uc3m | Universidad Carlos III de Madrid

Master in Cybersecurity

Course 2021-2022

Introduction

Florina Almenares Mendoza **florina@it.uc3m.es**

Andrés Marín López **amarin@it.uc3m.es**

Index

- What is this course about
  - Scope
- Basic concepts and definitions
- Phases of an intrusion
  - Reconnaissance
  - Vulnerability analysis
  - Exploitation
  - Post exploitation

What is this course about

- Our main goal is to improve the security of a site/organization
- We need to learn the attacking techniques, tools and procedures. What information attackers look for:
  - To passively and actively gather details about a site
  - To discover sites vulnerabilities
  - To organize attacks
  - To abuse authorization systems and software
  - To cover their traces and evade defenses
  - To social engineer (abuse) people
  - To persist attacks (backdoor systems)
  - To escalate privileges
  - To move laterally (pivoting) within the attacked network

What is not about

- **Black-mailing techniques**
  - We work for the sake of security of the organization, commanded by their authorities not for profit
- **Indiscriminated attacks**
  - We do not randomly select victims
  - We do not harvest to find the most easy and vulnerable sites
- **Creating malware and new exploitation techniques**
  - We do not work on improving the protocols and systems, just have a deeper knowledge of how and why they are vulnerable
  - They are studied in other subjects like Software Systems Exploitation, Malware Engineering and in Persistent Threats and Information Leakage
- **Working with commercial software and services**
  - We use open source software, even community versions, and some commercial versions, but not with services requiring payment.

Basic concepts

Basic Concepts

- **Security by obscurity**
- **Type of assessments**
  - **Vulnerability Analysis**
  - **Penetration Test**
  - **Red Team**
- **Black Hat**
- **Social engineering**

Security by obscurity

- **Securing software, protocols and algorithms**
  - Openness is a warranty
    - ✓ Secure algorithms and cryptography (standards)
    - ✓ Components and software (open source)
  - Better more people actively analyzing
    - ✓ Building theoretical attacks
    - ✓ Reporting vulnerabilities and solutions
- **Securing an organization network**
  - Openness is not in general a good idea
    - ✓ No similar benefits as we get for software/protocols/algorithms
    - ✓ Topology and information hiding complicates things for the attackers (as we'll see)

Vulnerability Assessment

- **Also known as vulnerability analysis**
- **Used to evaluate the security settings of an information system.**
  - Includes the evaluation of security patches applied to and missing from the system.
  - The Vulnerability Assessment Team, or VAT, can be external to the information system or part of the information systems supporting staff.
- **It is performed as part of a penetration test**
- **Authenticated or not authenticated**

Penetration testing

- **Penetration testing is the methodology and procedures followed…**
  - **…to achieve access beyond authorization**
  - **…to overpass the protection systems**
- **Always under the Organization Under Test (OUT) approval & SCOPE!**
- **Pentesters (also know as hackers, ethical hackers, white hat hackers, etc.) perform both**
  - **Vulnerability assessment, and**
  - **Exploitation and Proof of Concept (PoC) attacks**

Penetration test phases

- **Pre-engagement**
- **Reconnaissance**
- **Vulnerability analysis**
- **Exploitation**
  - Escalating privileges
  - Moving laterally
- **Post-exploitation**
  - Maintaining Access (backdoors, rootkits)
  - Covering tracks
- **Reporting - Extremely important!**

Malicious User Testing

- **The actor assumes the role of trusted insider acting maliciously (MalUser).**
- **Requires the credentials of an authorized general or administrative user**
- **With these credentials attempt to bypass security restrictions: the insider attack**
  - Viewing documents and settings in a way the account was not authorized.
  - Changing settings that should not be changed.
  - And elevating permissions beyond the account privs.
  - Simulating a rogue trusted insider.
- **This is also part of a penetration test where the credentials are acquired abusing the authentication systems**
- **Used in security metrics for exfiltration risks**

