中山大學
SUN YAT-SEN UNIVERSITY

Module II. Internet Security

Chapter 5

Network Attack and Defence

Web Security: Theory & Applications

School of Data & Computer Science, Sun Yat-sen University

Outline

- **5.1 Overview**
  - Network Security Crisis
  - Hacking & Hackers
  - Network Threats
  - Steps of Network Attack
  - Methods of Network Defense
- **5.2 Network Attack**
  - Computer Network Attack
  - Common Types of Network Attack
  - Port Scan
  - Idle Scan
- **5.3 Password Cracking**
  - The Vulnerability of Passwords
  - Password Selection Strategies
  - Password Cracking
  - Password Cracking Tools

Outline

- **5.4 Buffer Overflow**
  - Background
  - Classification
  - Practicalities
  - Protection
- **5.5 Spoofing Attack**
  - DNS Spoofing
  - Web Spoofing

5.3 Password Cracking

5.3.1 The Vulnerability of Passwords

- **The Vulnerability of Passwords**
  - A password is the secret word or phrase that is used for the authentication process in various applications. It is used to gain access to accounts and resources. A password protects our accounts or resources from unauthorized access.
  - The Vulnerability of Passwords May Be
    - ✧ Offline dictionary attack (离线字典攻击)
    - ✧ Specific account attack
    - ✧ Popular password attack
    - ✧ Password guessing against single user
    - ✧ Workstation hijacking
    - ✧ Exploiting user mistakes
    - ✧ Exploiting multiple password use
    - ✧ Electronic monitoring

5.3 Password Cracking

5.3.2 Password Selection Strategies

- **Considering**
  - User Education
  - Computer-generated Passwords
    - ✧ Quite random, but hard to remember
  - Reactive Password Checking
    - ✧ System periodically runs its own password cracker to find guessable passwords
  - Proactive Password Checking
  - Use of Hashed Password

5.3 Password Cracking

5.3.2 Password Selection Strategies

- **User Education**
  - 用户培训
    - ✧ 一般用户很难分辨口令的安全强度。
    - ✧ 指导用户认识到选择安全口令的重要性，并提供选择这类口令的指导原则。
- **Computer-generated Passwords**
  - 计算机自动生成密码口令
    - ✧ 用户口令字符串由算法生成，具有较强随机性。
    - ✧ 这类密码口令具备较强安全性，但其产生过程不支持关联记忆，用户难以记住自己的口令。
    - ✧ 对于普通用户，忘记密码带来的不便和损失可能比口令被攻破带来的损失更加严重。

5.3 Password Cracking

5.3.2 Password Selection Strategies

- **Reactive Password Checking**
  - 响应式的口令检查。
    - ✧ 由系统周期性运行自身的口令破解程序来对用户正在使用的有效口令进行检验 (猜测)，并将结果通告用户。
    - ✧ 系统自带的口令破解程序在运行时将消耗大量系统资源，而且易于猜测的口令在被检查出来之前一直存在 (活动状态)，其脆弱性给系统带来很大的安全隐患。

5.3 Password Cracking

5.3.2 Password Selection Strategies

- **Proactive Password Checking**
  - 先验口令检验
    - ✧ 先验口令检验是目前比较认可的一种提高口令安全的方法。这种方法允许用户自己选择口令，但是在用户确认口令设置时，由系统检测该口令是否是难以猜测的，如果不是，那么系统将拒绝接受该口令。
    - ✧ 先验口令检验的技巧在于寻找用户接受能力和口令安全强度之间的平衡点。如果系统拒绝太多的口令，用户会觉得选择口令太难，影响了用户体验；如果系统用来确定可接受用户口令的算法过于简单，又会提升口令被攻破的概率。
    - ✧ 简单系统可以采用一种规则强制的方法。例如口令字符串长度不得少于8个字母；在口令字符串的符号集中，必须包含大写字母、小写字母、数字和特殊字符 (如 ~!@#￥%&* 等等)。

