Feststellungen können der nachfolgenden Tabelle entnommen werden:

| Nr. | Feststellung | Risiko |
|---|---|---|
| 1 | Unix Betriebssystem-Version nicht länger unterstützt | Kritisch |
| 2 | Rechteerweiterung durch Ausnutzung der Copy-On-Write- (COW-)Funktion | Kritisch |
| 3 | Öffentlich zugänglicher, privater RSA-Schlüssel | Hoch |
| 4 | OpenSSL Heartbeat Informationsabfluss (Heartbleed Schwachstelle) | Mittel |
| 5 | Öffentlich zugängliche, vertrauliche Informationen | Mittel |

Tabelle 1: Wesentliche Feststellungen

Es wird empfohlen, die oben aufgezeigten Probleme schnellstmöglich beheben zu lassen.

Hintergrundinformationen zum Vorgehen im Rahmen der Tests finden Sie auf den Seiten 3 bis 10 (Auftrag und Auftragsdurchführung). Detailliertere Angaben zu den Feststellungen finden Sie auf den Seiten 11 bis 27 (Feststellungen). Eine Übersicht zu allen Handlungsempfehlungen befindet sich auf Seite 28.

# 1 Auftrag und Auftragsdurchführung

Die THB Pen-Testing-Group wurde von der KPMG Wirtschaftsprüfungsgesellschaft AG aus Berlin mit einem Penetration-Testing beauftragt. Für die Untersuchung wurde der Zeitraum vom 05.07.2018 bis zum 20.07.2018 gewählt. Als kundenseitige Ansprechpartner standen Herr Dolle, Herr Enders und Herr Koleczko zur Verfügung. Der Test wurde als Black-Box-Test konzipiert; es standen dem Testteam folglich keine Insiderinformationen zum zu untersuchenden System zu Verfügung.

Der nachfolgende Bericht beruht auf den Erkenntnissen des während des Untersuchungszeitraumes vorgefundenen Stands der Anwendungen und Systeme. Eventuelle Abweichungen zum jetzigen Zeitpunkt sind daher möglich. Die Untersuchung und der hier vorliegende Bericht stellen nur einen Ausschnitt möglicher Angriffsszenarien dar und erheben keinen Anspruch auf Vollständigkeit.

Zielgruppe des vorliegenden Berichts sind sowohl das Management als auch leitende Mitarbeiter der IT-Abteilung des Auftraggebers. Neben der Auflistung und risikobezogenen Einstufung der grundlegenden Findings umfassen die hier geschilderten Feststellungen daher mitunter auch Details zum technischen Hintergrund sowie grundlegende Handlungsempfehlungen.

## 1.1 Ziel der Untersuchung

Ziel der Untersuchung war das Identifizieren und Testen der praktischen Ausnutzbarkeit vorhandener Schwachstellen am Server des Auftraggebers. Es sollte geprüft werden, ob die genutzten Systeme und Anwendungen etwaige Anfälligkeiten gegenüber Angriffen auf die Vertraulichkeit und Integrität der Daten sowie der Verfügbarkeit aufweisen.

## 1.2 Untersuchungsgegenstand

Die nachfolgend aufgeführten Anwendungen und Systeme waren Bestandteil der Untersuchungen:

| Anwendung/System | IP-Adresse | URL(s) |
|---|---|---|
| Valentine Server | 10.10.10.79 | http://10.10.10.79<br>https://10.10.10.79 |

Tabelle 2: Untersuchungsgegenstand

Es wurden nur die oben aufgelisteten Anwendungen, Systeme, URLs und IP-Adressen im Rahmen der Tests berücksichtigt. Mit dem Auftraggeber wurde vereinbart, dass keine Beschränkungen in der Testtiefe zu berücksichtigen sind und auch ein aktives Eindringen und Beeinflussen der oben genannten Systeme und Anwendungen explizit zugelassen ist.

## 1.3 Verwendete Tools

Das Testing-Team setzte im Rahmen der Prüfung die nachfolgend aufgelisteten Tools in der jeweils angegebenen Version ein:

| Tool (Software) | Version | Art/Beschreibung |
|---|---|---|
| Burp Suite | Community Edition, v1.7.35 | Web Content Testing Suite |
| DIRB | v2.21 | Web Content Scanner |
| Firefox | v60.0.2 (64-bit), Quantum | Webbrowser |
| Metasploit | v4.16.49 | Pen-Test-Framework |
| Nessus | v6.11.1 | Schwachstellenscanner |
| Nikto | v2.1.6 | Schwachstellenscanner |
| Nmap | v7.70 | Portscanner, Netzwerkanalyse |
| OpenVAS | OpenVAS-9 (GSM 4.2.17) | Schwachstellenscanner |
| Uniscan | v6.2 | Schwachstellenscanner |

Tabelle 3: Testing-Tools

Die Tests erfolgten über das lokale Netzwerk (Adjacent Network) von einem vorbereiteten Notebook mit der Linux-Distribution „Kali“ aus. Es handelte sich um die Kali-Version 2018.2 für i386 (x86)-Prozessorarchitekturen. Die als Tools enthaltenen Programmkomponenten wurden vor der Nutzung noch aktualisiert.

## 1.4 Ablauf der Untersuchung

Die Sicherheitsanalyse des oben beschriebenen Servers wurde mittels der oben aufgelisteten Softwarewerkzeuge durchgeführt. Zusätzlich wurde die Analyse durch manuelle Tests ergänzt. Der Test setzte sich wie folgt zusammen:

1. **Identifikation von Netzwerkdiensten**

   Zu Beginn der Untersuchung wurde die Erreichbarkeit des Servers über das lokale Netzwerk überprüft und der Server mittels eines Netzwerkanalysetools (Nmap) auf aktive Netzwerkdienste hin gescannt. Der Portscanner zeigte auf, dass auf dem Server eine Webanwendung über die Ports 80 und 443 erreichbar ist sowie eine SSH Verbindung auf Port 22 offen steht für einen Fernzugriff auf den Server.

```
root@kali:~/Documents/00_Hacking/02_CTF/HTB/Valentine# nmap -sV --script=http-enum 10.10.10.79
Starting Nmap 7.70 ( https://nmap.org ) at 2018-07-07 23:23 CEST
Nmap scan report for 10.10.10.79
Host is up (0.047s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
| http-enum:
|   /dev/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|_  /index/: Potentially interesting folder
|_http-server-header: Apache/2.2.22 (Ubuntu)
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
| http-enum:
|   /dev/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|_  /index/: Potentially interesting folder
|_http-server-header: Apache/2.2.22 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.71 seconds
root@kali:~/Documents/00_Hacking/02_CTF/HTB/Valentine#
```

   Abbildung 1: Scannen offener Ports mit Nmap

2. **Informationssuche**

   Bereits durch den Portscan wurden mit Hilfe spezieller Überprüfungsmethoden (Enumeration-Skript) verschiedene Verzeichnisse (/dev/, /index/) ge-

funden, die auf dem Webserver zugänglich sind. Die Website bzw. IP des Servers wurde im nächsten Schritt mit Hilfe des Browsers angesteuert, während ein Analyse-Proxy im Hintergrund zugeschaltet war (Burp Suite). Mit Hilfe des Analyse-Proxys wurden dabei weitere Ordnerstrukturen aufgedeckt, die auch durch die Verwendung weiterer Tools zur Analyse der Webserverstrukturen (DIRB, Nikto, Uniscan) bestätigt wurden. Der nachfolgende Screenshot zeigt die mittels Uniscan erkannte Ordnerstruktur der Internetseite:

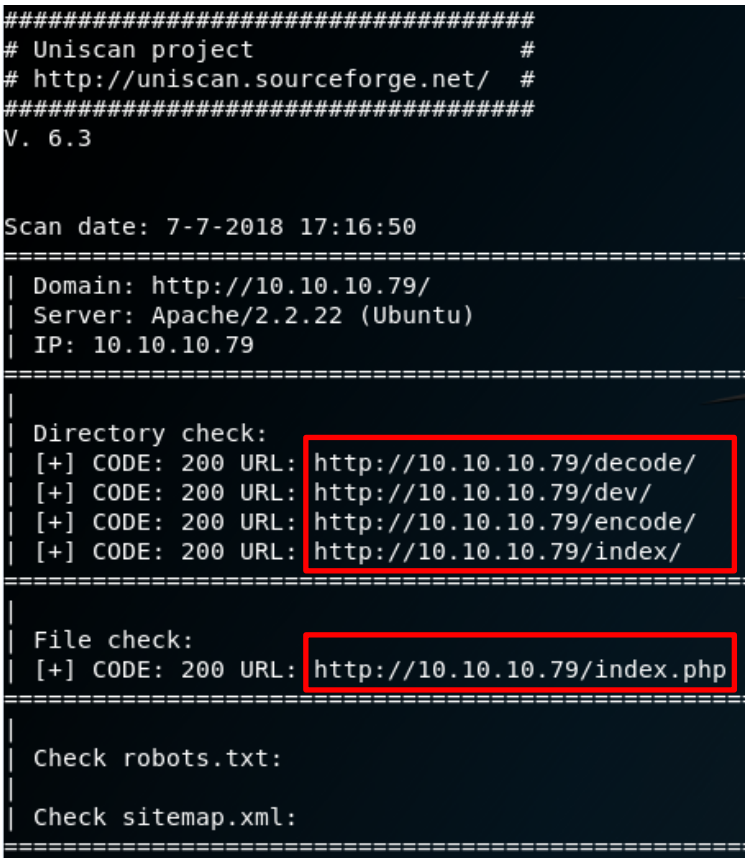



Abbildung 2: Ordnerstruktur des Webservers

## 3. Manuelle Untersuchung

Nachdem in den ersten beiden Schritten bereits einige Informationen über den Server gewonnen werden konnten, wurde die Suche nach weiteren Informationen manuell fortgesetzt. Dabei wurde der Fokus auf die gezielte Untersuchung der gefundenen Verzeichnisse gelegt. So wurden im Verzeichnis /dev/ einige interessante Dateien gefunden. Eine Datei mit Notizen (*notes.txt*) und eine offenbar in Hexadezimal codierte Datei (*hype.txt*).

Der nachfolgende Screenshot zeigt den Ordner im Browser sowie die beiden darin enthaltenen Dateien:

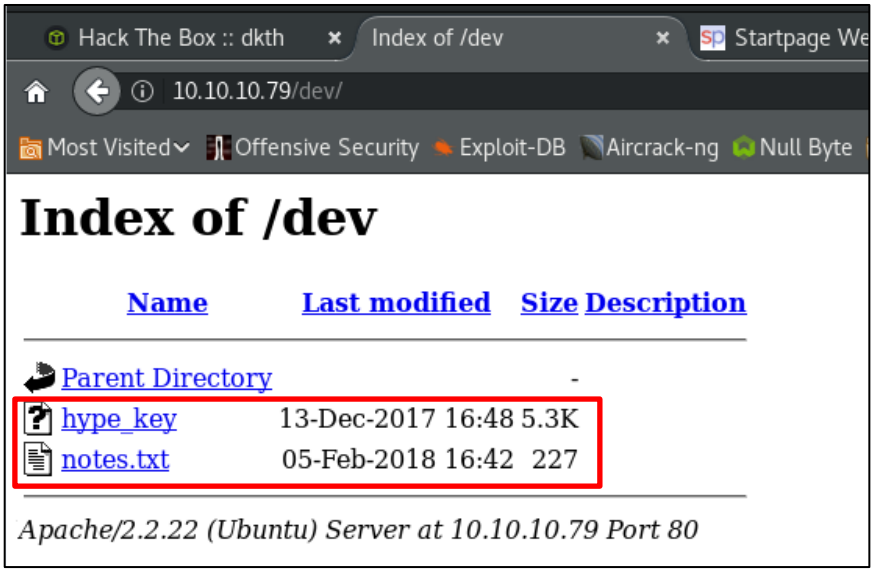



Abbildung 3: Index des /dev-Ordners auf dem Webserver

Eine kurze Überprüfung der Datei bestätigte, dass diese tatsächlich in Hexadezimal codiert war. Die Decodierung brachte einen privaten RSA-Schlüssel zum Vorschein:

