Targeted attacks: Tools and techniques

Performing « red-team » penetration tests
Lessons learned
Objective:
- Present tools techniques that can be used to simulate a targeted attack in a professional context

Selected goal:
- Gain access to the internal network

3 suggested attack vectors:
- Malicious e-mails
- Social engineering to gather remote access credentials (VPN)
- Physical intrusion to connect an 'implant' on the internal network

Warning:
- Respect legal constraints and ethics
- Anonymize all personal information in the report
The evolution of penetration tests

- **A bit of history:**
  - 1967: *Joint Computer Conference* by the experts of the RAND Corporation and the NSA
  - 1971: *tiger teams* & James P. Anderson for the USAF
  - 1995: First commercial penetration test offers in France

- **Today:**
  - Proliferation of methodologies and certifications
  - Integration of penetration tests in the software development life cycle

- **Limits:**
  - Integrating penetration tests in the software development life cycle limits their realism and impact
  - The security of an application or a system is not the security of the entire organization
Definitions

- **Targeted attacks:**
  - Reconnaissance and planning to tailor the attacks for a specific target
  - Specific objectives: retrieve sensitive information
  - Short-term (Hunting) or long-term (Farming) operations

- **Red-Team intrusion tests:**
  - Simulate a short-term targeted attack
  - 'Light' interactions with members of the targeted organization
  - Large perimeter
  - Last longer than a conventional penetration test
Reconnaissance and planning

Objectives:
- Identify systems accessible from the Internet
- Create a simplified organizational chart
- Identify physical locations
- Gather phone numbers and e-mails addresses
- Select the best attack scenarios
- Validate attack scenarios with the customer

Criteria for a good attack scenario:
- Efficiency (optimal result for a low complexity)
- Low risk of discovery
- In case of suspicion, plausible deniability
Reconnaissance tools

- **Search engines and social networks:**
  - Google, Google Maps & Street View, but also other search engines!
  - LinkedIn, Facebook, and local similar social networks
  - Whois databases, DNS enumeration
  - Iterative and exhaustive searches

- **Other tools:**
  - *theHarvester*: Gathering e-mails, etc.
    
    ```
    $ python theHarvester.py -d domaine.com -b all
    ```
  - *Metagoofil*: Gathering Office documents meta-data
    
    ```
    $ python metagoofil.py -d synacktiv.com -t pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx -l 200 -n 50 -o tmp -f results.html
    ```
Reconnaissance++

- Compromise a vulnerable system exposed on the Internet?
  - Is it likely to be connected, directly or indirectly, to the targeted WAN?
  - May it store passwords that could be reused on the targeted network?
  - Is the DNS name of the system in a domain that can be used in a phishing campaign?
  - Do members of the targeted organization connect regularly to this system (watering hole attack)?
Protect your organization from reconnaissance operations

- **Prevent:**
  - Identify, then protect or shut down all systems accessible from the Internet
  - Awareness sessions to explain the risks related to social networks

- **Monitor:**
  - Pro-active monitoring to identify publicly accessible information on the organization
  - Eliminate the most sensitive information
Sending malicious e-mails

- **Objectives:**
  - Compromise a workstation to establish a communication channel to the internal network
  - Then perform an internal penetration test from the compromised workstation (with a first set of credentials)

- **Target key services that must open attached files:**
  - Commercial department: call for tenders
  - Marketing department: fair participation information
  - HR department: candidate applications

- **Warning: avoid compromising personal systems**
  - Verify the HTTP User-Agent and the source IP address
  - Test the Windows domain of the compromised computer

- **Warning 2: avoid escalation if detected**
  - Specific SMTP header to alert forensic investigators that this is a test
Spear phishing tools

**Implementation:**
- Command & Control server
- Executable file
- Office document containing a macro
- Link to a web server
- Buy and use a credible domain name (*mycompany-llc.com*)
- Reliable client exploit (browser, JVM, Flash, Acrobat)
- No need for 0-days!
- Bypass anti-virus software using custom codes (or obfuscate existing code)
- Find a communication channel with the Internet (HTTP CONNECT reusing the user's password on the proxy server, DNS, SMTP)
- Use developer certificates
Protect your organization against e-mails attacks

