Uncover Cache Password Recovery by using Software Tools

Shailendra Nigam
Computer Science & Engineering Department
DIET, Kharar Mohali(Punjab) India.

Jyotinder Kaur
Computer Science & Engineering Department
BBSBEC, Fatehgarh sahib(Punjab) India

Abstract: Uncover Cache Password Recovery concept is based on Phishing technique. This paper is based on our thoughts & literature survey. Phishing is the act of attempting to acquire information such as user names, passwords, & credit card details. It is basically carried out by email spoofing or instant messaging. In this we discuss the problem of Uncovering Cache Password Recovery by Using Software Tools. In this, we present the optimization and analysis objective, the problem constraints, variables and network model involved.

Keyword: - Phishing Attacks, Security, User Protection, Password recovery.

I. INTRODUCTION

It is well known that all passwords are stored in encoded form. Cache passwords of any application or program can be uncovered; the hidden passwords can be extracted and displayed by using software tool. By using this recovery tool user can easily open the operating system and recover the characters of hidden passwords. This tool can used to provide forensics**,** criminal investigators, security officers and government authorities with the ability to retrieve a variety of passwords stored on a PC**.** This effective tool is developed with powerful engineering concepts and algorithms that enable it to accurately recover the password of FTP. Every bit of information is encrypted with the URL of a Web site, making it impossible to access the stored information without knowing the exact Web address of a resource. Software tool makes it possible to work around this new security model by analyzing cached URL history and identifying Web sites last visited in order to retrieve any login and password information stored for those Web sites. Everybody knows that all passwords are stored in encoded form. Uncover cache passwords of any application or program it extracts the hidden passwords and display them by using software tool. This effective tool is developed with powerful engineering concepts and algorithms that make it enable to accurately recover the password of FTP. This recovery tool user easily open the operating system and it recover the characters of hidden passwords. Every bit of information is encrypted with the URL of a Web site, making it impossible to access stored information without knowing the exact Web address of a resource. Software tool makes it possible to work around this new security model by analyzing cached URL history and identifying Web sites last visited in order to retrieve any login and password information stored for those Web sites. This tool to provide forensics, criminal investigators, security officers and government authorities with the ability to retrieve a variety of passwords stored on a PC. This topic is based on Phishing technique. Phishing is a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion The word “phishing" appeared around 1995, when Internet scammers were using email lures to “fish" for passwords and financial information from the sea of Internet users; “ph" is a common hacker replacement of \f", which comes from the original form of hacking, “phreaking" on telephone switches during 1960s. Early phisher copied the code from the AOL website and crafted pages that looked like they were a part of AOL, and sent spoofed emails or instant messages with a link to this fake web page, asking potential victims to reveal their passwords.A complete phishing attack involves three roles of phishers. Firstly, mailers send out a large number of fraudulent emails (usually through botnets), which direct users to fraudulent websites. Secondly, collectors set up fraudulent websites (usually hosted on compromised machines), which actively prompt users to provide confidential information. Finally, cashers use the confidential information to achieve a payout. Monetary exchanges often occur between those phishers.

1.2 Types of Phishing

Phishing has spread beyond email to include VOIP, SMS, instant messaging, social networking sites, and even multiplayer games. Below are some major categories of phishing.

Clone Phishing In this type phisher creates a cloned email. He does this by getting information such as content and recipient addresses from a legitimate email, which was delivered previously, and then he sends the same email with links replaced by malicious ones. He also employs address spoofing so that the email appears to be from the original sender. The email can claim to be a re-send of the original or an updated version as a trapping strategy.

Spear Phishing Spear phishing targets at a specific group. So instead of casting out thousands of emails randomly, spear phishers target selected groups of people with something in common, for example people from the same organization. Spear phishing is also being used against high-level targets, in a type of attack called \whaling". For example, in 2008, several CEOs in the U.S. were sent a fake subpoena along with an attachment that would install malware when viewed. Victims of spear phishing attacks in late 2010 and early 2011 include the Australian Prime Minister's office, the Canadian government, the Epsilon mailing list service, HBGary Federal, and Oak Ridge National Laboratory.

