

Segurança em redes sem fio

Nelson Murilo
<nelson@pangeia.com.br>

Segurança em redes sem fio

GTES/GTS-15

- Perfil
- Conceitos iniciais
- Tipos
 - Frequências
 - Características
 - Padrões atuais
- Problemas
- Defesa



Segurança em redes sem fio

Perfil

GTES/GTS-15

- **Atuação na área de segurança desde 1992**
- **Testes de intrusão** (Bancos, órgãos militares, governo, instituições financeiras, comp. aéreas, etc.)
- **Administrador do Centro de Resposta à Incidentes do Departamento de Polícia Federal**
- **Investigação forense computacional**
- **Projetos e implantação de políticas de segurança, em órgãos do governo, de inteligência e militares**
- **Monitoramento de *sites* em tempo real**
- **Desenvolvimento de ferramentas de segurança**
- **Colaborador do Grupo de Segurança do Comitê Gestor/BR**
- **Autor do livro “Segurança Nacional – Técnicas e ferramentas de ataque e defesa de rede de computadores”**

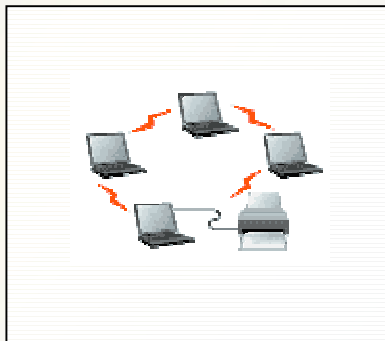
Segurança em redes sem fio

Conceitos

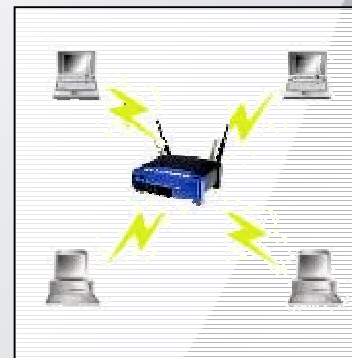
GTES/GTS-15

- Uso de frequências ISM ^[1] (900mhz/2.4Ghz/5Ghz)
 - Frequências também usadas por celulares, telefones sem fio, bluetooth, etc.
- Dois modos de operação

GRUPOS



INFRAESTRUTURA



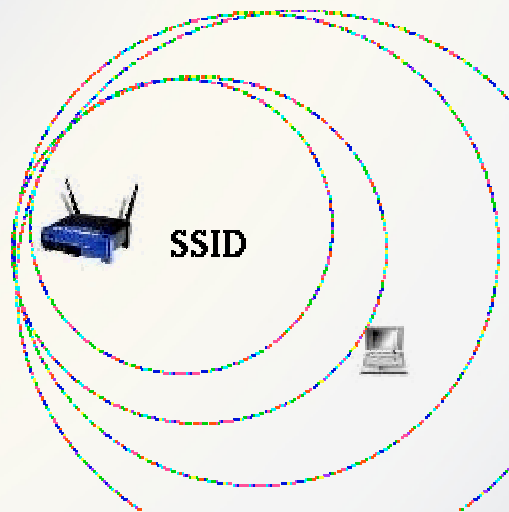
Segurança em redes sem fio

Conceitos

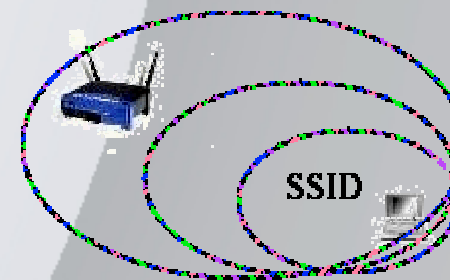
GTES/GTS-15

- Métodos de busca

PASSIVA



ATIVA



Segurança em redes sem fio

Tipos


GTES/GTS-15

- **IEEE 802.11**
 - Freqüências de 900, 2.4 e 5Ghz
- **802.11b** (padrão atual)
 - 2.4Ghz
 - Máximo de 22Mbs
 - Freqüência compartilhada
- **802.11g**
 - 2.4Ghz
 - Máximo de 54Mbs (72 em modo turbo)
 - Freqüência compartilhada
- **801.11.a**
 - 5Ghz
 - Máximo de 54mbs (108 em modo turbo)
 - Limitações de uso em alguns países
 - Menor área de abrangência

Segurança em redes sem fio

Ameaças

GTES/GTS-15

- Negação de serviço e jamming
- Análise do ambiente
- Captura de tráfego
- Monkey in  the middle
- Acesso não autorizado

