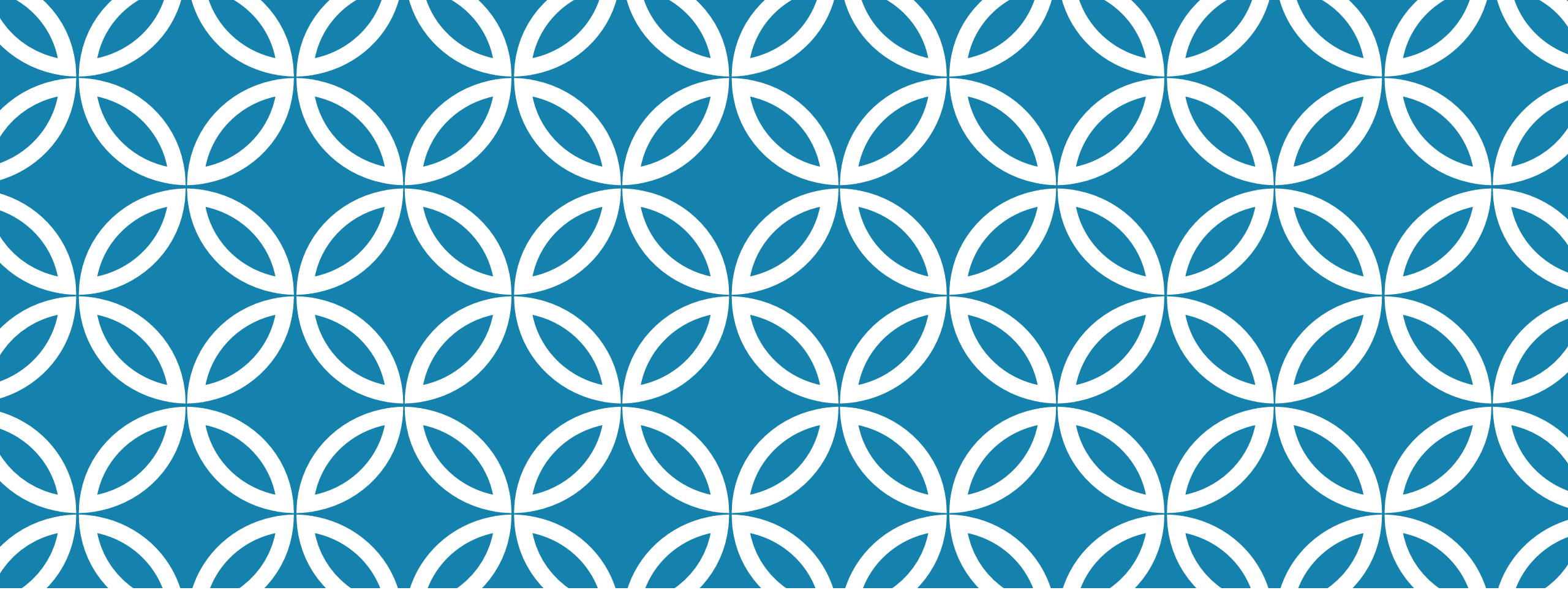


ZVYŠOVANIE POVEDOMIA O INFORMAČNEJ BEZPEČNOSTI

WIFI

Pri nastavovaní WiFi routra si môžeme zvoliť z niekoľkých možností zabezpečenia siete:

- Otvorená sieť – bez hesla, bez šifrovania (plaintextová prevádzka je viditeľná pre všetkých)
- WEP – prvé a najstaršie zabezpečenie siete, slabé šifrovanie (RC4 šifra), heslo do siete mohlo mať 5 ASCII alebo 10 ASCII znakov (prípadne 10 resp. 20 hexadecimálnych číslic), neodporúča sa používať
- WPA – vylepšené šifrovanie TKIP, kde sa heslo pre šifrovanie na pozadí stále menilo, nebola daná presná dĺžka hesla, staré a neodporúča sa používať
- WPA2 – šifrovanie modernou šifrovacou metódou AES, dnešný štandard
- WPA3 – najnovší štandard z roku 2018, staršie zariadenia ho nepodporujú

Nastavte si najvyššiu možnosť zabezpečenia, ktorú podporuje váš router a zároveň vaše koncové zariadenia (notebooky, smartfóny, tablety, tlačiarne ...)

