NET – 332

NETWORK SECURITY LAB

Lab 10. Automated Attack & Penetration Tools

What are automated attacks

- Attacks targeted at websites
- Enhanced speed and efficiency
- Uses easily accessible software readily available for penetration and hacking
- Most commonly used in web application breaches for:
  - Hacking
  - Cracking
  - Theft
  - Monetary benefits

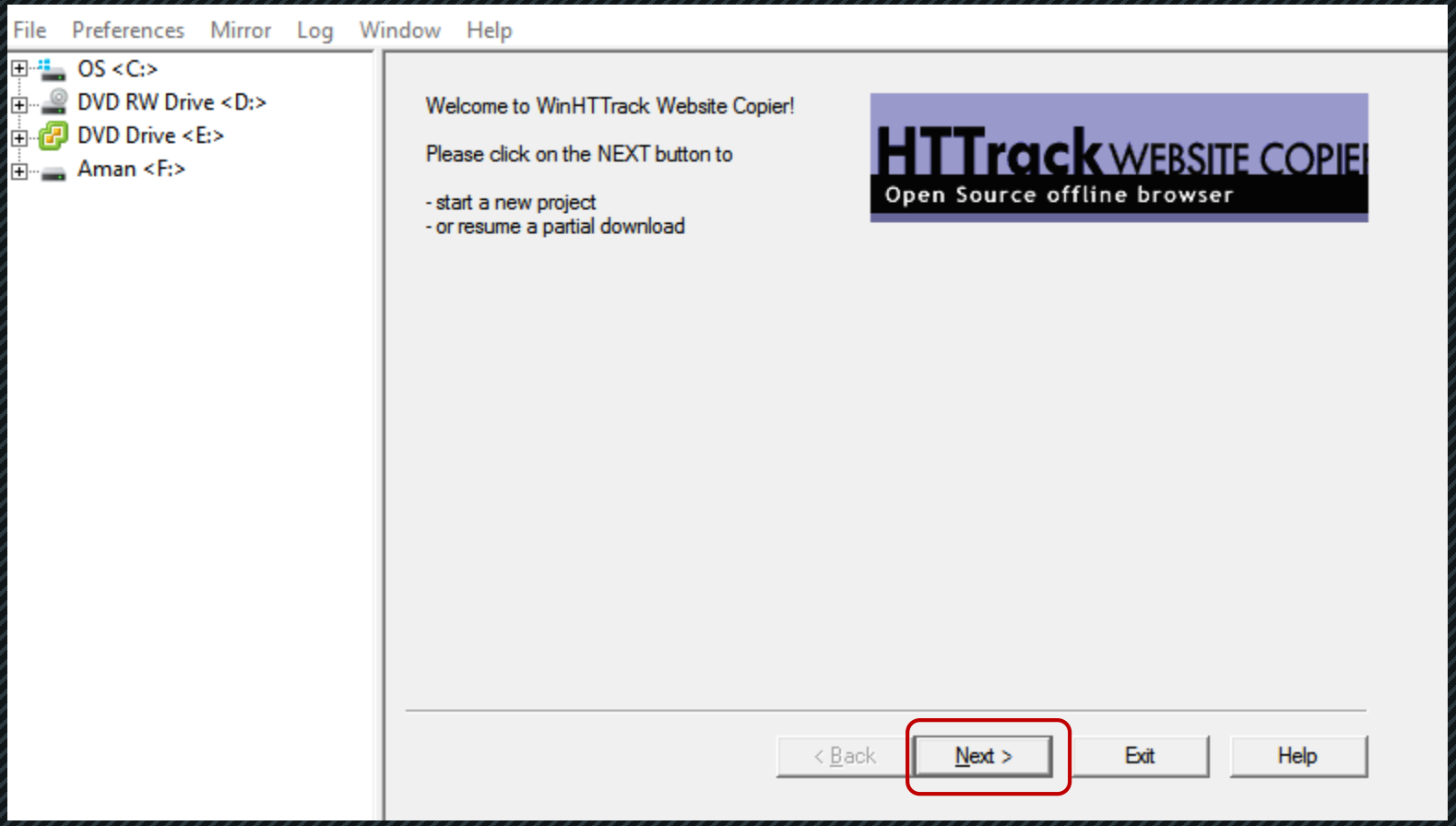
Other uses of Automated Attacks

- Allows to test the integrity of a web application.
- Intrude web-forms inside the hosted website for security verification.
- Helps in understanding the areas that need reinforcement to protect against website attacks.
- Tools that aid the automated attacks:
  - HTTrack
  - Burp site professional