Segurança em redes sem fio

Análise do ambiente

GTES/GTS-15

```
> [11] Homenet54 (00:07:40:4d:1a:5c) bn093:120:027 a SSID: Homenet54
[11] Inter (00:60:1d:f0:fb:60) bn000:000:000 r BSSID: 00:07:40:4d:1a:5c
[11] HININET (00:07:40:0f:42:53) an000:000:000 o Mfg: N/A
i Channel: 11 54.0/100
c Signal/Noise: 93/120/27
m First Seen: 0:6:24
Last Seen: 0:25:6

> [7959] 11.0 (00:06:25:a8:29:7c)a 3078:105:027 [ basic navigation ]——
[1050] 11.0 (00:e0:00:87:62:0d)a 1000:000:000 [ +/-]: ap up/down
[0] 11.0 (00:07:40:0f:42:53)a 000:000:000 [ </>]: node up/down
[u/d]: page ap up/down
[e/h]: end/home
[n/s]: newest/sort
[a/r]: autosel/resolve
[o/i]: nodes/audio
[w/k]: menu/refresh
[c/.]: chanlock/comment

[ file commands ]——
[l/b]: load/backup
[q]: quit

093:120:027 —————
111:138:027 —————
078:105:027 —————
078:105:027 —————
111:138:027 —————
108:135:027 —————
114:141:027 —————
111:138:027 —————
114:141:027 —————
111:138:027 —————
111:138:027 —————
093:120:027 —————
093:120:027 —————
093:120:027 —————
093:120:027 —————
069:096:027 —————
090:117:027 —————
084:111:027 —————
093:120:027 —————
090:117:027 —————
090:117:027 —————
081:108:027 —————
090:117:027 —————
078:105:027 —————
```


Segurança em redes sem fio

Análise do ambiente

GTES/GTS-15

- **SNMP** (.iso.member-body.us.ieee802dot11)
 - dot11StationID
 - dot11WEPDefaultKeyValue (somente leitura(?))
 - dot11ManufacturerID
 - ...

Segurança em redes sem fio

Negação de serviço

GTES/GTS-15

- 2.4Ghz é usado também por celular, telefones sem fio, bluetooth, cameras de vigilância e até por babás eletrônicas e forno de micro ondas.
- Não existem (ainda) outros aparelhos de baixo custo usando 5Ghz, mas os próprios equipamentos (antenas, placas, etc) podem ser modificados para gerar ruído.

Segurança em redes sem fio

Captura de tráfego

GTES/GTS-15

É possível a captura de tráfego mesmo não fazendo parte da rede

The screenshot shows a terminal window titled "Terminal" with a menu bar for "Font" and "Options". The terminal prompt is "kismet_hopper &". The main content is a green text dump of network traffic analysis. It includes a "Network List" header, a "Data Strings Dump" section containing HTML code with email links and a JavaScript snippet, and a footer indicating "Found IP 192.168.11.1 for Homenet54:1:00" and "Battery: 40% 0h0m0s".

```
Terminal
Font Options
kismet_hopper &
- Network List --(BSSID)----- -Info-
- Data Strings Dump-----
- [ ] <tr align=center><td height=40>
  <font face=uerdana size=1>
  <a href=mailto:suporte@zipmail.com.br>
  <a href=http://web.zipmail.com.br/su
  tica de privacidade</a>
  <a href=mailto:publicidade@bol.com.br>
  
  </td>
  </tr>
</table>
<script>document.dataentry.username.
<script language="JavaScript">
if (document.cookie.indexOf('zipnet')
document.cookie="name=zipnet;path=/";
window.open("http://www.bol.com.br/t
/--)
</script>
</body>
</html>
- [ ] borges
  eliot
  eliot
- Found IP 192.168.11.1 for Homenet54:1:00
- Battery: 40% 0h0m0s
1
abc 21:00
```