Phone Phishing This type of phishing refers to messages that claim to be from a bank asking users to dial a phone number regarding problems with their bank accounts. Traditional phone equipment has dedicated lines, so Voice over IP, being easy to manipulate, becomes a good choice for the phisher. Once the phone number, owned by the phisher and provided by a VoIP service, is dialed, voice prompts tell the caller to enter her account numbers and PIN. Caller ID spoofing, which is not prohibited by law, can be used along with this so that the call appears to be from a trusted source.

1.3 Phishing Techniques and Countermeasures

Various techniques are developed to conduct phishing attacks and make them less suspicious. Email spoofing is used to make fraudulent emails appear to be from legitimate senders, so that recipients are more likely to believe in the message and take actions according to its instructions. Web spoofing makes forged websites look similar to legitimate ones, so that users would enter confidential information into it. Pharming attracts traffic to those forged websites. Malware are installed into victims' computers to collect information directly or aid other techniques. PDF documents, which supports scripting and fillable forms, are also used for phishing.

- Email Spoofing
- Web Spoofing
- Pharming
- Malware
- Phishing through PDF Documents

1.4 Phishing Attack Stages

Phishing attacks involve several stages:

- The attacker obtains E-mail addresses for the intended victims. These could be guessed or obtained from a variety of sources.
- The attacker generates an E-mail that appears legitimate and requests the recipient to perform some action.
- The attacker sends the E-mail to the intended victims in a way that appears legitimate and obscures the true source.
- Depending on the content of the E-mail, the recipient opens a malicious attachment, completes a form, or visits a web site.
- The attacker harvests the victim’s sensitive information and may exploit it in the future.

II. SYSTEM DESIGN

Existing System

A spoofed email is one that claims to be originating from one source when it was actually sent from another. Email spooling is a common phishing technique in which a phisher sends spoofed emails, with the sender address and other parts of the email header altered, in order to deceive recipients. Spoofed emails usually appear to be from a website or financial institution that the recipient may have business with, so that an unsuspecting recipient would probably take actions as instructed by the email contents, such as: reply the email with their credit card number, click on the link labeled as \view my statement", and enter the password when the (forged) website prompts for it and open an attached PDF form, and enter confidential information into the form. Sending fake Mail concept it is also part of phishing technique

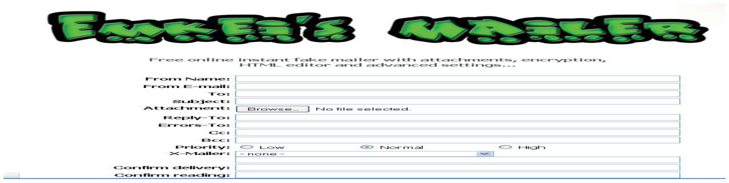


Figure 1 Fake Mailer format

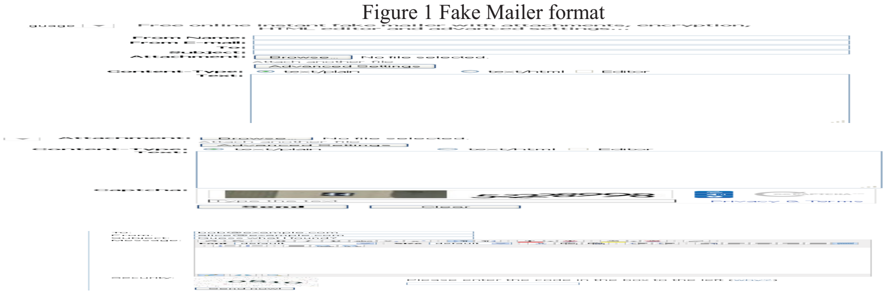
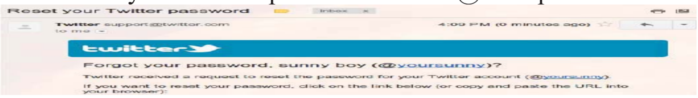


Figure 2 How to send fake mail

A. Sending a spoofed email

On a send mail-enabled UNIX system, one line of command is all you need to send a spoofed email that appears to be from Twitter:

```
Cat body. Html mail -a `From: Twitter <support@twi t t e r . com>' -a `
Content-Type : t ext /html ' -s ` Reset your Twitter password ' victim@example . net
```



Reset your Twitter password Inbox x

Twitter support@twitter.com 4:09 PM (0 minutes ago)
to me

Forgot your password, sunny boy (@yoursunny)?

