Administración de redes Wi-Fi seguras usando software libre

Linux Week 2008

Martes, 10 de Marzo de 2008

Jorge A. López Mori

jorge.lopez@pucp.edu.pe

Agenda

- Introducción
- Motivación
- Redes Wi-Fi
  - Aspectos de seguridad en redes Wi-Fi
- Software Libre utilizado
- Descripción del Sistema de Administración propuesto para una red Wi-Fi
- Análisis costo-beneficio
- Conclusiones

Introducción

- Notable expansión de redes Wi-Fi en los últimos años
- Ofrecer movilidad y un acceso a la Internet a los usuarios
- ¿Y la seguridad? … Bien gracias…
  - ‘Hotspots’ de libre acceso
  - Claves compartidas

- Los tres vértices de la seguridad se ven comprometidos:
  - Confidencialidad, Integridad, Disponibilidad
- Tomar las medidas de seguridad convenientes

(NO EXISTE LA RED 100% SEGURA)

Motivación

- Interés en el área de *networking* desde 1998 y de seguridad para redes desde 2003.
- Inicio en trabajos formales de seguridad desde Enero 2007:
  - Experiencia con equipos de seguridad tales como Firewalls, IDS/ IPS, VPN, antimalware, entre otros.
- Inclinación hacia la seguridad en redes Wi-Fi
  - Inseguridad que ofrecen las redes Wi-Fi '*default*'
  - Seguridad comprometida con facilidad:
    - Desde *lamers* hasta *crackers (wardriving)*
    - Ej: Ubuntu + aircrack
      - Tan fácil como: usuario@localhost# sudo apt-get install aircrack

Redes Wi-Fi

- IEEE 802.11: b, g, a, n draft2
- Permiten el acceso inalámbrico de usuarios a redes locales IP
  - Fácil y transparente para los usuarios

- Hacen uso de dos tipos de acceso al medio:
  - DSSS
  - OFDM
- Dos bandas de trabajo: 2.4 GHz (11/3 CH) y 5 GHz (16/8 CH)
- Distintas velocidades (1, 2, 5.5, 11, 24, 54 Mbps)
- Dos tipos de usos:
  - *Indoors* (*hotspots*) ← Aquí apuntamos
  - *Outdoors* (*wireless bridges*)

Seguridad en Redes Wi-Fi

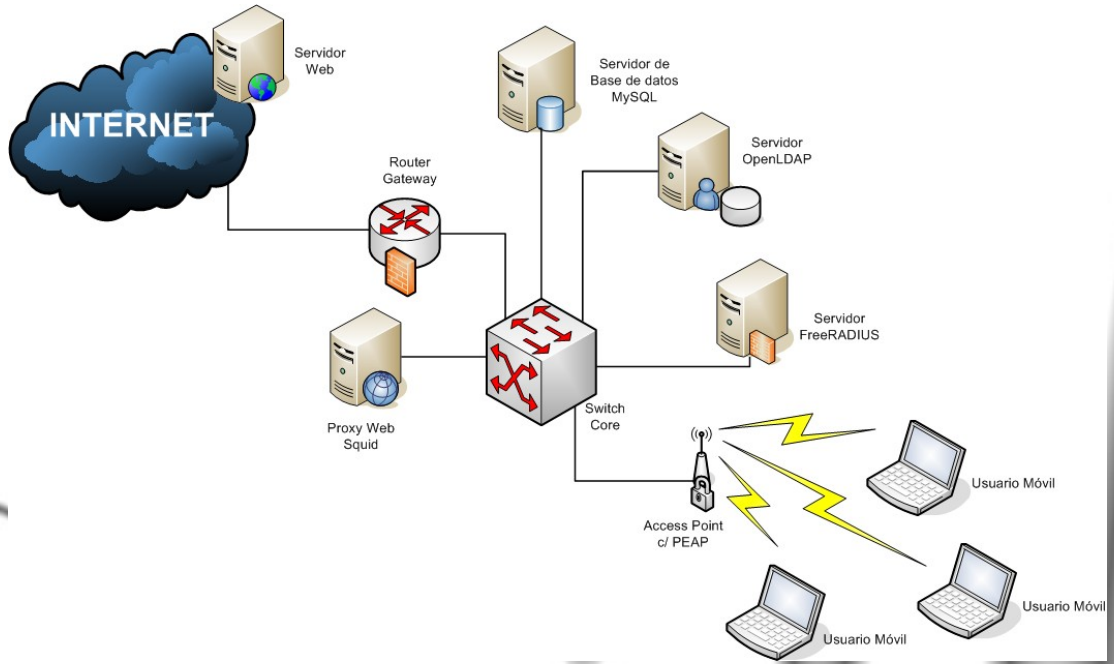
- *Open system*
- *Shared key*:
  - WEP: 64-bit, RC4, IV (24 bits), 40 bits
- WPA: TKIP, AES, 802.1x
  - WPA Personal
  - WPA Enterprise
- WPA2 → IEEE 802.11i: TKIP + AES
  - WPA2 Personal
  - WPA2 Enterprise
- WPA/WPA2 Enterprise:
  - 802.1x + EAP:
    - EAP-TLS (certificados en srv y clientes)
    - EAP-TTLS (certificado solo en srv)
    - EAP-PEAP ← Aquí apuntaremos

