A Major project work report submitted to

Verzeo

in the process of the ongoing internship

on

Cyber Security

Submitted by

Deboleena Bose

e-mail address: deboleenabose09@gmail.com

Computer Science and Technology

University of Engineering and Management

Kolkata

Topics
1. Scanning Module with Nmap tool
2. Vulnerability
3. SET Tool
4. Phishing page
5. SQL Injection
6. Mobile tracker free
7. SAM file usage and ophcrack tool

1. Scanning Module with Nmap tool

Objective: To perform scanning module by using Nmap tool (download from internet) and scan kalilinux and Windows 7 machine and find the open/ closed ports and services on machine.

Keywords: Nmap tool, Windows 10, Kalilinux, Windows 7

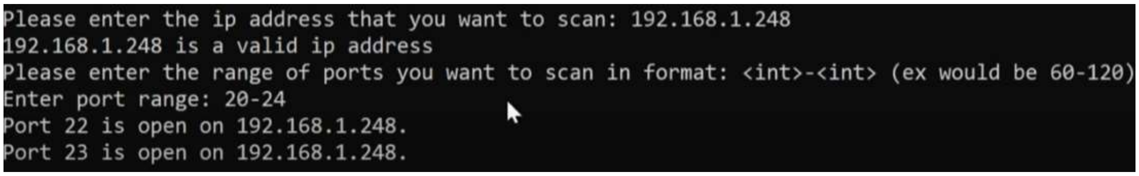
Theory:

Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network. Network scanning is used to create a profile of the target organization. Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.

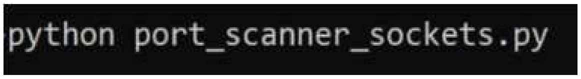
Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

Experiment and result analysis:

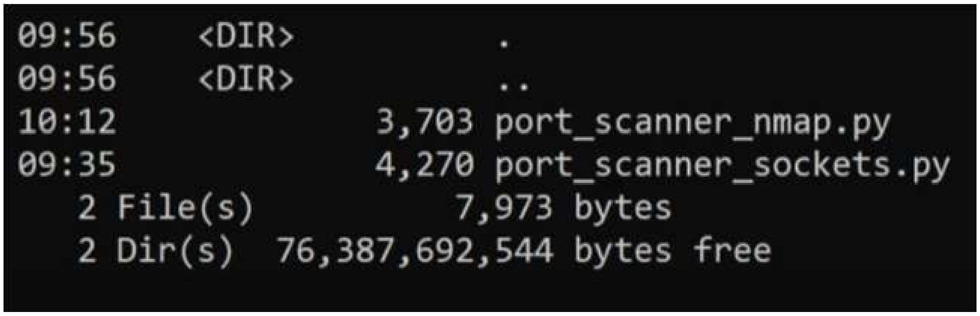
With kalilinux



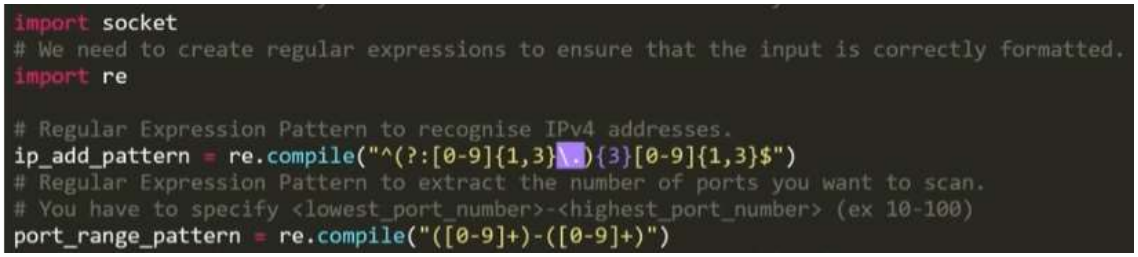
```
Please enter the ip address that you want to scan: 192.168.1.248
192.168.1.248 is a valid ip address
Please enter the range of ports you want to scan in format: <int>-<int> (ex would be 60-120)
Enter port range: 20-24
Port 22 is open on 192.168.1.248.
Port 23 is open on 192.168.1.248.
```



```
python port_scanner_sockets.py
```