Hands on with Automated Attack

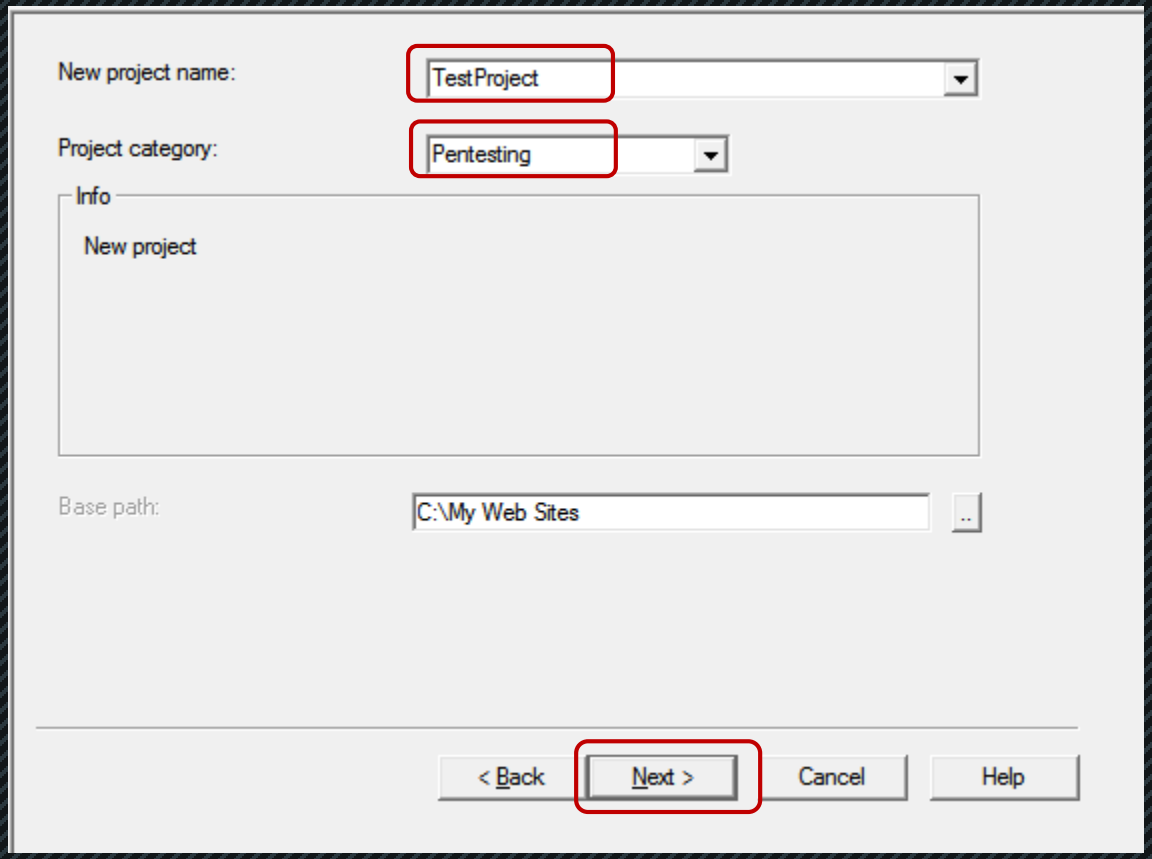
- Download the HTTrack from Vdrive folder of Lab 10 OR from here
- If downloading from Vdrive, rename the file extension to <<filename>>.exe
- Install the HTTrack software with its default settings.
- Post installation launch the HTTrack software from installed programs

HTTrack (1)