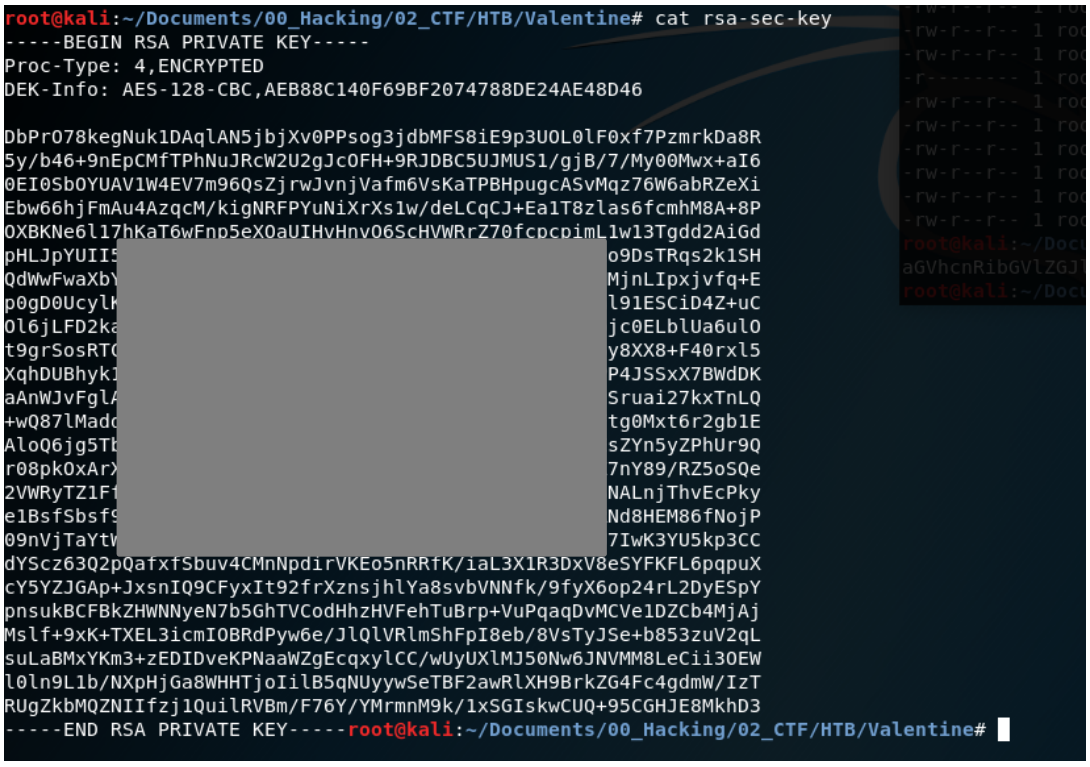



Abbildung 4: Öffentlich zugänglicher, privater RSA-Schlüssel

Des Weiteren offenbarte die Notizdatei, dass sich auf dem Server eine Eingabemaske für einen De- bzw. Encoder befindet. Dieser wurde auch bereits im vorherigen Schritt entdeckt. Durch schnelle Tests mit wahllosen Texten stellte sich heraus, dass hier Text im Zeichensatz Base64 codiert bzw. decodiert wird. Der nachfolgende Screenshot zeigt die Prüfung des Decoders mit Eingabe des in Base64 codierten Strings *Test*:

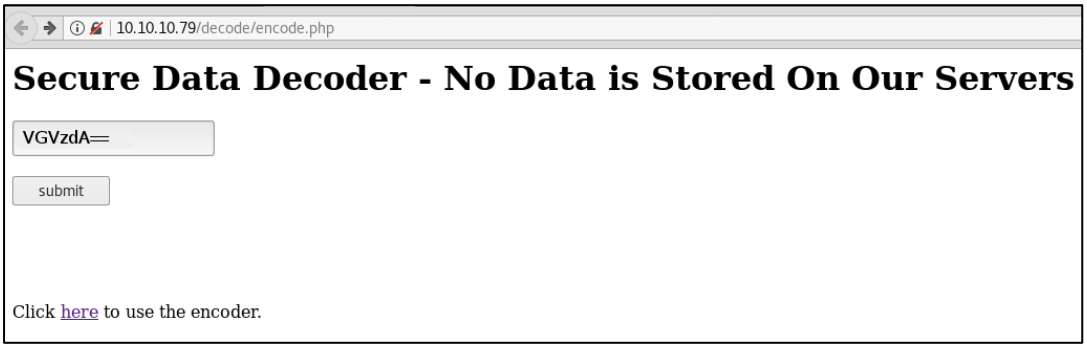



Abbildung 5: Eingabefeld des Base64-Decoders

## 4. Automatische Untersuchung

Nachdem bereits einige Informationen gewonnen und auf kritische Dateien zugegriffen werden konnte, wurden zusätzlich noch automatisierte Scanner (OpenVAS, Nessus) eingesetzt, die nach weiteren Schwachstellen auf dem Webserver suchten. Beide Scanner lieferten dabei dieselben Ergebnisse: Kritisch sind vor allem die stark veraltete Linux Version auf dem Server sowie eine alte OpenSSL-Bibliothek, die für die bekannte Heartbleed-Schwachstelle anfällig ist.

## 5. Ausnutzen der Schwachstellen

Mit Hilfe der erkannten Schwachstellen und der bereits gefundenen Dateien wurde getestet, in den Server einzudringen. Hierzu wurde zunächst versucht, die Heartbleed-Schwachstelle mit Hilfe eines vorgefertigten Exploits (per Metasploit) auszunutzen. Nach mehrmaligem Durchlaufen des Exploits wurde ein offenbar in Base64 codierter Textstring entdeckt, welchen der Server im Speicher hinterlegt hatte und der im Rahmen der Schwachstellenausnutzung zugänglich wurde.

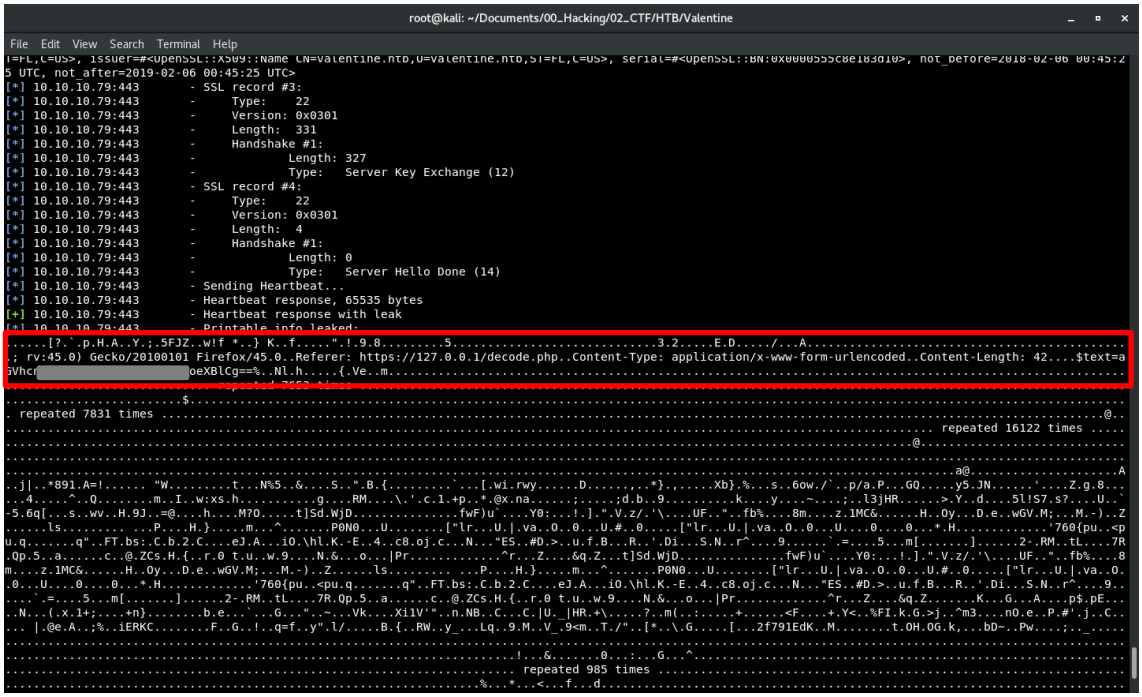



Abbildung 6: Serverantwort mit sensiblen Informationen (Heartbleed)

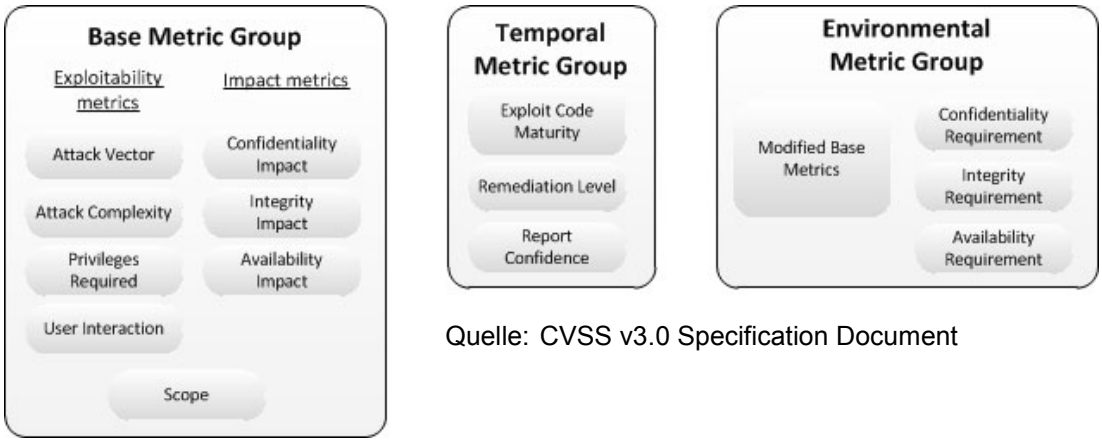
Der offenbarte Text wurde decodiert und heraus kam ein String, der den Anschein eines Passwortes hatte. Zusammen mit dem bereits extrahierten privaten RSA-Schlüssel wurde damit nun versucht, eine SSH Verbindung aufzubauen. Dies gelang nach einigen Versuchen für den Benutzer „hype“, wobei der richtige Benutzername mittels Trial-and-Error-Verfahren ermittelt wurde. Dadurch war ein Zugriff auf den Server mit Nutzerrechten, aber noch ohne Administratorrechte möglich. Um diese zu erlangen, wurde die veraltete Linux Version herangezogen. Ein Test ergab, dass diese anfällig für den „Dirty Cow“-Exploit zur Rechteausweitung ist. Ein entsprechendes Skript wurde mit Nutzerrechten auf den Server kopiert, kompiliert und ausgeführt. Damit wurde der vorhandene Root-Nutzer inklusive Passwort durch einen neuen Nutzer und ein neues Passwort ersetzt. Letztendlich gelang es dadurch, uneingeschränkte Administratorrechte zu erreichen.

## 6. Berichterstellung

Die Feststellungen und Schwachstellen wurden anschließend in diesem Dokument festgehalten und entsprechend ihres Risikos bewertet.

## 1.5 Bewertung

Die Bewertung der Schwachstellen erfolgt anhand des Common Vulnerability Scoring Systems (CVSS). Beim CVSS handelt es sich um ein Klassifizierungssystem, das die Verwundbarkeiten anhand ihres Schweregrades und risikoorientiert einordnet. Dabei werden neben Auswirkungen auf die Vertraulichkeit, die Integrität und die Verfügbarkeit auch Faktoren wie die Komplexität des Angriffs, notwendige Nutzerinteraktionen oder erforderliche Privilegien zur Durchführung des Angriffs mit einbezogen. Diese auch als „Metriken“ (Metrics) bezeichneten Faktoren lassen sich in drei Gruppen (Base, Temporal und Environmental) gliedern. Sie sind aus der nachfolgenden Abbildung ersichtlich:




Quelle: CVSS v3.0 Specification Document

Abbildung 7: Metriken (Bewertungsfaktoren) des CVSS

Die in dieser Arbeit vorgenommenen Bewertungen richten sich nach dem CVSS Base Score in der Version 3 (CVSSv3.0)[1]. Die Skala des Scoring-Systems bewegt sich dabei vom Wert 0 (keine Schwachstelle) bis 10 (kritische Schwachstelle):

| Wert (Score) | Bewertung (Rating) | Farbgebung |
|---|---|---|
| 0 | keine Schwachstelle [Hinweis] | |
| 0,1 - 3,9 | Niedrig | |
| 4,0 - 6,9 | Mittel | |
| 7,0 - 8,9 | Hoch | |
| 9,0 - 10,0 | Kritisch | |

Tabelle 4: Bewertungsskala nach CVSS

[1] vgl. CVSS, Common Vulnerability Scoring System v3.0, Specification Document (v1.8) unter https://www.first.org/cvss/cvss-v30-specification-v1.8.pdf

# 2 Feststellungen

In diesem Teil des Berichts werden die Feststellungen noch einmal detailliert betrachtet. Eine entsprechende Erläuterung zu den einzelnen Punkten findet sich in den folgenden Unterkapiteln.

Allein durch die eingesetzten automatisierten Schwachstellenscanner wurde auch eine Vielzahl an teils sehr niedrig eingestuften Schwachstellen gefunden. Hier soll jedoch der Fokus auf den Schwachstellen liegen, die unmittelbar zur Kompromittierung des Servers beigetragen haben. Diese wesentlichen Schwachstellen sind in der nachfolgenden Tabelle aufgelistet:

| Nr. | Feststellung | | Risiko |
|---|---|---|---|
| 1 | Unix Betriebssystem-Version nicht länger unterstützt | *S. 12 ff.* | Kritisch |
| 2 | Rechteerweiterung durch Ausnutzung der Copy-On-Write- (COW-)Funktion | *S. 14 ff.* | Kritisch |
| 3 | Öffentlich zugänglicher, privater RSA-Schlüssel | *S. 17 ff.* | Hoch |
| 4 | OpenSSL Heartbeat Informationsabfluss (Heartbleed Schwachstelle) | *S. 20 ff.* | Mittel |
| 5 | Öffentlich zugängliche, vertrauliche Informationen | *S. 23 ff.* | Mittel |

Tabelle 5: Wesentliche Feststellungen mit Seitenverweisen

Die Reihenfolge der Auflistung entspricht der Kritikalität der jeweiligen Schwachstelle entsprechend ihres CVSS-Scores. Weitere Angaben zum Risiko und zu den jeweils konkret möglichen Schäden finden sich für jede der aufgezeigten Schwachstellen in derselben Reihenfolge in den nachfolgenden Unterpunkten 2.1 bis 2.5.