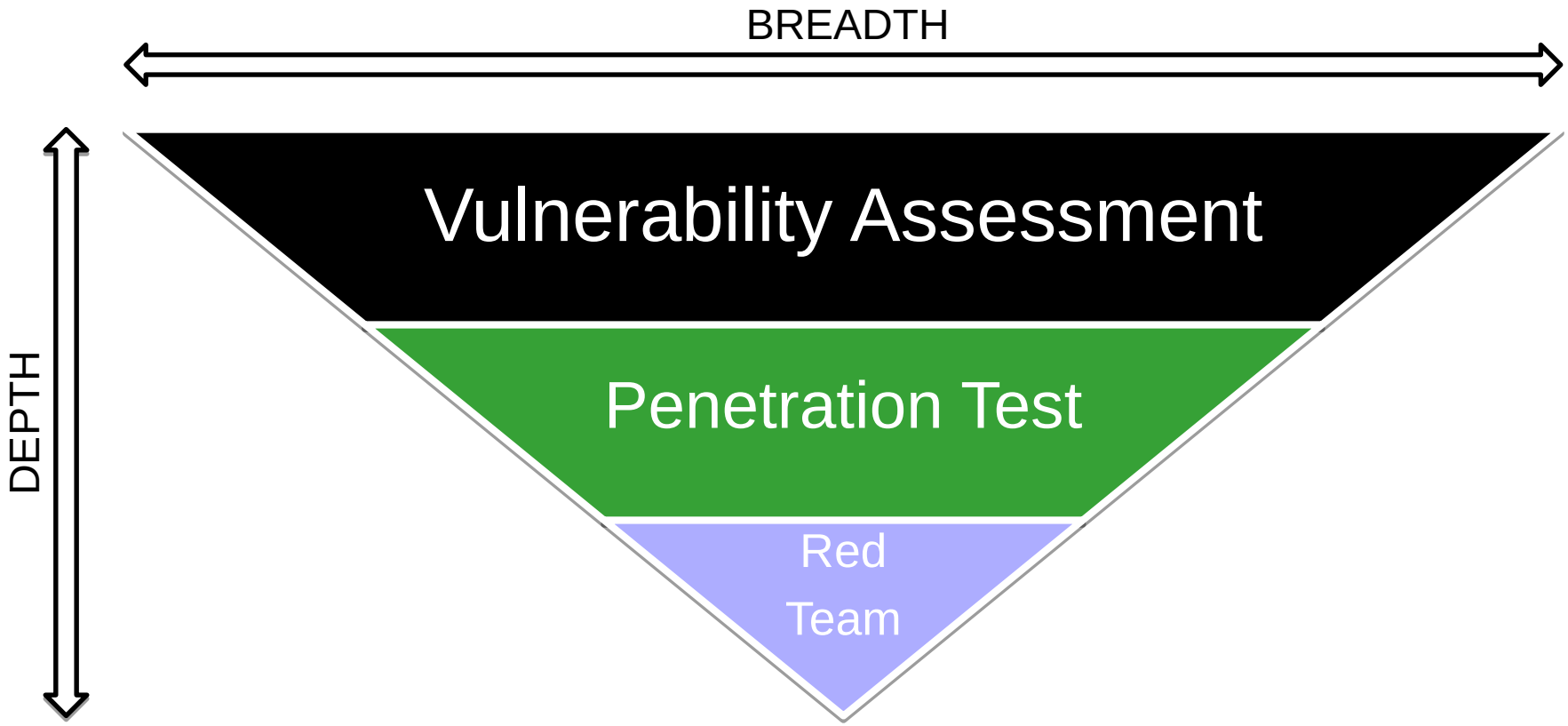
Red Team

- **Simulates techniques and methodology of a potential adversary**
- **They define/identify the adversary**
- **Goes far beyond pentesting in social and physical attacks (can't be illegal):**
  - Phishing and spear phishing
  - Dumpster diving
  - Lock picking, etc.
- **Only a small group is aware of their activities**

Comparison

	Vulnerability Assessment	Penetration Test	Red Team Engagement
Description	Automated Security Assessment	Methodical Security Asessment	Flexible Security Assessment
Goal	Identify vulnerabilities	Identify and exploit vulnerabilities. Find attack paths	Test blue teams policies, tools and skills
Scope	Wide Scan the attack surface	Restrictive, accorded, Deep Generally announced	No rules Deep Not announced
Duration	1-2 days	1-2 week	1-6 months