Software Libre utilizado

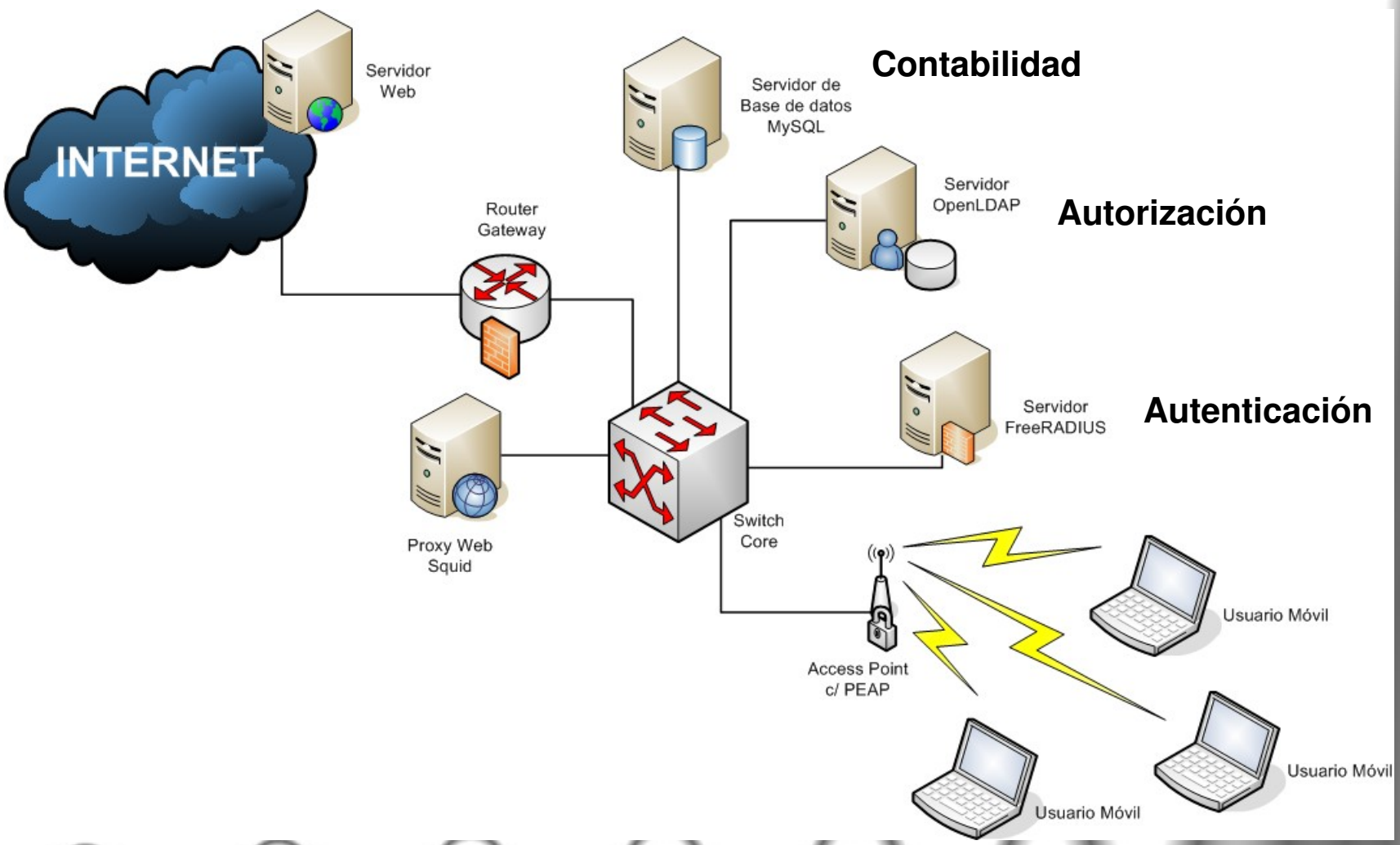
- FreeRADIUS
  - Implementa el protocolo RADIUS con múltiples soportes EAP
- OpenLDAP + SAMBA
  - Implementa un *Domain Controller*
- MySQL Server
  - Almacena *logs* de accesos de usuarios
- Squid
  - Implementa un Proxy Web con control de acceso
- DD-WRT
  - Firmware basado en Linux para *wireless routers* Linksys WRT54g

