Testing for vulnerabilities

Information gathering

PURPOSE

- The process by which as much information as possible about the target is accumulated
- Every piece of information obtained can be used in the attack stage
- OSINT (Open Source Intelligence) consists of obtaining information from public sources
  - Linkedin, Facebook, Blogs, Forums, etc.
- Through OSINT you can obtain numerous entry points into the organization
  - Physical, Electronic, Human
- Accuracy may be lacking!
  - Information not up to date

PURPOSE (II)

- Usually, obtaining information can be done at several levels:
  - From the outside
    - OSINT - DNS, SMPT, Google, WhoIs, Linkedin, Facebook, Twitter, etc.
  - From the inside
    - SNMP, NetBIOS, AD, etc.
  - Social engineering

OSINT

- Active Information Gathering (IG)
  - The target organization is aware of the pentesting action
  - The attacker is active in the organization
  - Port scanning, banner grabbing, OS fingerprinting, Web scanning, etc.
  - It usually leaves visible traces for a forensic analyst
  - A lot of information is obtained
  - The pentesting process can be very fast
  - A lot of entry points are identified

OSINT

- Semi-pass
  - Doesn't attract as much attention
    - Avoid brute force approaches
  - Scan public known services
    - Preferably mimicking normal traffic
    - No visible traces are left in the logs
  - Important information can be obtained
    - … not as much information as in the case of active IG

OSINT

- Passive IG
  - You don't want the target to know about the pentesting activity
  - Traffic between the attacker and the organization is not allowed
    - The attacker relies on public information
  - Information such as:
    - Host-names, IP addresses, sub-domains, etc.
    - Contacts in your organization (emails, phone numbers)
    - Physical locations of the company
    - Partners
    - News

OSINT

- Active vs. Semi-Passive vs. Passive IG
  - Active – traffic between the attacker and the target(s)
  - Semi-passive – limited traffic, mimicking regular traffic
  - Passive – 0 traffic, using the internet
- Depending on the contract with the targeted organisation, active, semi-passive or passive IG may be allowed
- In general, it is preferred that the IG activity does not leave traces
  - A real attacker can be patient…

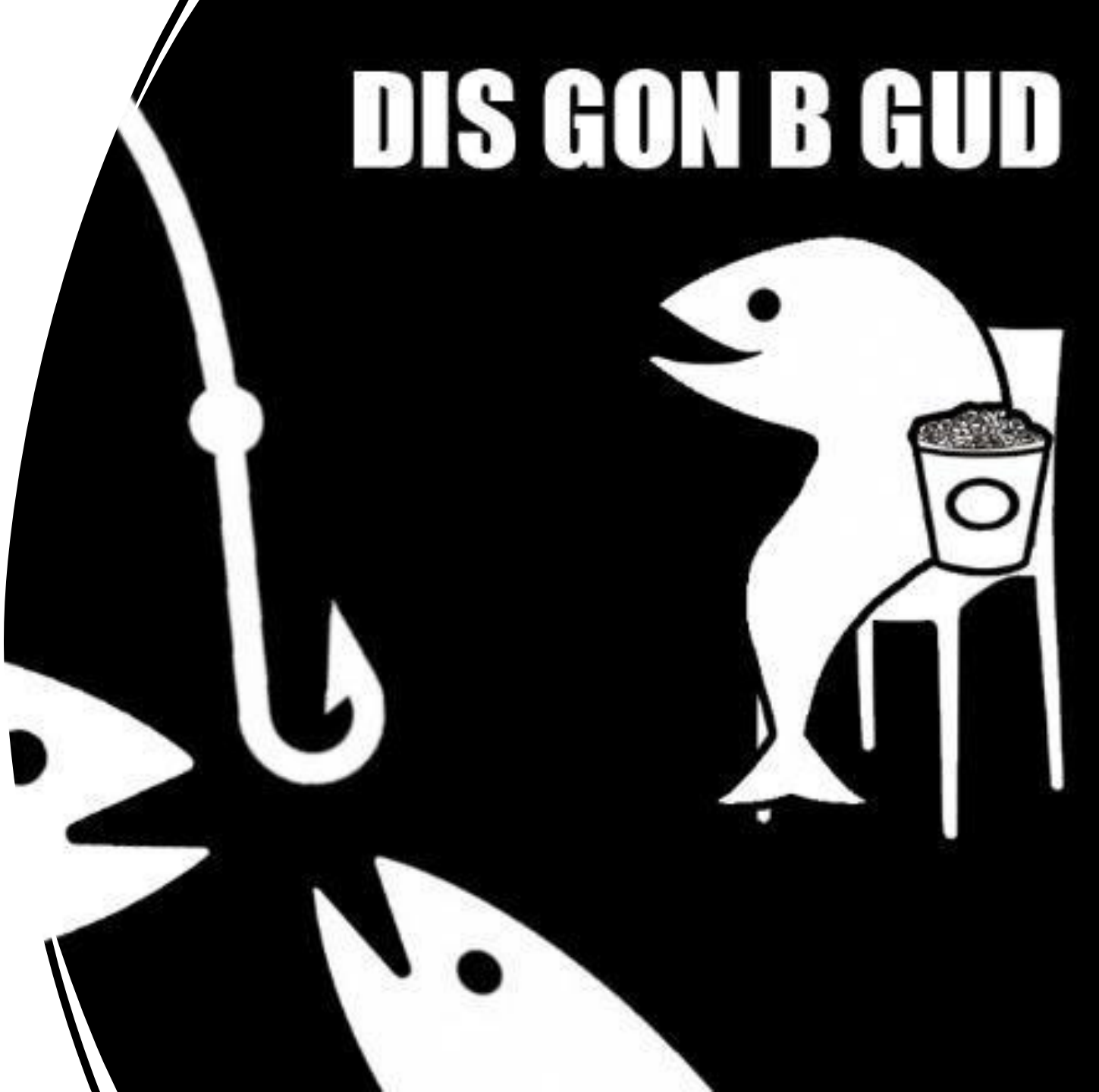
SOCIAL ENGINEERING

- „... the use of manipulation techniques to force people to divulge secret information or perform certain actions"
- Considered a passive or semi-passive technique
  - ... sometimes it's downright active!
- The greatest vulnerability is represented by the people of the organisation
- Facebook, Twitter, Linkedin, etc.
- The trust of the human victim must be earned