Twitter received a request to reset the password for your Twitter account (@yoursunny).

If you want to reset your password, click on the link below (or copy and paste the URL into your browser):

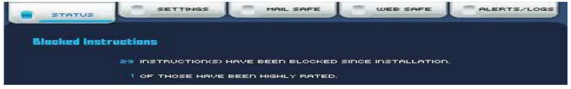
Figure 3 spoofed email appears to be from twitter

a)

III. EXPERIMENTAL STUDY

Phishing is the internet's today's demon, as it aims to trick the user to enter his personal information such as credit card, bank account or social security numbers. The personal info entered by the deceived user is then received by a remote server that forwards the information to the fraudsters, who can use the stolen information in many ways; your credit card can be used for unauthorized purchase, and even worse, your account may be cleared out. Phishing Zapper monitors the incoming emails and web pages that might be phishing. Phishing Zapper also gives you the ability to choose which security level you want to set for your system. Phishing Zapper's database is updated regularly to be as close as possible to real time.The program runs in the system tray with user easy access.

Blocked Instructions: shows you the number of instructions (either mail or websites) that you have chosen to block so far. Also displays you the number of instructions that were marked highly rated.



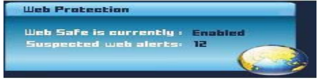
Blocked Instructions

23 INSTRUCTION(S) HAVE BEEN BLOCKED SINCE INSTALLATION.

1 OF THOSE HAVE BEEN HIGHLY RATED.

Figure 4 Blocked instructions Phishing Zapper's

Web Safe: shows you whether you are currently enabling the web protection, or you are disabling it, and also displays you the number of phishing-web alerts shown to you so far

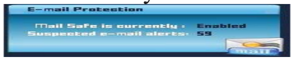


Web Protection

Web Safe is currently : Enabled
Suspected web alerts: 12

Figure 5 Web Protection Phishing Zapper's

Mail Safe: shows you whether you are currently enabling the mail protection, or you are disabling it, and also displays you the number of phishing-mail alerts shown to you so far

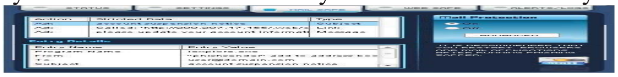


E-mail Protection

Mail Safe is currently : Enabled
Suspected e-mail alerts: 59

Figure 6 E-mail Protection Phishing Zapper's

The **Mail Safe** Panel provides you with all the information you need to know about your PC Mail Protection.



Action	Stricted Data	Type
Ask	account suspension notice	Subject
Ask	Called: 'http://200.207.17.155/.web/c	Link
Ask	please update your account informati	Message

Entry Details

Entry Name	Entry Value
Program Name	iexplore.exe
From	"phishsender" add to address boo
To	user@domain.com
Subject	account suspension notice

Mail Protection

● On
○ Off

ADVANCED

IT IS RECOMMENDED THAT YOU RESTART BROWSERS AND MAIL APPLICATIONS AFTER RUNNING PHISHING ZAPPER.

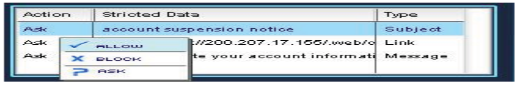
Figure 7 E-mail Protection on and show the entry details Phishing Zapper's

Mail Safe Level: you can choose to set your mail protection level to:

On: this level in turn is divided into 3 sub-levels
- Always Allow Receive.
- Always Deny Receive.
-Apply Custom Action meaning that the action that will be taken, when receiving a phishing mail, will be the one chosen by you. If you haven't set any specific action, then the default action taken will be the **Ask** action
Off: meaning that you can access all your mails normally, and if one of them is a phishing mail, no action will be taken at all by ***Phishing Zapper***

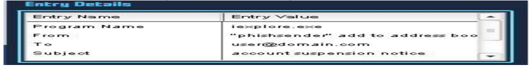
Figure 8 Change the Setting Phishing Zapper's tool

Phishing Mails List: displays you all the phishing mails' instructions caught so far, and their related details.
- Stricted Data: the suspected phishing instruction caught in your mail.
- Type: the suspected phishing instruction type.
- Action: the action applied to this phishing instruction. You can change this action by left clicking the **Action** column, and then selecting the proper action you want to apply for this phishing instruction, either to allow it to automatically block it or to show you an alert asking you what to do with it.