Descripción del Sistema de Administración propuesto para una red Wi-Fi

- Sistema AAA de acceso inalámbrico
  - Autenticación: Servidor RADIUS
  - Autorización: Servidor LDAP
  - *Accounting* (contabilidad): Servidor Base de Datos
- Con control de acceso Web
  - Proxy Web: Autentica al usuario y controla su ancho de banda



Descripción del Sistema de Administración propuesto para una red Wi-Fi



Captura de tramas con Wireshark

Conexión de una cliente a la WLAN

AP: 192.168.0.253
RADIUS: 192.168.0.103
LDAP: 192.168.0.60
Usuario: rlopez

captura-desde-freeradius-con-wpa-enterprise-feb-2008 - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
47	4.864501	192.168.0.103	192.168.0.253	RADIUS	Access-Challenge(11) (id=0, l=96)
48	4.868320	192.168.0.253	192.168.0.103	RADIUS	Access-Request(1) (id=0, l=170)
49	4.872703	192.168.0.103	192.168.0.60	LDAP	searchRequest(38) "ou=Users,dc=mg,dc=com,dc=pe" wholeSubtree
50	4.874391	192.168.0.60	192.168.0.103	LDAP	searchResEntry(38) "uid=rlopez,ou=Users,dc=mg,dc=com,dc=pe"
51	4.875429	192.168.0.60	192.168.0.103	LDAP	searchResDone(38) [1 result]
52	4.880882	192.168.0.103	192.168.0.253	RADIUS	Access-Accept(2) (id=0, l=168)
53	4.914718	192.168.0.103	192.168.0.60	TCP	46481 > ldap [ACK] Seq=10913 Ack=1926 Win=2264 Len=0 TSV=1263643 TSER=1453579
54	5.616019	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xd6abd4f5
55	5.617620	ZyxelCom_fc:f4:6e	Broadcast	ARP	Who has 192.168.0.7? Tell 192.168.0.254
56	5.622596	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xd6abd4f5

```
Frame 47 (138 bytes on wire, 138 bytes captured)
Ethernet II, Src: Vmware_7c:cc:9b (00:0c:29:7c:cc:9b), Dst: Cisco-Li_59:40:6d (00:1a:70:59:40:6d)
Internet Protocol, Src: 192.168.0.103 (192.168.0.103), Dst: 192.168.0.253 (192.168.0.253)
User Datagram Protocol, Src Port: radius (1812), Dst Port: nmsd (1239)
Radius Protocol
    Code: Access-Challenge (11)
    Packet identifier: 0x0 (0)
    Length: 96
    Authenticator: 6D8FADDBBE482D683F3039B79C1FC2A8
  Attribute Value Pairs
    AVP: l=40  t=EAP-Message(79) Last Segment[1]
        EAP fragment
      Extensible Authentication Protocol
          Code: Request (1)
          Id: 7
          Length: 38
          Type: PEAP [Palekar] (25)
          Flags(0x0):
          PEAP version 0
        Secure Socket Layer
          TLSv1 Record Layer: Application Data Protocol: Application Data
              Content Type: Application Data (23)
              Version: TLS 1.0 (0x0301)
              Length: 27
              Encrypted Application Data: 700D45AAA47ADB7D1225E879C096949A63E57CF44236E2EA...
    AVP: l=18  t=Message-Authenticator(80): 6B41C5F057DC4018291AA88813F549FA
        Message-Authenticator: 6B41C5F057DC4018291AA88813F549FA
    AVP: l=18  t=State(24): 80F01046248256638472DCF376E7122D
        State: 80F01046248256638472DCF376E7122D
```

1ro)