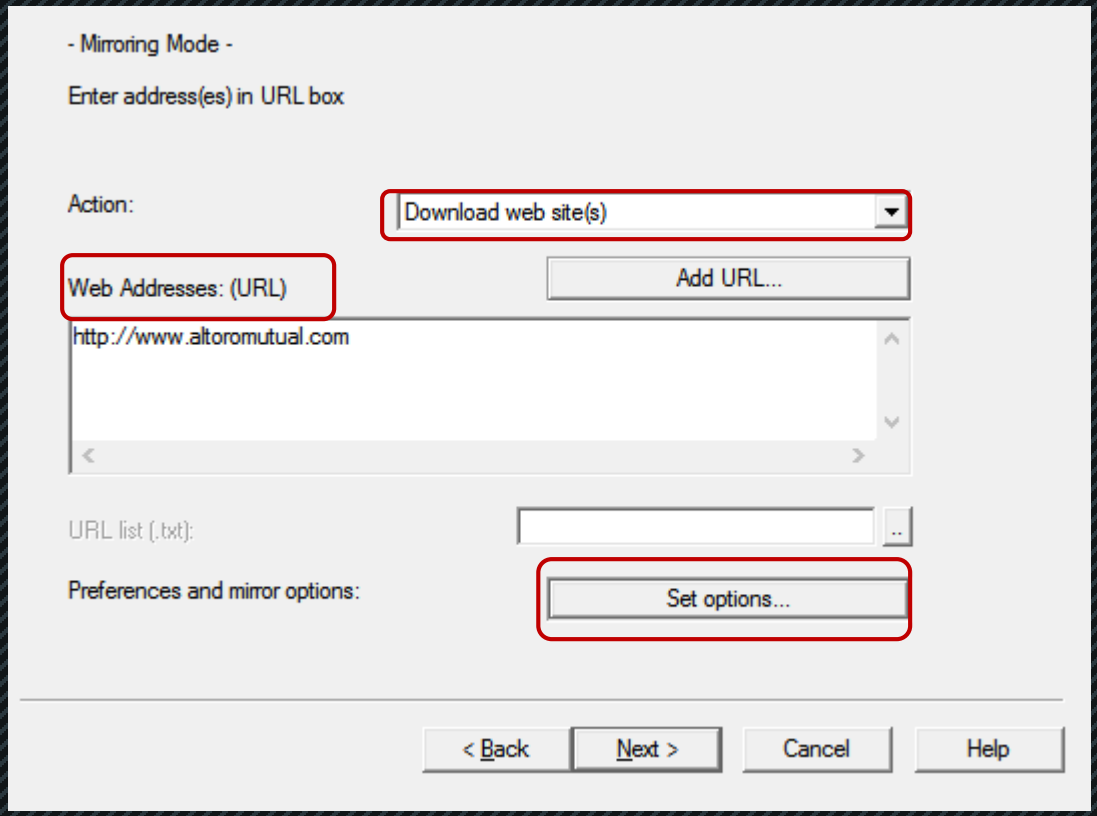
– Click on Next

HTTrack (2)



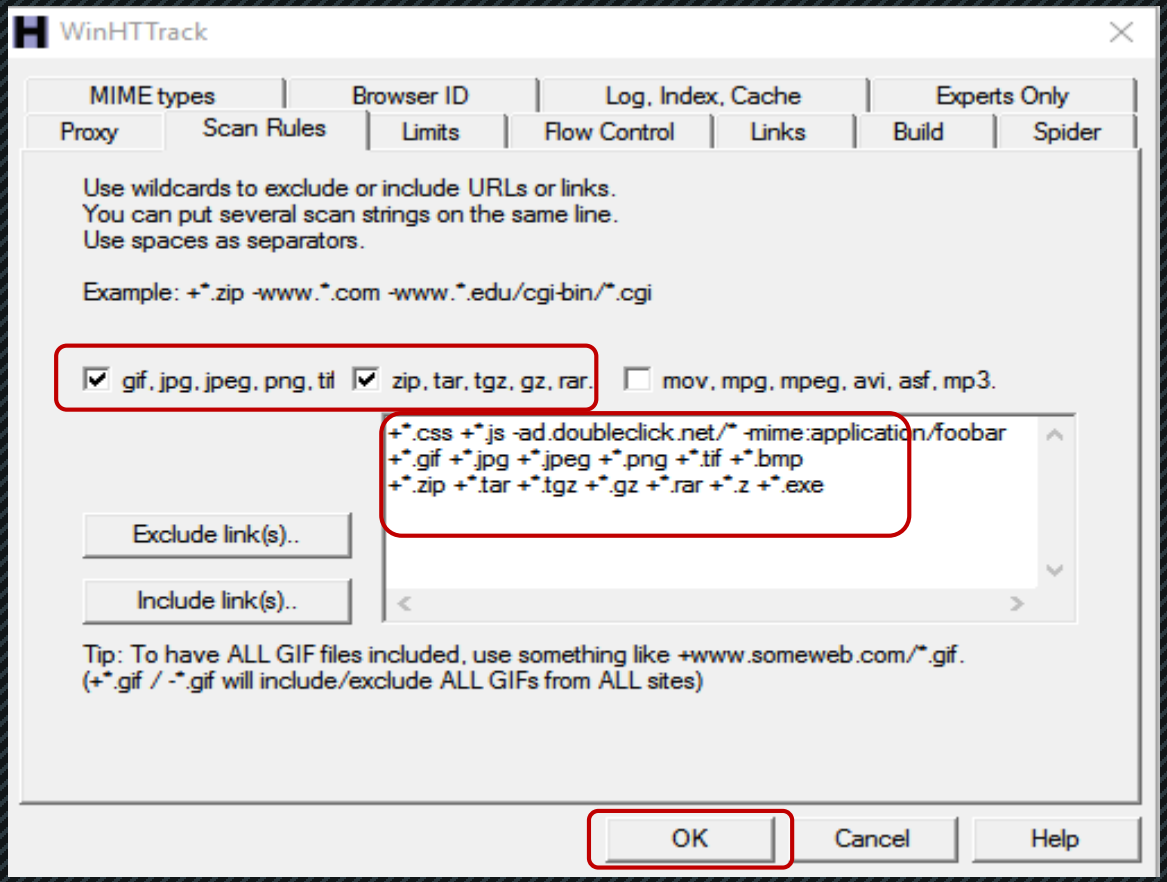
- Give a name to the project
- Give a name to the category
- Click ‘Next’

