Wybrane problemy bezpieczeństwa w urządzeniach sieciowych SEConference 2014

Michał Sajdak, Securitum
sekurak.pl

O mnie

- Realizuję pentesty / szkolę z bezpieczeństwa
  - securitum.pl
- Założyciel sekurak.pl
- CISSP, CEH

Agenda

- Kilka przykładów moich badań
  - Cisco RVS 4000
    - Zdalne wykonanie kodu jako root
    - Ominięcie uwierzytelnienia
    - Pokaz na żywo
  - SA500 – Cisco Security Appliance
    - Zdalne wykonanie kodu jako root / ominięcie uwierzytelnienia
    - Pokaz na żywo
  - Routery TP-Link
    - Zdalne wykonanie kodu jako root
    - Pokaz na żywo
  - Jak wystarczy czasu – mały bonus ☺

Uwaga

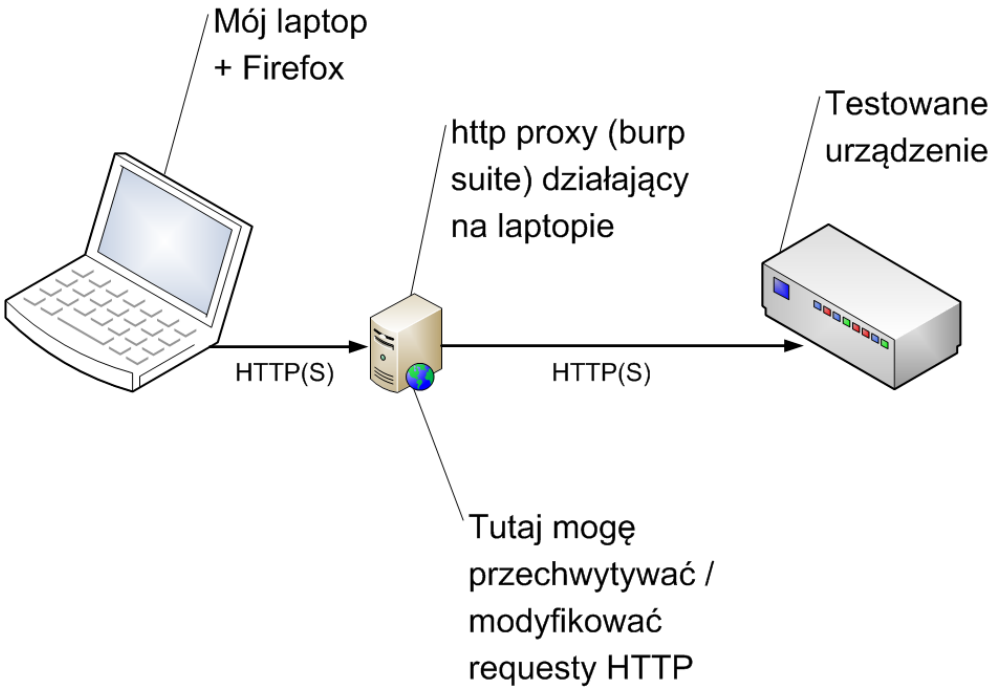
- Wszystkie prezentowane informacje należy wykorzystywać jedynie do celów edukacyjnych
- Wszystkie prezentowane bugi są załatane w najnowszych firmware

Pierwsze urządzenie

- Cisco RVS4000 security router
  - OS Command exec
  - Authentication bypass
  - Zobaczmy

Pierwsze urządzenie

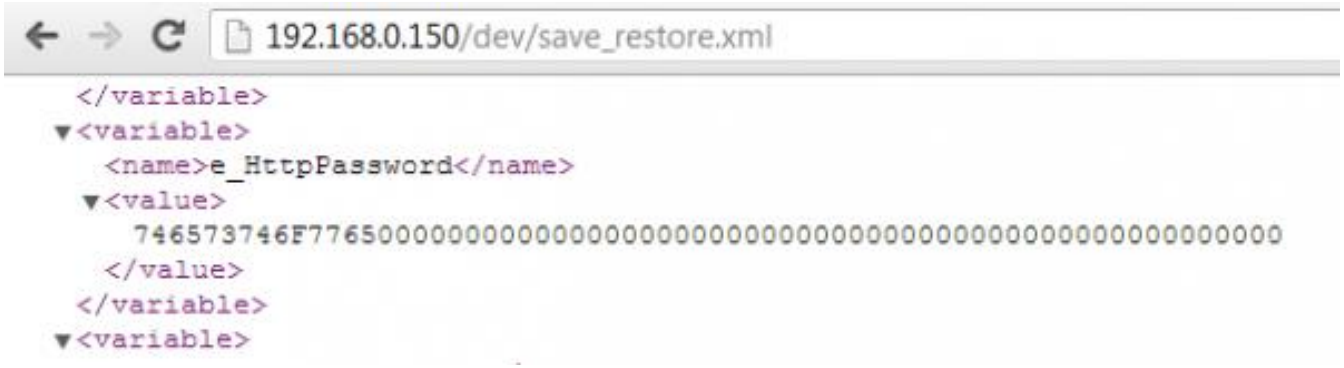
- Architektura LAB



Pierwsze urządzenie

- Swoją drogą ciekawy bug w drukarkach HP LaserJet Pro

Pierwsze urządzenie



- Świetna metoda na odzyskiwanie zapomnianego hasła ;-)
- http://sekurak.pl/hp-laserjet-pro-printers-remote-admin-password-extraction/