Envío del desafío por parte de FreeRADIUS

```
0000  00 1a 70 59 40 6d 00 0c  29 7c cc 9b 08 00 45 00   ..pY@m.. )|....E.
0010  00 7c 00 00 40 00 40 11  b7 bc c0 a8 00 67 c0 a8   .|..@.@. .....g..
0020  00 fd 07 14 04 d7 00 68  40 01 0b 00 00 60 6d 8f   .......h @....`m.
```

Frame (138 bytes) | Reassembled EAP (38 bytes)

File: "I:\captura-desde-freeradius-con-wpa-enterprise-feb-2008" 26 KB 00:00:33 | Packets: 103 Displayed: 103 Marked: 0

captura-desde-freeradius-con-wpa-enterprise-feb-2008 - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
47	4.864501	192.168.0.103	192.168.0.253	RADIUS	Access-challenge(11) (id=0, l=96)
48	4.868320	192.168.0.253	192.168.0.103	RADIUS	Access-Request(1) (id=0, l=170)
49	4.872703	192.168.0.103	192.168.0.60	LDAP	searchRequest(38) "ou=Users,dc=mg,dc=com,dc=pe" wholeSubtree
50	4.874391	192.168.0.60	192.168.0.103	LDAP	searchResEntry(38) "uid=rlopez,ou=Users,dc=mg,dc=com,dc=pe"
51	4.875429	192.168.0.60	192.168.0.103	LDAP	searchResDone(38) [1 result]
52	4.880882	192.168.0.103	192.168.0.253	RADIUS	Access-Accept(2) (id=0, l=168)
53	4.914718	192.168.0.103	192.168.0.60	TCP	46481 > ldap [ACK] Seq=10913 Ack=1926 Win=2264 Len=0 TSV=1263643 TSER=1453579
54	5.616019	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xd6abd4f5
55	5.617620	ZyxelCom_fc:f4:6e	Broadcast	ARP	Who has 192.168.0.7? Tell 192.168.0.254
56	5.622596	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xd6abd4f5

```
Frame 48 (212 bytes on wire, 212 bytes captured)
Ethernet II, Src: Cisco-Li_59:40:6d (00:1a:70:59:40:6d), Dst: Vmware_7c:cc:9b (00:0c:29:7c:cc:9b)
Internet Protocol, Src: 192.168.0.253 (192.168.0.253), Dst: 192.168.0.103 (192.168.0.103)
User Datagram Protocol, Src Port: nessus (1241), Dst Port: radius (1812)
Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0x0 (0)
    Length: 170
    Authenticator: F22F62E6D6EFDABCC204E0E5B0A448F5
    [The response to this request is in frame 52]
  Attribute Value Pairs
    AVP: l=8  t=User-Name(1): rlopez
    AVP: l=6  t=NAS-IP-Address(4): 192.168.0.253
    AVP: l=14  t=Called-Station-Id(30): 001a7059406f
    AVP: l=14  t=Calling-Station-Id(31): 0013e877a6e7
    AVP: l=14  t=NAS-Identifier(32): 001a7059406f
    AVP: l=6  t=NAS-Port(5): 54
    AVP: l=6  t=Framed-MTU(12): 1400
    AVP: l=18  t=State(24): 80F0104624825663847 2DCF376E7122D
    AVP: l=6  t=NAS-Port-Type(61): Wireless-802.11(19)
    AVP: l=40  t=EAP-Message(79) Last Segment[1]
      EAP fragment
      Extensible Authentication Protocol
        Code: Response (2)
        Id: 7
        Length: 38
        Type: PEAP [Palekar] (25)
        Flags(0x0):
        PEAP version 0
        Secure Socket Layer
          TLSv1 Record Layer: Application Data Protocol: Application Data
            Content Type: Application Data (23)
            Version: TLS 1.0 (0x0301)
            Length: 27
            Encrypted Application Data: 9AF0675B11AF9B9C0C88FA10D64350F50ACC8534D7AA9C41...
    AVP: l=18  t=Message-Authenticator(80): FEE898B73BFF78A650EEF323CBA28150
```