5.3 Password Cracking

5.3.2 Password Selection Strategies

- **Proactive Password Checking**
  - 先验口令检验
    - ✧ 另一种可采纳的方法是编辑一份比较完整的“不可行”口令过滤字典。当用户选择口令时，系统检查该口令并确定它未出现在字典中。但是这种方法通常存在两个问题：
      - ◌ 空间消耗：过滤字典必须保存足够多的词汇。
      - ◌ 时间消耗：对规模庞大的过滤字典进行搜索可能需要很长的时间。此外，字典中各个词汇存在着各种变换方式。如果将这些可能的变换也加以考虑，将大量增大过滤字典的规模；如果过滤字典不考虑这些变化，则每次搜索都要增加额外的处理开销。

5.3 Password Cracking

5.3.2 Password Selection Strategies

- **Use of Hashed Password**
  - A widely used password security technique is the use of *hashed passwords* and a *salt value*.
  - The purposes salt value serves:
    - ✧ prevents duplicate passwords from being visible in the password file
    - ✧ increases the difficulty of offline dictionary attacks
  - Noting that whatever security measurement we take, once somebody got a hash, they would be able to reverse it eventually. The only thing we can do is make it as hard (and thus not efficient for adversaries) to take on your hashes.

5.3 Password Cracking

5.3.2 Password Selection Strategies

- **Use of Hashed Password**
  - To make a password longer enough, we could:
    - ✧ Make sure the user must enter a ridiculous long password with loads of special characters (between 20 and 30 chars for instance)
    - ✧ Make the passwords longer by the system.
  - Salt value
    - ✧ The first option is not really feasible. Nobody in their right mind would enter such a long password. The second one is easier to achieve with something called a "*salt*". Before we hash a password we add a "*salt*" to it:

      ```
      $saltedpassword = sha1(SALT.$password);
      ```

      If somebody happens to enter '1234' as a password, and the SALT is '*NaCl*', the hash we store is '*NaCl*1234', which is hashed with the sha1() function to 160 bits of

      '53a99f2dc3c5ce993609e6ffdc5049e61363f9c7'

5.3 Password Cracking

5.3.2 Password Selection Strategies

- **Discussion.**
  - Discuss Hashed password with salted value in more detail.

5.3 Password Cracking

5.3.3 Password Cracking

- **What is Password Cracking**
  - *Password Cracking* is the process of recovering passwords from data that have been stored in or transmitted by a computer system.
  - The purpose of password cracking might be to help a user recover a forgotten password, to gain unauthorized access to a system, or as a preventive measure by system administrators to check for easily crackable passwords.
  - Main methods of password cracking
    - ✧ using system bug
    - ✧ brute-force
      - ◌ Brute-force tries guesses repeatedly for the password and check them against an available cryptographic hash of the password.
    - ✧ precomputing potential hash values

5.3 Password Cracking

5.3.3 Password Cracking

- **口令破解的三种基本方法**
  - 利用系统漏洞直接提取口令
    - ✧ 这种方法需要获取一定的系统访问权限，或者控制系统，窃取信息。
  - 暴力破解
    - ✧ 对可能的口令空间进行穷举来破解密码。目前有些口令破解工具采用这种方法，如 cain&abel, aircrack。
  - 字典破解
    - ✧ 使用一些比较常用的口令字符串的哈希值构造口令字典。借用口令字典可以大大减少运算的次数，提高破解成功率。

5.3 Password Cracking

5.3.3 Password Cracking

- **How to create a password that is hard to crack**
  - The longer the password, the harder it is to crack
    - ✧ Password length is the most important factor. Password cracking tools can easily crack a small password by using few words combinations. A longer password will take a longer time in guessing. A password should be at least 8 characters long.
  - Always use a combination of characters, numbers and special characters
    - ✧ This will make passwords hard to crack. Password cracking tools try the combination of one by one. Having a password combination of a-z, A-Z, 0-9 and other special characters with a good length will make it harder to crack. This kind of password sometimes takes weeks to crack.

