



PO Box 64070,
Highlands North
2037
admin@telspace.co.za
Landline Telephone: (011) 875-4319
Fax: (011) 802-6683

Telspace Systems Wireless Security Training – Hacking Wireless and Bluetooth 101 .

Dear Client,

Due to popular demand from our clients, Telspace Systems has decided to run a secondary course during 2008 for Hacking Wireless and Bluetooth 101. Telspace Systems provides training courses ranging from Wireless and Bluetooth Hacking through to Web Application Hacking. We would like to invite you to participate in our training session on the 3rd and 4th July 2008.

Please find the training details in the below document, detailing Wireless and Bluetooth hacking 101. Wireless Hacking will be held on Day 1, while Bluetooth Hacking will be held on Day 2.

Our training is on a very practical basis and we only have space for approximately 15 applicants during each training session. This allows the training sessions to be on a more personal level. Therefore it is best to book early for guaranteed availability.

Training will take place at:

FNB Conference and Training Centre

114 Grayston Drive, Sandown, Sandton
P O Box 781944
Sandton 2146

Telephone: 011 269 8003

The total cost for the 2 day training, on “Hacking Wireless and Bluetooth 101” is R7490 excluding VAT per person. This includes training, course material, lunch, coffee and tea breaks. For those of you who will be coming from out of JHB, there is accommodation available at the conference centre if required, for an additional cost.

If you have any queries regarding this specific training course, please feel free to contact us.

Dino Covotsos
Telspace Systems
Web: www.telspace.co.za
Telephone: (011) 875-4319
Email: dino@telspace.co.za
Executive Member

Introduction to Telspace Systems

Telspace Systems provides top level IT Security solutions in various sectors locally and internationally. Our client database is broad and includes companies in many different sectors.

Telspace Systems has, and always will, focus on vendor independent reporting. We pride ourselves of being one of the only IT Security companies in South Africa to present at international level.

A few of the organisations and companies that we have serviced include:

- Numerous South African Government Departments
- Banking institutions
- Telecommunications providers throughout Africa
- Petroleum and logistics companies
- Mining institutions
- Radio stations and broadcasting companies
- Various Airlines worldwide
- South Africa Law firms
- Recruitment companies
- Internet Service Providers

Telspace Systems also regularly releases brand new(0day) IT Security advisories as part of the “give back to open source” scheme. This is IT Security innovation at its best. A few of our releases include:

- Serious Vulnerabilities in Article Dashboard
- Serious Vulnerabilities in Iware Professional
- Various Commercial software flaws found by Telspace Systems Research.
- ActiveX Component Vulnerabilities
- Many more...

All of our research and releases are co-ordinated with the vendor and are part of a responsible disclosure effort.

Telspace Systems also has very strategic partnerships with BEE companies, such as Business Connexion Namibia, enabling us to expand through Africa and service the needs of clients throughout Africa. More about this agreement can be obtained at <http://www.telspace.co.za/press-020.php> .

Telspace Systems Competence and Exposure

Telspace Systems regularly presents at high level Government and Internationally recognised security conferences. We are often interviewed locally and internationally by magazines, television and newspapers.

A few of our latest (2007) are as follows:

- Sector 2007 – **Toronto, Canada – Speaker**
- BBC Television - BBC Program "Click" - The Truth Behind Big Screen Hacks(http://news.bbc.co.uk/2/hi/programmes/click_online/7029540.stm)
- Hack In the Box 2007 - **Dubai – Speaker** (<http://conference.hitb.org/>)
- Hack In the Box 2007 – **Malaysia (Kuala Lumpur) – Speaker**
- Regular writers for Iweek Magazine (www.iweek.co.za)
- Regular writers for PMR Africa (Governmental Magazine)
- Writers for CEO Magazine
- Regular writers and authors for ITweb (www.itweb.co.za)
- Regular writers for local and international newspapers (Sundaytimes, New Strait times etc)
- Mobileworld Magazine – **Malaysia** – Hacking the Bluetooth Stack
- CESPAM Executive Training Programme - "Combating Cybercrime in the SADC Region." – Cape Town – **Speaker**
- Business zone - International Cyber Terrorism – **Speaker**
- Information Security Practice - Information Security workshop
- Marcus Evans - Combating Financial Crimes in **Africa – Speaker**
- Various local and international websites publish our work and advisories, such as Secunia(<http://secunia.com/>) .