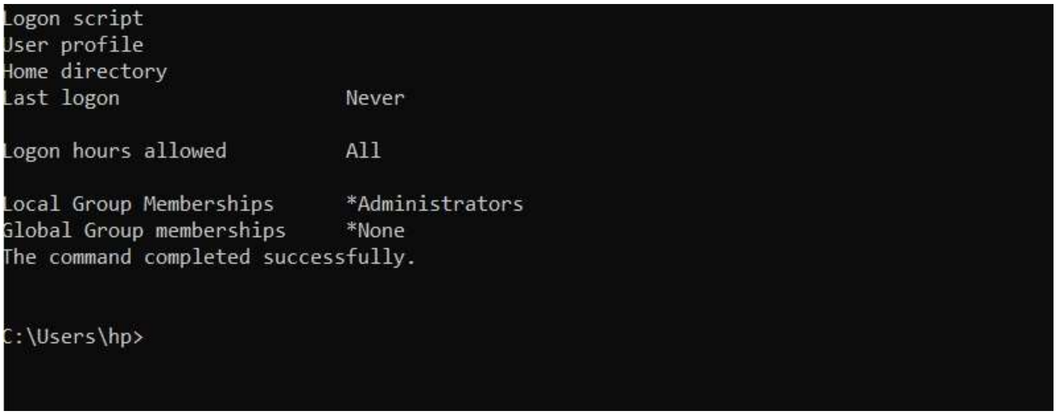
```
09:56    <DIR>          .
09:56    <DIR>          ..
10:12             3,703 port_scanner_nmap.py
09:35             4,270 port_scanner_sockets.py
   2 File(s)          7,973 bytes
   2 Dir(s)  76,387,692,544 bytes free
```



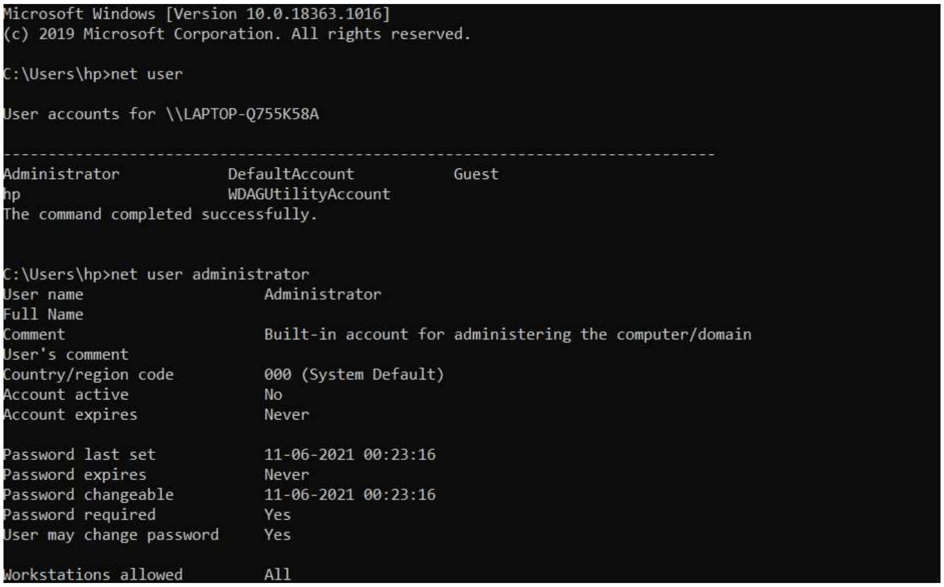
```
import socket
# We need to create regular expressions to ensure that the input is correctly formatted.
import re

# Regular Expression Pattern to recognise IPv4 addresses.
ip_add_pattern = re.compile("^(?:[0-9]{1,3}\.){3}[0-9]{1,3}$")
# Regular Expression Pattern to extract the number of ports you want to scan.
# You have to specify <lowest_port_number>-<highest_port_number> (ex 10-100)
port_range_pattern = re.compile("([0-9]+)-([0-9]+)")
```