WIFI CRACKING

Na prienik do WiFi siete (cracking) môže útočník použiť hotový nástroj dostupný na internete s názvom WiFite

Dnes si ukážeme dva útoky na WiFi sieť:

- Útok na WEP sieť – spočíva v zachytení cca 10000 – 20000 paketov (resp. rámcov) na sieti a analýze tzv. inicializačných vektorov (IV); po zachytení dostatočne veľkého množstva IV vieme heslo prelomiť za pár sekúnd
- Útok na WPA/WPA2 sieť – spočíva v donútení klientov, aby sa odpojili od WiFi routra a následnom zachytení dát, ktoré si klient s routrom vymieňajú pri pripojení; z takýchto dát je potom možné nástrojom na lámanie hesiel (napr. hashcat) prelomiť heslo (čím zložitejšie heslo, tým to dlhšie trvá)

Útočník po pripojení do siete vie odchytávať komunikáciu a tiež sa nabúrať do administračnej sekcie WiFi routra a zmeniť jeho nastavenia, prípadne ho zničiť

```
┌─[root@parrot]─[~]
└──╼ #wifite --kill

   .               .
 .´  ·  .     .  ·  `.  wifite 2.2.5
 :  :  :  (¯)  :  :  :  automated wireless auditor
 `.  ·  ` /¯\ ´  ·  .´  https://github.com/derv82/wifite2
   `     /¯¯¯\     ´

 [+] option: kill conflicting processes enabled
 [!] Warning: Recommended app hcxdumptool was not found. install @ https://github.com/ZerBea/hcxdumptool
 [!] Warning: Recommended app hcxpcaptool was not found. install @ https://github.com/ZerBea/hcxtools
 [!] Killing 2 conflicting processes
 [!] Terminating conflicting process wpa_supplicant (PID 1280)
 [!] stopping network-manager (service network-manager stop)

   Interface   PHY   Driver              Chipset
-----------------------------------------------------------------------
 1. wlan0      phy0  ath9k               Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)
 2. wlan1      phy2  rt73usb             Belkin Components F5D7050 Wireless G Adapter v3000 [Ralink RT2571W]

 [+] Select wireless interface (1-2): 2
 [+] enabling monitor mode on wlan1... enabled wlan1mon

   NUM                      ESSID   CH  ENCR  POWER  WPS?  CLIENT
   ---  -------------------------  ---  ----  -----  ----  ------
     1                OPTUS_B8E926    1   WPA   24db   yes     1
     2               Telstra962013   10   WPA   19db    no
     3               TelstraD22F23   11   WPA   19db    no
     4         (5C:A8:6A:12:78:28)    6   WPA   17db    no
     5               Telstra13AF29    5   WPA   15db    no
 [+] select target(s) (1-5) separated by commas, dashes or all: 1

 [+] (1/1) Starting attacks against F4:6B:EF:B8:E9:27 (OPTUS_B8E926)
 [+] OPTUS_B8E926 (28db) WPS Pixie-Dust: [4m8s] Sending EAPOL (Timeouts:4, Fails:5)
```

ODPORÚČANIA PRE WIFI

Po zakúpení a prvotnom pripojení nového routra do siete vykonajte nasledovné:

- Čo najskôr zmeňte heslo do administrátorskej sekcie routra
- Nastavte si najvyššiu úroveň zabezpečenia WiFi siete (WPA2 alebo WPA3)
- Aktualizujte firmvér routra – starý môže obsahovať zraniteľnosti
- Vypnite vzdialenú správu zo strany internetu/WAN (Remote management)

Čo môžete ešte urobiť pre zvýšenie zabezpečenia:

- Zapnúť MAC filtering (pripoja sa len zariadenia s presne definovanými MAC adresami) – dá sa obísť ale aspoň trocha spomalí útočníka
- Vypnúť SSID broadcast – sieť nebude vysielať svoj názov a parametre pre pripojenie, ale značne sa nám skomplikuje nastavovanie koncových zariadení
- Zapnúť izoláciu klientov (AP client isolation) – zariadenia pripojené cez WiFi sa navzájom nebudú môcť kontaktovať

BADUSB / MALDUINO / RUBBER DUCKY

Špeciálne USB zariadenie, ktoré sa tvári ako USB kľúč, ale je to vo svojej podstate klávesnica (HID zariadenie), ktorá do počítača vysiela stlačenia klávesov (scan codes) zapísaných na SD karte

Samo o sebe nie je malvérom a preto ho nedetegujú antivírusové programy a firewally

Umožňuje rýchlym stlačením klávesov (aj niekoľko tisíc slov za minútu) napríklad pridať výnimku do antivírusového programu, vyvolať príkazový riadok, stiahnuť a spustiť škodlivý kód

Obrázok: https://hackingpills.blogspot.com/2018/10/configurando-mi-malduino.html

OCHRANA PRED BADUSB

Nestrkajte si neznáme USB kľúče (nájdené, darované, požiadané o vytlačenie dokumentu...) do počítača

Ak už musíte takéto médium vložiť do počítača, majte nainštalovanú ochranu, ktorou je:

- Zapnutý virtuálny počítač, ktorý má presmerované reálne USB radiče do seba
- Ochranný program duckhunt, ktorý obmedzí príliš rýchle zadávanie znakov zablokovaním klávesnice
- Aktualizovaný antivírusový program, ktorý môže zachytiť prípadné stiahnuté škodlivé programy
- Zamykajte si počítač (Win+L), aby vám niekto takéto zariadenie nezastrčil do PC vo vašej neprítomnosti