Segurança em redes sem fio

Captura de tráfego

GTES/GTS-15

Dentro da rede a captura pode ser feita com ferramentas tradicionais

The screenshot shows the Ethereal interface with a list of captured packets. Packet 20 is selected, showing a NetBIOS name query from 10.61.5.118 to 10.61.7.255. The detailed view below shows the protocol stack (Ethernet II, Internet Protocol, User Datagram Protocol, NetBIOS Name Service) and the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
13	0.470135	10.61.5.79	204.152.184.75	TCP	4035 > 49293 [ACK] Seq=2
14	0.470185	204.152.184.75	10.61.5.79	TCP	49293 > 4035 [ACK] Seq=1
15	0.470273	10.61.5.79	204.152.184.75	TCP	4035 > 49293 [ACK] Seq=2
16	0.472842	204.152.184.75	10.61.5.79	TCP	49293 > 4035 [ACK] Seq=1
17	0.472934	10.61.5.79	204.152.184.75	TCP	4035 > 49293 [ACK] Seq=2
18	0.472961	204.152.184.75	10.61.5.79	TCP	49293 > 4035 [ACK] Seq=1
19	0.473077	10.61.5.79	204.152.184.75	TCP	4035 > 49293 [ACK] Seq=2
20	0.601446	10.61.5.118	10.61.7.255	NBNS	Name query NB WORKGROUP<
21	0.602748	10.61.5.10	10.61.7.255	BROWSER	Domain/workgroup Announc

Frame 20 (92 on wire, 92 captured)

- Ethernet II
- Internet Protocol, Src Addr: 10.61.5.118 (10.61.5.118), Dst Addr: 10.61.7.255 (10.61.7.255)
- User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
- NetBIOS Name Service

```
0000  ff ff ff ff ff ff 00 03 47 ad d0 c6 08 00 45 00  .....G.....E.
0010  00 4e d1 b1 00 00 80 11 46 ff 0a 3d 05 76 0a 3d  .N.....F..=.v.=
0020  07 ff 00 89 00 89 00 3a bf 3b 9b c1 01 10 00 01  .....:;.....
0030  00 00 00 00 00 00 20 46 48 45 50 46 43 45 4c 45  .....FHEPFCELE
0040  48 46 43 45 50 46 46 46 41 43 41 43 41 43 41 43  HFCEPFFFACACACAC
0050  41 43 41 43 41 42 4d 00 00 20 00 01  ACACABM. . .
```

Segurança em redes sem fio

Captura de tráfego

GTES/GTS-15

O uso de chaves pré-configuradas facilita a quebra do tráfego criptografado

Encrypt the wireless communications by WEP(1/2)

Encrypt No encrypt


Encryption Key

1: ASCII

2: ASCII

3: ASCII

4: ASCII



Segurança em redes sem fio

Monkey in the middle

GTES/GTS-15



- Redes sem fio são mais susceptíveis a este tipo de ataque
- Muitas soluções de segurança confiam nas camadas mais baixas
- Muitas soluções de VPN são inadequadas para redes sem fio

Segurança em redes sem fio

Monkey in the middle – cenário comum GTES/GTS-15



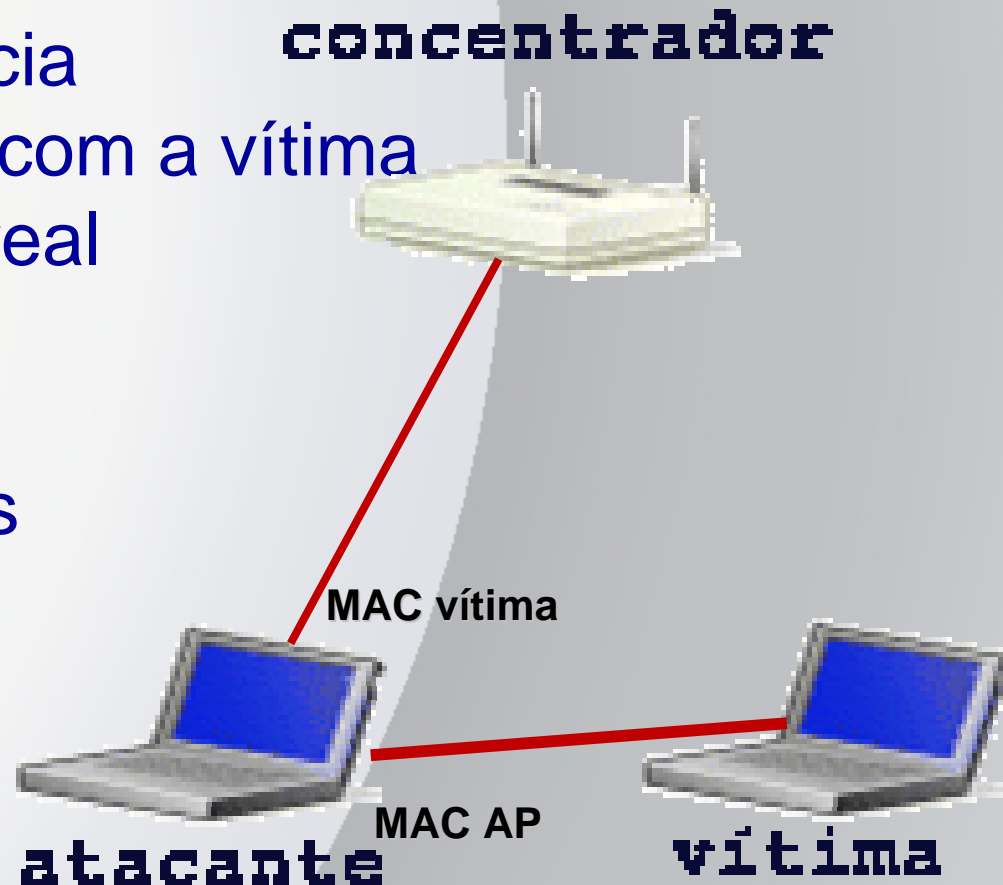
- 1) Vítima procura por um concentrador qualquer
- 2) Vítima se associa ao falso concentrador do atacante
 - Falso concentrador pode ou não usar um canal diferente do real
 - Falso concentrador duplica o endereço MAC e ESSID do real

