

Smartphone vs SmartTV



OSCAR LEONARDO BANCHIERO

CEH/CCNP Security

TWITTER: @banchiero

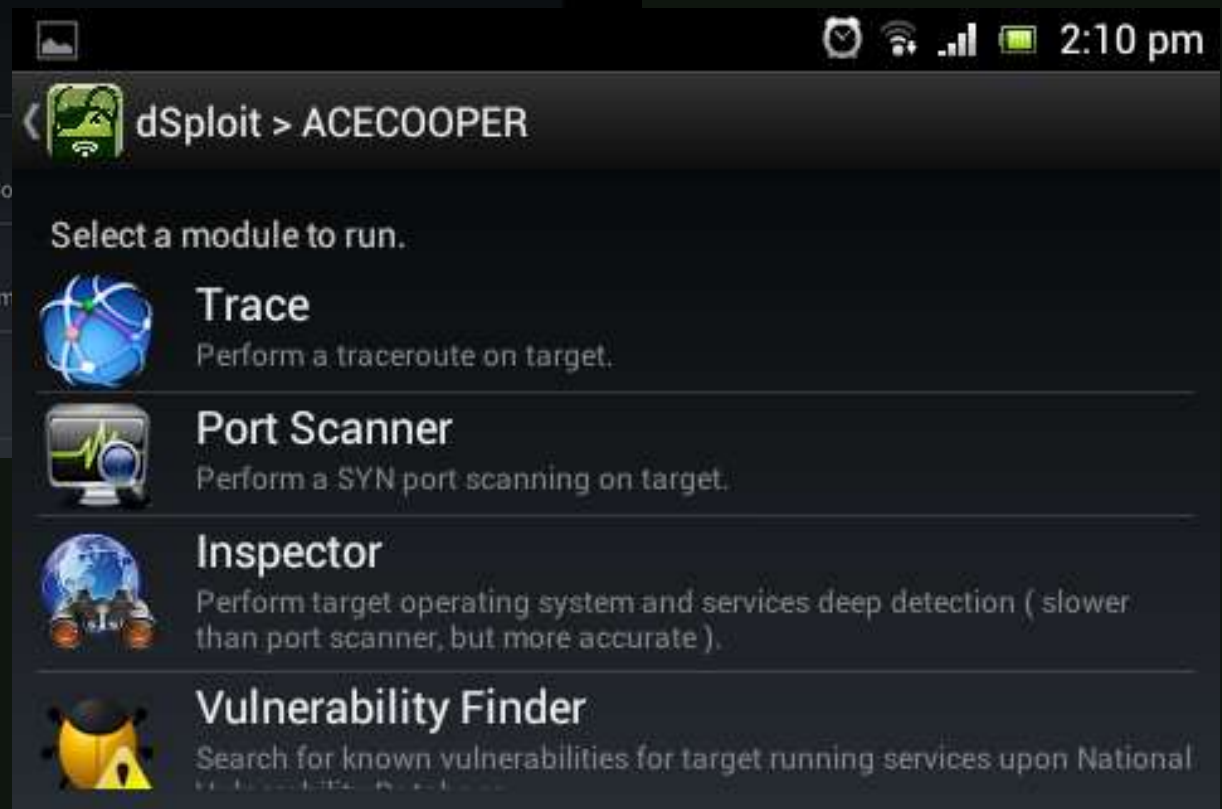
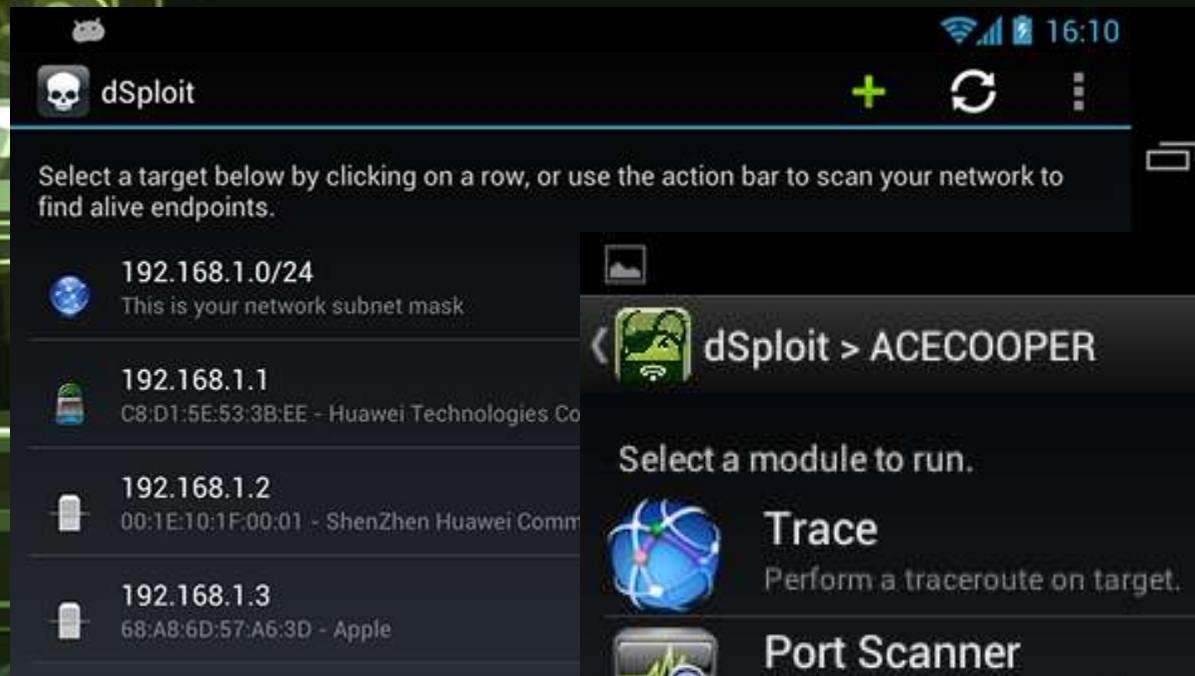
Email: oscar.banchiero@isec-global.com

