Penetration Testing

Philipp Lachberger

29.11.2011

1. Defining our context
2. 4 Phases of Penetration Testing
    - Information Gathering
    - Links
    - Service Discovery/Mapping
        - Automatic Discovery
        - Semi-automatic Discovery
    - Exploitation
    - Documentation
    - Non-Standard Protocols
3. APT
    - Patching
4. Education?
    - Know your tools!
    - Use available possibilities
    - Talks/Workshops

- Security/Vulnerability Assessment/Audit
- Penetration Testing
- Red/Tiger Team Testing

- Information Gathering
- Service Discovery/Mapping
- Exploitation
- Documentation

Online

Using Information we can already find online ....

Information Gathering

- Google Groups
- DNS
- Whois

Expanding the search:

- Google Hacking
- Parsing publicly available metadata
- Finding Trust Relationships between companies

Portscanning

nmap and it's GUI

Demo FOCA and Maltego

Links

Available links:

- http://www.robtex.com
- https://www.hackersforcharity.org/ghdb
- http://www.paterva.com
- http://www.informatica64.com

Let Google be your friend! ;-)

Service-Discovery und -Mapping

Target:

- Identify available Services
- Find relationships between Services
- Find and document vulnerabilities

Webapplications

Multiple ways to find vulnerabilities

- automatic discovery
    - Crawler automates finding vulnerabilities
- semi-automatic discovery
    - Based on the user-input/surfing, crawling is performed
- manual discovery
    - Manually searching for problems

(Freely) available frameworks allow to automate the requests

Examples

- Nessus/OpenVAS?
- W3AF
- Commercial Tools: Acunetix/Qualys/Rapid7

Less support of the auditor - but better customization

Examples

- FIREFOX
- nikto
- Burp Suite
- OWASP WebScarab
- DirBuster

Exploitation

Last step for attackers

- Metasploit
- W3AF
- Exploit-DB
- ... depending on what you found ...

- https://cirt.net/nikto
- http://portswigger.net/burp/
- https://www.exploit-db.com
- https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project
- https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
- http://w3af.sourceforge.net/

Documentation

Being one of the main reasons for the customer

- Finding and Mapping of vulnerabilities
- Risk- and Threat-Analysis
- Recommendations for fixing vulnerabilities

Non-Standards

If you encounter no standard protocols during service discovery ... use all the information you can get!

- Wireshark
- sslcat/netcat

Combine potentially with ...

- dsniff
- Cain&Abel

- http://www.bindshell.net/tools/sslcat.html
- http://www.wireshark.org
- http://monkey.org/ dugsong/dsniff/
- http://www.oxid.it/cain.html

What if your/framework/here is recognized and killed by AV?

Well, it's gonna get dirty (somehow) ...

How can you avoid detection

- rename well known files (msf.dll) - 2005 called, they want their signatures back
- recompile your .dll/.so or your exploit
- replace you NOOPs (0x90) by something else

Other alternatives:

- Custom Malware
- Spear Phishing

The target usually is your data, and not „domain-admin“

That’s how the Buzzword APT - Advanced Persistent Threat came to existence.

Tools

imho you'll only be as good as the tools you can handle! (Though our opinions may differ, on what we call a „tool“)

- Perl/Python/Ruby/Bash/...
- Backtrack Linux
- Samurai WebTestingFramework

Use available possibilities

- Hackerspaces/Hacking-Groups/Security-Events
- Try to organise/participate at a conference
- Capture the Flag
- freely available ressources
  - Damn Vulnerable Linux
  - OWASP WebGoat
  - McAffee Foundstone Hacme *
  - different „Hackme“ sites like hellboundhackers.org

In case you've got money to spend on security workshops...

- SANS - offers a „relatively“ fair price in the „work to study“ program
- CEH - wouldn't recommend that, fairly old stuff (SQL Slammer)
- OCSP - immensely expensive, but you're getting your certificate only by participation in a 24h CTF

Cheap security conferences

- Chaos Communication Congress
- *BSides (Vienna, Berlin, ...)

Thank you!