Eine Auflistung zusätzlich festgestellter Mängel und weiterer Schwachstellen, jeweils mit einer kurzen Beschreibung, befindet sich zudem am Ende dieses Kapitels unter Punkt 2.6 (Sonstige Befunde, S. 25 ff.).

## 2.1 Unix-Betriebssystem Version nicht länger unterstützt

### 2.1.1 Sachverhalt

Das auf dem Server laufende Linux-Betriebssystem (Ubuntu 12.04) wird vom Hersteller bzw. Entwickler nicht länger unterstützt. Dadurch werden auch keine Updates mehr zur Verfügung gestellt, die mögliche Schwachstellen im System schließen könnten. Das vorhandene System ist stark veraltet.

### 2.1.2 Möglicher Schaden

Durch die nicht mehr unterstützte Version werden entdeckte Schwachstellen nicht länger behoben. Dies ermöglicht Angreifern eine Intrusion unter Ausnutzung bekannter Schwachstellen durch Exploits. Die Folge sind schwerwiegende Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit.

### 2.1.3 Risiko

CVSS-Wert: 10.0

(Berücksichtigte Metriken: /AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

**Kritisch**

### 2.1.4 Nachweise

Durch die Analyse mit Hilfe der automatisierten Schwachstellenscanner wurde die Betriebssystem-Version ermittelt und automatisch festgestellt, dass diese vom Entwickler nicht länger unterstützt wird.

Der auf der nachfolgenden Seite abgebildete Screenshot zeigt den entsprechenden Befund des Scanners Nessus, aus dem auch das Supportende des genutzten Linux-Betriebssystems ersichtlich ist:

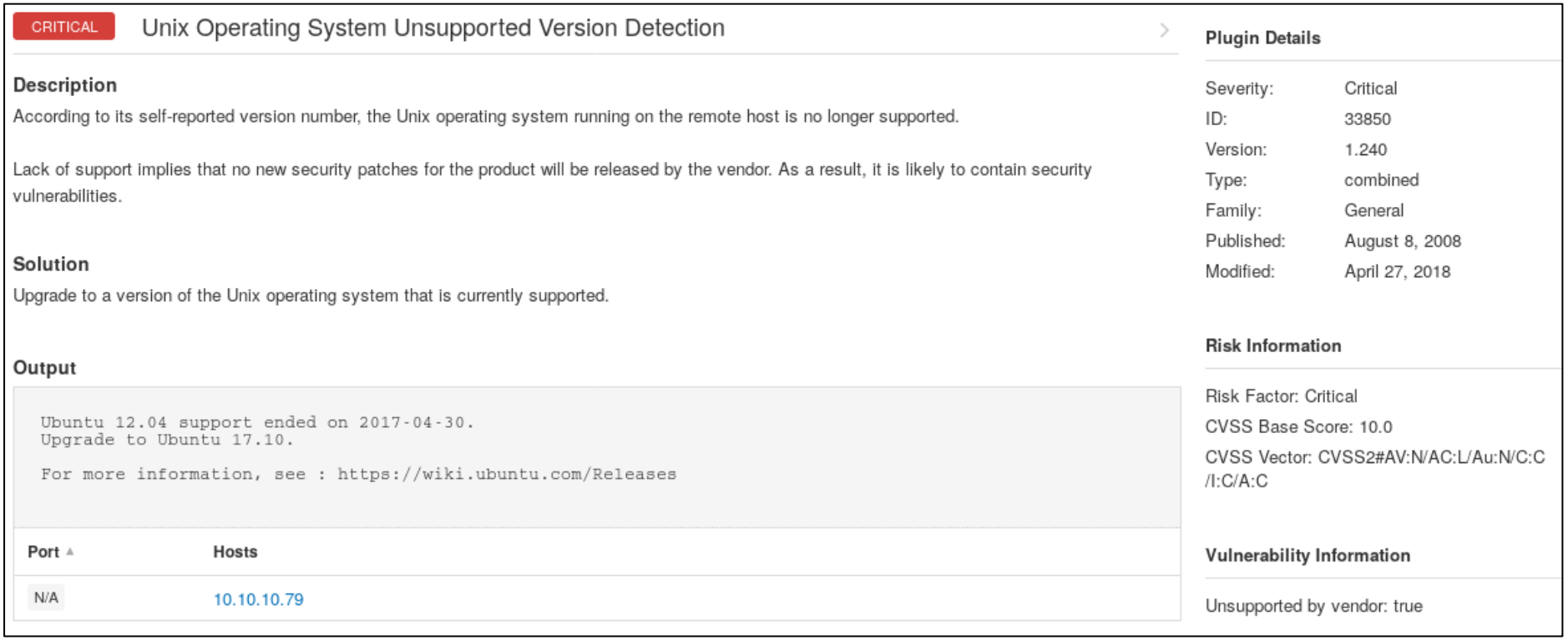



Abbildung 8: Veraltetes Server-Betriebssystem

### 2.1.5 Handlungsempfehlungen und Maßnahmen

[M1] Das System sollte auf ein derzeit unterstütztes Betriebssystem aktualisiert werden (z.B.: Ubuntu Version 17.10).

## 2.2 Rechteerweiterung durch Ausnutzung der Copy-On-Write (COW) Funktion

### 2.2.1 Sachverhalt

Die Linux Kernel Versionen 2.x bis 4.x (Versionen vor 4.8.3) erlauben lokalen Benutzern an Administratorrechte zu gelangen, indem eine Schwachstelle in der Copy-on-Write-Funktion (CoW) ausgenutzt wird (CVE-2016-5195). Dabei wird der ursprüngliche root-Benutzer (Administrator) in der Passwort-Datei (passwd) überschrieben und durch einen Account des Angreifers ersetzt. Es handelt sich dabei um eine Methode der Rechteausweitung (privilege escalation).

### 2.2.2 Möglicher Schaden

Da durch die Rechteausweitung von jedem lokalen Nutzer Administratorrechte erlangt werden können, ist das gesamte System gefährdet. Sind einmal Administratorrechte erhalten worden, hat ein Angreifer die vollständige Kontrolle über das System.

### 2.2.3 Risiko

CVSS-Wert: 7.8

(Berücksichtigte Metriken: /AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

**Hoch**

### 2.2.4 Nachweise

Nach der Anmeldung im System des Servers als normaler Benutzer war ersichtlich, dass es sich um einen anfälligen Linux Kernel handelt. Hierzu kann mit dem Befehl *uname -a* die Version des Kernels ausgegeben werden.

Der nachfolgende Screenshot zeigt einen Ausschnitt des Quelltextes der für die Rechteausweitung durch den Exploit *Dirty CoW* maßgeblichen Datei *dirty.c* auf dem Server:

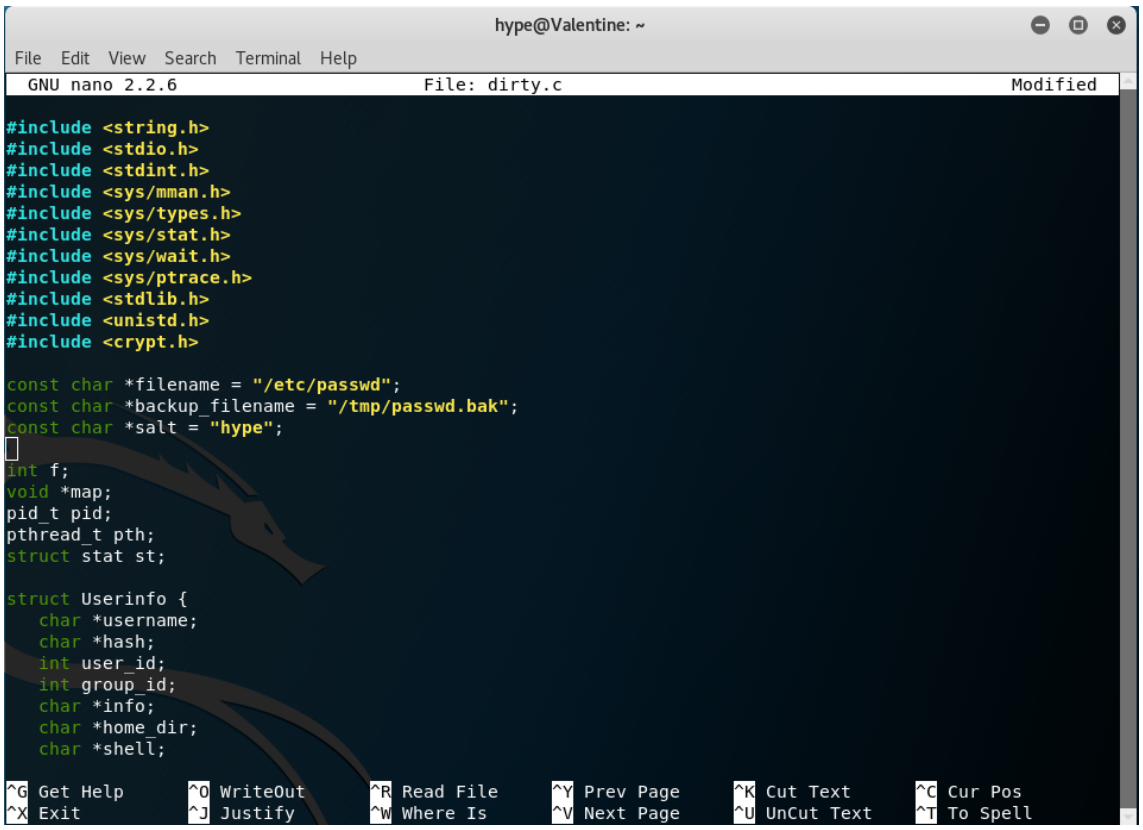



Abbildung 9: Quellcode des Dirty CoW-Exploits

Nach dem Speichern und Kompilieren wurde der Exploit ausgeführt und ein Passwort für den neuen Administrator festgelegt:

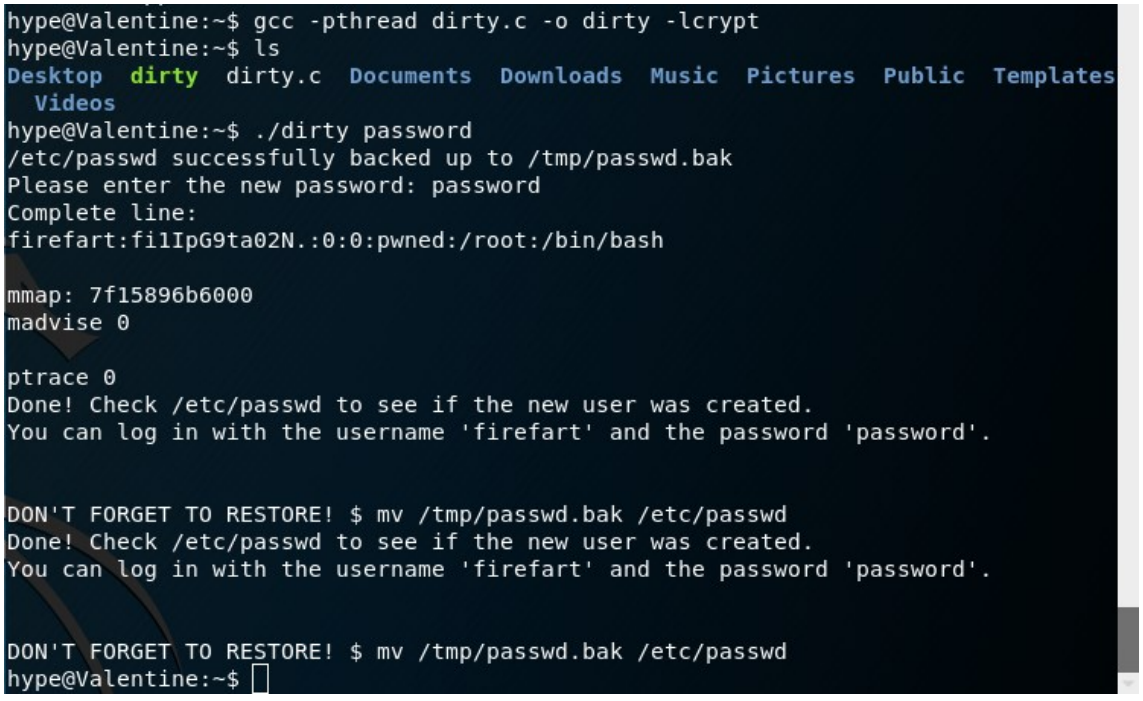



Abbildung 10: Kompilieren und Ausführen von Dirty CoW

Anschließend war die Anmeldung über den Account des neu eingerichteten Administrators möglich. Der Befehl *whoami* sowie ein Blick in die durch den Exploit manipulierte *passwd*-Datei ergaben, dass tatsächlich uneingeschränkte Rechte erlangt wurden. Somit konnte auch der Inhalt vertraulicher, nur vom Administrator lesbarer Dateien wie der *root.txt* in Erfahrung gebracht werden:

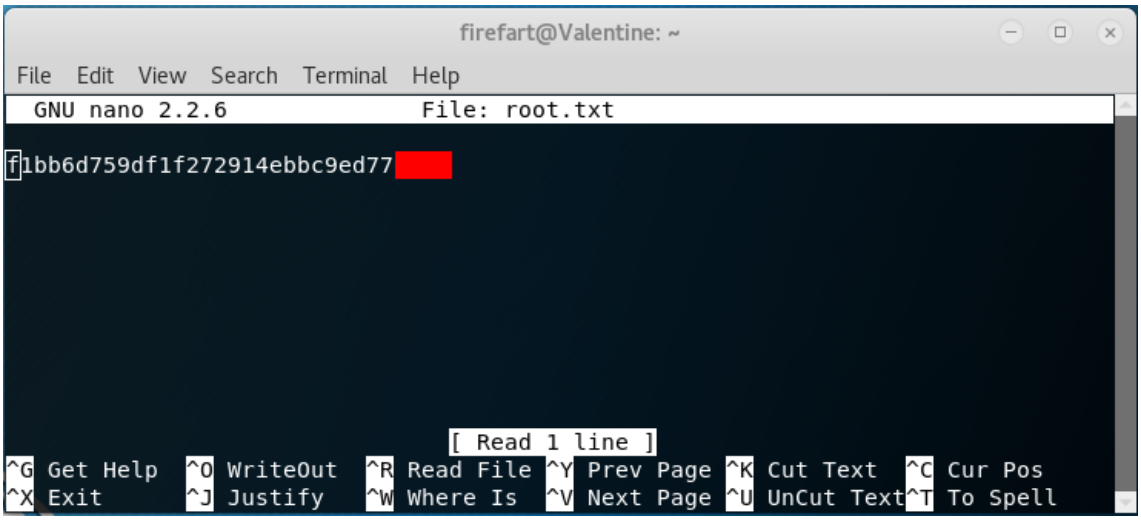



Abbildung 11: Auslesen der root.txt-Datei

### 2.2.5 Handlungsempfehlungen und Maßnahmen

[M2] Der Linux Kernel sollte sofort einem Update unterzogen werden. Gegebenenfalls muss das System durch ein neueres ersetzt werden.

Alternativ hierzu kann die vorhandene Lücke im verwendeten Linux Kernel selbst gepatcht und dieser neu kompiliert werden.

[M3] Möglicherweise hat eine Kompromittierung des Systems durch Angreifer bereits stattgefunden. Es sollten daher sämtliche Passwörter erneuert und Maßnahmen ergriffen werden, die zur Begrenzung der Schäden (durch missbräuchliche Nutzung entwendeter Passwörter oder sonstiger Informationen) beitragen.

## 2.3 Öffentlich zugänglicher, privater RSA-Schlüssel

### 2.3.1 Sachverhalt

Auf dem Server ist ein privater RSA-Schlüssel abgelegt, der öffentlich zugänglich ist und von jedermann heruntergeladen werden kann. Die Tatsache, dass dieser als Hexadezimal-Datei vorliegt, bietet hierbei keinen Schutz vor Missbrauch. Diese „Encodierung“ kann mit Hilfe einfacher Webtools rückgängig gemacht werden.

### 2.3.2 Möglicher Schaden

Ein privater kryptographischer Schlüssel erfüllt seinen Zweck nur, wenn dieser ausschließlich dem Ersteller bekannt ist. Können andere auf den Schlüssel zugreifen, so kann die Identität einer Entität gefälscht werden und mögliche vertrauliche Inhalte können von Dritten eingesehen werden.

In diesem Fall diente der Schlüssel der Authentifikation mit dem Server. Zusammen mit der einfachen Passphrase, die den Schlüssel schützt aber aufgrund anderer Schwachstellen ausgelesen werden konnte, kann sich ein Angreifer am System authentisieren und per SSH Zugriff zum Server erhalten.

### 2.3.3 Risiko

CVSS-Wert: 8.6

(Berücksichtigte Metriken: /AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

**Hoch**

### 2.3.4 Nachweise

Über einen Scan wurden die Ordnerstrukturen des Webservers aufgedeckt. Durch das aktivierte Directory Listing wurde über das Inhaltsverzeichnis des Ordners */dev* die Datei *hype_key* mit dem ungeschützt zugänglichen, privaten Schlüssel entdeckt.

Der nachfolgende Screenshot zeigt das Verzeichnis mit der Schlüsseldatei:

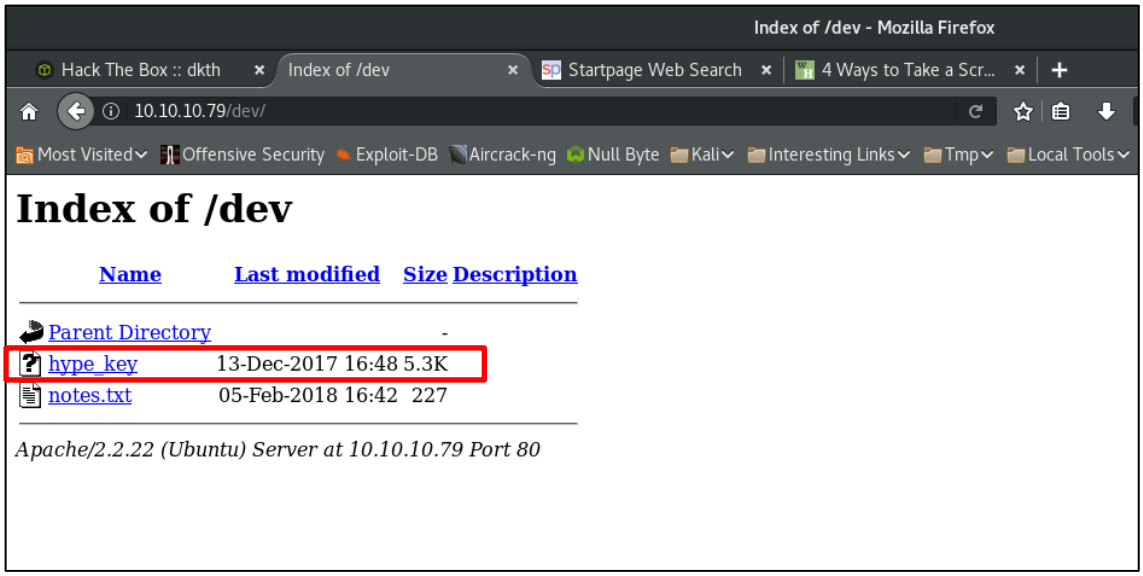



Abbildung 12: Web-Verzeichnis mit ungeschützter Schlüsseldatei

Es stellte sich heraus, dass die Inhalte der Schlüsseldatei im Hexadezimalsystem gespeichert waren:

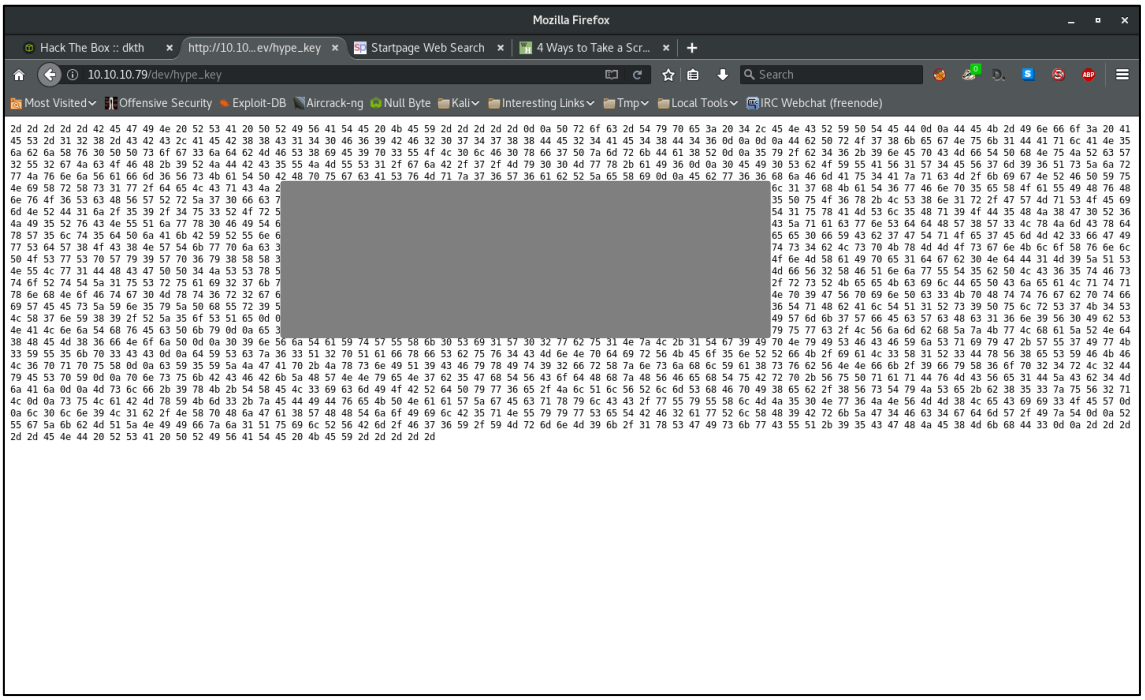



Abbildung 13: Inhalt der Schlüsseldatei in Hexadezimal

Nach einer Recherche konnte die Hexadezimal-Datei konvertiert und mit Hilfe des durch die Heartbleed-Schwachstelle bekannt gewordenen Passworts decodiert werden. Es wurde so der Zugriff auf den privaten RSA-Schlüssel ermöglicht. Der nachfolgende Sreenshot zeigt rechts die noch codierte Schlüsseldatei, unten das Terminalfenster mit der Eingabeaufforderung zur Decodierung und links den decodierten privaten RSA-Schlüssel:

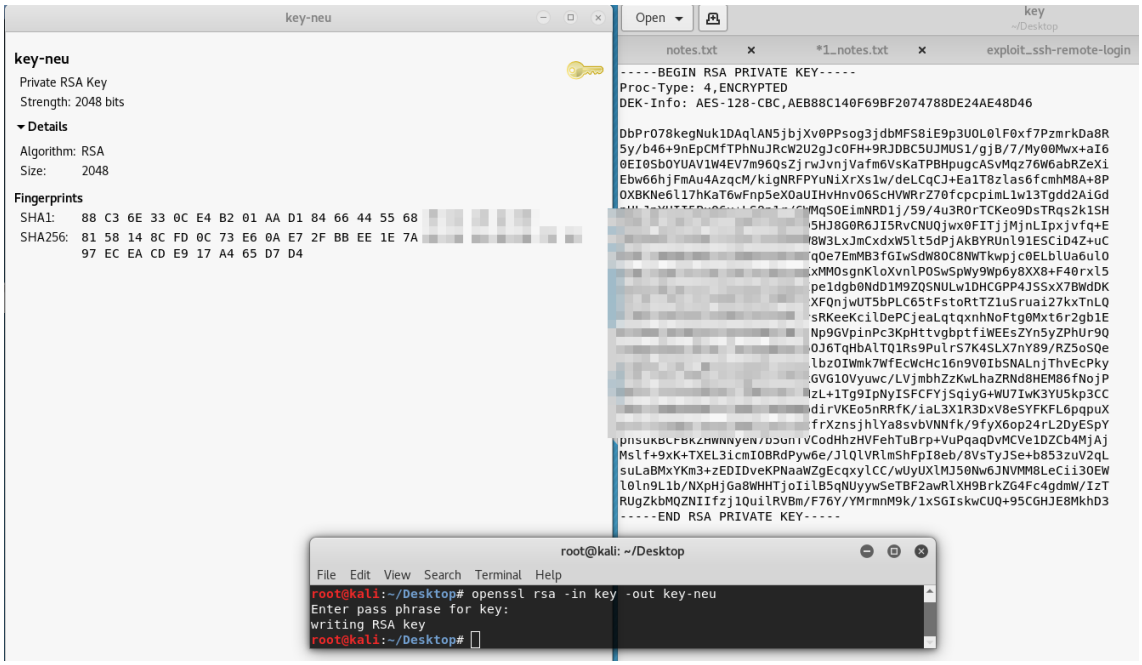



Abbildung 14: Decodierter privater RSA-Schlüssel

Der in Erfahrung gebrachte RSA-Schlüssel dient als Credential im Rahmen der Nutzer-Authentifizierung dem direkten Zugriff per SSH auf den Server.

### 2.3.5 Handlungsempfehlungen und Maßnahmen

[M4] Ein privater Schlüssel darf keinesfalls für jedermann zugänglich auf dem Server abgelegt werden. Er kann (nach Möglichkeit verschlüsselt) bestenfalls im Administratorverzeichnis des Servers abgelegt werden, sollte prinzipiell aber gar nicht auf dem System vorliegen, sondern auf einem gesicherten Speichermedium (z.B. einem verschlüsselten USB-Stick) separat aufbewahrt werden.

## 2.4 OpenSSL Heartbeat Informationsabfluss (Heartbleed Schwachstelle)

### 2.4.1 Sachverhalt

Basierend auf der Antwort des Servers auf eine TLS-Anforderung zum Aufbau einer verschlüsselten Verbindung (HTTPS) wurde erkannt, dass das System anfällig für Informationsabfluss ist. Durch die eine in der genutzten OpenSSL-Bibliothek vorhandene Schwachstelle ist es Angreifern möglich, aufgrund eines durch einen Programmfehler möglichen Pufferüberlaufs, bis zu 64 Kilobyte an Serverspeicher auszulesen.