5.3 Password Cracking

5.3.3 Password Cracking

- **How to create a password that is hard to crack**
  - Variety in passwords
    - ✧ One important thing that must always be taken care is that never use same password everywhere. Cyber criminals can steal passwords from one website and then try it on other websites too.
  - In case you are not sure about the strength of your password, you can check it from variety of online tools available for free.
    - ✧ Try this official Microsoft Tool for checking the password strength: https://www.microsoft.com/zh-CN/security

5.3 Password Cracking

5.3.3 Password Cracking

- **What to avoid while selecting passwords**
  - Most of the password cracking tools start from a few things which were very common a few years back and still exist. These are the few password mistakes which should be avoided:
    - ✧ never use a dictionary word
    - ✧ avoid using your pet's name, parent name, your phone number, driver's license number or anything which is easy to guess.
    - ✧ avoid using passwords with sequence or repeated characters: For Ex: 1111111, 12345678 or qwerty, asdfgh.
    - ✧ avoid using passwords that fall in worst password list. Every year, data analysis companies publish the list of worst passwords of the year from analyzing the leaked password data.
      - ◌ The top 11 worst passwords of 2012 are: password, 123456, 12345678, abc123, qwerty, monkey, letmein, dragon, 111111, baseball, iloveyou.

5.3 Password Cracking

5.3.4 Password Cracking Tools

- **Top 10 - 2017**
  - Computer programmers have been trying to create algorithms for password cracking in less time. Most of the password cracking tools try to login with every possible combination of words. If login is successful, it means the password was found. If the password is strong enough with a combination of numbers, characters and special characters, this cracking method may take hours to weeks or months. A few password cracking tools use a dictionary that contains passwords. These tools are totally dependent on the dictionary, so success rate is lower.

5.3 Password Cracking

5.3.4 Password Cracking Tools

- **Top 10 - 2017**
  - 1. Brutus
  - 2. RainbowCrack
  - 3. Wfuzz
  - 4. Cain and Abel
  - 5. John the Ripper
  - 6. THC Hydra
  - 7. Medusa
  - 8. OphCrack
  - 9. L0phtCrack
  - 10. Aircrack-NG

5.3 Password Cracking

5.3.4 Password Cracking Tools

- **Top 10 - 2017**
  - **Brutus**
    - ✧ *Brutus* is one of the most popular remote online password cracking tools. It claims to be the fastest and most flexible password cracking tool. *Brutus* is free and is only available for Windows systems. It was released back in October 2000.
    - ✧ It supports HTTP (Basic Authentication), HTTP (HTML Form/CGI), POP3, FTP, SMB, Telnet and other types such as IMAP, NNTP, NetBus, etc. Users can also create their own authentication types. This tool also supports multi-stage authentication engines and is able to connect 60 simultaneous targets. It also has resume and load options, thus users can pause the attack process any time and then resume whenever they want to resume.

5.3 Password Cracking

5.3.4 Password Cracking Tools

- **Top 10 - 2017**
  - **RainbowCrack**
    - ✧ *RainbowCrack,* available for free, is a hash cracker tool for both Windows and Linux. It uses a large-scale *time-memory trade off* process (时空权衡算法) for faster password cracking than traditional brute force tools. Time-memory trade off is a computational process in which all plain text and hash pairs are calculated by using a selected hash algorithm. After computation, results are stored in the rainbow table. This process is very time consuming. But, once the table is ready, it can crack a password must faster than brute force tools.
    - ✧ Developers of *RainbowCrack* have also generated LM rainbow tables, NTLM rainbow tables, MD5 rainbow tables and Sha1 rainbow tables. These tables are also available for free. Users can download these tables and use for password cracking processes.

5.3 Password Cracking

5.3.4 Password Cracking Tools

- **Top 10 - 2017**
  - **RainbowCrack**
    - Time-memory trade off process
      - In 1980 Martin Hellman described a cryptanalytic time-memory trade-off which reduces the time of cryptanalysis by using precalculated data stored in memory. This technique was improved by Rivest before 1982 with the introduction of distinguished points which drastically reduces the number of memory lookups during cryptanalysis.

5.3 Password Cracking

5.3.4 Password Cracking Tools

- **Top 10 - 2017**
  - **Wfuzz**
    - ✧ *Wfuzz* tries to crack passwords with brute forcing. It can also be used to find hidden resources like directories, servlets and scripts. This tool can also identify different kind of injections including SQL Injection, XSS Injection, LDAP Injection, etc. in Web applications.
      - ○ Capability of injection via multiple points with multiple dictionary
      - ○ Output in colored HTML
      - ○ Post, headers and authentication data brute forcing
      - ○ Proxy and SOCK Support, Multiple Proxy Support
      - ○ Multi Threading
      - ○ Brute force HTTP Password
      - ○ POST and GET Brute forcing
      - ○ Time delay between requests
      - ○ Cookies fuzzing