Pentest con un Smartphone?

Fases de un pentesting:


- 1- Reconocimiento
- 2- Scanning
- 3- Enumeración
- 4- Vulnerabilidades
- 5- Reporte final

Pentesting: DSPL0IT




Pentesting: DSPL0IT





<  dSploit > HD2

Select a module to run.

 **Vulnerability Finder**
Search for known vulnerabilities for target running services upon National Vulnerability Database.

 **Login Cracker**
A very fast network logon cracker

 **MITM**
Perform various man-in-the-middle manipulation, etc.


 **Packet Forger**




COSMOTE




< 192-168-0-105.rdsnet.ro > MITM

 **Simple Sniff**
Redirect target's traffic through this device and show some stats while dumping it to a pcap file.

 **Password Sniffer**
Sniff passwords of many protocols such as http, ftp, imap, imaps, irc, msn, etc from the target.

 **Session Hijacker**
Listen for cookies on the network and hijack sessions.

 **Kill Connections**
Kill connections preventing the target to reach any website or server.

Queremos comprar el mejor TV



Vulnerabilities SmartTV

Televisor LED 3D de 46 pulgadas con SmartTV (Full HD 1080p, Clear Motion Rate 100 Hz)

Vulnerabilidad: fallo que permite el acceso ROOT al shell del firmware basado en Linux.

Consecuencias: control total. Un atacante podría por ejemplo acceder al contenido del TV o de cualquier dispositivo USB conectado o incluso espiar al usuario activando la cámara y el micrófono remotamente

TENER EN CUENTA:

Navegación en Internet
Uso de redes sociales
Servicios basados en streaming y
posibilidad de jugar juegos en línea

CONCLUSION



+



+



The TV is Watching You



Muchas gracias!!!

OSCAR LEONARDO BANCHIERO

CEH/CCNP Security/UCAD, entre otras,
Especialista IT Networking y Seguridad Informática,
experiencia en implementación de
auditoría de infraestructuras y de seguridad.

Desempeña tareas en Telefónica Argentina,
cumpliendo funciones con la seguridad informática
y administración de redes, en grandes empresas.

Orador en Latinoamérica sobre seguridad de la
información, como también es Instructor de cursos de
Ethical Hacking, Android Security y Wireless Security.

Autor de artículos relacionados con la seguridad,
white papers y documentos de investigación

TWITTER: @banchiero

Email: oscar.banchiero@isec-global.com