Hacking Wireless and Bluetooth 101

Training Brief:

Wireless networks are continually growing in our modern world and society. This 2 day course aims to demystify wireless network security and inform attendees on how to improve wireless LAN security and Bluetooth security. This will be achieved via theory and practical.

Attendees will first obtain detailed theoretical analysis of different wireless security schemas (i.e. Theory), thereafter have hands on experience in how the attacks are performed (i.e. Practical).

Attendees will also be issued with challenges in the form of wireless hacking.

Who should attend this course?

- General IT Security Specialists and Administrators.
- IT Security Specialists who are interested in Wireless hacking specifically.
- Security Officers for organizations and companies.
- Wireless Network Administrators.
- Any individual who may be interested in these topics.

Contents of the course:

Proposed program is as follows:

- Introduction to Wireless Hacking
- Wireless Protocols and Architecture
- Network Mapping
- Methodology for securing wireless networks
- Wireless hacking tools and attacks
- Defending against wireless hacking
- Introduction to Bluetooth
- Bluetooth vulnerabilities overview
- Bluetooth hacking tools and techniques
- Defending against Bluetooth attacks

Course Duration - 2 Days

Prerequisites

Basic knowledge of Wireless networks.

Participants must bring their own laptop with CDROM device (N.B for bootable software) .

Participants must have administrative rights to install software on their laptop.

Day 1 Breakdown – Wireless Hacking– 3rd July 2008

Introduction to Wireless Hacking:

- Wireless and its technology usage
- Wireless networking breakdown
- Security of wireless and progression
- What is wardriving?
- Attacking wireless brief

Wireless Protocols and Architecture:

- Analysis of various wireless protocols
- Wireless architecture and design
- 802.11 Protocol Analysis

Network Mapping and Methodology for securing wireless networks:

- Discovery of wireless networks
- Antenna variations
- Monitoring the wireless network, including packet analysis
- Various toolsets including Netstumbler, Kismet, the Aero suites and so fourth

Wireless hacking tools and attacks:

- Traffic injection tools
- Spoofing
- Flooding
- Aircrack and Aero suite of tools
- Airsnort
- WEP hacking cracking
- WPA, WPA2 hacking techniques
- Frame generation
- Defeating MAC Filtering
- Fake Access Point
- Other Attacks

Defending against wireless hacking:

- Site layout and planning
- Improving your wireless systems against hacker attacks
- Filtering

Day 2 – Breakdown - Bluetooth Hacking – 4th July 2008

Introduction to Bluetooth:

- What is Bluetooth?
- What does it allow for?
- How Bluetooth works
- Bluetooth data rates
- Bluetooth ranges and specifications
- Introduction Bluetooth security (Scatternets)
- Latest developments with Bluetooth

Bluetooth vulnerabilities overview:

- The Snarfing attack
- The Bluebug attack
- The backdoor attack
- Bluechop
- Bluedump
- Bluebump
- Bluesmack
- The social engineering factor
- Bluetooth viruses
- Bluetooth implementation problems

Bluetooth hacking tools and techniques:

- BTscan , Bluestumbler , Bluescan , BT Browser
- Bluesnarf
- Bluebug
- Bloover II
- Carwhisperer
- Blueprinting (SDP tool)
- Brute force discovery - Redfang
- Optimising range of Bluetooth attacks

Defending against Bluetooth attacks:

- Bluetooth recommendations
- Standard organizations practice
- The future for Bluetooth security and implementations

Training signup form

Training Course: Hacking Wireless & Bluetooth 101 – 3rd - 4th July 2008

Today's Date: _____

Cost: R7490 Excl VAT , per person.

Client Name(Company): _____

Client Contact number: _____

Client Address:

Number of Participants: ____

Participants Full Names:

Company or persons responsible for settling the account:

Full Name: _____

Signature: _____

Position: _____

Authorised relevant parties:

Full Name: _____

Signature: _____

Position: _____

Please fax this entire document to: 011-802-6683 as soon as possible.
Cancellations must be made in writing and not less than 2 weeks before start
of training.