### 2.4.2 Möglicher Schaden

Der ausgelesene Speicher könnte unter anderem Passwörter, geheime, private Schlüssel oder andere vertrauliche Informationen enthalten. Diese Informationen könnten dem Angreifer bei weiteren Versuchen, das System zu kompromittieren, behilflich sein.

### 2.4.3 Risiko

CVSS-Wert: 5.0

(Berücksichtigte Metriken: /AV:N/AC:L/Au:N/C:P/I:N/A:N)

**Mittel**

### 2.4.4 Nachweise

Nachdem die Anfälligkeit auf Heartbleed mit Hilfe der automatisierten Vulnerabilitätsscanner festgestellt werden konnte, wurde zur Ausnutzung der Schwachstelle das Tool Metasploit herangezogen. Dieses beinhaltet einen Exploit, durch den der Heartbleed-Bug leicht ausnutzbar ist.

Auf der nachfolgenden Seite ist der Befund des Scanners Nessus abgebildet, der detaillierte Informationen zur Schwachstelle beinhaltet:

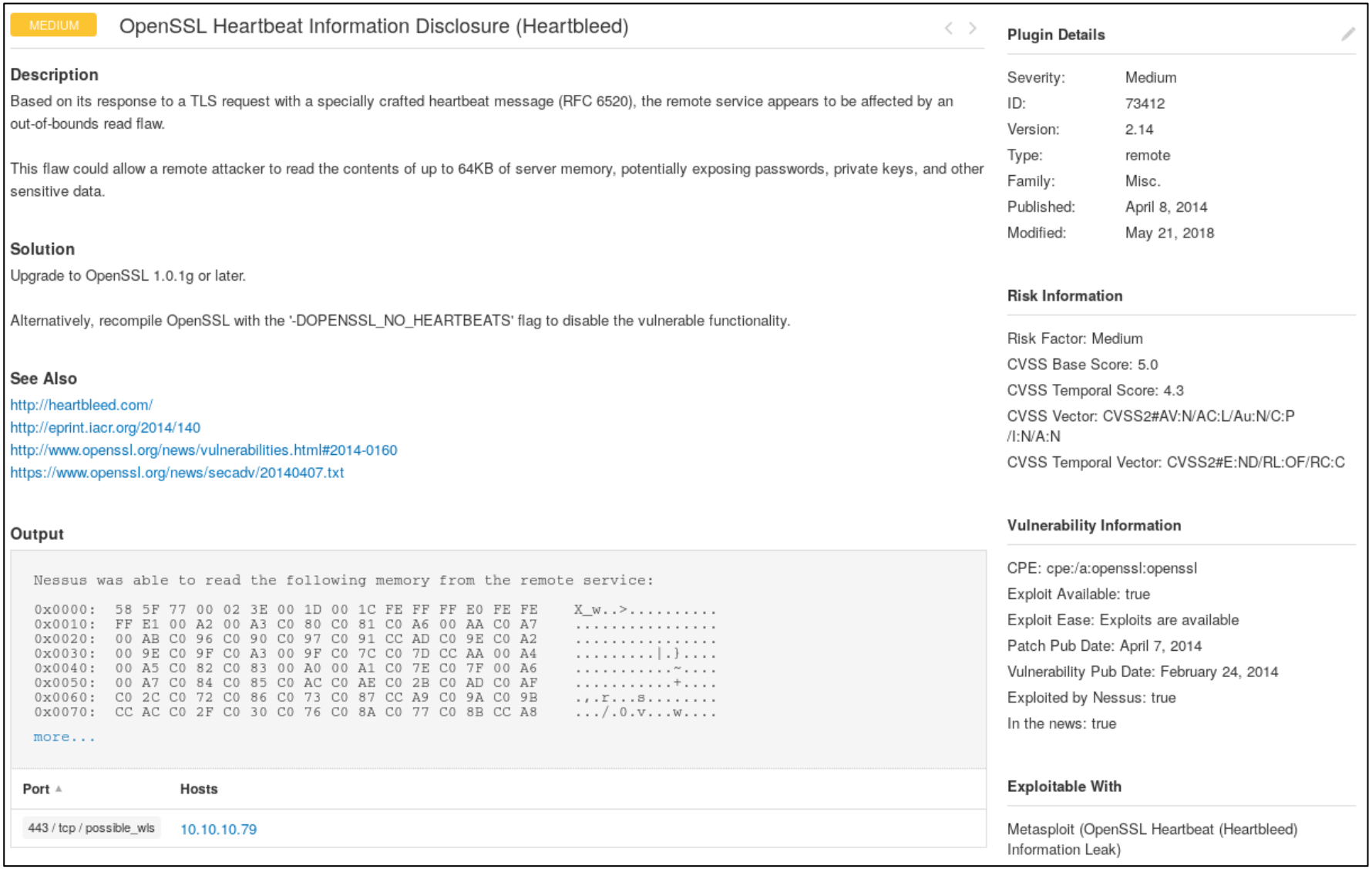



Abbildung 15: Auffinden der Heartbleed-Schwachstelle durch Nessus

Durch Ausführen des vorgefertigten Exploits konnten Daten aus dem Speicher des Servers ausgelesen werden. Der mehrmalige Durchlauf brachte ein in Base64 encodiertes Passwort zum Vorschein:

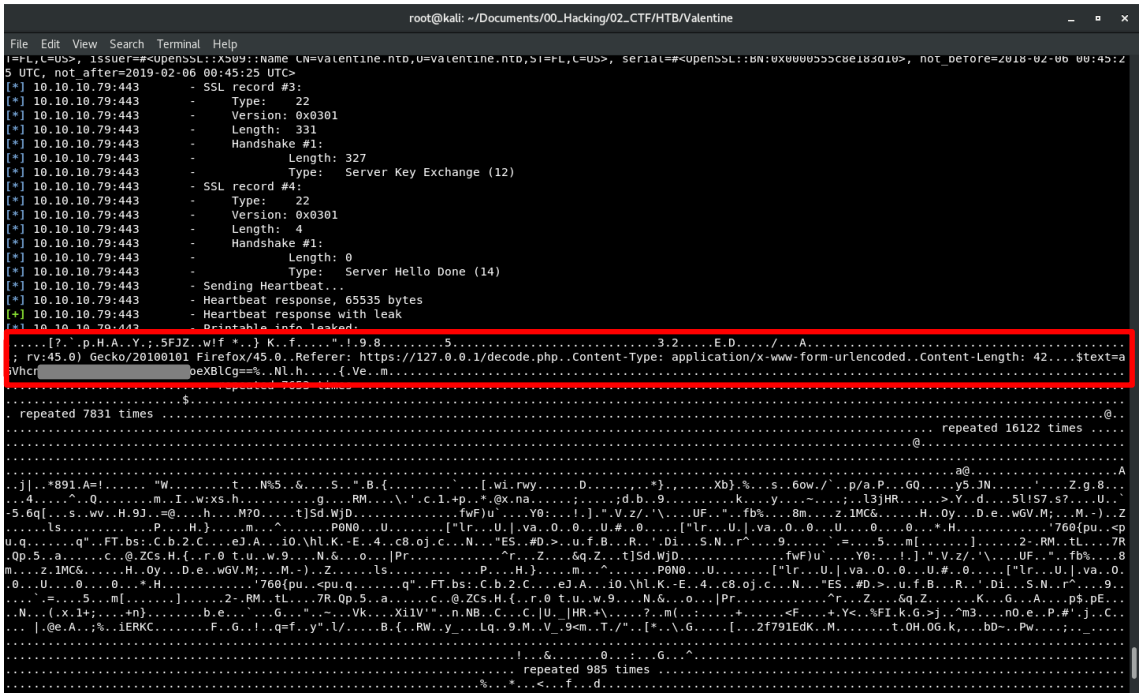



Abbildung 16: Ausnutzen von Heartbleed durch Metasploit

Das aus den Daten des Pufferüberlaufs herausgefischte Passwort wurde anschließend decodiert:


Abbildung 17: Decodiertes Passwort.

### 2.4.5 Handlungsempfehlungen und Maßnahmen

[M5] Die OpenSSL-Version sollte auf die Version OpenSSL 1.0.1g oder höher aktualisiert werden. Alternativ kann die bestehende Version mit dem Flag *-DOPENSSL_NO_HEARTBEAT* neu kompiliert werden.

## 2.5 Öffentlich zugängliche, vertrauliche Informationen

### 2.5.1 Sachverhalt

Analog zum öffentlich zugänglichen privaten Schlüssel konnten auch vertrauliche Notizen frei zugänglich auf dem Webserver gefunden werden.

### 2.5.2 Möglicher Schaden

Die Notizen, die scheinbar vom Administrator stammen, können Aufschluss über verschiedene Schwachstellen des Servers liefern oder andere vertrauliche Informationen offenbaren. Im vorliegenden Fall gaben sie Aufschluss über ein vorhandenes Encodier- bzw. Decodiertool, das auf dem Webserver läuft und offenbar ein Problem hat, das behoben werden muss.

Diese Informationen können einem Angreifer im Rahmen der Informationsgewinnung helfen und das System dadurch leichter angreifbar machen.

### 2.5.3 Risiko

CVSS-Wert: 5.3

(Berücksichtigte Metriken: /AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

**Mittel**

Das Risiko wurde im konkreten Fall auf mittel festgelegt. Die gewonnenen Erkenntnisse trugen zu einer schnelleren Informationsgewinnung bei. Abhängig davon, welche Informationen ein Nutzer öffentlich zugänglich macht, kann das Risiko jedoch signifikant höher oder auch niedriger ausfallen.

### 2.5.4 Nachweise

Der nachfolgende Screenshot zeigt den Browser und die Inhalte des Ordners */dev* auf der Internetseite. Durch das aktivierte Directory Listing ist die darin enthaltene Textdatei *notes.txt* direkt auffindbar:

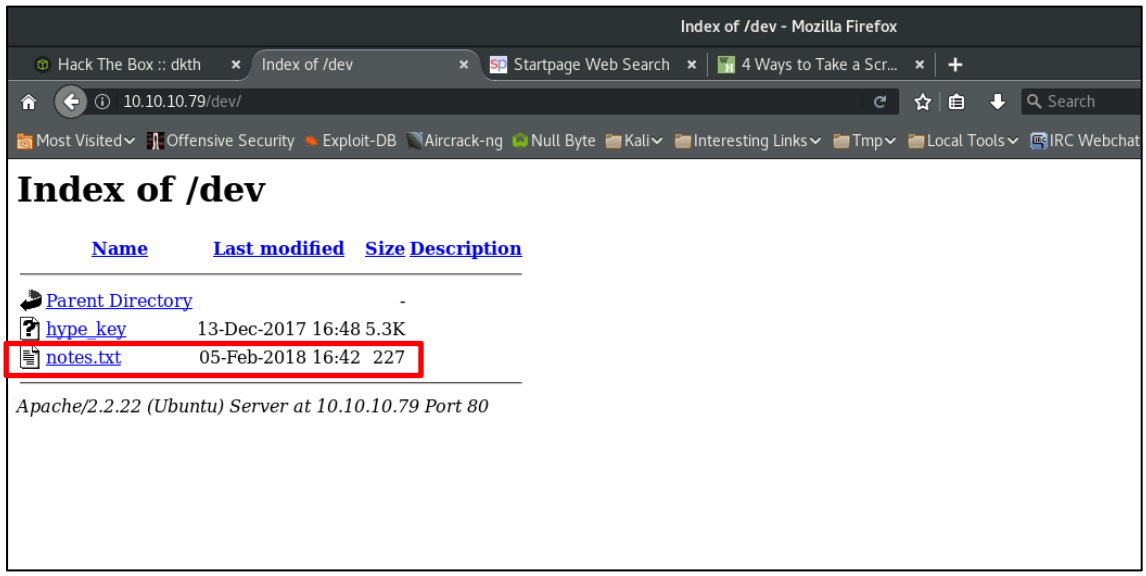



Abbildung 18: Ungeschütztes Verzeichnis mit der Textdatei notes.txt

Aus dem nachfolgenden Screenshot ist der Inhalt der Textdatei ersichtlich:

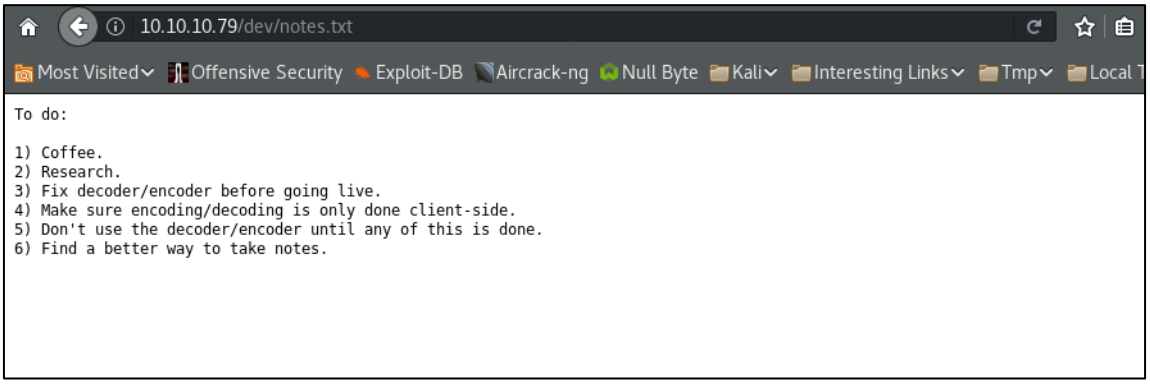



Abbildung 19: Öffentlich zugängliche Notizen auf dem Webserver

### 2.5.5 Handlungsempfehlungen und Maßnahmen

[M6] Diese Informationen sollten ebenfalls nur für den Administrator ersichtlich sein und sich keinesfalls in Verzeichnissen befinden, auf die Webseitenbesucher Zugriff haben. Sensible Informationen sollten zudem in verschlüsselter Form gespeichert und gegebenenfalls auf getrennten Speichermedien aufbewahrt werden. Sofern nicht aus einem bestimmten Grund erforderlich, kann zudem ergänzend das Directory Listing deaktiviert werden.