HTTrack (3)



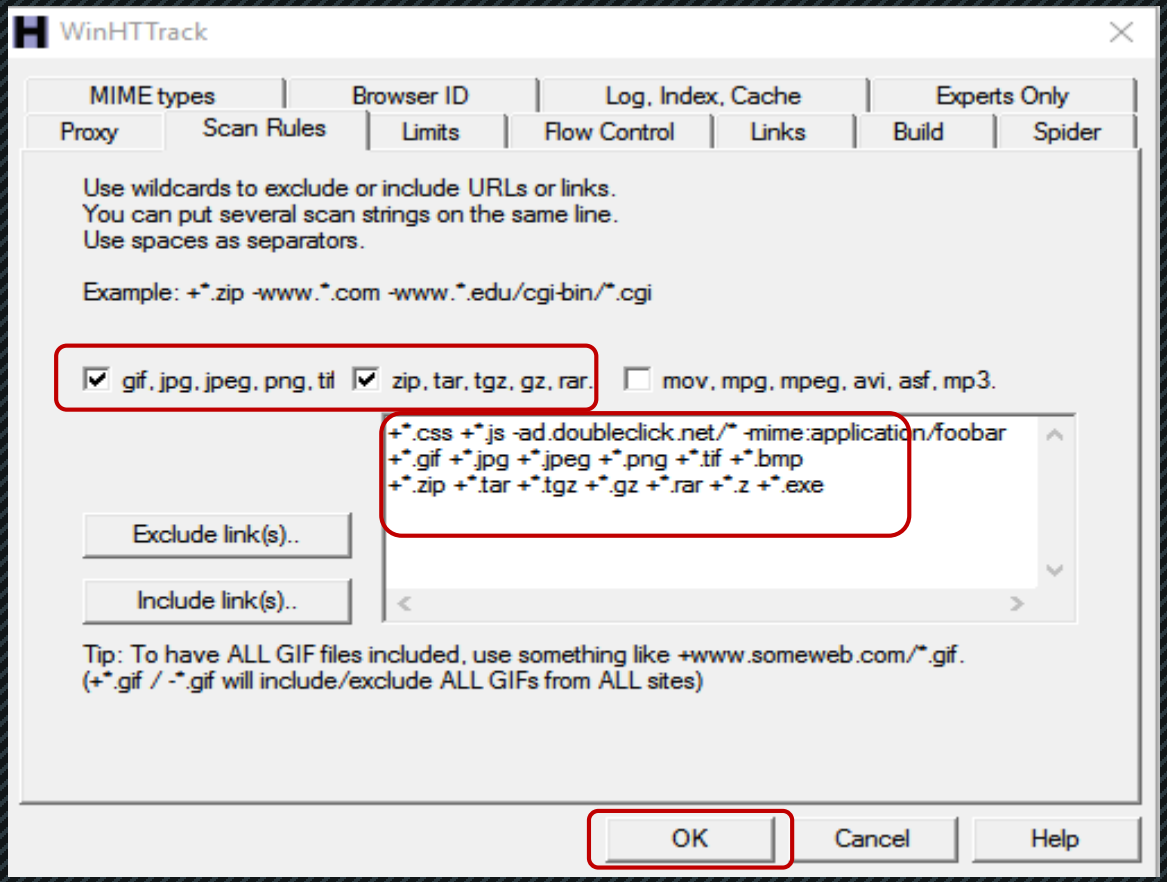
- Enter ‘www.altoromutual.com’ in web addresses
- Click on ‘Set Options’