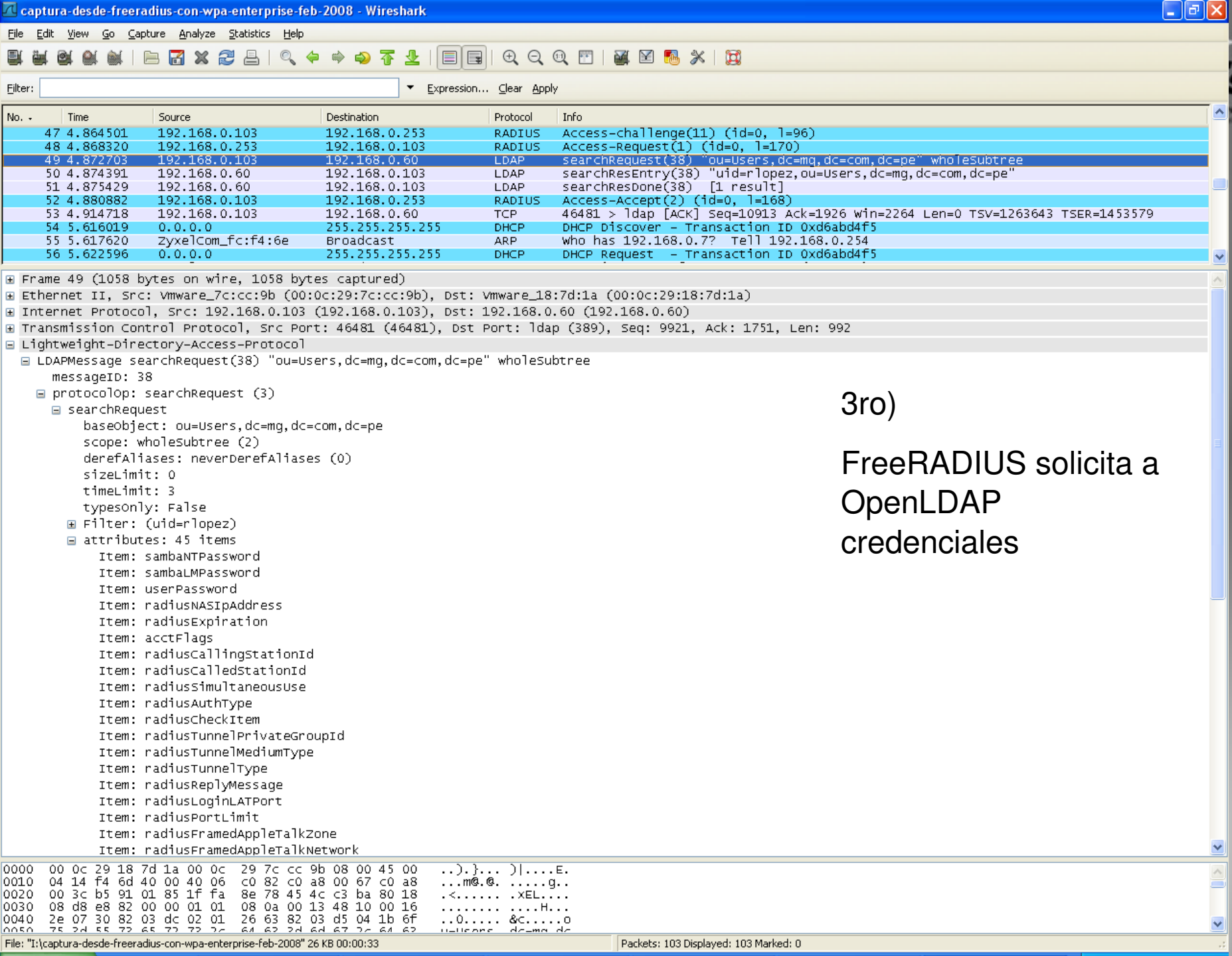
```
0000  00 0c 29 7c cc 9b 00 1a  70 59 40 6d 08 00 45 00   ..)|.... pY@m..E.
0010  00 c6 01 ce 00 00 40 11  f5 a4 c0 a8 00 fd c0 a8   ......@. ........
0020  00 67 04 d9 07 14 00 b2  cf 0e 01 00 00 aa f2 2f   .g...... .......
```

Frame (212 bytes) | Reassembled EAP (38 bytes)

File: "I:\captura-desde-freeradius-con-wpa-enterprise-feb-2008" 26 KB 00:00:33 | Packets: 103 Displayed: 103 Marked: 0

2do)

Solicitud de acceso por parte del AP, enviando la rpta al desafío



3ro)