Action	Stricted Data	Type
Ask	account suspension notice	Subject
Ask	t//200.207.17.155/.web/c	Link
Ask	te your account informati	Message

Figure 9 Phishing Mails List



Entry Details

Entry Name	Entry Value
Program Name	iexplore.exe
From	"phishsender" add to address boo
To	user@domain.com
Subject	account suspension notice

Figure 10 Phishing Mails Entry Details

Another tool is Wireshark. Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. A packet sniffer (also known as a network analyzer or protocol analyzer) is computer software that can intercept and log data traffic passing over a data network. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC or other specifications. Wireshark is programmed to recognize the structure of different network protocols. This enables it to display the encapsulation and individual fields of a PDU and interpret their meaning. To capture PDUs the computer on which Wireshark is installed must have a working connection to the network and Wireshark must be running before any data can be captured. When Wireshark is launched, the screen below is displayed.

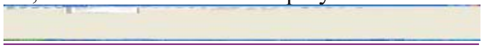
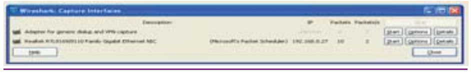


Figure No 11 Wireshark Menu Bar

To start data capture it is first necessary to go to the Capture menu and select the Options choice. The Options dialog provides a range of settings and filters which determines which and how much data traffic is captured.



Wireshark: Capture Interfaces

Description	IP	Packets	Packets/s
Adapter for generic dialup and VPN capture			
Realtek RTL8169/8110 Family Gigabit Ethernet NIC (Microsoft's Packet Scheduler)	192.168.0.27	10	2

Figure No 12 Wireshark Capture Interfaces

This main display window of Wireshark has three panes.

Figure No 13 Wireshark Capture Interfaces

The PDU (or Packet) List Pane at the top of the diagram displays a summary of each packet captured. By clicking on packets in this pane, you control what is displayed in the other two panes. The PDU (or Packet) Details Pane in the middle of the diagram displays the packet selected in the Packet List Pane in more detail. The PDU (or Packet) Bytes Pane at the bottom of the diagram displays the actual data (in hexadecimal form representing the actual binary) from the packet selected in the Packet List Pane, and highlights the field selected in the Packet Details Pane.

b) IV. RESULTS AND DISCUSSIONS

On the initial stage of our research we have used two software tools Phishing Zapper and wiresharks. We have analyze there result and come to this result that out put was not as the expected format because with the help of phishing zapper tool we only the monitors the incoming emails and web pages that might be phishing. Phishing Zapper also gives you the ability to choose which security level you want to set for your system.but we can not recover uncover cache password that's I moved to another software tool wireshark.wirehark software tool is capturing the packets generated by the Ping program. You may recall that the Ping program is simple tool that allows anyone to verify if a host is live or not. The Ping program in the source host sends a packet to the target IP address; if the target is live, the Ping program in the target host responds by sending a packet back to the source host. As you might have guessed both of these Ping packets are ICMP (Internet Control Message Protocol) packets.

Do the following

- Opening the Windows Command Prompt application
- Start up the Wireshark packet sniffer, and begin Wireshark packet capture.
- The ping command is in c:\windows\system32, so type either "ping –n 10 hostname" or "c:\windows\system32\ping –n 10 hostname" in the MS-DOS command line (without quotation marks), where hostname is a host on another continent. If you're outside of Asia, you may want to enter www.ust.hk for the Web server at Hong Kong University of Science and Technology. The argument "-n 10" indicates that 10 ping messages should be sent. Then run the Ping program by typing return.
- When the Ping program terminates, stop the packet capture in Wireshark.

At the end of the experiment, your Command Prompt Window should look something like Figure 6.1. In this example, the source ping program is in Massachusetts and the destination Ping program is in Hong Kong. From this window we see that the source ping program sent 10 query packets and received 10 responses. Note also that for each response, the source calculates the round-trip time (RTT), which for the 10 packets is on average 375 msec.

