

SOIT

# Etický hacking

—

## niekoľko tipov s OSS nástrojmi

Martin Šechný, 9. 3. 2014, OSS víkend

# Etický hacking

---

## Obsah

**Prečo?**

**Hacking vs. Ethical hacking**

**ISO OSI sieťový referenčný model**

**Niekoľko tipov na útoky a obranu proti útokom**

**Backtrack/Kali Linux**

**Čo ďalej?**

# Etický hacking

---

..... Angela Merkel & CeBIT 2014

Warum?



# Etický hacking

## Hacking vs. Ethical hacking

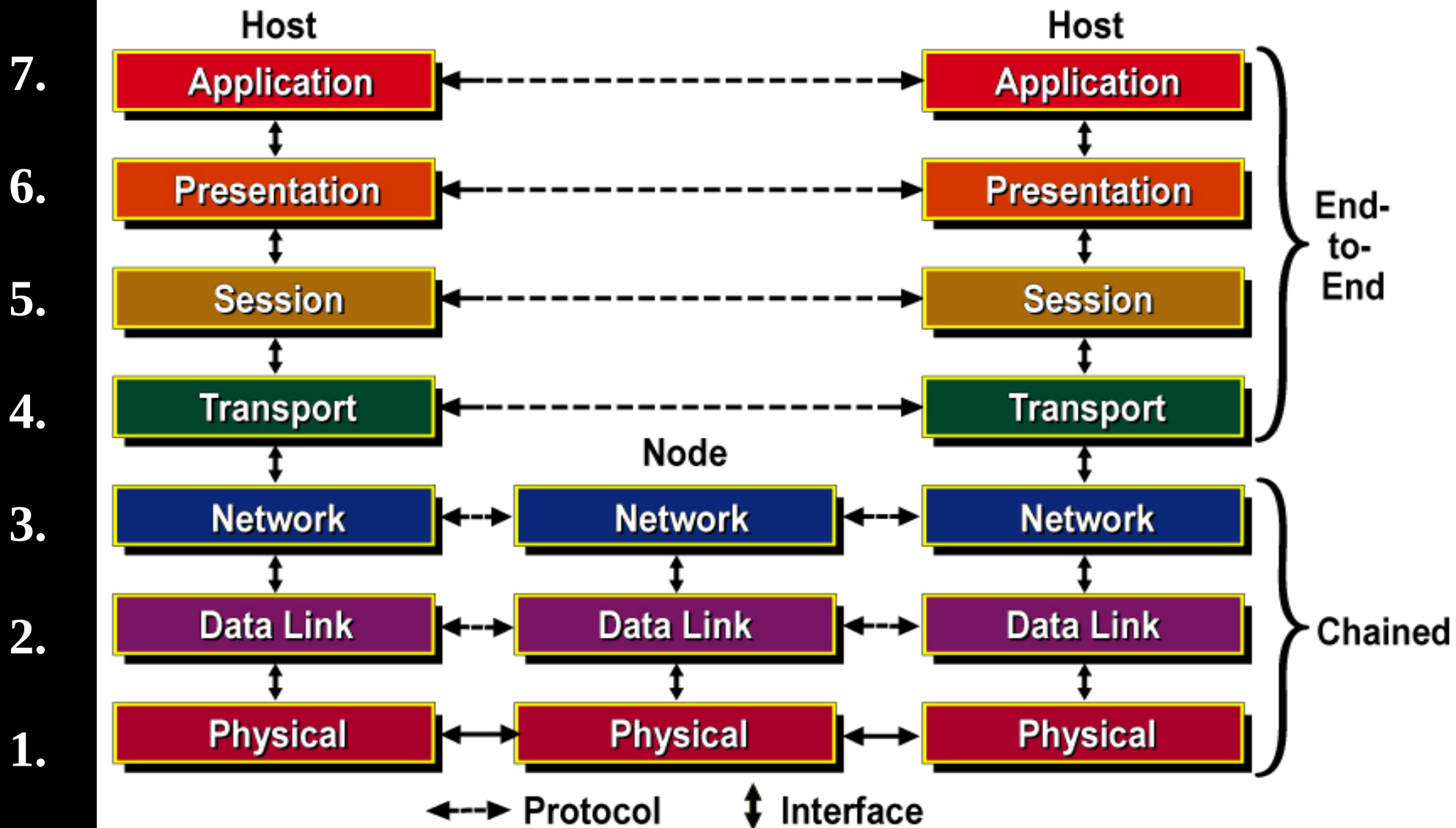
Ciel'