FreeRADIUS solicita a OpenLDAP credenciales

captura-desde-freeradius-con-wpa-enterprise-feb-2008 - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
47	4.864501	192.168.0.103	192.168.0.253	RADIUS	Access-Challenge(11) (id=0, l=96)
48	4.868320	192.168.0.253	192.168.0.103	RADIUS	Access-Request(1) (id=0, l=170)
49	4.872703	192.168.0.103	192.168.0.60	LDAP	searchRequest(38) "ou=Users,dc=mg,dc=com,dc=pe" wholeSubtree
50	4.874391	192.168.0.60	192.168.0.103	LDAP	searchResEntry(38) "uid=rlopez,ou=Users,dc=mg,dc=com,dc=pe"
51	4.875429	192.168.0.60	192.168.0.103	LDAP	searchResDone(38) [1 result]
52	4.880882	192.168.0.103	192.168.0.253	RADIUS	Access-Accept(2) (id=0, l=168)
53	4.914718	192.168.0.103	192.168.0.60	TCP	46481 > ldap [ACK] Seq=10913 Ack=1926 Win=2264 Len=0 TSV=1263643 TSER=1453579
54	5.616019	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xd6abd4f5
55	5.617620	ZyxelCom_fc:f4:6e	Broadcast	ARP	Who has 192.168.0.7? Tell 192.168.0.254
56	5.622596	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xd6abd4f5

```
⊞ Frame 50 (227 bytes on wire, 227 bytes captured)
⊞ Ethernet II, Src: Vmware_18:7d:1a (00:0c:29:18:7d:1a), Dst: Vmware_7c:cc:9b (00:0c:29:7c:cc:9b)
⊞ Internet Protocol, Src: 192.168.0.60 (192.168.0.60), Dst: 192.168.0.103 (192.168.0.103)
⊞ Transmission Control Protocol, Src Port: ldap (389), Dst Port: 46481 (46481), Seq: 1751, Ack: 10913, Len: 161
⊟ Lightweight-Directory-Access-Protocol
  ⊟ LDAPMessage searchResEntry(38) "uid=rlopez,ou=Users,dc=mg,dc=com,dc=pe" [2 results]
      messageID: 38
    ⊟ protocolOp: searchResEntry (4)
      ⊟ searchResEntry
          objectName: uid=rlopez,ou=Users,dc=mg,dc=com,dc=pe
        ⊟ attributes: 2 items
          ⊟ Item sambaLMPassword
              type: sambaLMPassword
            ⊟ vals: 1 item
                7E930AAF8D117BF2AAD3B435B51404EE
          ⊟ Item sambaNTPassword
              type: sambaNTPassword
            ⊟ vals: 1 item
                4077F54139014515EF0B84F2B6B88AB7
      [Response To: 49]
      [Time: 0.001688000 seconds]
```

4to)

OpenLDAP devuelve credenciales

```
0000  00 0c 29 7c cc 9b 00 0c  29 18 7d 1a 08 00 45 00   ..)|.... ).}...E.
0010  00 d5 77 f2 40 00 40 06  40 3d c0 a8 00 3c c0 a8   ..w.@.@. @=...<..
0020  00 67 01 85 b5 91 45 4c  c3 ba 1f fa 92 58 80 18   .g....EL .....X..
0030  3e 96 65 36 00 00 01 01  08 0a 00 16 2e 0b 00 13   >.e6.... ........
0040  48 10 30 81 9e 02 01 26  64 81 98 04 26 75 69 64   H.0....& d...&uid
0050  3d 72 6c 6f 70 65 7a 2c  6f 75 3d 55 73 65 72 73   -rlopez, ou=Users
```