With windows 7

In command line



```
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *None
The command completed successfully.


C:\Users\hp>
```



```
Microsoft Windows [Version 10.0.18363.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\hp>net user

User accounts for \\LAPTOP-Q755K58A

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
hp                       WDAGUtilityAccount
The command completed successfully.


C:\Users\hp>net user administrator
User name                    Administrator
Full Name
Comment                      Built-in account for administering the computer/domain
User's comment
Country/region code          000 (System Default)
Account active               No
Account expires              Never

Password last set            11-06-2021 00:23:16
Password expires             Never
Password changeable          11-06-2021 00:23:16
Password required            Yes
User may change password     Yes

Workstations allowed         All
```

Solutions:

The main defence against port scanning is to use a good firewall. A firewall will block anonymous requests so will not reply to a random scan from the internet.

Set up correctly, which more firewalls are by default now, a firewall will block any connection from the internet that was not set up from your computer. So if you don't have a browser open and are using it to surf the net, the firewall will block a hacker pretending to be a firewall because your computer did not set up that connection.

Aside from a firewall, not using port forwarding on your router is the best way to protect against it. You shouldn't need to use port forwarding anymore as firewalls are intelligent enough to figure out what traffic is real and should be let through and what is not.

It is well worth checking your router to make sure port forwarding is not enabled. It should be under security or firewall depending on the router. Make sure there are no ports being forwarded for any reason.

Conclusions:

As we perform port scan using Nmap it will give us information about all port state and services running on that port by using various techniques. It will help us to narrow our choice to whether to attack on that host or not. But here we should keep in are mind that it is the first step to hack or protect any network after that there is lot more things remaining to do further. It will just give as an idea about which type of network is there.

2. Vulnerability

Objective: To test the System Security by using Metasploit tool from Kalilinux and hack the Windows 7. Execute the command to get the keystrokes/ screenshots/ webcam, and etc. Write a report on vulnerability issues along with screenshots and how you performed and suggest the security patch to avoid these types of attacks.

Keywords: PRORAT, Kalilinux, Windows 7

Theory: A vulnerability is, in broad terms, a weak spot in your defence. Every organization has multiple security measures that keeps intruders out and important data in. Through security vulnerabilities, an attacker can find their way into your systems and network, or extract sensitive information.

Types of Vulnerabilities:

1. Software vulnerabilities-

Software vulnerabilities are when applications have errors or bugs in them. Attackers look at buggy software as an opportunity to attack the system making use of these flaws.

Example: Buffer overflow, race conditions etc.

2. Firewall Vulnerabilities-

Firewalls are software and hardware systems that protect intra-network from attacks. A firewall vulnerability is an error, weakness or invalid assumption made during the firewall design, implementation or configuration that can be exploited to attack the trusted network that the firewall is supposed to protect.

3. TCP/IP Vulnerabilities-

These vulnerabilities are of the various layers of a network. These protocols may lack features that are desirable on the insecure network.

Example: ARP attacks, Fragmentation attacks etc

4. Wireless Network Vulnerabilities-

Wireless LANs have similar protocol-based attacks that plague wired LAN. Unsecured wireless access points can be a danger to organizations as they offer the attacker a route around the company's network. Example: SSID issues, WEP issues etc.

5. Operating System Vulnerabilities-

The security of applications running on depends on the security of the operating system. Slightest negligence by the system administrator can make the operating systems vulnerable.

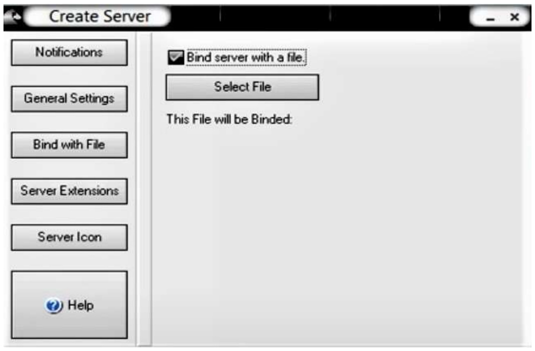
Example: Windows vulnerabilities, Linux vulnerabilities.