HTTrack (4)



- Include all gifs and zip files on target website
- Click on ‘Ok’

HTTrack (5)

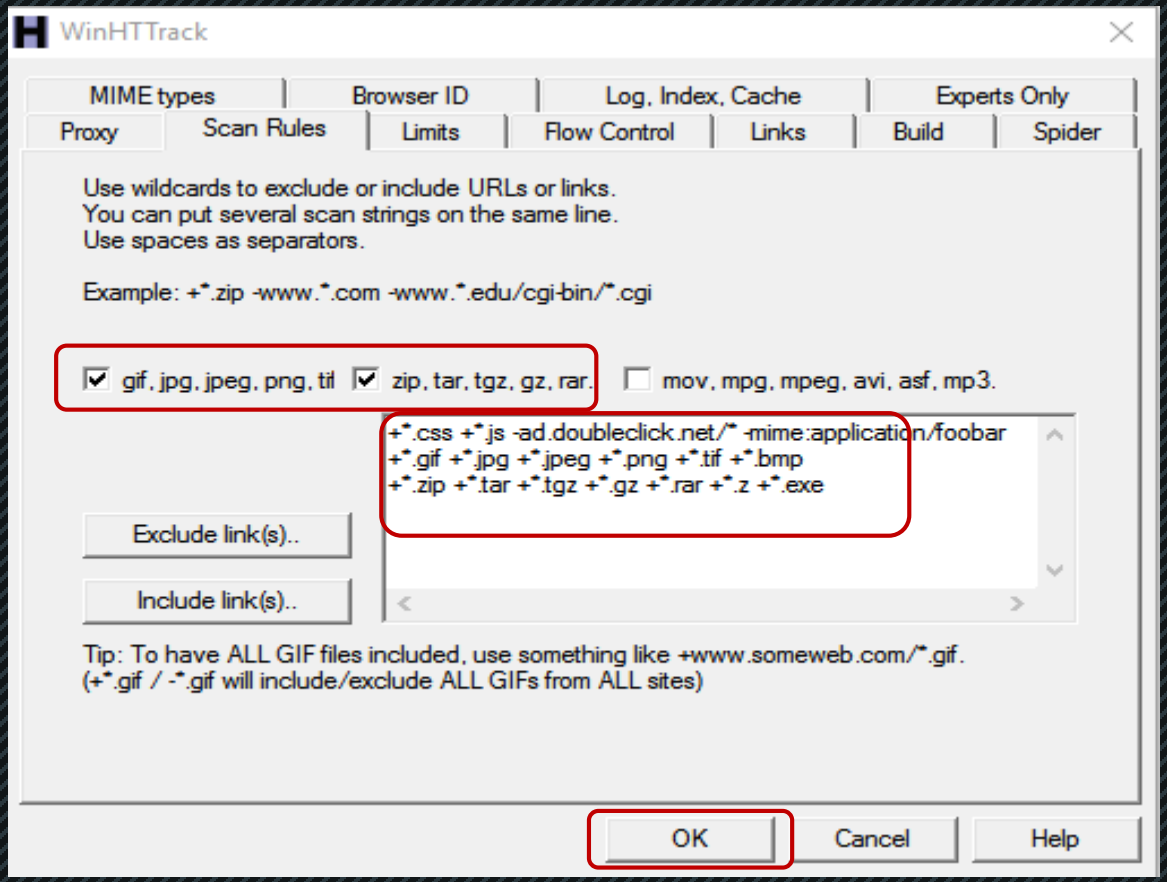


– Include all gifs and zip files on target website

– Click on ‘Ok’