File: "I:\captura-desde-freeradius-con-wpa-enterprise-feb-2008" 26 KB 00:00:33

Packets: 103 Displayed: 103 Marked: 0

captura-desde-freeradius-con-wpa-enterprise-feb-2008 - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
47	4.864501	192.168.0.103	192.168.0.253	RADIUS	Access-Challenge(11) (id=0, l=96)
48	4.868320	192.168.0.253	192.168.0.103	RADIUS	Access-Request(1) (id=0, l=170)
49	4.872703	192.168.0.103	192.168.0.60	LDAP	searchRequest(38) "ou=Users,dc=mg,dc=com,dc=pe" wholeSubtree
50	4.874391	192.168.0.60	192.168.0.103	LDAP	searchResEntry(38) "uid=rlopez,ou=Users,dc=mg,dc=com,dc=pe"
51	4.875429	192.168.0.60	192.168.0.103	LDAP	searchResDone(38) [1 result]
52	4.880882	192.168.0.103	192.168.0.253	RADIUS	Access-Accept(2) (id=0, l=168)
53	4.914718	192.168.0.103	192.168.0.60	TCP	46481 > ldap [ACK] Seq=10913 Ack=1926 Win=2264 Len=0 TSV=1263643 TSER=1453579
54	5.616019	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xd6abd4f5
55	5.617620	ZyxelCom_fc:f4:6e	Broadcast	ARP	Who has 192.168.0.7? Tell 192.168.0.254
56	5.622596	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xd6abd4f5

```
⊞ Frame 51 (80 bytes on wire, 80 bytes captured)
⊞ Ethernet II, Src: Vmware_18:7d:1a (00:0c:29:18:7d:1a), Dst: Vmware_7c:cc:9b (00:0c:29:7c:cc:9b)
⊞ Internet Protocol, Src: 192.168.0.60 (192.168.0.60), Dst: 192.168.0.103 (192.168.0.103)
⊞ Transmission Control Protocol, Src Port: ldap (389), Dst Port: 46481 (46481), Seq: 1912, Ack: 10913, Len: 14
⊟ Lightweight-Directory-Access-Protocol
  ⊟ LDAPMessage searchResDone(38) [2 results]
      messageID: 38
    ⊟ protocolOp: searchResDone (5)
      ⊟ searchResDone
          resultCode: success (0)
          matchedDN:
          errorMessage:
      [Response To: 49]
      [Time: 0.002726000 seconds]
```

5to)

OpenLDAP indica que el usuario es válido

```
0000  00 0c 29 7c cc 9b 00 0c  29 18 7d 1a 08 00 45 00   ..)|.... ).}...E.
0010  00 42 77 f3 40 00 40 06  40 cf c0 a8 00 3c c0 a8   .Bw.@.@. @....<..
0020  00 67 01 85 b5 91 45 4c  c4 5b 1f fa 92 58 80 18   .g....EL .[...X..
0030  3e 96 64 4a 00 00 01 01  08 0a 00 16 2e 0c 00 13   >.dJ.... ........
0040  48 10 30 0c 02 01 26 65  07 0a 01 00 04 00 04 00   H.0...&e ........
```

File: "I:\captura-desde-freeradius-con-wpa-enterprise-feb-2008" 26 KB 00:00:33

Packets: 103 Displayed: 103 Marked: 0

captura-desde-freeradius-con-wpa-enterprise-feb-2008 - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
47	4.864501	192.168.0.103	192.168.0.253	RADIUS	Access-Challenge(11) (id=0, l=96)
48	4.868320	192.168.0.253	192.168.0.103	RADIUS	Access-Request(1) (id=0, l=170)
49	4.872703	192.168.0.103	192.168.0.60	LDAP	searchRequest(38) "ou=Users,dc=mg,dc=com,dc=pe" wholeSubtree
50	4.874391	192.168.0.60	192.168.0.103	LDAP	searchResEntry(38) "uid=rlopez,ou=Users,dc=mg,dc=com,dc=pe"
51	4.875429	192.168.0.60	192.168.0.103	LDAP	searchResDone(38) [1 result]
52	4.880882	192.168.0.103	192.168.0.253	RADIUS	Access-Accept(2) (id=0, l=168)
53	4.914718	192.168.0.103	192.168.0.60	TCP	46481 > ldap [ACK] Seq=10913 Ack=1926 Win=2264 Len=0 TSV=1263643 TSER=1453579
54	5.616019	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xd6abd4f5
55	5.617620	ZyxelCom_fc:f4:6e	Broadcast	ARP	Who has 192.168.0.7? Tell 192.168.0.254
56	5.622596	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0xd6abd4f5

```
Frame 52 (210 bytes on wire, 210 bytes captured)
Ethernet II, Src: Vmware_7c:cc:9b (00:0c:29:7c:cc:9b), Dst: Cisco-Li_59:40:6d (00:1a:70:59:40:6d)
Internet Protocol, Src: 192.168.0.103 (192.168.0.103), Dst: 192.168.0.253 (192.168.0.253)
User Datagram Protocol, Src Port: radius (1812), Dst Port: nessus (1241)
Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x0 (0)
    Length: 168
    Authenticator: 20A1A2E3F986E467208399B8FCDB9136
    [This is a response to a request in frame 48]
    [Time from request: 0.012562000 seconds]
  Attribute Value Pairs
    AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
    AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
    AVP: l=6  t=EAP-Message(79) Last Segment[1]
      EAP fragment
      Extensible Authentication Protocol
        Code: Success (3)
        Id: 7
        Length: 4
    AVP: l=18  t=Message-Authenticator(80): 555749A0F59B70E42F62AB673FCA0CB5
      Message-Authenticator: 555749A0F59B70E42F62AB673FCA0CB5
    AVP: l=8  t=User-Name(1): rlopez
```