Obrázok: https://maltronics.com/collections/malduinos

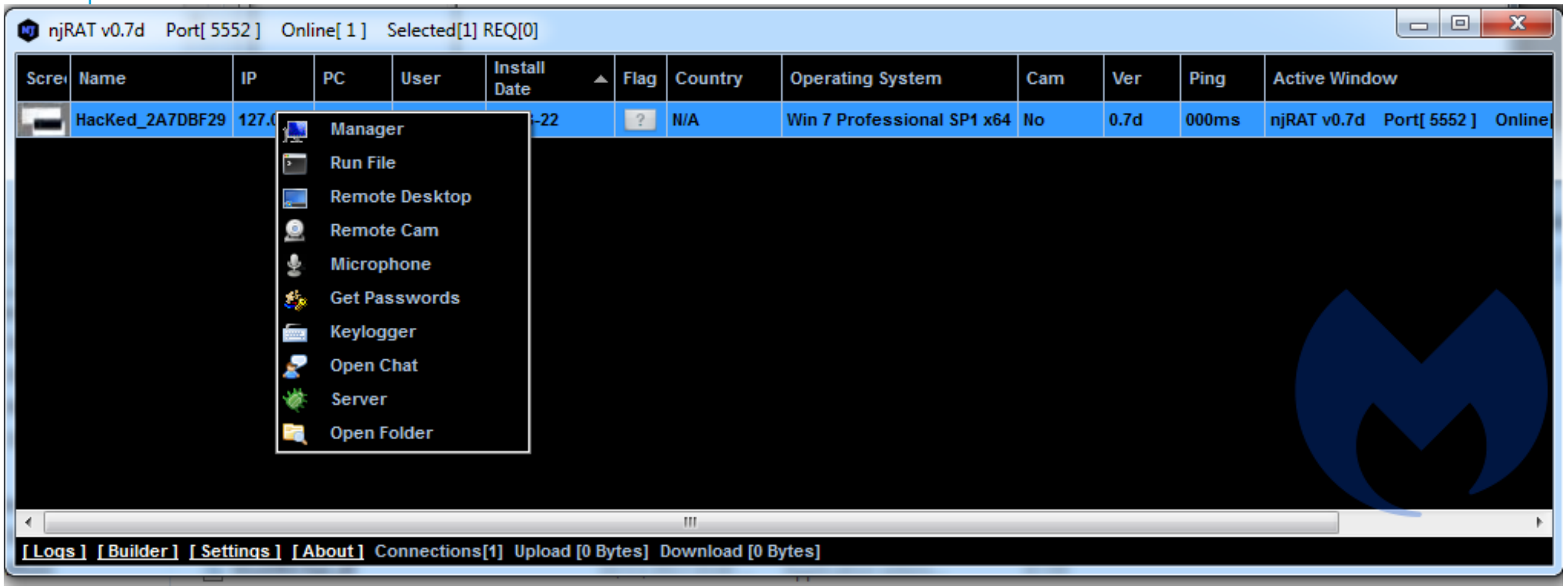
REMOTE ADMINISTRATION TOOL (RAT)

Zneužitím BadUSB môže útočník do počítača stiahnuť program na vzdialenú správu počítača (Remote Administration Tool)

Takýto program môže sledovať stlačenia klávesov (keylogger), pridávať/mazať/spúšťať súbory na disku, odpočúvať mikrofón, sledovať kameru, plochu, pristupovať do registrov a pod.

Môže byť dokonca chránený pred vypnutím

Obrázok: https://openclipart.org/detail/321970/a-dirty-rotten-rat



Obrázok: https://blog.malwarebytes.com/detections/backdoor-njrat/

ÚTOK KOPÍROVANÍM Z WEBU

Pri riešení problémov z počítačom sa často spoliehame na rady na rôznych fórach

Súčasťou týchto rád býva niekedy aj potreba nakopírovania kódu do príkazového riadku

Často používaná technológia na webových stránkach – JavaScript – však umožňuje vymeniť obsah schránky za úplné iný text, ako je viditeľný na stránke

Obeť si tak nakopírovaním a spustením škodlivého príkazu môže infikovať počítač malvérom, prípadne nenávratne zmazať dáta z počítača

TIETO INFORMÁCIE SME VÁM PRINIESLI V RÁMCI PROJEKTU

ZVYŠOVANIE POVEDOMIA O INFORMAČNEJ BEZPEČNOSTI NA STREDNÝCH ŠKOLÁCH

KTORÝ JE REALIZOVANÝ V SPOLUPRÁCI S UNIVERZITOU PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

CSIRT UPJS