AC 2009-1697: EXPERIMENTS WITH COMPUTER PASSWORD CRACKING AND SHIELDING TECHNIQUES

Veeramuthu Rajaravivarma, State University of New York, Farmingdale

V. Rajaravivarma is currently with the Electrical and Computer Engineering Technology at SUNY, Farmingdale State College. Previously, he was with Tennessee State University,Morehead State University, North Carolina A&T State University, and Central Connecticut State University. Dr. Rajaravivarma teaches electronics, communication, and computer networks courses to engineering technology students. His research interest areas are in the applications of computer networking and digital signal processing.

Cajetan Akujuobi, Prairie View A&M University

Dr. Akujuobi is a Professor of Electrical Engineering and the founding Director of the DSP Solutions, Mixed Signal Systems and Broadband Access Technologies Programs and Laboratories at Prairie View A&M University. He is also the founding Director of the Center of Excellence for Communication Systems Technology Research (CECSTR). His research interests include High-Speed (Broadband) Communication Systems, Mixed Signal Systems and DSP Solutions. He is also the Department Head for Engineering Technology at Prairie View A&M University.

Experiments with Computer Password Cracking and Shielding Techniques

Abstract

Internet is dominating almost every aspect of our life. Internet applications are too many in today's business world. It is hard to imagine any office or home without a computer network. All kinds of money transactions are possible today because of the fast changes in computer technology. As a result, everyone with an online account can buy or sell anything over the Internet in a secured environment. Therefore, it is important to secure the computer with the easy username and an unbreakable password. This topic can be integrated into anyone of the Computer Networks or Network Security courses for undergraduate students majoring in Computer Engineering Technology. This paper explains the importance of secured password and examines the kinds of passwords that are breakable. The password cracking uses simple open source software tools available in the Internet. In addition, this paper also discusses different types of password related attacks and password shielding techniques. Summary of the experimental results are also provided for different passwords with various lengths, characters, and complexity.

1. Introduction

Internet has allowed remote access to any organization in the world anytime of the day or night. This generated lot of attention around the world and easy way of entering into anyone's network was made possible. At the same time easy access to open source software codes allowed the computer hackers to grow in numbers and get smarter. Password security has become more important part of today's computer network. Although the security of a password encryption algorithm is an intellectual and mathematical problem, it is only one tiny facet of a very large problem [1]. It has become a common practice in every organization that computer system administrators are constantly looking for new ways to protect and better the password. There are several ways of building a secured system and also keep up with the hardware speeds and software updates [2]. In general passwords have always been the primary security to authenticate entry and to keep away unwanted people from gaining access to the network.

Password guessing attacks can be categorized by the amount of interaction they require with an authentication system [2]. In *on-line* attacks, the perpetrator must make use of an authentication system to check each guess of a password. In *off-line* attacks, an attacker obtains information--such as a password hash--that allows him to check password guesses on his own, with no further access to the system. On-line attacks are generally considerably slower than off-line ones. Systems can detect on-line attacks fairly easily and defend against them by slowing the rate of password checking and limiting the number of tries to crack the password. In contrast, once an attacker has obtained password verification information, the only protection a system has from off-line attacks is the computational cost of checking potential passwords.

2. Password Cracking

There are many kinds of passwords in the computer world [3]. The most commonly used and attacked are passwords used to logon to a machine or domain. In a domain environment all of the usernames and passwords are kept on a domains controller. This allows administrators to secure physical access to the machine. However when a machine joins a domain it still must have a local administrator account. This can allow hackers a staging point to attack other network devices. Password cracking in a workgroup or stand alone machine is easy as long as one has physical access to the machine. For remote users, as long as one can hack into the router, it is also easy to sniff passwords. In this case the remote connection software becomes the primary way of grabbing username and passwords sent over public network. Domain Password Cracking is much harder and needs physical access to one machine and the local administrator account.

There are numerous password crackers available openly in the Internet. Based on the release of the 2006 survey [4], the top 10 password crackers are Cain and Abel, John the Ripper, THC Hydra, Aircrack, L0phtcrack (LC4), Airsnort, SolarWinds, Pwdump, Rainbow Crack, and Brutus.

