Kick-Off P3

Daniel Kales

Information Security – WT 2019/20

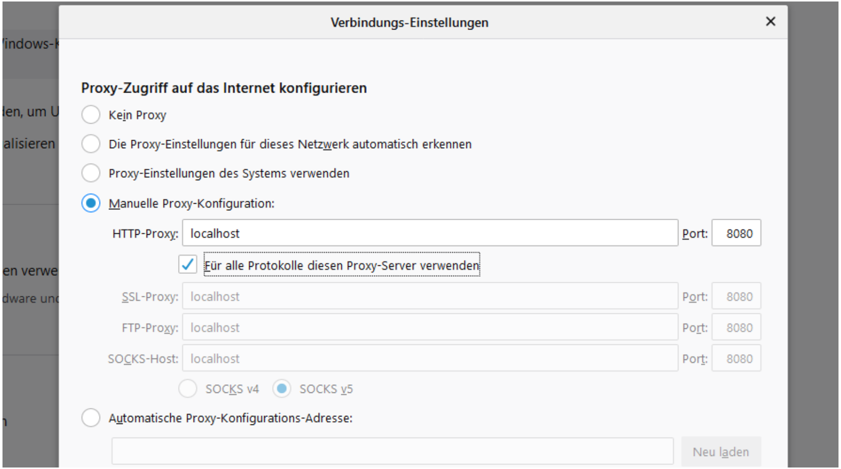
Organizational

- We may have some solo groups again
- If you want to be merged with another solo group...
  - ... come down to us after this lecture
  - ... send me a mail today!
- We will try to merge groups with similar point total

Kick-off for P3: Network-Security

Data in transit

P3: Overview



Verbindungs-Einstellungen

Proxy-Zugriff auf das Internet konfigurieren

○ Kein Proxy

○ Die Proxy-Einstellungen für dieses Netzwerk automatisch erkennen

○ Proxy-Einstellungen des Systems verwenden

● Manuelle Proxy-Konfiguration:

HTTP-Proxy: localhost Port: 8080

☑ Für alle Protokolle diesen Proxy-Server verwenden

SSL-Proxy: localhost Port: 8080

FTP-Proxy: localhost Port: 8080

SOCKS-Host: localhost Port: 8080

○ SOCKS v4 ● SOCKS v5

○ Automatische Proxy-Konfigurations-Adresse:

P3: Overview

Task P3: **Man-In-The-Middle (MITM) HTTP proxy**

- ✓ Implement a basic HTTP proxy
- ✓ Upgrade your proxy to a basic HTTPS proxy
- ✓ Implement plugins to attack users:
  - Load scripts
  - Change content
  - Downgrade to SSL
  - . . .

P3: Timeline

- Kickoff - Now
- Tutorial & Question hour - 10.01.2020, 13:30
- Question hour - 17.01.2020, 13:30
- **Deadline** - 24.01.2020, 23:59

P3: Assignment

Detailed specification in the teaching wiki

- Link available on course website
- Read the assignment carefully!

Submission and file-distribution using git

- use the same-repository (P3 subfolder)
- pull the assignment files from the upstream repository
  - see course website for instructions!

✓ Points will be published online

- Automated test system with daily tests for each task
- Links on course website

P3: Assignment

- Detailed specification in the teaching wiki
  - Link available on course website
  - Read the assignment carefully!
- Submission and file-distribution using git
  - use the same-repository (P3 subfolder)
  - pull the assignment files from the upstream repository
    - see course website for instructions!
- ✓ Points will be published online
  - Automated test system with daily tests for each task
  - Links on course website

P3: Assignment

- Detailed specification in the teaching wiki
  - Link available on course website
  - Read the assignment carefully!
- Submission and file-distribution using git
  - use the same-repository (P3 subfolder)
  - pull the assignment files from the upstream repository
    - see course website for instructions!
- ✓ Points will be published online
  - Automated test system with daily tests for each task
  - Links on course website

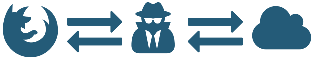
P3: Framework

- You will get a skeleton project written in Java
  - Argument parsing already implemented
  - You need to implement the proxy and plugins
- Where should you begin?
  - Install your favorite Java IDE (Eclipse, IntelliJ IDEA)
  - Clone the assignment from the upstream repo
  - Read the task description, read the hints
  - Checkout the resources on Java Socket programming

P3: Framework

- You will get a skeleton project written in Java
  - Argument parsing already implemented
  - You need to implement the proxy and plugins
- Where should you begin?
  - Install your favorite Java IDE (Eclipse, IntelliJ IDEA)
  - Clone the assignment from the upstream repo
  - Read the task description, read the hints
  - Checkout the resources on Java Socket programming

MITM Proxy



♫ I’m starting with the man in the middle ♫

Overview

- HTTP Proxy (3 Points)
- HTTPS Extension (2 Points)
- Chunked Encoding (2 Points)
- Dumping Headers/Cookies (1 Point)
- Plugins
  - Improved Requests (1 Point)
  - (Un)trusted Javascript (2 Points)
  - Fake Content (0.5 Points)
  - R.I.P SSl (0.5 Points)
  - Phishing in the dark (2 Points)
  - Superfish (2 Points)

HTTP Proxy (3 Points)

- Basic proxy functionality
  - Nothing malicious yet...
- Get familiar with:
  - HTTP
  - Java Socket programming
  - Java multithreading
- Test in your local browser!
  - Suitable websites in assignment document

HTTPS Extension (2 Points)

- Allow users to connect to secure websites
  - Relay traffic between client and server
  - Nothing malicious yet...
- Get familiar with:
  - HTTP CONNECT requests
- Test in your local browser!
  - Suitable websites in assignment document

Chunked Encoding (2 Points)

- Large responses can be split up in smaller chunks
  - Useful when total lenght of response is not known
  - Nothing malicious yet...
- Get familiar with:
  - HTTP Chunked Encoding
- Test in your local browser!
  - Suitable websites in assignment document

Dumping Headers/Cookies (1 Points)

- Log HTTP headers and cookies for all requests
  - Starting to get worrysome…
  - but could be useful for debugging
- Get familiar with:
  - HTTP Headers & Cookies
- Test in your local browser!
  - Suitable websites in assignment document

Plugins I

Active attacks, time to go to the dark side…

- “Improved” Requests (1 Point)
  - Manipulating HTTP requests and responses
  - Add, remove, change HTTP Headers
- (Un)trusted Javascript (2 Points)
  - Injecting javascript into HTTP responses
  - enabling everything from alerts to keyloggers

Plugins II

- Fake Content (0.5 Points)
  - Replace any string in a response with a chosen one
  - change image sources, insert fake news, …
- R.I.P SSL (0.5 Points)
  - Downgrade HTTPS requests to HTTP (if possible)
  - Allows proxy to read normally encrypted communication
- Phishing in the dark (2 Points)
  - Redirect a user to a phishing page without him noticing
  - Rewrite links in phishing page to point to original page

Plugins III

- Superfish (2 Points)
  - Ever got asked to install a root certificate?
  - What could go wrong…
  - Be a real man-in-the-middle, even for SSL connections!
  - All other attacks now even work on pages secured with SSL
- Test all plugins in your local browser!
  - Suitable websites in assignment documents

Contact & Finding Help

- Course website: `https://www.iaik.tugraz.at/infosec`
- `infosec@iaik.tugraz.at`
- If you need help for the exercises, try (in this order):
  - Newsgroup `graz.lv.infosec`
    - Don't post your solution there...
  - Contact the responsible teaching assistant
  - Contact the responsible lecturer for the practicals
- Come to the question hours

Questions