

WPP	Praktikum IT-Sicherheit	HBN/NMN
SS 2014	Aufgabe 1 – Angriffstechniken (unter Linux)	Seite 1 von 3

1. Footprinting über das Internet

Wählen Sie als Ziel den Webserver einer beliebigen Hochschule. Ermitteln Sie den genauen Typ (inkl. Versionsnr.) des verwendeten Webserver und geben Sie mindestens eine URL mit Informationen über eine bekannte Schwachstelle für diese Webserver-Softwareversion an.

2. Buffer Overflow

3.1. Schreiben Sie ein C-Programm, das einen beliebigen Input-String von der Standard-Eingabe liest und mittels der Funktion `strcpy` einer Variablen zuweist.

Benutzen Sie hierzu eine Unterfunktion `exploit` sowie zwei Character-Arrays `buf1` und `buf2`, die sie vorher mit Konstanten initialisieren. Weisen Sie anschließend genau einer der beiden Buffer-Variablen den Inhalt des Input-Strings zu.

Reservieren Sie für den Input-String ausreichend Speicherplatz, aber nehmen Sie keine Längen-Überprüfung des aktuell übergebenen Wertes vor!

Beispiel (setzen Sie für „...“ eigene Konstanten ein!):

```
void exploit(char *InputString) {
    char buf1[...];
    char buf2[...];

    strcpy (buf1, "...");      /* Initialisierung mit Konstante */
    strcpy (buf2, "...");      /* Initialisierung mit Konstante */
    ... }
```

Konstruieren Sie das Programm so, dass ein Angreifer durch geschickte Wahl des Eingabestrings folgende Stack-Manipulationen erreichen kann (Überprüfung durch Ausgabe mit `printf`):

1. Fall: `buf1: <leer>`
`buf2: <Kompletter Input-String>`

2. Fall: `buf1: AAA ... (Länge von buf1)`
`buf2: <Kompletter Input-String>`

3.2. Testen Sie Ihr Programm bzgl. o.g. Anforderungen.

3.3. Bei welcher Länge des Input-Strings tritt ein „Segmentation fault“ auf? Warum?

Tipps:

- Character-Array-Variablen („Strings“) sind in C Zeiger auf die Adresse des ersten Zeichens; das Ende eines Character-Arrays wird durch ein Byte mit dem Wert `\0` definiert.
- Informationen zur Stackorganisation finden Sie in dem klassischen Paper „Smashing The Stack For Fun And Profit“ (im Pub)

WPP	Praktikum IT-Sicherheit	HBN/NMN
SS 2014	Aufgabe 1 – Angriffstechniken (unter Linux)	Seite 2 von 3

3. Passwort – Cracking

3.1. Installieren Sie das Passwort-Cracking-Tool „John-the-Ripper“ (Datei john-1.8.tar.gz, Informationen sind in der Datei ../doc/INSTALL enthalten).

Compilieren Sie das Programm `makepasswd`:

```
gcc makepasswd.c -o makepasswd -lcrypt
```

Verwenden Sie das Programm `makepasswd`, um eine UNIX-Passwortdatei für ein Klartext-Passwort zu erzeugen.

- Eingabe: Passwort im Klartext
- Ausgabe: entsprechende Zeile einer UNIX-Passwortdatei auf Standardausgabestrom
- Mögliche Optionen:
 - `-u Username` Name des Benutzers
 - `-s Salt` 2 beliebige Buchstaben zur Erhöhung der Komplexität (ansonsten werden Zufallswerte verwendet)

Beispiel:

```
makepasswd Passwort1 > passwd1.txt
```

3.2. Erzeugen Sie jeweils Passworte der Länge 1, 2, 3, 4 und 5 und notieren Sie die Zeit, bis das Programm `john` das Passwort erraten hat.

3.3. Erzeugen Sie ein Passwort, das aus 8 Ziffern besteht (z.B. 85248723), geben Sie beim Start von `john` als Option eine Einschränkung auf Ziffern an und notieren Sie die Zeit für das Erraten.

3.4. Erzeugen Sie ein komplexes Passwort mit mindestens 8 Stellen (z.B. Xuj73NmpO82) und fügen Sie dieses Passwort dem Wörterbuch `password.lst` hinzu. Notieren Sie dann die Zeit, bis das Programm `john` das Passwort anhand des Wörterbuchs erraten hat.

4. Website-Spoofing (Phishing)

4.1. Erstellen Sie eine „böse“ Website, die einem unbedarften Benutzer vortäuscht, die Seite www.haspa.de zu sein.

Modifizieren Sie den Link „Login Online Service“ (rechts oben) auf ihrer gefälschten Seite so, dass er auf eine weitere gefälschte Seite `login.htm` verweist, die Sie auf ihrer bösen Website ebenfalls selbst hosten:

WPP	Praktikum IT-Sicherheit	HBN/NMN
SS 2014	Aufgabe 1 – Angriffstechniken (unter Linux)	Seite 3 von 3

Diese Seite soll Kontonummer und PIN an ein eigenes PHP-Skript *Haspa-Fehlermeldung.php* weitergeben. Dieses Skript soll folgenden Text ausgeben:

4.2. Stellen Sie die Dateien ihrer bösen Website zur Vorführung ihrer Aufgabenlösung in ihr html-Verzeichnis, so dass diese unter <https://users.informatik.haw-hamburg.de/~<IhrName>/ITS-Praktikum/Haspa.de.htm> aufrufbar ist.

- Entfernen Sie Ihre böse Website direkt nach dem Praktikum aus ihrem html-Verzeichnis!
- Achten Sie darauf, dass **kein Link** in einer existierenden Webseite auf ihre böse Website angelegt wird (damit Sie in keinen Suchmaschinen-Cache geraten)!

Tipp: Klonen Sie Webseiten, statt diese nachzuprogrammieren!

P.S.: Fertigen Sie ein Protokoll an (Ein-/Ausgaben mitprotokollieren)!

P.P.S.: Berücksichtigen Sie §202 und §303 des StGB!