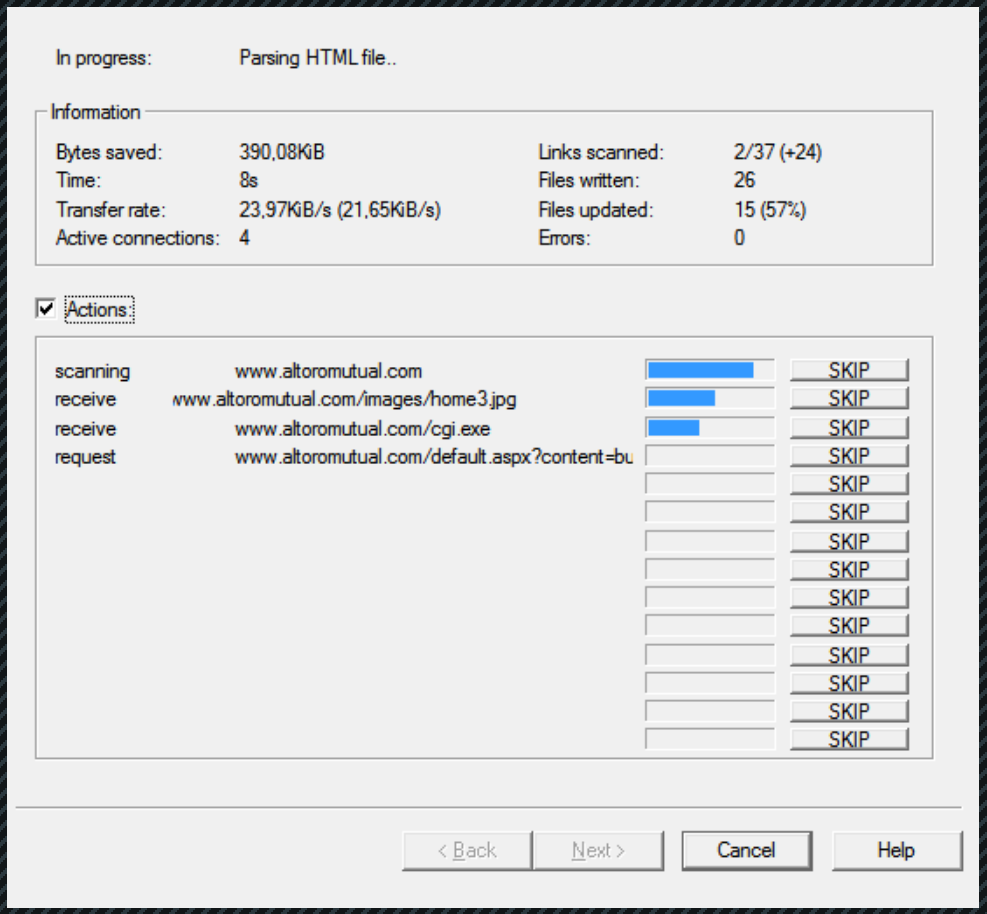
– *Click on ‘Next’ in HTTRack window*

HTTrack (6)



– Include all gifs and zip files on target website
– Click on ‘Ok’
– *Click on ‘Next’ in HTTRack window*

HTTrack (7)



- HTTrack will now start mirroring the website
- Downloads all webpages as linked on target website
- *Saves the mirrored website to local disk for assessment.*

Penetration tools

- Penetration tools are categorized into:
  - *Hardware based tools*
  - *Application based tools*
  - *Programming tools*
- For testing purposes its recommended:
  - *That the testing is done with consent.*
  - *In a closed network*
  - *On nodes that don't have any sensitive data.*

Hardware based tools

- Examples:
  - *PWN Plug*
  - *Plugged into the network.*
  - *Have built-in tools to monitor and report the network activity.*
  - *Configured with apps for smartphones*
  - *Enabled with wifi and Bluetooth*
  - *Downside: expensive*
  - *Inexpensive Alternative: WRT65G programmable accesspoint*

Software Based tools

- Examples:
  - *Nmap Scanner*
    - *Just not a port scanner*
    - *Comes with extensive instruction manuals*
  - *Metasploit*
  - *Nessus*
  - *Wireshark – Network Sniffer / Protocol Analyzer*
  - *Microsoft Network Monitor*
  - *Microsoft Message Analyzer*
  - *KISMET*
  - *AirCrack –NG (part of Kali Linux)*
  - *John the Ripper / Rainbow Crack Software*
  - *Knoppix*

Questions