SOCIAL ENGINEERING

- The most common methods of social engineering are:

1. Identity theft
   - Impersonation of the victim, using accumulated information
2. Vishing
   - Voice phishing – phishing via phone
3. Baiting
   - Using a bait to compromise an individual



SOCIAL ENGINEERING

- Seemingly irrelevant information, put together, can take on a very high value
- A kind of cybernetic "dumpster diving"
- Such information can be obtained via the internet, relatively easily
- Eavesdropping
- Shoulder surfing

WHOIS

- Query & response protocol, used to obtain information about registered, assigned, or resource holders
- The protocol stores and delivers the database in human-readable format
- Utilities:
  - Online: who.is, whois.net, etc.
  - Applications: whois.exe (Sysinternals), Kali
- Very often, the first step in information gathering

WHOIS

- WhoIs Information:
  - Subdomains
  - DNS information
  - Server used
  - Domain owners (name, address, contact)
  - This information can be made private

DNS

- Domain Name System
  - Name – IP address
- Many online query tools
  - http://www.dnsstuff.com/
  - http://www.domaintools.com/
  - http://www.dnswatch.info/
  - Nslookup (Windows & Linux)
- Provides a lot of public information (but also private)

DNS

- Reverse lookup - getting host name from IP address (ping, nslookup)
- ex. ubbcluj.ro
- MX queries - example for ubbcluj.ro

```
❯ nslookup -type=mx ubbcluj.ro
Server:         fe80::1%12
Address:        fe80::1%12#53

Non-authoritative answer:
ubbcluj.ro      mail exchanger = 0 ubbcluj-ro.mail.protection.outlook.com.

Authoritative answers can be found from:
```

DNS

- NS queries – identifies all DNS servers for a domain

```
❯ nslookup -type=ns ubbcluj.ro
Server:         fe80::1%12
Address:        fe80::1%12#53

Non-authoritative answer:
ubbcluj.ro      nameserver = ns2.ubbcluj.ro.
ubbcluj.ro      nameserver = ns1.ubbcluj.ro.
ubbcluj.ro      nameserver = ns.ubbcluj.ro.

Authoritative answers can be found from:
ns.ubbcluj.ro   internet address = 193.231.20.1
ns1.ubbcluj.ro  internet address = 193.0.225.1
ns2.ubbcluj.ro  internet address = 193.231.20.2
```

DNS

- IG using DNS
  - forward lookup Brute-force
  - reverse lookup Brute-force
  - Zone transfers
- forward lookup Brute-force
  - Brute force on domain names
  - eg. mail.ubbcluj.ro, imap.ubbcluj.ro, etc.
  - Easy to automa
  - List of possible subdomains
    - mail, imap, pop, smtp, proxy, dnd, etc.

DNS

- reverse lookup Brute-force
  - Usually after forward-lookup brute-force
  - Relies on PTR (pointers) records for reverse lookup
  - Entire IP ranges can be scanned
  - Example: ubb…
- Zone transfers
  - Part of the DNS update & replication mechanism
  - Many poorly configured servers – allow replication anywhere…
  - All names and addresses in your organization are exposed

SNMP

- Simple Network Management Protocol
- Handling & monitoring of network devices
- UDP-based
- … so susceptible to IP spoofing
- Usually the weakest link in an organization
- SNMP is useful when the attacker has access to the targeted network
- It is useless from the outside of the organization

SNMP

- Windows User Enumeration
- Listing of services
- Enumerate open TCP ports
- List of installed software packages
- Kali's snmpwalk utility

SMTP

- Simple Mail Transfer Protocol
- Protocol used for… Email Transfer
- Essentially, plain text (but SSL/TLS is usually used)
- SMTP Commands:
- HELO, MAIL FROM, QUIT, VRFY
- The VRFY command can be used to verify the existence of a user
- VRFY john
- The server will respond with "User unknown" or their email address (if any)
- On most servers, the command is usually disabled

SMTP (II)

- SMTP bounce back
- Mail bouncing
- An email sent to an invalid address will cause an error
- A reply is sent to the sender to report that the message cannot be delivered
- In general, there are a lot of public email addresses
- Business addresses
- Personal addresses

OTHER RESOURCES

- Maltego
  - Utility used to gather information from public sources
  - Maltego organizes information by semantics:
    - Network infrastructure
    - NS, MX records, area transfers, SMTP checks, etc.
    - Social infrastructure
    - Email addresses, resumes, documents, etc.
- robots.txt
  - Indicates which pages you want to be hidden or shown in search results

OTHER RESOURCES

- Shodan
  - Device search engine
  - Some describe it as a banner search engine
  - Shodan collects information from:
  - HTTP, FTP, SSH, TELNET, SNMP, SIP, RTSP
- Google Hacking
  - https://www.exploit-db.com/google-hacking-database/

Conclusions

- The most important step in pentesting
- There is a lot of public information
- Both about organizations and individuals
- Some information can point directly to entry points into the organization
- Organizations and individuals need to be careful about what information they make public
- Social Engineering can be an extremely useful tool