Comparison


BREADTH
DEPTH
Vulnerability Assessment
Penetration Test
Red
Team

Black Hat

- **Person who uses technical techniques to bypass a systems security without permission to commit computer crimes**
  - No permission, illegal act
  - Aimed at personal benefit
- **Not interested in finding all the vulnerabilities**
  - only those required to abuse the system
- **Blackmails and extorts victims after successful intrusion**
- **Often involved in organizations/groups**
  - **Black hat has a technical role**
  - **Many other roles: commercial, campaigns management, auctions/muling management, etc.**
  - **Evolving to malware as a service (MaaS):**
    - ✓ **Ransomware campaigns, botnet hiring, ...**

Social Engineering

- **Attempting to trick system users or administrators into doing something in the interest of the social engineer**
  - Beyond the engineer's access or rights.
  - Uses people's inherent need to help others to compromise the information system.
- **Common techniques**
  - Get help desk analysts to reset user account passwords
  - Convince the end users to reveal their passwords
  - Phishing and spear phishing
  - Abusing other user info, like last whatsapp account hijacking using voicemail

Phishing

- **The social engineer attempts to get the targeted individual to disclose personal information:**
  - Like usernames, telephone numbers, account numbers, passwords, etc.
- **Using Fake emails from corporations, banks, and customer support staff.**
  - Attempt to get users to click on malicious links
  - Allow installation of malware
  - To steal data from the computer or use the computer to attack others
- **Not targeted at specific users**
- ***Vishing:* Phising attacks over voice communications**

Spear Phishing

- **Form of phishing in which the target users are specifically identified.**
  - Accounting and human resources staff
  - Privileged staff (with admin rights)
  - ***Whaling*** is a subset of spear phising sent to high value targets such senior executives.

06/2015, Ubiquiti Networks Inc. lost $46.7 Million

> "Employee impersonation and fraudulent requests from an outside entity targeting the Company's finance department. This fraud resulted in transfers of funds held by a company subsidiary incorporated in Hong Kong to other overseas accounts held by third parties." The **transfers** were **performed directly by Ubiquiti employees** tricked into thinking that they were getting legitimate requests from executives.
>
> **Source**: U.S. Securities and Exchange Commission

Types of attacks

- **Attending the exploited security function:**
  - **Confidentiality:** Information leaks
  - **Integrity:** Intruders, worms and virii
  - **Availability:** Denial of service (distributed with botnets and using reflectors)
  - **Identity:** Impersonation, identity theft
- **Attending the source of attack:**
  - **Cybercriminals**
  - **Governmental agencies**
  - **Non profit organizations**
- **All aim at identified security threats**