Drugie urządzenie

- Cisco SA 520

Drugie urządzenie

- Cisco SA 520. Menu:
  - OS command Exec
  - SQLi – ekran logowania
  - Dane uwierzytelniające w plain text
  - Zobaczmy

SQL injection - przykład

- http://site.pl/news.php?id=10
- SELECT * FROM news WHERE id = 10 AND active = 1
- http://site.pl/news.php?id=10%20OR%201=1%23
- SELECT * FROM news WHERE id = 10 OR 1=1# AND active = 1

SQL injection

- Zobaczmy jak możemy to wykorzystać w SA520

SQL injection

- Cisco Security Appliance (SA 520)
  - $SQL = „SELECT * FROM users WHERE login = ‘$login’ AND password = ‘$password’
    - Kontrolujemy login i hasło
    - Zobaczmy co się stanie jeśli użyjemy jako login/password ciągu: ‘ or ‘1’=‘1
  - $SQL = „SELECT * FROM users WHERE login = ‘’ or ‘1’=‘1’ AND password = ‘’ or ‘1’=‘1’

SQL injection

- SA 500 Appliance
  - $SQL = „SELECT * FROM users WHERE login = ‘’ or ‘1’=‘1’ AND password = ‘’ or ‘1’=‘1’
  - Zwraca wszystkie wiersze z tabeli
  - Użyjmy tego na SA500
  - Możemy tutaj użyć techniki blind SQL injection

SQL injection

- SA 500
  - Cel – chcemy pobrać wszystkie loginy i hasła (w plaintext)

SQL injection

- Następne kroki
  - Potrzebujemy znać typ bazy danych
  - Potrzebujemy wiedzieć w jakiej tabeli przechowywane są dane o użytkownikach oraz:
  - jak nazywają się kolumny przechowujące loginy / hasła
  - Wszystkie te informacje mogą być uzyskane dzięki analizie whitebox
  - Baza: SQLLite
  - Nazwa tabeli: SSLVPNUsers
  - Kolumny: Username and Password

SQL injection

- Pełne zapytanie pobierające użytkowników / hasła wygląda tak:
  - SELECT Username, Password FROM SSLVPNUsers
- Ale nie możemy tego użyć bezpośrednio
  - Ekran logowania nie wyświetla nic poza komunikatami o błędach

SQL injection

- Pobierzemy więc użytkowników hasła litera po literze
- Jak to zrobić?
  - Potrzebujemy trochę praktyki z SQL ;-)

SQL injection

- SELECT Password FROM SSLVPNUser LIMIT 1 OFFSET 0
  - Pobiera pierwsze hasło w bazie
- substr((SELECT Password FROM SSLVPNUser LIMIT 1 OFFSET 0),1,1)
  - Pobiera pierwszą literę pierwszego hasła w bazie

SQL injection

- Nasz login będzie następujący:
- ‘ OR substr((SELECT Password FROM SSLVPNUser LIMIT 1 OFFSET 0),1,1)=‘a’--
- Co skutkuje następującym zapytaniem:
- SELECT * FROM SSLVPNUser WHERE login = ‘‘ OR substr((SELECT Password FROM SSLVPNUser LIMIT 1 OFFSET 0),1,1)=‘a’--’ AND password = ‘$password’
  - Zwraca ono „invalid username” kiedy pierwsza litera hasła != ‘a’
  - Zwraca ono „inny błąd” kiedy pierwsza litera hasła = ‘a’

Urządzenia TP-Link

- TP-Link TL-WDR4300
- Firmware: 12.2012
- Pozostałe modele również podatne
  - (prawdopodobnie wszystkie?)

- http://sekurak.pl/more-information-about-tp-link-backdoor/

Urządzenia TP-Link

- Menu:
  - path traversal
  - chroot bypass
  - configuration overwrite
  - backdoor?
    - Remote code execution as root
    - TP-link twierdzi że to ‘standardowa’ metoda kalibracji WiFi w fabryce
      - Tyle że zapomnieli usunąć kod deweloperski z firmware :P
  - Zobaczmy

Urządzenia TP-Link

- Samba hint
  - http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html
  - **root preexec (S)**
  - This is the same as the *preexec* parameter except that the command is run as root. This is useful for mounting filesystems (such as CDROMs) when a connection is opened.

Dziękuję za uczestnictwo

- Pytania?
- Sekurak Hacking Party:
  - http://sekurak.pl/sekurak-hacking-party/
- Securitum
  - http://www.securitum.pl/oferta/szkolenia
- Kontakt: michal.sajdak@securitum.pl