- Cain and Abel - This Windows-only password recovery tool handles an enormous variety of tasks. It can recover passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols.
- John the Ripper - A powerful, flexible, and fast multi-platform password hash cracker
- THC Hydra - Fast network authentication cracker which support many different services
- Aircrack –The fastest available wireless cracking tool
- L0phtcrack - Windows password auditing and recovery application (LC 4 and LC5).
- Airsnort – Wireless LAN tool that recovers encryption keys
- SolarWinds - Network discovery/monitoring/attack tools for system administrators
- Pwdump - Widows password recovery tool capable of displaying password histories
- Rainbow Crack - Innovative password hash cracker tool that makes use of a large-scale time-memory trade-off
- Brutus - Windows-only cracker uses network brute-force authentication

Based on the experiment done using the available OPH Crack tool for Windows based system [5], it was shown to crack alphanumerical passwords in seconds.

Password Cracking Experiments

In our case, the main objective of the classroom experiments is to see what kinds of passwords are breakable. In addition our students also learn to use the existing software tools and more importantly to use it for a productive purpose. Our students also learn to manage the domain as a system administrator. To add the pedagogic value of peer-learning, students are encouraged to do the hands-on experiments in teams where one student comes with the password and other tries to break it

These experiments can be conducted in any networking laboratory set up with available free open source software tools. It is strongly recommended to consult with the school system administrator before conducting this experiment to know more about security threats. Make sure to enforce the rule to turn off the Internet connection while conducting the experiment. Students should have exposure to basic networking and fundamentals of computer security before doing these experiments.

In our class, the experiments were conducted in a Windows environment laboratory without Internet connection. We chose two popular open source password cracking software tools L0phtcrack (LC4) [6] and SAM Inside [7] for our experiments. As noted above, LC4 is a password auditing and recovery application tool. It provides two critical capabilities to Windows network administrators, (1) to secure Windows-authenticated networks through comprehensive auditing of Windows NT and Windows 2000 user account passwords (2) to recover Windows user account passwords to streamline migration of users to another authentication system or to access accounts whose passwords are lost. SAM Inside is another password recovery program used in the experiment which can crack passwords much faster than LC4 and the core part of the program is written in assembly language. This program also supports Mask attack, Dictionary attack, Hybrid attack, and Attack with Rainbow tables.

All the experiments were conducted in Windows environment computers and students were able to login as administrators. The demo versions of both software tools have limited access with few testing features. For instance, LC4 demo version can not perform Brute Force attack where as this is possible with SAMInside demo version. Following steps were performed during the experiments:

- Download software tools demo versions LC4 [5] and SAMInside [6]
- Create several accounts with passwords. Select Start → Control Panels → Account Users → Add new user and set password. Create four accounts with usernames Arthur, Boxworthy, Carmella, and Dixon
    - 4 local users
        - Username – Arthur; Password – up77
        - Username – Boxworthy; Password – b0xw0rthy
        - Username – Camela; Password – Arthur
        - Username – Dixon; Password – Dixon51
- Install LC4. Run LC4 and choose retrieve from local machine, select strong password audit, and select all reporting styles

After selecting the default settings, passwords like “77up” with one to three leading digits. First attempt to crack password “77up” took 17 hours, 25 minutes and 45 seconds. For this run, the default settings are two appended digits at the end and added an additional two digits to the front. By turning off the last two digits and running the test again and cracked the password “up77” in 5 minutes and 51 seconds. Then turned on a feature to substitute letter for symbol like e=3, a=@, s=5, 1=! etc, it took 1 hour, 50 minutes, and 32 seconds to crack the password “p@55w0rd”.

- Install SAMInside. Run SAMInside. Click on the “people” icon to import the local users on the machine. Click on the “run attack” to start the password scan.
  SAMInside demo version can perform two to eight alpha characters only with a maximum of 50 minutes runtime. The following are the results from SAMInside’s Brute Force attack:
  - aa 0 second
  - B3d 1 second
  - lfhh 1 second
  - gurtk 2 seconds
  - dacwed 18 seconds
  - huhaccs 36 minutes
  - luftyput – ran past the 50 minutes limit

Results and Student Feedback

Students found that not all words of the same type are going to be found at the same time. In User Info attack, all words will be broken almost instantaneously. With Dictionary attack, some words will be found faster than others due to the order in which words are placed in the dictionary file. With a hybrid or brute attack words of the same type and length may also take different quantities of time for the same reason. For instance first run to find “77up” in LC4 test attack took over 17 hours and was more than 95% scan process was complete before finding the password. At the same time “P@55w0rd” search took almost two hours and finished only 20% scan process. Overall students found the times for the longer experiments hardly have enough data to show how long a typical word of that length and type would take to crack.