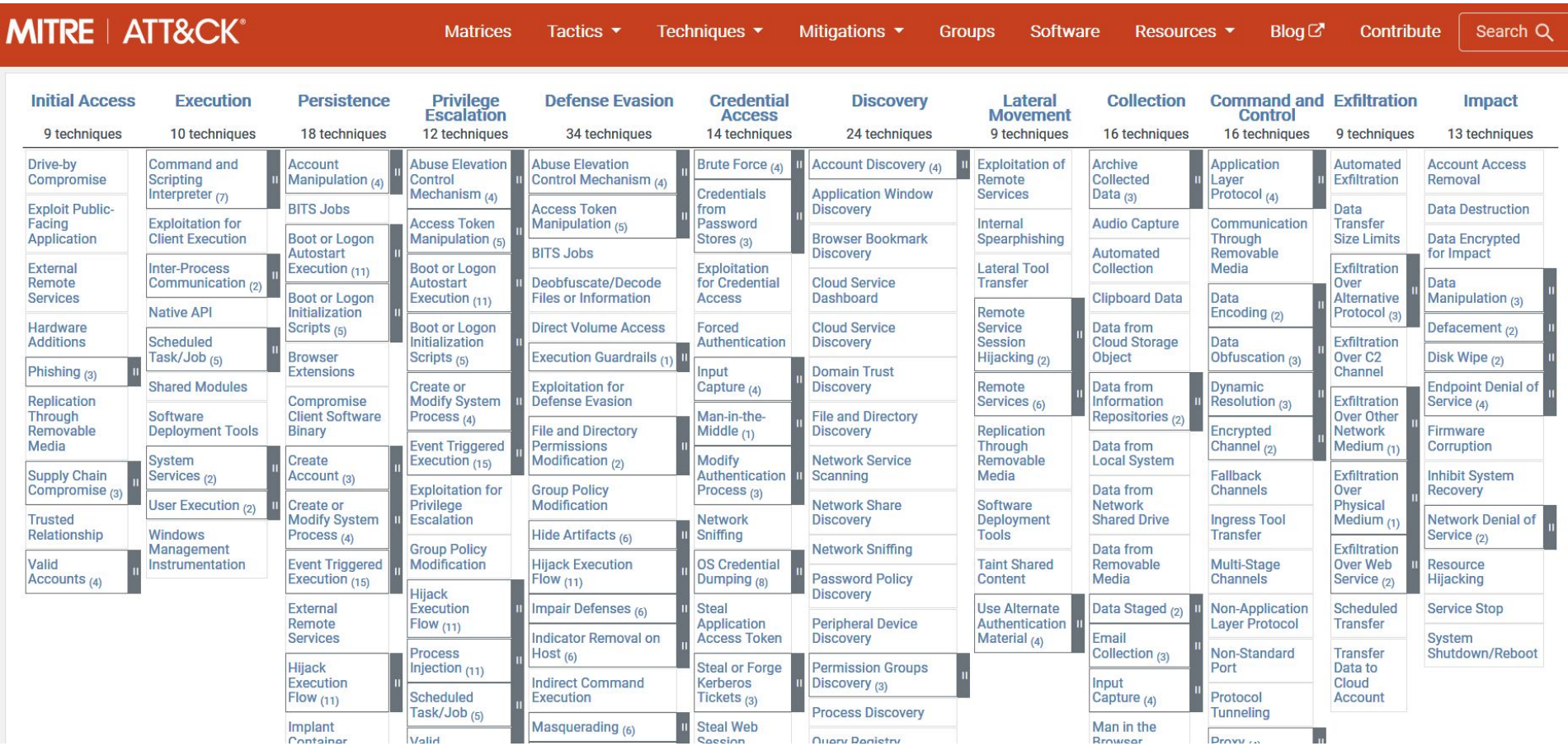
INDICATIVE SECURITY THREATS USED FOR EVALUATION OF IDS FOR VEHICLES

Attack	Descripti
Wormhole	Force a r to be the
Blackhole	Compron informin
Greyhole	Compron through i
Rushing attack	Flood a r before a
Sybil Attack	Generate on a repu
Denial of Service (incl. message flooding)	Disrupt c large volu about roa
Bus-off attack	Exploit th an uncon forcing it
Message Distortion	Generate activate c
Timing attack	An integ
Replay attack	A valid d recorded
Command Injection	Request cally to a
Impersonation (or masquerade or spoofing) attack	An adver nodes in

Packet Duplication	Transmit unnecessary network messages to exhaust bandwidth or trigger unnecessary processing
Selective Forwarding	Retransmit data selectively in a vehicular network
GPS Jamming	Jam legitimate GPS signals; possibly followed by GPS spoofing
GPS Spoofing	Transmit false GPS signals to disrupt or hijack navigation of a GPS-dependent vehicle, such as a UAV
Fuzzing (Fuzz testing)	Send random messages to the in-vehicle network to trigger critical instructions in a brute force manner)
False Data Injection	Transmit false data to trigger malicious events or affect situational/environmental awareness
False Information Dissemination	Transmit false data, e.g. a reputation score, to affect a collaborative process in a network
Location Spoofing	Share false location coordinates within a vehicular network
Malware	Infect vehicle with malicious software/firmware by compromising supply chain or hijacking an update
Resource exhaustion attack	Exhaust a vehicle's battery/fuel, network, processing or other resource by repeating requests, infecting with malware, etc.
Ranging Manipulation	Share incorrect time tags within a vehicular network to disrupt a vehicle's ranging capabilities
Sensory channel attack	Manipulate the physical environment so as to deceive a vehicle's critical sensors, such as lidar or cameras used by driverless vehicles
Adversarial machine learning attack on driverless vehicle	Maliciously craft input data to sensors specifically aiming to affect its machine learning policies
Hardware Tampering	Tamper with hardware or gain physical access to modify/damage components or infect with malware
Hardware Failure	Physical damage or natural degradation of a vehicle's components
Fraudulent ADS-B Messages	Transmit false ADS-B messages to affect aircraft safety
AIS spoofing	Transmit false AIS signals to impede vessel tracking
Isolation attack	Isolate a node from a network by dropping all messages going to or coming from it