6. Web Server Vulnerabilities-

These vulnerabilities are caused due to design and engineering errors or faulty implementation. Example: sniffing, spoofing etc.

Experiment and result analysis:

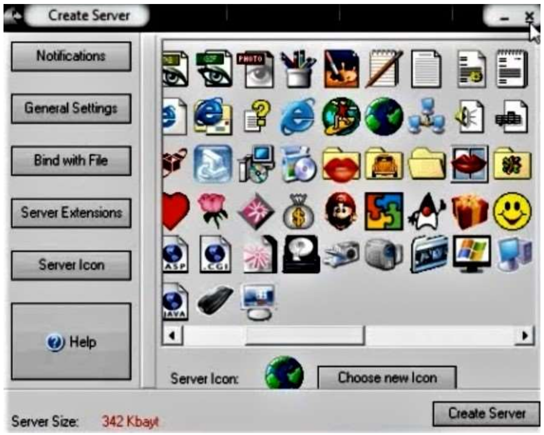
- Download ProRat
  Open ProRat
- Create ProRat trojan horse
- Click on general setting
- Select bind with file.



☑ Bind server with a file.

This File will be Binded:

- Server extensions
- Choose a server icon



Server Icon:

Server Size: 342 Kbayt

- click on the Create Server button to create the server file which is bound with the file you chose
- Click Yes and continue., simulate the trojan

Solutions:

Using a vulnerability scanner such as Rapid7 Nexpose or Tenable Nessus.

Conclusion: Data aggregation, analysis, and transfer occur at scales that organizations are unprepared for, creating a slew of cybersecurity risks. Privacy, data protection, and security of systems, networks, and data are interdependent. In view of that, to protect against cybercrime, security measures are needed that are designed to protect data and user's privacy.

3. SET Tool

Objective: To use a SET Tool and create a fake Gmail page and try to capture the credentials in command line

Keywords: Kalilinux, Windows 7, SET Tool

Theory: It is the Metasploit of social engineering in a way. It provides a very easy user interface to perform attacks like phishing, browser exploitation etc. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

Experiment and result analysis:

Start SET in a terminal. It should come up with its welcome screen.

Now for this particular attack type we need to select "Social-Engineering Attacks" from the main menu. Type 1 and press enter. It will again present with a menu that would look like this

Over here we have the option to select from various kinds of social engineering attacks. For our purpose select option 2 thats "Website Attack Vectors". Again, will come another menu like below

This time along with this menu, there would be some explanation about each attack. As can be seen the Credential Harvester Attack Method is there on number 3 which we are going to use. It is explained as

So, select number 3 and proceed. It will present another menu like

Now over here we are going to clone gmail.com to construct our phishing page. So, select option 2.

On selecting option 2, it will ask for 2 important pieces of information. The first is the ip address, to which it would submit the data and second is the url to clone which is in this case gmail.com

So, enter the details and press enter when it asks to press return. Now the credential harvester would start a web server on port 80 which would serve the page gmail.com. Open the ip address of the machine in the browser from some other machine or just localhost. For example, if SET is running on machine with ip address 192.168.1.10 then open that ip in a browser from another machine "http://192.168.1.10". Or give the ip address to someone else over the network :)

Now, when the username, password is entered and submitted, SET would capture the data and display on the terminal. Moreover, after capturing the data SET would redirect the user to the actual site, that is gmail.com

See the fields Email and Passwd, they contain the details typed by user. If you want to carry out this hack on a real user like your friend or someone, then you have to give them a link that they can open from their computer and access the SET clone of gmail.

Solutions:

- **Use a password manager and two-factor authentication wherever possible**
- Use a reputable password manager to change all of your online passwords to strong, unique ones for each login. We can’t stress this enough. Hackers today use a tactic called credential stuffing, whereby they literally cram previously stolen usernames and passwords into as many online services as possible. Why? Because a lot of usernames and passwords are identical across accounts.