Segurança em redes sem fio

Monkey in the middle – cenário IPSec GTES/GTS-15

1) Falso concentrador inicia negociação de chaves com a vítima e com o concentrador real

2) Dois túneis são criados



Segurança em redes sem fio

Acesso não autorizado

GTES/GTS-15

- **Servidores**
- **Clientes**
- **Roteadores**
- **Concentradores**

Segurança em redes sem fio

Acesso não autorizado

GTES/GTS-15

Clientes

The screenshot shows the Kismet application window with the 'Results' tab selected. It displays a list of detected wireless clients. Two clients are identified as 'GTER 15' with MAC addresses 00:40:96:54:30:62 and 00:40:96:54:4C:BC. A third client, named 'hotel', has a MAC address of 00:05:5D: [redacted]. The 'hotel' client is expanded to show details: Channel 0, Clients 0, First Seen 10:1:56, IP Block 0.0.0.0, Last Seen 10:2:22, MAC 00:05:5D: [redacted], Packets 54 (with sub-items: Crypt Packets 0, Data Packets 0, LLC Packets 54), Speed 0Mbps, Type AdHoc (circled in red), and Wep No. The Windows taskbar at the bottom shows the time as 10:02.

Client Name	MAC Address	Channel	Clients	First Seen	IP Block	Last Seen	MAC	Packets	Crypt Packets	Data Packets	LLC Packets	Speed	Type	Wep
GTER 15	00:40:96:54:30:62													
GTER 15	00:40:96:54:4C:BC													
hotel	00:05:5D: [redacted]	0	0	10:1:56	0.0.0.0	10:2:22	00:05:5D: [redacted]	54	0	0	54	0Mbps	AdHoc	No

Segurança em redes sem fio

Acesso não autorizado

GTES/GTS-15

Acesso ao concentrador

- Configuração padrão (incluindo senhas)
- Gerenciamento sem uso de criptografia
 - HTTP
 - Telnet
 - SNMP

Segurança em redes sem fio

Defesa

GTES/GTS-15

Acesso ao concentrador

- Mudança das configurações padrão
 - Senhas, chaves wep, SSID e canal
- Gerenciamento com criptografia
 - SSH (Primeira troca de chaves segura)
- Gerenciamento sem criptografia via LAN
- Configurar concentrador como ponte

Segurança em redes sem fio

Defesa

GTES/GTS-15

- Concentrador (AP)
 - Desabilitar propagação da identificação da rede
 - Não usar nomes que identifiquem a empresa
 - Não usar padrões de fábrica (ID, WEP, etc)
 - Usar WEP
 - Restringir MAC quando possível
 - Segurança física (posição e potência do concentrador)
 - VPN com autenticação mútua quando possível (PKI)
- Cliente
 - Desabilitar modo AD HOC
 - Desligar o retirar a placa após o uso



Segurança em redes sem fio

Segurança física

GTES/GTS-15

Posição do concentrador influencia no desempenho e na segurança



Segurança em redes sem fio

Segurança física

GTES/GTS-15

Propagação em ambiente aberto

802.11a	~240mt
802.11b	~320Mt
80211g	~500mt

Segurança em redes sem fio

Freqüências

GTES/GTS-15

Canal	Freq
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462
12	2.467
13	2.472
14	2.484

Segurança em redes sem fio

Considerações finais

GTES/GTS-15

E possível ter redes sem fio seguras utilizando camadas de segurança, e principalmente, utilizando VPN com autenticação mútua.

Grande expectativa pelo fechamento do 802.11i (ênfase em autenticação e extensão de mobilidade)

Segurança em redes sem fio

Nelson Murilo
<nelson@pangeia.com.br>