Obrana

Testovanie



# Etický hacking



# Etický hacking

---

## 1. fyzická vrstva

**Otvorené dvere – fyzický prístup k hardvéru**

**Odpočúvanie komunikácie na fyzickom médiu**

**Bezpečnosť v budove – oprávnenie prístupu**

**Sociálne inžinierstvo**

# Etický hacking

---

## 2. linková vrstva

**Ethernet, WiFi**

**Ethernet broadcast**

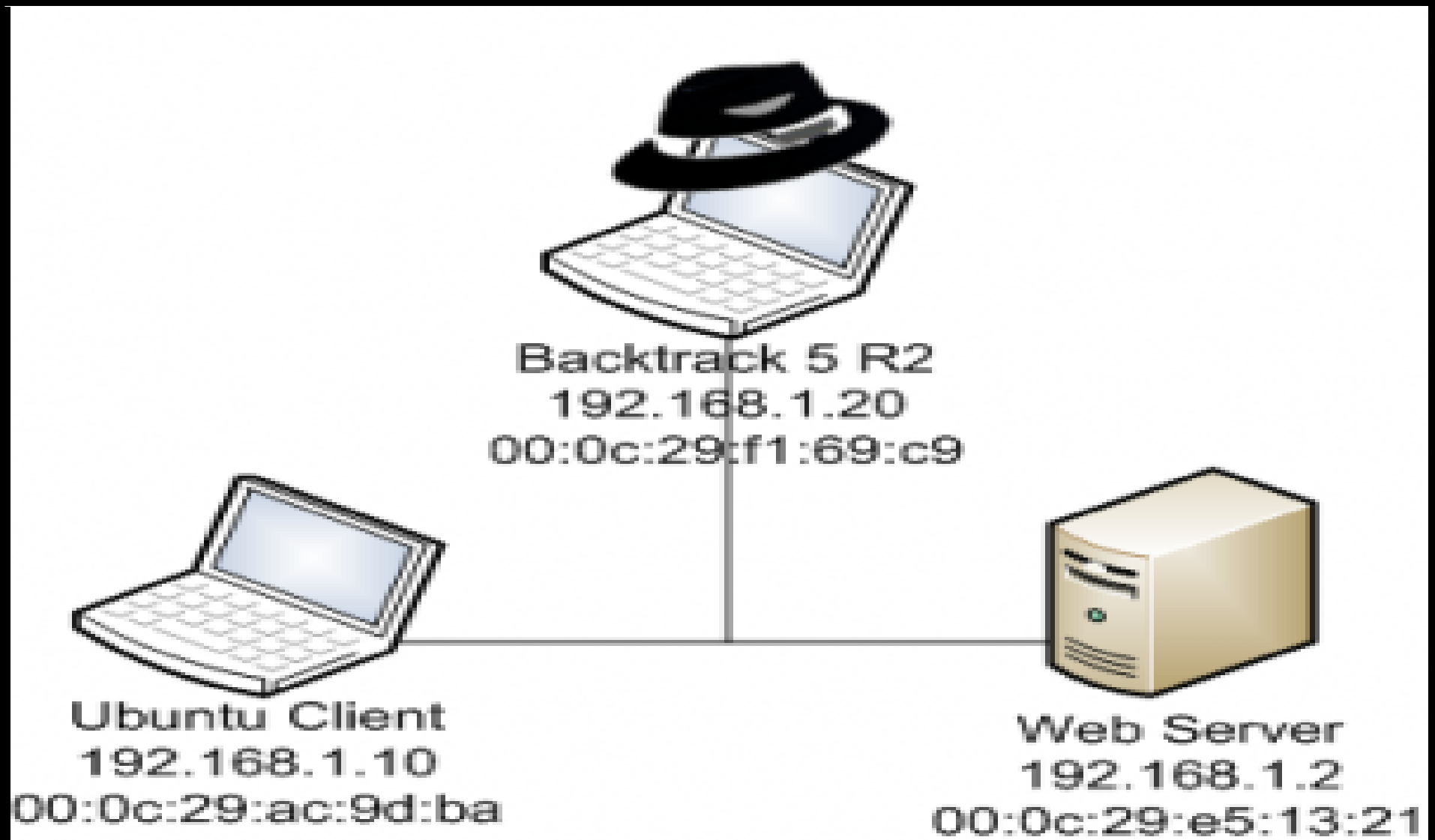
**ARP poisoning – man in the middle on LAN**