When using LC4’s dictionary attack, it did not find even simple two letter words. This could have been due to the limited use of very small dictionary and no Brute Force attack with the LC4 demo version. On the other hand two letter words were found very easily by the SAMInside Brute Force attack. In general students were able to break almost all the chosen passwords.

Student also learned the best practices for making a password. They are as follows:

- for Windows use 7 to 14 character
- don’t use small words even if they are separated by numbers or symbols
- select the letters in unpronounceable combinations
- include three or more numbers, not attaching all at the beginning or end

In conclusion, students were able to perform experiments with various password lengths, characters and complexity. They were able to conduct different types of attacks used in the experiments and were able to understand how and why they work.

Various methods were used to formally assess the effectiveness of this project including the instructor's assessment of laboratory work and classroom presentation. Based on the student's feedback, the overall response from students regarding whether the class project met their expectations was very positive and the project integrated into the course was positive.

3. Passwords Shielding Techniques

The above experiments enabled students to understand that password cracking can be easily done if the system is not properly protected. Passwords can be cracked the easiest if the machine is not part of a domain and if there is physical access to the machine. By installing high quality security software on computer systems hackers may not be able to install the software they require to hack a password. Disabling access to drives to boot from other than ones needed may stop a hacker from cracking a password. Installing a hardware device can also help by not allowing machines to access the network that do not meet the company's security policies. Also having a unified threat management system at the gateway can help to keep outsiders that don't belong outside. Also informing and educating the employees on how to protect them and how important it is to keep passwords safe can help. Using a VPN solution can help remote users to stay secure.

Many programs can be used to gain the local administrator password of the machine with only physical access to it. To prevent a potential hacker from getting this password, a network administrator can do a few things. First disable booting from the CD and floppy drives as well as USB and network ports. Secure the bios with a strong password and use a zip-tie or lock to secure the machine closed. This will prevent potential hackers from gaining local administrative rights.

To help safe guard domain accounts and administrator can place good password policy. Using group polices manager for active directory an administrator can place polices for passwords. Polices can include password length, complexity and length of time it's good for. Doing this allows the user to still pick their own password and adhering corporate polices.

One of the hardest tasks for administrators is securing remote access. Remote Desktop protocol is commonly used to remotely access the corporate network. The flaw with this is that it sends all data as plain text including passwords. To stop this system administrator can use a VPN solution. An administrator can use an IPsec or SSL client to have the remote user VPN in before using remote desktop. The IPsec Client is great for logging into a machine using remote desktop. The SSL is better suited for remote desktop web connection and web logins. Most companies have an appliance that can handle VPNs and would require very little cost to make them operational.

The password is only protected if the network is protected. Using a good security software can help to protect passwords by detecting malicious software and removing it as well as stopping suspicious network activity. Using a network access server can prevent unwanted guests from gaining access to the network. Using a network access server should be used for both wired and wireless access. A secure gateway security appliance can help to block ports and activity coming in that may harm the network. Using a smart card or biometric scanner as a second form of authentication can greatly improve security.

4. Conclusion

There are many ways for someone to get a password they shouldn't have. By following several basic steps and guidelines you can create a well designed password security police that can help to safeguard your data. This policy along with proper education to the user can help safeguard passwords therefore protecting data. In conclusion, this experiment forced students to learn the following password shielding techniques

- Encrypt the password files – Windows does this automatically
- 3rd party software tools to protect passwords
- Disable booting to Disk drives other than hard drive and removable devices
- Use SSL or IPsec VPN software to stop passwords from being sniffed
- Use hard password polices and change often
- Proper setting permissions of each user
- Strong perimeter security and Training
- Add smart card or biometrics as a second form of authentication

5. Bibiliography

[1] R. Morris and K. Thompson, "Password Security: A Case History", Communications of the ACM, Volume 22, Number 11, November 1979, pp. 594-597

[2] N. Provos and D. Mazières, "A Future-Adaptable Password Scheme - The OpenBSD Project", Proceeding of the 1999 USENIX Annual Technical Conference, June 6-11, 1999, Monterey, CA

[3] I. Dubrawsky, M. Cross, J. Faircloth , "Security+ Study Guide", Elsevier Science & Technology Books , 2007

[4] "Top 10 Password Crackers" Released by insecure.org, Retrieved on January 30, 2009

[5] "Ophcrack - Windows password cracker", ophcrack.sourceforge.net

[6] "L0phtCrack (LC4) Tools", http://www.net-security.org/software.php?id=17

[7] CNET.com free download from http://www.download.com/SAMInside/3000-2092_4-10484381.html