Figure 14 Command Prompt window after entering Ping command

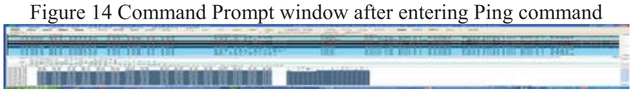


Figure 15 Wireshark capture of ping packet with ICMP packet expanded

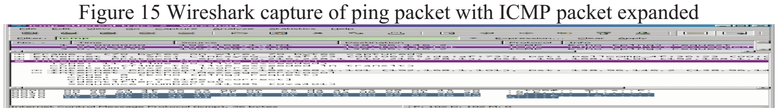


Figure 16 Wireshark window of ICMP fields expanded for one ICMP error packet.

For one of the programming assignments you created a UDP client ping program. This ping program, unlike the standard ping program, sends UDP probe packets rather than ICMP probe packets. Use the client program to send a UDP packet with an unusual destination port number to some live host. At the same time, use Wireshark to capture any response from the target host. The result was more appropriate compare to Phishing zapper but they were very hard to understand because they were not simple format so we will used some more different tool for our research so that we can get an appropriate result that we will be simple and easy to understand.

V. CONCLUSION AND FUTURE SCOPE

The decoded information which came as results while using Wire Shark tool can be much easily understood with the help of another software which is also user for uncovering the password i.e. Cain & Abel. It is also an open source password recovery tool. It is capable of recovering various kinds of passwords by sniffing the network.

REFERENCES

[1] David Matthews , Xiaohong Yuan , Edmundson Effort , D. Huiming Yu *," Laboratory Design for Demonstrating Phishing*", Dept. of Computer Science, North Carolina A&T State University, Greensboro, NC, United States.

[2] Tyler Moore, Richard Clayton," *Evil Searching: Compromise and Recompromise of Internet Hosts for Phishing*", Harvard University, Center for Research on Computation and Society, USA.

[3] Engin Kirda, Christopher Kruegel," *Protecting Users Against Phishing Attacks with AntiPhish***",** Engin Kirda and Christopher Kruegel Technical University of Vienna.

[4] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Cranor, Julie Downs," Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions", Indraprastha Institute of Information Technology.

[5] Cormac Herley and Dinei Florencio," *A Profitless Endeavor: Phishing as Tragedy of the Commons*", Redmond, WA, USA.

[6] Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer," *Social Phishing"*, School of Informatics Indiana University, Bloomington December 12, 2005.

[7] Peter Finn , Markus Jakobsson," *Designing and Conducting Phishing Experiments*", Indiana University Bloomington, IN 47406.

[8] A Sophos white paper," *Phishing and the threat to corporate networks*", August 2005.

[9] Chuan Yue and Haining Wang," Anti-Phishing in Offense and Defense", The College of William and Mary.

[10] Wagner, P. J. and Wudi, J. M. "Designing and implementing a cyberwar laboratory exercise for a computer security course," Proceedings of SIGCSE'04 - the 35th technical symposium on computer science education, 2004, pp. 402 – 406.

[11] Hill, J. M. D., Carver, C. A., Humphries, J. W. and Pooch U. W. "Using an isolated network laboratory to teach advanced networks and security," Proceedings of SIGCSE'01 - the 32th technical symposium on computer science education, 2001, pp. 36 – 40.

[12] Brustoloni, J. C. "Laboratory experiments for network security instruction," ACM Journal on Educational Resources in Computing, Vol. 6, No. 4, 2006.

[13] D. E. Knutb, The Art of Computer Programming, Vol. III: Sorting and Searching. Reading, MA Addison-Wesley, 1973.

[14] Lakshmi M. and Sankaranarayanan P.E., “Performance analysis of three routing protocols in wireless ad hoc networks”, Information technology Journal 5 (1): 114-120, © 2006 Asian Network for Scientific Information.

[15] Andrew Zonenberg, “Distributed Hash Cracker: A Cross-Platform GPU-Accelerated Password Recovery System “, Rensselaer Polytechnic Institute 110 8th Street Troy, New York U.S.A. 12180, April 28, 2009.