**Cisco Packet Tracer**

**Wireshark**

**Cain & Abel**

# Etický hacking





# Etický hacking

---

## 2. linková vrstva

**Switch(config-if)# switchport mode access**

**Switch(config-if)# switchport port-security**

**Switch(config-if)# switchport port-security mac-address sticky**

**Switch(config-if)# switchport port-security violation shutdown**

**WiFi access point MAC filter**

**OS firewall – MAC filter, allow localhost, deny all**

# Etický hacking

---

## 3. sieťová vrstva

**IPv4, IPv6, IPsec**

**Magic IP**

**Ping of death**

**DNS poisoning**

**Router ACL**

**OS firewall – iptables**

# Etický hacking

---

## 4. transportná vrstva

Open ports

SSL/TLS

fragment

nmap

iptables

# Etický hacking

---

..... 5. relačná vrstva

6. prezentačná vrstva

**Password**

**Hash**

**Kódovanie znakov, kódovanie jazyka**

**AJAX, JQuery, XML, SQL**

# Etický hacking

---

## 7. aplikačná vrstva

**SNMP**

**SMTP, POP, IMAP**

**HTTP & WWW – OWASP, Firefox plugin Hacktool**

**SMB**

**NTP**

**Hackxor, exploit**

# Etický hacking

---

Backtrack/Kali Linux

<http://www.kali.org>

*Čím budeš tichšie,  
tým viac budeš počuť.*



<< KALI | LINUX 1

the quieter you become, the more you are able to hear

# Etický hacking

---

Čo ďalej?

**Správa internetu:**

**neutralita vs. regulácia**

**Bezpečnosť internetu:**

**sloboda vs. cenzúra**

## Zdroje

<http://static.guim.co.uk/sys-images/Guardian/Pix/pixies/2013/10/23/1382553028804/Angela-Merkel-with-phone-009.jpg>

[http://www.bubblews.com/assets/images/news/475914001\\_1390042848.jpg](http://www.bubblews.com/assets/images/news/475914001_1390042848.jpg)

[http://www.hill2dot0.com/wiki/images/8/86/G0355\\_Layers-of-the-OSI-Mod.jpg](http://www.hill2dot0.com/wiki/images/8/86/G0355_Layers-of-the-OSI-Mod.jpg)

[http://2.bp.blogspot.com/-ZDX29AohknI/UavwNlS4vaI/AAAAAAAAAaj0/cxEEOkoIIys/s1600/391166\\_554599997896685\\_1719224629\\_n.jpg](http://2.bp.blogspot.com/-ZDX29AohknI/UavwNlS4vaI/AAAAAAAAAaj0/cxEEOkoIIys/s1600/391166_554599997896685_1719224629_n.jpg)



Creative Commons BY-NC-SA 4.0 international licence

<http://creativecommons.org/licenses/by-nc-sa/4.0/>