uc3m | Universidad Carlos III de Madrid

MITRE ATT&CK



https://attack.mitre.org/

Reconnaissance

Reconnaissance

- **Input:** [Name of a company or organization]
- **Output:** [As much information as possible]
  - **Information about structure:**
    - ✓ **Organizational chart, working teams**
    - ✓ **Staff (emails, roles, contact, social profiles, habits, relations between staff…)**
  - **Information regarding related companies:**
    - ✓ **Partners, subsidiaries, competitors, customers**
  - **Technical Information about machines:**
    - ✓ **Domain and mail exchanger servers**
    - ✓ **IP ranges, netblock allocation**
    - ✓ **Architectures, OS, exposed services**

Types of reconnaissance

- **Reconnaissance information can be collected using passive or active means**
- **Since we are on the technical part, we understand "passive" means as those which do not directly address our target machines**
- **Passive means include information systems not in the target**
  - Web search sites, social networks sites, wikis and public blogs and archives of mailing lists, collaborative sites, etc.
  - There are sites who collect and process such public information and offer API or database access
    - ✓ Processing or specializing, for instance in passwords.
    - ✓ "Hackers Posted Details of 300,000 Accounts on Pastebin in the Last 12 Months"- Feb 2014
    - ✓ Cyberwar: Hacker leaks massive list of Israeli vulnerable SQLi websites on pastebin
    - ✓ https://www.databreaches.net/ http://www.databreachtoday.com/

Data and computer security

Spambot leaks more than 700m email

The LinkedIn Hack: Understanding Why It Was So Easy to Crack the Passwords

Publicado el May 21, 2016

Tyler Cohen Wood CISSP | Follow
Cyber Security Expert, Former ...

52 16 0

By Tyler Cohen Wood

LinkedIn was breached in 2012 with a reported 6.5 million user accounts compromised. LinkedIn sent a request to known hacked users advising them to change their passwords. However, on May 16, 2016, 117 million LinkedIn accounts--reportedly from the 2012 hack--were found to be up for sale on a hacker site. LinkedIn stated that after the initial 2012 breach, they added enhanced protection, most likely adding the "salt" functionality to their passwords. However, if you have not changed your password since 2012, you do not have the added protection of a salted password hash. You may be asking yourself--what on earth are hashing and salting and how does this all work?

00:21 00:27 HD

DNS enumeration

- **Background knowledge on DNS is required**
- **Questions you are supposed to answer:**
  - **How is DNS information organized?**
    - What does TLD and GTLD/ccTLD mean?
    - What are the root servers? How do they work? Who operates them?
    - What is the difference between a zone and a domain?
  - **How does the DNS protocol work**
    - Transport, port, iterative/recursive queries
    - What is the function of a resolver?
  - **What are resource records? How can you obtain**
    - An authoritative answer
    - A reverse query
    - A zone transfer

DNS hands-on exercise

- `dig, host, nslookup`
- Internet Systems Consortium tools
- Linux
  - Dig is in package dnsutils
- Windows
  - Download latest Bind distribution at http://www.isc.org/downloads/
  - Run cvredist_x86.exe
- Use dig to query nameservers

```
> dig –t SOA uc3m.es
```

DNS hands-on exercise

- d
- In
- L
- W
- U

>

C:\Windows\system32\cmd.exe

```
C:\Users\amarin>Downloads\BIND9.10.0-P2.x86\dig.exe -t SOA uc3m.es

; <<>> DiG 9.10-P2 <<>> -t SOA uc3m.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1983
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 8

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;uc3m.es.                       IN      SOA

;; ANSWER SECTION:
uc3m.es.                0       IN      SOA     vorteX.uc3m.es. netmaster.uc3m.e
s. 2014091901 86400 7200 2592000 172800

;; AUTHORITY SECTION:
uc3m.es.                82145   IN      NS      saruman.uc3m.es.
uc3m.es.                82145   IN      NS      vorteX.uc3m.es.
uc3m.es.                82145   IN      NS      sun.rediris.es.
uc3m.es.                82145   IN      NS      chico.rediris.es.

;; ADDITIONAL SECTION:
saruman.uc3m.es.        25104   IN      A       163.117.131.43
saruman.uc3m.es.        2781    IN      AAAA    2001:720:410:b131:4c1a:1bff:fe15
:23ac
vorteX.uc3m.es.         17275   IN      AAAA    2001:720:410:b131:18ea:4aff:fed4
:6975
vorteX.uc3m.es.         17275   IN      A       163.117.131.31
sun.rediris.es.         11133   IN      A       130.206.1.2
chico.rediris.es.       8921    IN      A       130.206.1.3
chico.rediris.es.       5169    IN      AAAA    2001:720:418:caf1::3

;; Query time: 22 msec
;; SERVER: 163.117.139.253#53(163.117.139.253)
;; WHEN: Fri Sep 19 14:02:09 Hora de verano romance 2014
;; MSG SIZE  rcvd: 326
```