## 2.6 Sonstige Befunde

Im Rahmen der Untersuchung wurden weitere Schwachstellen gefunden und Sachverhalte festgestellt, von denen ein potenzielles Risiko ausgeht. Diese spielten jedoch beim Ablauf des Penetration-Testings keine besondere Rolle. Es handelt sich dabei auch größtenteils nicht um direkt ausnutzbare Schwachstellen, sondern um Sachverhalte, die einem Angreifer weitere Ansatzpunkte liefern können oder um technische Aspekte, die einer weiteren Prüfung bedürfen. Aus Gründen der Vollständigkeit und da auch diese Punkte ein potenzielles Risiko in sich bergen, sind sie nachfolgend aufgeführt:

**MITTEL** **OS Identification; Apache Banner Linux Distribution Disclosure; SSH Server Type, Version and Protocol Information; HTTP-Server Type and Version; HTTP Information; PHP Version Detection; mDNS Detection (Information Gathering):**

Es ist Angreifern leicht möglich, Informationen zum eingesetzten Betriebssystem und zum Webserver zu erhalten. Diese Angaben werden genauso wie Informationen zu genutzten Diensten und unterstützten Protokollen vom Server selbst bekannt gegeben bzw. lassen sich via Bannergrabbing ermitteln. Darüber hinaus ist der mDNS -Service (bzw. Bonjour, ZeroConf) aktiv, welcher detaillierte Systeminformationen liefert.

**MITTEL** **OpenSSL 'ChangeCipherSpec' MiTM Vulnerability:**

Die SSL-Implementierung OpenSSL ist als Bibliothek in der verwendeten Version verwundbar. Angreifer können durch einen fehlerhaften Handshake mittels ChangeCipherSpec-Anfrage den Server auf eine unsichere Methode herunterhandeln. Als Folge werden eine Man-in-the-Middle-Attacke (MitM) und das Dechiffrieren verschlüsselter Datenpakete ermöglicht.

**MITTEL** **SSH Weak Algorithms Supported:**

Der SSH-Server erlaubt die Nutzung schwacher Verschlüsselungsalgorithmen bzw. schwacher Schlüssel.

**MITTEL** **SSL Certificate Cannot Be Trusted / SSL Self-Signed Certificate:**

Das verwendete SSL-Zertifikat (X.509) ist nicht vertrauenswürdig, da es nicht von einer anerkannten Zertifikatsstelle stammt. Es handelt sich um ein selbst-signiertes Zertifikat.

**MITTEL** **SSL Certificate Signed Using Weak Hashing Algorithm:**

Die Zertifikatskette zum genutzten SSL-Zertifikat ist unsicher. Möglicherweise ist ein übergeordnetes Zertifikat aufgrund der Verwendung verwundbarer Algorithmen angreifbar. Ein Angreifer ist gegebenenfalls in der Lage, sich ein anderes Zertifikat mit derselben Signatur auszustellen, um sich als „Valentine“ auszugeben.

**NIEDRIG** **SSH Server CBC Mode Ciphers Enabled:**

Der SSH-Server unterstützt die Verschlüsselung im Cipher Block Chaining-Modus (CBC). Bei der Verwendung des CBC-Modus können Angreifer möglicherweise die Verschlüsselung brechen und Texte entschlüsseln.

**NIEDRIG** **SSH Weak MAC Algorithms Enabled:**

Der SSH-Server unterstützt MD5 bzw. 96-bit MAC-Algorithmen. Beide Verfahren sind unsicher und können gebrochen werden.

**N/A** **HSTS Missing From HTTPS Server:**

Der Webserver hat keinen HTTP Strict Transport Security (HSTS)-Header gesetzt. Der Seitenaufruf kann auch folglich ohne HTTPS erfolgen und der Browser wird nicht angewiesen, ausschließlich einen verschlüsselten Verbindungsaufbau zu akzeptieren. Angreifer könnten diesen Umstand für eine Downgrade-Attacke oder im Rahmen des Session Hijacking nutzen.

**N/A** **ICMP Timestamp Request Remote Date Disclosure:**

Der Server antwortet auf eine ICMP-Timestamp-Anfrage mit der genauen Serverzeit. Dies kann von Angreifern bei der Verwendung zeitbezogener Authentisierungsverfahren ausgenutzt werden.

**N/A** **Script-/SQL-Injection:**

Die Eingabemaske des Base64-Decoders/Encoders könnte gegenüber Injections mit schädlichem Code verwundbar sein, sofern keine Validierung der Eingaben erfolgt.

Eine detaillierte Bewertung der oben aufgeführten Punkte hinsichtlich des jeweils davon ausgehenden Risikos wurde an dieser Stelle nicht durchgeführt. Der jeweilige CVSS-Score kann jedoch dem Bericht des Schwachstellenscanners Nessus entnommen werden, der sich im Anhang befindet.

Die Auflistung der Schwachstellen erhebt keinen Anspruch auf Vollständigkeit. Auf Grund der knappen Zeitvorgabe wurden nicht alle potenziellen Schwachstellen erschöpfend analysiert. Im Rahmen des durchgeführten Penetration-Testings wurde das primäre Ziel verfolgt, Administratorrechte auf dem Server zu erlangen. Dies ist auch ohne eine Ausnutzung der in dieser Liste dargestellten Mängel möglich. Einige Aspekte, wie die Script-/SQL-Injection, bedürfen außerdem einer tiefergehenden Abklärung durch den Programmierer des Decoders/Encoders. Zudem sind nicht alle Aspekte unmittelbar sicherheitsrelevant.

Dennoch sollten die oben aufgelisteten Punkte im Rahmen einer umfassenden Evaluierung herangezogen werden, um zusammen mit den Verantwortlichen eine Verbesserung der Server-Sicherheit zu erreichen.

# 3 Handlungsempfehlungen (Übersicht)

Die nachfolgenden Handlungsempfehlungen stellen eine gekürzte Gesamtübersicht der in den vorherigen Kapiteln abgegebenen Einzelempfehlungen dar:

| ID | Maßnahme | Kategorie |
|---|---|---|
| [M1] | Das System sollte auf ein derzeit unterstütztes Betriebssystem aktualisiert werden (z.B. Ubuntu Version 17.10). | Technisch |
| [M2] | Der Linux Kernel sollte sofort einem Update unterzogen werden. Gegebenenfalls muss das System durch ein neueres ersetzt werden.<br>Alternativ hierzu kann die vorhandene Lücke im verwendeten Linux Kernel selbst gepatcht und dieser neu kompiliert werden. | Technisch |
| [M3] | Möglicherweise hat eine Kompromittierung des Systems durch Angreifer bereits stattgefunden. Es sollten daher sämtliche Passwörter erneuert und Maßnahmen ergriffen werden, die zur Begrenzung der Schäden (durch missbräuchliche Nutzung entwendeter Passwörter oder sonstiger Informationen) beitragen. | Organisatorisch |
| [M4] | Ein privater Schlüssel darf keinesfalls für jedermann zugänglich auf dem Server abgelegt werden. Er kann (nach Möglichkeit verschlüsselt) bestenfalls im Administratorverzeichnis des Servers abgelegt werden, sollte prinzipiell aber gar nicht auf dem System vorliegen, sondern auf einem gesicherten Speichermedium (z.B. einem verschlüsselten USB-Stick) separat aufbewahrt werden. | Organisatorisch |
| [M5] | Die OpenSSL-Version sollte auf die Version OpenSSL 1.0.1g oder höher aktualisiert werden. Alternativ kann die bestehende Version mit dem Flag -DOPENSSL_NO_HEARTBEAT neu kompiliert werden. | Technisch |
| [M6] | Vertrauliche Informationen sollten nur für den Administrator ersichtlich sein und sich keinesfalls in Verzeichnissen befinden, auf die Webseitenbesucher Zugriff haben. Sensible Informationen sollten zudem in verschlüsselter Form gespeichert und gegebenenfalls auf getrennten Speichermedien aufbewahrt werden. Sofern nicht aus einem bestimmten Grund erforderlich, kann zudem ergänzend das Directory Listing deaktiviert werden. | Technisch/ Organisatorisch |

Tabelle 6: Maßnahmenübersicht

# Anlagen

- Nessus Scan Report
  vom 08. Juli 2018

# Nessus Report

## Nessus Scan Report

## Sun, 08 Jul 2018 15:31:25 CEST

# Table Of Contents

# Vulnerabilities By Host

## 10.10.10.79

### Scan Information

| | |
|---|---|
| Start time: | Sun Jul 8 15:19:56 2018 |
| End time: | Sun Jul 8 15:31:25 2018 |

### Host Information

| | |
|---|---|
| IP: | 10.10.10.79 |
| OS: | Linux Kernel 3.0 on Ubuntu 12.04 (precise) |

### Results Summary

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 1 | 0 | 7 | 2 | 36 | 46 |

### Results Details

#### 0/icmp

#### 10114 - ICMP Timestamp Request Remote Date Disclosure

**Synopsis**

It is possible to determine the exact time set on the remote host.

**Description**

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

**Solution**

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

**Risk Factor**

None

**References**

| | |
|---|---|
| **CVE** | CVE-1999-0524 |
| **XREF** | OSVDB:94 |
| **XREF** | CWE:200 |

**Plugin Information:**

Publication date: 1999/08/01, Modification date: 2012/06/18

**Ports**

**icmp/0**

```
The remote clock is synchronized with the local clock.
```

#### 0/tcp

#### 33850 - Unix Operating System Unsupported Version Detection

**Synopsis**

The operating system running on the remote host is no longer supported.

**Description**

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

**Solution**

Upgrade to a version of the Unix operating system that is currently supported.

### Risk Factor

Critical

### CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

### CVSS Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### Plugin Information:

Publication date: 2008/08/08, Modification date: 2018/04/27

### Ports

**tcp/0**

```
Ubuntu 12.04 support ended on 2017-04-30.
Upgrade to Ubuntu 17.10.

For more information, see : https://wiki.ubuntu.com/Releases
```

## 11936 - OS Identification

### Synopsis

It is possible to guess the remote operating system.

### Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2003/12/09, Modification date: 2018/04/19

### Ports

**tcp/0**

```
Remote operating system : Linux Kernel 3.0 on Ubuntu 12.04 (precise)
Confidence level : 95
Method : SSH


The remote host is running Linux Kernel 3.0 on Ubuntu 12.04 (precise)
```

## 18261 - Apache Banner Linux Distribution Disclosure

### Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.

### Description

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

### Solution

If you do not wish to display this information, edit 'httpd.conf' and set the directive 'ServerTokens Prod' and restart Apache.
n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2005/05/15, Modification date: 2017/03/13

### Ports
#### tcp/0

```
The Linux distribution detected was :
 - Ubuntu 12.04 (precise)
 - Ubuntu 12.10 (quantal)
 - Ubuntu 13.04 (raring)
```

## 19506 - Nessus Scan Information

### Synopsis

This plugin displays information about the Nessus scan.

### Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2005/08/26, Modification date: 2017/10/26

### Ports
#### tcp/0

```
Information about this scan :

Nessus version : 6.11.1
Plugin feed version : 201807062021
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Basic Network Scan
Scanner IP : 10.10.14.100
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2018/7/8 15:20 CEST
Scan duration : 685 sec
```

## 45590 - Common Platform Enumeration (CPE)

### Synopsis

It was possible to enumerate CPE names that matched on the remote system.

### Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

### See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2010/04/21, Modification date: 2017/06/06

### Ports

**tcp/0**

```
The remote operating system matched the following CPE :

  cpe:/o:canonical:ubuntu_linux:12.04

Following application CPE's matched on the remote system :

  cpe:/a:openbsd:openssh:5.9 -> OpenBSD OpenSSH 5.9
  cpe:/a:apache:http_server:2.2.22 -> Apache Software Foundation Apache HTTP Server 2.2.22
  cpe:/a:php:php:5.3.10 -> PHP 5.3.10
```

## 54615 - Device Type

### Synopsis

It is possible to guess the remote device type.

### Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

### Ports

**tcp/0**

```
Remote device type : general-purpose
Confidence level : 95
```

## 66334 - Patch Report

### Synopsis

The remote host is missing several patches.

### Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

### Solution

Install the patches listed below.

### Risk Factor

None

### Plugin Information:

Publication date: 2013/07/08, Modification date: 2018/06/20

### Ports

#### tcp/0

```
. You need to take the following action :

[ OpenSSL 'ChangeCipherSpec' MiTM Vulnerability (77200) ]

+ Action to take : OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za.
 OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m. OpenSSL 1.0.1 SSL/
TLS users (client and/or server) should upgrade to 1.0.1h.
```

## 110723 - No Credentials Provided

### Synopsis

Nessus was able to find common ports used for local checks, however, no credentails were provided in the scan policy.

### Description

Nessus was unable to execute credentialed checks because no credentials were provided.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2018/06/27, Modification date: 2018/06/27

### Ports

#### tcp/0

```
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.
```

## 0/udp

## 10287 - Traceroute Information

### Synopsis

It was possible to obtain traceroute information.

### Description

Makes a traceroute to the remote host.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 1999/11/27, Modification date: 2017/08/22

### Ports

#### udp/0

```
For your information, here is the traceroute from 10.10.14.100 to 10.10.10.79 :
10.10.14.100
10.10.14.1
10.10.10.79

Hop Count: 2
```

## 22/tcp

### 90317 - SSH Weak Algorithms Supported

#### Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

#### Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

#### See Also

https://tools.ietf.org/html/rfc4253#section-6.3

#### Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

#### Risk Factor

Medium

#### CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

#### Plugin Information:

Publication date: 2016/04/04, Modification date: 2016/12/14

#### Ports

**tcp/22**

```
The following weak server-to-client encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256

The following weak client-to-server encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256
```

### 70658 - SSH Server CBC Mode Ciphers Enabled

#### Synopsis

The SSH server is configured to use Cipher Block Chaining.

#### Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.
Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

#### Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

#### Risk Factor

Low

#### CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

#### CVSS Temporal Score

2.6 (CVSS2#E:ND/RL:ND/RC:ND)

#### References

| | |
|---|---|
| **BID** | 32319 |
| **CVE** | CVE-2008-5161 |

| | |
|---|---|
| **XREF** | OSVDB:50035 |
| **XREF** | OSVDB:50036 |
| **XREF** | CERT:958563 |
| **XREF** | CWE:200 |

### Plugin Information:

Publication date: 2013/10/28, Modification date: 2016/05/12

### Ports

**tcp/22**

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

## 71049 - SSH Weak MAC Algorithms Enabled

### Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

### Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.
Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

### Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

### Risk Factor

Low

### CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

### Plugin Information:

Publication date: 2013/11/22, Modification date: 2016/12/14

### Ports

**tcp/22**

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
  hmac-sha2-256-96
  hmac-sha2-512-96
```

```
The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
  hmac-sha2-256-96
  hmac-sha2-512-96
```

## 10267 - SSH Server Type and Version Information

### Synopsis

An SSH server is listening on this port.

### Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 1999/10/12, Modification date: 2017/12/19

### Ports

**tcp/22**

```
SSH version : SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.10
SSH supported authentication : publickey,password
```

## 10881 - SSH Protocol Versions Supported

### Synopsis

A SSH server is running on the remote host.

### Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2002/03/06, Modification date: 2017/05/30

### Ports

**tcp/22**

```
The remote SSH daemon supports the following versions of the
SSH protocol :

  - 1.99
  - 2.0
```

## 11219 - Nessus SYN scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/05/22

### Ports

**tcp/22**

```
Port 22/tcp was found to be open
```

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2007/08/19, Modification date: 2018/05/03

### Ports

**tcp/22**

```
An SSH server is running on this port.
```

## 39520 - Backported Security Patch Detection (SSH)

### Synopsis

Security patches are backported.

### Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.
Banner-based checks have been disabled to avoid false positives.
Note that this test is informational only and does not denote any security problem.

### See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2009/06/25, Modification date: 2015/07/07

### Ports

**tcp/22**

```
Give Nessus credentials to perform local checks.
```

## 70657 - SSH Algorithms and Languages Supported

### Synopsis

An SSH server is listening on this port.

### Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

### Solution

n/a

## Risk Factor

None

## Plugin Information:

Publication date: 2013/10/28, Modification date: 2017/08/28

## Ports

### tcp/22

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  ssh-dss
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha2-256
  hmac-sha2-256-96
  hmac-sha2-512
  hmac-sha2-512-96
```

```
  umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha2-256
  hmac-sha2-256-96
  hmac-sha2-512
  hmac-sha2-512-96
  umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

  none
  zlib@openssh.com
```

## 80/tcp

## 10107 - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

This plugin attempts to determine the type and the version of the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2000/01/04, Modification date: 2018/05/23

### Ports

#### tcp/80

```
The remote web server type is :

Apache/2.2.22 (Ubuntu)
```

## 11219 - Nessus SYN scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/05/22

### Ports

#### tcp/80

```
Port 80/tcp was found to be open
```

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2007/08/19, Modification date: 2018/05/03

### Ports

#### tcp/80

```
A web server is running on this port.
```

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2007/01/30, Modification date: 2017/11/13

### Ports

#### tcp/80

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Sun, 08 Jul 2018 13:24:51 GMT
  Server: Apache/2.2.22 (Ubuntu)
  X-Powered-By: PHP/5.3.10-1ubuntu3.26
  Vary: Accept-Encoding
  Content-Length: 38
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<center><img src="omg.jpg"/></center>
```

## 39521 - Backported Security Patch Detection (WWW)

### Synopsis

Security patches are backported.

### Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.
Banner-based checks have been disabled to avoid false positives.
Note that this test is informational only and does not denote any security problem.

### See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2009/06/25, Modification date: 2015/07/07

### Ports

**tcp/80**

```
Give Nessus credentials to perform local checks.
```

## 48204 - Apache HTTP Server Version

### Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

### Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2010/07/30, Modification date: 2018/01/22

### Ports

**tcp/80**

```
URL        : http://10.10.10.79/
Version    : 2.2.99
backported : 1
os         : ConvertedUbuntu
```

## 48243 - PHP Version Detection

### Synopsis

It was possible to obtain the version number of the remote PHP installation.

### Description

Nessus was able to determine the version of PHP available on the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2010/08/04, Modification date: 2017/07/07

### Ports

**tcp/80**

```
Nessus was able to identify the following PHP version information :

  Version : 5.3.10-1ubuntu3.26
  Source  : X-Powered-By: PHP/5.3.10-1ubuntu3.26
```

## 84574 - Backported Security Patch Detection (PHP)

### Synopsis

Security patches have been backported.

### Description

Security patches may have been 'backported' to the remote PHP install without changing its version number.
Banner-based checks have been disabled to avoid false positives.
Note that this test is informational only and does not denote any security problem.

### See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2015/07/07, Modification date: 2015/07/07

### Ports

#### tcp/80

```
Give Nessus credentials to perform local checks.
```

## 443/tcp

## 35291 - SSL Certificate Signed Using Weak Hashing Algorithm

### Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

### Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.
Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.
Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

### See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?e120eea1

http://technet.microsoft.com/en-us/security/advisory/961509

### Solution

Contact the Certificate Authority to have the certificate reissued.

### Risk Factor

Medium

### CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

### CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

### References

| | |
|---|---|
| **BID** | 11849 |

| | |
|---|---|
| **BID** | 33065 |
| **CVE** | CVE-2004-2761 |
| **XREF** | OSVDB:45106 |
| **XREF** | OSVDB:45108 |
| **XREF** | OSVDB:45127 |
| **XREF** | CERT:836068 |
| **XREF** | CWE:310 |

### Plugin Information:

Publication date: 2009/01/05, Modification date: 2018/05/21

### Ports

**tcp/443**

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

|-Subject             : C=US/ST=FL/O=valentine.htb/CN=valentine.htb
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Feb 06 00:45:25 2018 GMT
|-Valid To            : Feb 06 00:45:25 2019 GMT
```

## 51192 - SSL Certificate Cannot Be Trusted

### Synopsis

The SSL certificate for this service cannot be trusted.

### Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

### See Also

http://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

### Solution

Purchase or generate a proper certificate for this service.

### Risk Factor

Medium

### CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

### CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

### Plugin Information:

Publication date: 2010/12/15, Modification date: 2017/05/18

### Ports

tcp/443

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : C=US/ST=FL/O=valentine.htb/CN=valentine.htb
|-Issuer  : C=US/ST=FL/O=valentine.htb/CN=valentine.htb
```

## 57582 - SSL Self-Signed Certificate

### Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

### Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

### Solution

Purchase or generate a proper certificate for this service.

### Risk Factor

Medium

### CVSS Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

### Plugin Information:

Publication date: 2012/01/17, Modification date: 2016/12/14

### Ports

tcp/443

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : C=US/ST=FL/O=valentine.htb/CN=valentine.htb
```

## 73412 - OpenSSL Heartbeat Information Disclosure (Heartbleed)

### Synopsis

The remote service is affected by an information disclosure vulnerability.

### Description

Based on its response to a TLS request with a specially crafted heartbeat message (RFC 6520), the remote service appears to be affected by an out-of-bounds read flaw.
This flaw could allow a remote attacker to read the contents of up to 64KB of server memory, potentially exposing passwords, private keys, and other sensitive data.

### See Also

http://heartbleed.com/

http://eprint.iacr.org/2014/140

http://www.openssl.org/news/vulnerabilities.html#2014-0160

https://www.openssl.org/news/secadv/20140407.txt

### Solution

Upgrade to OpenSSL 1.0.1g or later.
Alternatively, recompile OpenSSL with the '-DOPENSSL_NO_HEARTBEATS'

flag to disable the vulnerable functionality.

### Risk Factor

Medium

### CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### CVSS Temporal Score

4.3 (CVSS2#E:ND/RL:OF/RC:C)

### References

| | |
|---|---|
| **BID** | 66690 |
| **CVE** | CVE-2014-0160 |
| **XREF** | OSVDB:105465 |
| **XREF** | CERT:720951 |
| **XREF** | EDB-ID:32745 |
| **XREF** | EDB-ID:32764 |
| **XREF** | EDB-ID:32791 |
| **XREF** | EDB-ID:32998 |

### Exploitable with

Core Impact (true)Metasploit (true)

### Plugin Information:

Publication date: 2014/04/08, Modification date: 2018/05/21

### Ports

**tcp/443**

```
Nessus was able to read the following memory from the remote service:

0x0000:  58 5F 77 00 02 3E 00 1D 00 1C FE FF FF E0 FE FE    X_w..>..........
0x0010:  FF E1 00 A2 00 A3 C0 80 C0 81 C0 A6 00 AA C0 A7    ................
0x0020:  00 AB C0 96 C0 90 C0 97 C0 91 CC AD C0 9E C0 A2    ................
0x0030:  00 9E C0 9F C0 A3 00 9F C0 7C C0 7D CC AA 00 A4    .........|.}....
0x0040:  00 A5 C0 82 C0 83 00 A0 00 A1 C0 7E C0 7F 00 A6    ...........~....
0x0050:  00 A7 C0 84 C0 85 C0 AC C0 AE C0 2B C0 AD C0 AF    ...........+....
0x0060:  C0 2C C0 72 C0 86 C0 73 C0 87 CC A9 C0 9A C0 9B    .,.r...s........
0x0070:  CC AC C0 2F C0 30 C0 76 C0 8A C0 77 C0 8B CC A8    .../.0.v...w....
0x0080:  C0 2D C0 2E C0 74 C0 88 C0 75 C0 89 C0 31 C0 32    .-...t...u...1.2
0x0090:  C0 78 C0 8C C0 79 C0 8D C0 AA C0 AB C0 A4 C0 A8    .x...y..........
0x00A0:  00 A8 C0 A5 C0 A9 00 A9 C0 94 C0 8E C0 95 C0 8F    ................
0x00B0:  CC AB 00 AC 00 AD C0 98 C0 92 C0 99 C0 93 CC AE    ................
0x00C0:  C0 9C C0 A0 00 9C C0 9D C0 A1 00 9D C0 7A C0 7B    ............z.{
0x00D0:  00 63 00 65 00 11 00 13 00 32 00 38 00 44 00 87    .c.e.....2.8.D..
0x00E0:  00 12 00 66 00 99 00 8F 00 90 00 91 00 8E 00 14    ...f............
0x00F0:  00 16 00 33 00 39 00 45 00 88 00 15 00 9A 00 0B    ...3.9.E........
0x0100:  00 0D 00 30 00 36 00 42 00 85 00 0C 00 97 00 0E    ...0.6.B........
0x0110:  00 10 00 31 00 37 00 43 00 86 00 0F 00 98 00 19    ...1.7.C........
0x0120:  00 17 00 1B 00 34 00 3A 00 46 00 89 00 1A 00 18    .....4.:.F......
0x0130:  00 9B C0 08 C0 09 C0 0A C0 06 C0 07 C0 12 C0 13    ................
0x0140:  C0 14 C0 10 C0 11 C0 03 C0 04 C0 05 C0 01 C0 02    ................
0x0150:  C0 0D C0 0E C0 0F C0 0B C0 0C C0 15 C0 17 C0 18    ................
0x0160:  C0 19 C0 16 00 29 00 26 00 2A 00 27 00 2B 00 28    .....).&.*.'.+.(
0x0170:  00 23 00 1F 00 22 00 1E 00 25 00 21 00 24 00 20    .#..."...%.!.$.
0x0180:  00 00 00 8B 00 8C 00 8D 00 8A 00 62 00 61 00 60    ...........b.a.`
0x0190:  00 64 00 08 00 06 00 03 00 93 00 94 00 95 00 [...]
```

## 77200 - OpenSSL 'ChangeCipherSpec' MiTM Vulnerability

### Synopsis

The remote host is affected by a vulnerability that could allow sensitive data to be decrypted.

