Steeve Barbeau's blog

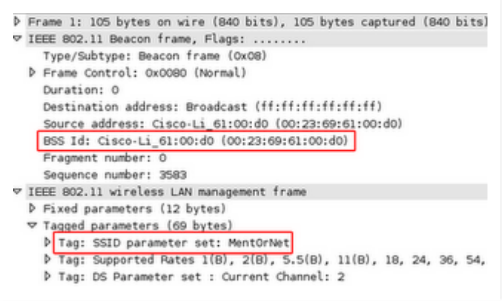
A blog on computer security ...

Saturday, July 2, 2011

Network Forensics Puzzle #8 Write-Up

I'll explain you my solution to this network forensic contest. It was the second challenge organized by forensicscontest.com that I do, and it was very interesting.
During this short contest, I've used the awesome tool Scapy, **Wireshark**, ivstools and aircrack-ng.

1) Joe’s WAP is beaconing. Based on the contents of the **packet capture**, what are:
a. The SSID of his access point? Ment0rNet
b. The BSSID of his access point? 00:23:69:61:00:d0
Answers can be found in the first frame when we open pcap file in **Wireshark** :



```
▷ Frame 1: 105 bytes on wire (840 bits), 105 bytes captured (840 bits)
▽ IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x08)
  ▷ Frame Control: 0x0080 (Normal)
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: Cisco-Li_61:00:d0 (00:23:69:61:00:d0)
    BSS Id: Cisco-Li_61:00:d0 (00:23:69:61:00:d0)
    Fragment number: 0
    Sequence number: 3583
▽ IEEE 802.11 wireless LAN management frame
  ▷ Fixed parameters (12 bytes)
  ▽ Tagged parameters (69 bytes)
    ▷ Tag: SSID parameter set: Ment0rNet
    ▷ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54,
    ▷ Tag: DS Parameter set : Current Channel: 2
```

2) How long is the **packet capture**, from beginning to end (in SECONDS - please round to the nearest full second)? 414
There are two possibilities to find this time with **Wireshark** :
- Statistic menu > Summary > Time elapsed : 6:53 minutes (413 seconds)
- Go to last frame (n°133068) and look Time's column where we have a more precise time : 413.576954

3) How **many WEP-encrypted data frames** are **there** **total** in the **packet capture**? 59274
We can use this "wlan.fc.protected==1" filter in **Wireshark** to show only WLAN **frames** with Protected Flag set to 1.

4) How **many** *unique* WEP initialization vectors (IVs) are **there** **TOTAL** in the **packet capture** relating to Joe’s access point? 15417
We just have to count **WEP-encrypted data frames** where BSSID is set to 00:23:69:61:00:d0 (cf Scapy script).

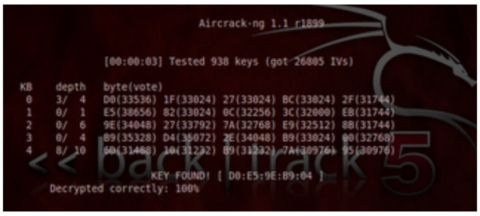
5) What was the MAC address of the station executing the Layer 2 attacks? de:ad:be:ef:13:37
This MAC address corresponds to 192.168.1.109 which is attacker's IP.

6) How **many** *unique* IVs were generated (relating to Joe’s access point):
a. By the attacker station? 8
b. By all *other* stations combined? 15409
Same technique that question 4 with source address equal to "de:ad:be:ef:13:37" for a) or different for b).

7) What was the WEP key of Joe’s WAP? D0:E5:9E:B9:04
To find the WEP key, we can use two tools : ivstools and aircrack-ng :
ivstools --convert evidence08.pcap extract.ivs
aircrack-ng extract.iv
We obtain the WEP key : D0:E5:9E:B9:04.

Threat Level

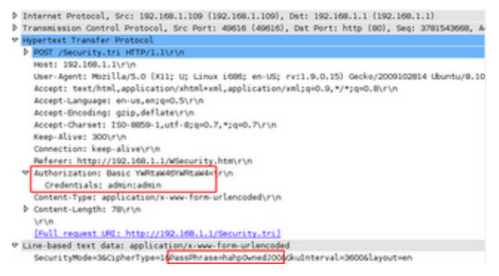
INTERNET STORM CENTER infocon:GREEN http://isc.sans.org



```
                    Aircrack-ng 1.1 r1899


           [00:00:03] Tested 938 keys (got 26805 IVs)

KB    depth   byte(vote)
 0    3/  4   D0(33536) 1F(33024) 27(33024) BC(33024) 2F(31744)
 1    0/  1   E5(38656) 82(33024) 0C(32256) 3C(32000) EB(31744)
 2    0/  6   9E(34048) 27(33792) 7A(32768) E9(32512) 8B(31744)
 3    0/  4   B9(35328) D4(35072) 2E(34048) B9(33024) 00(32768)
 4    8/ 10   6D(31488) 10(31232) B9(31232) 7A(30976) 95(30976)

              KEY FOUND! [ D0:E5:9E:B9:04 ]
    Decrypted correctly: 100%
```

8) What were the administrative username and password of the targeted wireless access point? Username : admin & Password : admin
Username and password can be found with this **Wireshark** filter : "http.authbasic" because the administrative interface of the victim wireless access point use basic HTTP authentication. We can see this : YWRtaW46YWRtaW4= which corresponds to a base64 encoded version of "admin:admin".

9) What was the WAP administrative passphrase changed to? hahp0wnedJ00
In the **capture**, **there** is only one HTTP POST request sent by the attacker (http.request.method=="POST" && ip.src==192.168.1.109) which contains what we are looking for :



```
▷ Internet Protocol, Src: 192.168.1.109 (192.168.1.109), Dst: 192.168.1.1 (192.168.1.1)
▷ Transmission Control Protocol, Src Port: 49616 (49616), Dst Port: http (80), Seq: 3781543668, A
▽ Hypertext Transfer Protocol
  ▷ POST /Security.tri HTTP/1.1\r\n
    Host: 192.168.1.1\r\n
    User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.15) Gecko/2009102814 Ubuntu/8.10
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://192.168.1.1/WSecurity.htm\r\n
  ▽ Authorization: Basic YWRtaW46YWRtaW4=\r\n
      Credentials: admin:admin
    Content-Type: application/x-www-form-urlencoded\r\n
  ▷ Content-Length: 78\r\n
    \r\n
    [Full request URI: http://192.168.1.1/Security.tri]
▽ Line-based text data: application/x-www-form-urlencoded
    SecurityMode=3&CipherType=1&PassPhrase=hahp0wnedJ00&GkuInterval=3600&layout=en
```

In this last screenshot, we can see that the attacker seems to be using an Ubuntu 8.10 32bits with Firefox browser.

My scapy script can be downloaded here.

at 4:18 PM 0 comments Labels: EN, Forensic, Prog, Python, Wifi
0

Newer Posts Home Older Posts

Subscribe to: Posts (Atom)

We're sorry...

This gadget is configured incorrectly. Webmaster hint: Please ensure that "Friend Connect Settings - Home URL" matches the URL of this site.