5.3 Password Cracking

5.3.4 Password Cracking Tools

- **Top 10 - 2017**
  - **Cain and Abel**
    - ✧ *Cain and Abel* is a well-known password cracking tool that is capable of handling a variety of tasks. The most notable thing is that the tool is only available for Windows platforms. It can work as sniffer in the network, cracking encrypted passwords using the dictionary attack, recording VoIP conversations, brute force attacks, cryptanalysis attacks, revealing password boxes, uncovering cached passwords, decoding scrambled passwords (混编口令), and analyzing routing protocols.
    - ✧ Cain and Abel does not exploit any vulnerability or bugs. It only covers security weakness of protocols to grab the password. This tool was developed for network administrators, security professionals, forensics staff (取证人员), and penetration testers.

5.3 Password Cracking

5.3.4 Password Cracking Tools

- **Top 10 - 2017**
  - **John the Ripper**
    - ✧ *John the Ripper* is another well-known free open source password cracking tool for Linux, Unix and Mac OS X. A Windows version is also available. This tool can detect weak passwords. A pro version of the tool is also available, which offers better features and native packages for target operating systems. Openwall GNU/*/Linux also comes with John the Ripper.

5.3 Password Cracking

5.3.4 Password Cracking Tools

- **Top 10 - 2017**
  - **THC Hydra**
    - ✧ *THC Hydra* is a fast network logon password cracking tool. New modules are easy to install in the tool. Users can easily add modules and enhance the features. It is available for Windows, Linux, Free BSD, Solaris and OS X. This tool supports various network protocols. Currently it supports Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP, SOCKS5, SSH (v1 and v2), Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.

5.3 Password Cracking

5.3.4 Password Cracking Tools

- **Top 10 - 2017**
  - **Medusa**
    - ✧ *Medusa* also claims to be a speedy parallel, modular and login brute forcing tool. It supports HTTP, FTP, CVS, AFP, IMAP, MS SQL, MYSQL, NCP, NNTP, POP3, PostgreSQL, pcAnywhere, rlogin, SMB, rsh, SMTP, SNMP, SSH, SVN, VNC, VmAuthd and Telnet. While cracking the password, host, username and password can be flexible input while performing the attack.
    - ✧ Medusa is a command line tool. Efficiency of the tool depends on network connectivity. On a local system, it can test 2000 passwords per minute.
    - ✧ With Medusa, users can also perform a parallel attack like cracking passwords of a few email accounts simultaneously. You can specify the username list along with the password list.

5.3 Password Cracking

5.3.4 Password Cracking Tools

- **Top 10 - 2017**
  - **OphCrack**
    - ✧ *OphCrack* is a free rainbow-table based password cracking tool for Windows. It is the most popular Windows password cracking tool, but can also be used on Linux and Mac systems. It cracks LM and NTLM hashes. For cracking Windows XP, Vista and Windows 7, free rainbow-tables are also available.
    - ✧ A live CD of OphCrack is also available to simplify the cracking. One can use the Live CD of OphCrack to crack Windows-based passwords. This tool is available for free.

5.3 Password Cracking

5.3.4 Password Cracking Tools

- **Top 10 - 2017**
  - **L0phtCrack**
    - ✧ *L0phtCrack* is an alternative to OphCrack. It attempts to crack Windows password from hashes. For cracking passwords, it uses Windows workstations, network servers, primary domain controllers, and Active Directory. It also uses dictionary and brute force attacking for generating and guessing passwords. It was acquired by Symantec and discontinued in 2006. Later L0pht developers again re-acquired it and launched L0phtCrack in 2009.
    - ✧ It also comes with a schedule routine audit feature. One can set daily, weekly or monthly audits, and it will start scanning on the scheduled time.

5.3 Password Cracking

5.3.4 Password Cracking Tools

- **Top 10 - 2017**
  - **Aircrack-NG**
    - ✧ *Aircrack-NG* is a WiFi password cracking tool that can crack WEP or WPA passwords. It analyzes wireless encrypted packets and then tries to crack passwords via its cracking algorithm. It uses the FMS attack along with other useful attack techniques for cracking password. It is available for Linux and Windows systems.
    - ✧ A live CD of Aircrack is also available.

End of Chapter 5.3