DNS hands-on exercise

1. Find out the IP address of www.amazon.es

2. Get an authorized answer

3. Find out the name associated to the IP 193.110.128.199

4. Which are the IP addresses of the primary and secondary name servers of the domain abc.es?
what is the email address of the Administrator?
How much time can this information be stored in the cache of servers different than the zone nameservers?

5. What is the IP of the mail server of the Administrator of the previous zone, the one doing the hosting?

6. Which hosts serve www.google.com using the DNS load balancing mechanism?

7. Who is the Administrator of the found IPs?

8. Try to make a non recursive query for www.bmw.com

9. Try the same query but specifying the flag +trace.

DNS related information

- DNS SOA record identifies admin email
- But what about who pays for the domain:
  - Registrar
  - Responsible organization
  - Point of contact: phone, address, email
  - `whois` queries

REGISTRY	AREA COVERED
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	Canada, USA, and some Caribbean Islands
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

DNS attacks

- DNS hijacking
- DNS rebinding (mitigated by DNS pinning)
- DNS spoofing (aka Rogue DNS or DNS pharming)
- DNS poisoning
- Kaminsky attack:
  - Guessing (flooding src) source ports and XIDs (just 65536 values)
  - Randomising worked as a patch, though system remains vulnerable
  - PAT at routers may break randomization

http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

DNS security

- To secure DNS, DNSSec is required
  - Auditable way
  - Based in strong PKI
  - Excellent solution for Root Servers
    - ✓ At http://data.iana.org/ksk-ceremony/30/ are the official records of the complicated procedures for renewing keys and distributing SKR (Signed Key Response)
  - signed records can be verified and validated
- PKI inconvenients:
  - Cost expenses limits spread to small zones
  - PKI not flexible enough, so self signed certs are common.
    - ✓ DANE and TLSA is a potential solution
- DNS is increasingly being used for traffic analysis, anti-spamming, anti-phishing, …
  - IoT & Dynamic DNS can challenge them
    - ✓ See https://www.abuseat.org/iotcc.txt

[END OF THE CLASS]


The Simple
CRACKING
CHALLENGE

TSCC I

IHaveATrust.xlsx

TSCC II

- **Some intel…**
  - **Password size: 9 to 11 characters**
  - **Composition: [‘&’]+[word]+[number]**
  - **Word: 6 to 8 characters**
    - **Based on the target personal information:**

      https://en.wikipedia.org/wiki/<Suspect>
    - **Case:**

      Lowercase (i.e “house”)

      Uppercase (i.e “HOUSE”)

      First uppercase, rest lowercase (i.e “House”)
    - **Leetify:** i = 1; e=3; o=0
  - **Number: 2 decimal digits**

TSCC III

- **Password premises:**
  - **Short and memorable**
  - **Composition: [word][number]**
  - **Word: 6 to 8 characters**
    - **Based on the target personal information:**
      https://en.wikipedia.org/wiki/Tom_Cruise
    - **Case:**
      Lowercase (i.e “house”)
      Uppercase (i.e “HOUSE”)
      First uppercase, rest lowercase (i.e “House”)
    - **Leetify:** i = 1; e=3; o=0
  - **Number: 2 decimal digits**

Initial wordlist (~1.100 words):

Minority

Mangled wordlist (~1.300.000 words):

&Minority00

&M1NOR1TY20

&min0rity99

...

TSCC IV

- **Tools:**
  - **CeWL**
  - **Mentalist**
  - **Hashcat/John**

- **One Excel file and one name for each student in Aula Global**
- **To get the 0.5 extra points you will need to send the flag AND a short report (3-4 pages) showing the process (screenshots!!!)**