## Description

The OpenSSL service on the remote host is vulnerable to a man-in-the-middle (MiTM) attack, based on its acceptance of a specially crafted handshake.
This flaw could allow a MiTM attacker to decrypt or forge SSL messages by telling the service to begin encrypted communications before key material has been exchanged, which causes predictable keys to be used to secure future traffic.
Note that Nessus has only tested for an SSL/TLS MiTM vulnerability (CVE-2014-0224). However, Nessus has inferred that the OpenSSL service on the remote host is also affected by six additional vulnerabilities that were disclosed in OpenSSL's June 5th, 2014 security advisory :
- An error exists in the 'ssl3_read_bytes' function that permits data to be injected into other sessions or allows denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2010-5298)
- An error exists related to the implementation of the Elliptic Curve Digital Signature Algorithm (ECDSA) that allows nonce disclosure via the 'FLUSH+RELOAD' cache side-channel attack. (CVE-2014-0076)
- A buffer overflow error exists related to invalid DTLS fragment handling that permits the execution of arbitrary code or allows denial of service attacks.
Note that this issue only affects OpenSSL when used as a DTLS client or server. (CVE-2014-0195)
- An error exists in the 'do_ssl3_write' function that permits a NULL pointer to be dereferenced, which could allow denial of service attacks. Note that this issue is exploitable only if SSL_MODE_RELEASE_BUFFERS is enabled. (CVE-2014-0198)
- An error exists related to DTLS handshake handling that could allow denial of service attacks. Note that this issue only affects OpenSSL when used as a DTLS client.
(CVE-2014-0221)
- An error exists in the 'dtls1_get_message_fragment'
function related to anonymous ECDH cipher suites. This could allow denial of service attacks. Note that this issue only affects OpenSSL TLS clients. (CVE-2014-3470)
OpenSSL did not release individual patches for these vulnerabilities, instead they were all patched under a single version release. Note that the service will remain vulnerable after patching until the service or host is restarted.

## See Also

http://www.nessus.org/u?d5709faa

https://www.imperialviolet.org/2014/06/05/earlyccs.html

https://www.openssl.org/news/secadv/20140605.txt

## Solution

OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za. OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m. OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h.

## Risk Factor

Medium

## CVSS v3.0 Base Score

5.6 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)

## CVSS Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

## CVSS Temporal Score

5.9 (CVSS2#E:ND/RL:OF/RC:C)

## References

| | |
|---|---|
| **BID** | 66363 |
| **BID** | 66801 |
| **BID** | 67193 |
| **BID** | 67898 |
| **BID** | 67899 |
| **BID** | 67900 |

| | |
|---|---|
| **BID** | 67901 |
| **CVE** | CVE-2010-5298 |
| **CVE** | CVE-2014-0076 |
| **CVE** | CVE-2014-0195 |
| **CVE** | CVE-2014-0198 |
| **CVE** | CVE-2014-0221 |
| **CVE** | CVE-2014-0224 |
| **CVE** | CVE-2014-3470 |
| **XREF** | OSVDB:104810 |
| **XREF** | OSVDB:105763 |
| **XREF** | OSVDB:106531 |
| **XREF** | OSVDB:107729 |
| **XREF** | OSVDB:107730 |
| **XREF** | OSVDB:107731 |
| **XREF** | OSVDB:107732 |
| **XREF** | CERT:978508 |

### Exploitable with

Core Impact (true)

### Plugin Information:

Publication date: 2014/08/14, Modification date: 2018/06/03

### Ports

**tcp/443**

```
The remote service on port 443 accepted an early ChangeCipherSpec message, which caused
the MAC and encryption keys to be derived entirely from public information. The entire SSL
handshake was completed, with the server accepting and producing messages encrypted and
authenticated using these weak keys.
```

## 10107 - HTTP Server Type and Version

### Synopsis

A web server is running on the remote host.

### Description

This plugin attempts to determine the type and the version of the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2000/01/04, Modification date: 2018/05/23

### Ports

**tcp/443**

```
The remote web server type is :
```

```
Apache/2.2.22 (Ubuntu)
```

## 10863 - SSL Certificate Information

### Synopsis

This plugin displays the SSL certificate.

### Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2008/05/19, Modification date: 2015/12/30

### Ports

#### tcp/443

```
Subject Name:

Country: US
State/Province: FL
Organization: valentine.htb
Common Name: valentine.htb

Issuer Name:

Country: US
State/Province: FL
Organization: valentine.htb
Common Name: valentine.htb

Serial Number: 00 85 EC 6D F5 C5 84 B1 F2

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Feb 06 00:45:25 2018 GMT
Not Valid After: Feb 06 00:45:25 2019 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C3 28 17 AC F8 19 2A 41 D2 8A 3F CE 79 1C 19 F4 FB 48 FA
            D3 2F 33 6B 6F C8 9C F9 A3 BF 19 66 A8 A1 8D F9 22 62 0E E1
            9E 45 50 1F 59 2F AC BA 95 CF AF 23 AA 54 C9 64 40 0F 25 A8
            C5 DD CB C4 1C 87 0C D2 73 12 2E 77 76 CF 89 48 FB 39 4A E1
            F5 3D 40 C3 B5 9A 82 68 F6 8D 8C B2 4D 3F 4F 03 09 C0 BA AD
            74 5D 53 64 B0 57 6A 44 0F 1F B7 F6 FB 05 88 AE B2 C1 CA DE
            A6 FB C5 66 77 46 29 75 60 D0 AF 91 DD 59 30 3A 0B 8F 85 21
            E5 5D C8 22 1C 56 EA 7A 2F 0D 27 5C E2 A7 D6 2E 55 46 17 87
            22 D5 1B 66 62 25 85 FA 09 1C 38 6D 1B 14 9E A9 7A E0 31 4D
            43 26 CE B0 91 E6 D0 9B 48 D8 CF 4F 79 F9 AF 12 44 D4 65 E4
            FF 77 47 56 85 4D 3B E9 AD DB 4D EB 2D 29 97 F8 5A 9A 99 C3
            AD 17 1A 6C 73 A4 04 1F E5 D5 8E A8 C7 A6 20 AE 8A E0 50 B8
            F1 B2 D2 48 DE 7D B3 89 0D B6 E8 6D C7 A3 82 5E 97
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 27 37 36 30 7B 70 75 17 8D 3C 70 75 E1 71 91 8D 04 15 83
           CF CB 71 22 1D FB 46 54 BA 62 73 3A C4 43 B3 62 1D 32 C6 43
           A6 A9 BF 17 65 4A 10 41 84 A5 91 69 4F 8D 5C 68 6C 0E 4B C1
           2D 45 89 DC 34 96 C1 63 38 A4 6F 6A 99 63 D3 DB 8D 4E 09 A6
           A2 22 45 53 E0 A7 23 44 87 3E C7 EF 75 19 66 0D 42 FB DD 9C
           52 CE E4 27 EB 44 69 05 1F 02 53 D4 4E AF 19 72 5E 8F 1E A7
           85 39 A2 B3 CF 01 C9 0F 60 F4 3D 8D 81 C1 C4 35 F4 0F 01 6D
           5B CB B3 8D 92 A8 97 B5 5D D2 AB 9E 97 EE AD 32 2D 07 52 4D
```

```
[...]
```

## 11219 - Nessus SYN scanner

### Synopsis

It is possible to determine which TCP ports are open.

### Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.
Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

### Solution

Protect your target with an IP filter.

### Risk Factor

None

### Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/05/22

### Ports

#### tcp/443

```
Port 443/tcp was found to be open
```

## 22964 - Service Detection

### Synopsis

The remote service could be identified.

### Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2007/08/19, Modification date: 2018/05/03

### Ports

#### tcp/443

```
A TLSv1 server answered on this port.
```

#### tcp/443

```
A web server is running on this port through TLSv1.
```

## 24260 - HyperText Transfer Protocol (HTTP) Information

### Synopsis

Some information about the remote HTTP configuration can be extracted.

### Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2007/01/30, Modification date: 2017/11/13

### Ports

### tcp/443

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Sun, 08 Jul 2018 13:24:52 GMT
  Server: Apache/2.2.22 (Ubuntu)
  X-Powered-By: PHP/5.3.10-1ubuntu3.26
  Vary: Accept-Encoding
  Content-Length: 38
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<center><img src="omg.jpg"/></center>
```

## 39521 - Backported Security Patch Detection (WWW)

### Synopsis

Security patches are backported.

### Description

Security patches may have been 'backported' to the remote HTTP server without changing its version number.
Banner-based checks have been disabled to avoid false positives.
Note that this test is informational only and does not denote any security problem.

### See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2009/06/25, Modification date: 2015/07/07

### Ports

#### tcp/443

```
Give Nessus credentials to perform local checks.
```

## 48204 - Apache HTTP Server Version

### Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

### Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2010/07/30, Modification date: 2018/01/22

### Ports

#### tcp/443

```
URL        : https://10.10.10.79/
Version    : 2.2.99
backported : 1
os         : ConvertedUbuntu
```

## 48243 - PHP Version Detection

### Synopsis

It was possible to obtain the version number of the remote PHP installation.

### Description

Nessus was able to determine the version of PHP available on the remote web server.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2010/08/04, Modification date: 2017/07/07

### Ports

**tcp/443**

```
Nessus was able to identify the following PHP version information :

  Version : 5.3.10-1ubuntu3.26
  Source  : X-Powered-By: PHP/5.3.10-1ubuntu3.26
```

## 50845 - OpenSSL Detection

### Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

### Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.
Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

### See Also

http://www.openssl.org

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2010/11/30, Modification date: 2013/10/18

### Ports

**tcp/443**

## 56984 - SSL / TLS Versions Supported

### Synopsis

The remote service encrypts communications.

### Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2011/12/01, Modification date: 2018/02/15

### Ports

**tcp/443**

```
This port supports SSLv3/TLSv1.0/TLSv1.1/TLSv1.2.
```

## 84502 - HSTS Missing From HTTPS Server

### Synopsis

The remote web server is not enforcing HSTS.

### Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

### See Also

https://tools.ietf.org/html/rfc6797

### Solution

Configure the remote web server to use HSTS.

### Risk Factor

None

### Plugin Information:

Publication date: 2015/07/02, Modification date: 2015/07/02

### Ports

**tcp/443**

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

## 84574 - Backported Security Patch Detection (PHP)

### Synopsis

Security patches have been backported.

### Description

Security patches may have been 'backported' to the remote PHP install without changing its version number.
Banner-based checks have been disabled to avoid false positives.
Note that this test is informational only and does not denote any security problem.

### See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

### Solution

n/a

### Risk Factor

None

### Plugin Information:

Publication date: 2015/07/07, Modification date: 2015/07/07

### Ports

**tcp/443**

```
Give Nessus credentials to perform local checks.
```

## 94761 - SSL Root Certification Authority Certificate Information

### Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

### Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

### See Also

https://technet.microsoft.com/en-us/library/cc778623

### Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

### Risk Factor

None

### Plugin Information:

Publication date: 2016/11/14, Modification date: 2016/11/14

### Ports

**tcp/443**

```
The following root Certification Authority certificate was found :

|-Subject             : C=US/ST=FL/O=valentine.htb/CN=valentine.htb
|-Issuer              : C=US/ST=FL/O=valentine.htb/CN=valentine.htb
|-Valid From          : Feb 06 00:45:25 2018 GMT
|-Valid To            : Feb 06 00:45:25 2019 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

**5353/udp**

## 12218 - mDNS Detection (Remote Network)

### Synopsis

It is possible to obtain information about the remote host.

### Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.
This plugin attempts to discover mDNS used by hosts that are not on the network segment on which Nessus resides.

### Solution

Filter incoming traffic to UDP port 5353, if desired.

### Risk Factor

Medium

### CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### Plugin Information:

Publication date: 2004/04/28, Modification date: 2013/05/31

### Ports

**udp/5353**

```
Nessus was able to extract the following information :

  - mDNS hostname       : Valentine.local.

  - Advertised services :
    o Service name      : Valentine [00:50:56:b9:9c:2a]._workstation._tcp.local.
      Port number       : 9
    o Service name      : Valentine._udisks-ssh._tcp.local.
      Port number       : 22

  - CPU type            : X86_64
  - OS                  : LINUX
```

# Remediations

## Suggested Remediations

Taking the following actions across 1 hosts would resolve 9% of the vulnerabilities on the network:

| Action to take | Vulns | Hosts |
|---|---|---|
| OpenSSL 'ChangeCipherSpec' MiTM Vulnerability: OpenSSL 0.9.8 SSL/TLS users (client and/or server) should upgrade to 0.9.8za. OpenSSL 1.0.0 SSL/TLS users (client and/or server) should upgrade to 1.0.0m. OpenSSL 1.0.1 SSL/TLS users (client and/or server) should upgrade to 1.0.1h. | 1 | 1 |