- Security awareness reaches its limits
- Importance of technical measures:
  - Top 35 Strategies to Mitigate Targeted Cyber Intrusions
  - « At least 85% of the targeted cyber intrusions that the Australian Signals Directorate (ASD) responds to could be prevented by following the Top 4 mitigation strategies »
    1) Application whitelisting
    2) Patch applications such as Java, PDF viewers, Flash, web browsers and Microsoft Office
    3) Patch operating system vulnerabilities
    4) Restrict administrative privileges
Social engineering

- **Objectives:**
  - Get a password to access the internal network from the Internet (VPN access)
  - Gather other information to ease the next steps of the intrusion

- **Selecting the targets:**
  - Department assistants (receive a lot of calls from external contacts)
  - New employees
  - *Help desk*

- **Important:**
  - Rehearse various possible conversation scripts
  - Caller ID spoofing
  - Iterate calls to various contacts, each time with more information and confidence
Protect your organization against social engineering

- In this field, security awareness is important:
  - Don't give your passwords to anyone, especially over the phone!
  - Alert and correlation procedure

- Importance of Help desk awareness:
  - Management support to refuse answering suspicious requests, even from a VIP
  - Scripts to harmonize ID checks and legitimate refusal in case of suspicion

- Deploy strong authentication technologies with a secret that cannot be communicated over the phone:
  - Biometry, smart cards, etc.
Physical intrusion

- **Objectives:**
  - Connect an 'implant' to the internal network to set up a communication channel on the Internet
  - Gather written passwords in offices

- **Two teams:**
  - Field team
  - Internet team

- **Selecting the 'field' operator:**
  - Expertise and complementarity of profile
  - Seriousness

- **Criteria for selecting the attack scenario:**
  - Company size
  - Visible physical security measures (mechanicals, electronics and humans)
  - Physical risks for the field team
  - Possibility or not to destroy some security measure in place
Some scenarios

- **Connecting the 'implant':**
  - Follow someone going in, a phone in the hand, saying: “I'm in the lobby, I'll be there in a minute”
  - Arrive early (before the IT team), with a T-shirt printed with the logo of the company doing the printers' maintenance

- **Other tools:**
  - Lock-picking kit or RFID cloning
  - Keyloggers
  - Implant to connect to the internal network
  - Attacks tools on Firewire or USB
  - USB key emulating a keyboard (Teensy)
Remark on connecting unknown USB key...

- **Webkey** a connected mail solution by La Poste:
  - Generate traffic to an Internet website using Webkey, an innovating and creative material that enhance the efficiency of marketing mail
  - Allow your client to browse safely with a USB support with a limited content and an antivirus warranty
Connecting the implant

- **Teams coordination:**
  - **LED display:**
    ```
    # echo 1 > /sys/class/leds/plug\:green\:health/brightness
    ```
  - **Sending SMS:**
    ```
    # gsmsendsms -d /dev/ttyUSB0 0612345678 "dhcp lease obtained"
    ```

- **Creating a communication channel between the implant and the Internet team:**
  - Simple case: 2G / 3G / 4G coverage
  - Otherwise automatic configuration and research to establish the communication channel with the Internet
Connecting the implant

Successive tests of various techniques:

- If necessary, circumvent MAC filtering or NAC (bridge behind a printer)
- DHCP
- Network eavesdropping and selection of available IP addresses
- Search for default gateway
- Search for an HTTPS or DNS relay server
Protect your organization against physical intrusion

- Security awareness reaches its limits
- But training the Security Department is important:
  - Detect suspicious behaviors
  - Keep an incident log book
- Physical security measures:
  - Avoid tailgating
  - Disable network plugs in public areas
- IT security measures:
  - Detect connexion of unknown devices on the internal network
  - Alert and investigate in case of suspicious behavior
  - Forbid connexion of unauthorized USB devices
Face targeted attacks

- **Awareness: success and failure**
  - Social engineering: Possible to convince people that a password shall not be given over the phone :-)
  - Physical intrusion: Difficult to ask employees to stop people without ID cards in the office :
  - Malicious e-mails: Difficult to prevent users from opening attached files or from clicking on links in “common” e-mails :

- **Importance of technical mitigation measures**

- **Testing and measuring progress:**
  - Metrics don't give the real security level
  - But help measure works that contribute (or not) to the security level

- **There are success stories in several organizations**
THANK YOU FOR YOUR ATTENTION,

DO YOU HAVE ANY QUESTIONS?

THANK YOU FOR YOUR ATTENTION,