6to)

FreeRADIUS verifica los datos y envía el mensaje al AP para que brinde acceso al usuario

```
0000  00 1a 70 59 40 6d 00 0c  29 7c cc 9b 08 00 45 00   ..pY@m.. )|....E.
0010  00 c4 00 00 40 00 40 11  b7 74 c0 a8 00 67 c0 a8   ....@.@. .t...g..
0020  00 fd 07 14 04 d9 00 b0  4e eb 02 00 00 a8 20 a1   ........ N..... .
```

Frame (210 bytes) | Reassembled EAP (4 bytes)

File: "I:\captura-desde-freeradius-con-wpa-enterprise-feb-2008" 26 KB 00:00:33 | Packets: 103 Displayed: 103 Marked: 0

Descripción del Sistema de Administración propuesto para una red Wi-Fi

- FreeRADIUS + 802.1x + WPA2 + OpenLDAP + SAMBA

- WPA2 *Enterprise*, ¿por qué?
  - Uso obligatorio de AES (128 bits)
  - Soporte de control de acceso de usuarios con 802.1x

- 802.1x y EAP-PEAP, ¿por qué?
  - Acceso seguro a la WLAN
    - 1ro) Túnel TLS cifrado
    - 2do) En su interior el método de auth: MS-CHAPv2
  - Todos los usuarios de la WLAN eran portátiles con Window$
    - Se evita tener que instalar software adicional
    - Facilita la administración cuando son muchos usuarios

Descripción del Sistema de Administración propuesto para una red Wi-Fi

- FreeRADIUS, ¿por qué?
  - Servidor RADIUS: *the most widely deployed*
  - Soporte de muchísimos protocolos de autenticación
- OpenLDAP + SAMBA, ¿por qué?
  - OpenLDAP: Servidor de directorios ligero y extra rápido
  - Añadiéndole SAMBA: Se convierte en un *Domain Controller*
  - O+S: Posibilita que las Window$ se autentiquen directamente con el asistente de acceso a redes inalámbricas
- Adicional: MySQL y Squid
  - MySQL: Se registran todos los accesos de los usuarios
  - Squid: Se gestiona el acceso a la Web

Análisis costo-beneficio

- Analizar los distintos beneficios que nos pueden ofrecer los variados equipos Wi-Fi que hay en el mercado

- Zyxel Prestige 660HW-T1 (US$ 30~40)
  - Permite WPA/WPA2 Enterprise y Logging
- Linksys WRT54g (US$ 100~120)
  - Permite WPA/WPA2 Enterprise, pero no logging
  - Cambiándole el firmware por DD-WRT permite logging y muchas otras funcionalidades
- D-Link DWL-3200AP (US$180~250)
  - Permite:
    - WPA/WPA2 Enterprise y Logging
    - Tener múltiples SSID
    - Asignación de VLAN
    - Detección de Rouge AP

Conclusiones

- Es posible usando SW Libre (serio, seguro y rentable)
- Se ofrece un acceso al medio seguro para los usuarios
- No es posible capturar la información de otros
- Cada usuario usa su propia contraseña
  - Ventajas vs Desventajas
- Análisis:
  - Squid vs Traffic control
  - TLS vs TTLS vs PEAP
- Propuesta a futuro:
  - Desarrollar el módulo de *billing*

Referencias

- **IEEE 802.11 Standards**
- **ZDNet & TechRepublic Whitepapers** (George Ou)
- **Wi-Foo, The secrets of wireless hacking**
- **Trainsignal Wireless Videos**
- **Wi-Fi Alliance** (http://www.wi-fi.org)
- **Cisco Systems** (http://www.cisco.com)
- **FreeRADIUS** (http://www.freeradius.org)
- **OpenLDAP** (http://www.openldap.org)
- **MySQL** (http://www.mysql.com)
- **Squid** (http://www.squid-cache.org)
- **Samba** (http://www.samba.org)
- **DD-WRT** (http://www.dd-wrt.com)

Administración de redes Wi-Fi seguras usando software libre
¿Preguntas?

¡Muchas gracias por su atención!

Jorge A. López Mori
jorge.lopez@pucp.edu.pe