- **If signing up for a new email service, check for 2FA support** Not all email providers provide 2FA. So, when signing up with an email provider, check to see what layers of security are available such as 2FA either through SMS (less secure) or app-based such as Google Authenticator or Authy.
-

  The main benefit of 2FA is that it provides a second layer of security such as a text message sent to a smartphone with a one-time password. Only the person with your device can ostensibly complete a new login. Not to mention, it can inform you when someone is trying to log into your email account.

- **Don't click suspicious links in email or texts**

- Phishers often send links via email or text that look legitimate, but once clicked on, allow them to steal your information. Email attachments that contain malware are also popular vessels for cyber mayhem. The easiest way to avoid these scams is by not clicking the links or attachments. Instead, open another tab, and go to the website of the company in the email or link to see if the information presented matches the official source. As a general rule, never open links or download attachments from unknown senders. Emails from known senders that contain links or attachments without any context are also bad news.

- This will also help you catch one of the more notorious types of phishing emails—the fake password reset (for example, "Your account has been compromised! Click here to reset your login and password.")

- **Use a VPN on your computer and your phone** Be anonymous by using a VPN to encrypt your internet connections. There's no reason not to when it comes to protecting your personal information. While you're at it, the VPN will make your browsing experience even better, with fewer ads, less tracking, and, of course, more peace of mind knowing you’re secure.

- **Don’t use public Wi-Fi or public computers, if you can help it**
  When you’re traveling or not at home, try to use the internet only through your own computer or mobile device, with your VPN turned on, of course. Public computers at hotels, for example, are accessible by other people who can put keyloggers or other malware on them, which can come back to haunt you. Wait to do your online banking or access other highly personal accounts on your protected home network, whenever possible.

- **Get a strong antivirus**
  A good antivirus raises the bar on securing your information, with real-time protection from phishing attacks and threats like malware, ransomware, and more. Antivirus should be installed on your PC, Mac, Android phone, and other devices.

- **Secure your router and Wi-Fi**
  Whether a home user or a small business owner, identifying who and what is on your network is as important as ever, as unauthorized users could be trying to hack into your system. Ensure you change the admin password for your router and set your Wi-Fi password to something really strong that a hacker could not crack.

- **Keep your computer and smartphone OS up-to-date**
  Whenever a security update is released for your operating system, update it immediately. Consider this a basic tenet of information security.

- **Keep all of your computer and smartphone apps regularly updated**
  Updates often include security improvements, so if an update is available, get it right away.

- **Consider putting a credit freeze on your account**
  As a last resort, if your email has been hacked, put a credit freeze on your account. It's easy to do and gives you more control over who has access to your accounts. When making purchases (like a car), if someone needs to access your credit report, you can easily turn the account back on, then reinstate the freeze afterward.

Conclusion:

Social media scams are omnipresent and dynamic in nature, operating across national borders. To ensure the greatest benefits for consumers, solutions must also adopt a cross-border approach. When it comes to tracking down criminals that perpetrate scams on social media and enforcing the law, international cooperation and collaboration is crucial to ensure a consistent approach and sharing of intelligence. Voluntary agreements between stakeholders also help to set clear rules in terms of detecting, preventing and responding to scams. International standards could be a valuable tool in tackling global online fraud, detailing good practice for social media platforms and other businesses about how to identify, and respond to, harmful content. Standards already exist in the digital space, but the potential for new standards should be explored.

4. Phishing page

Objective: To install social phish page from GitHub and try to execute the tool in phishing page and perform in lab setup only.

Keywords: Social phish page, Kalilinux, Windows 7.

Theory: Social phish is a powerful open source tool **Phishing Tool**. Social phish is becoming very popular nowadays that is used to do **phishing attacks** on Target. Social phish is easy then Social Engineering Toolkit. Social phish also provides option to use a custom template if someone wants. This tool makes easy to perform phishing attack. There is a lot of creativity that they can put into making the email look as legitimate as possible. A hacker impersonates a trusted person or company in order to obtain confidential data from the target device.
The hacker forwards you codes, images, or messages that are strange and so on.

Experiment and analysis:

Step 1: Open your Kali Linux operating system. Move to desktop. Here you have to create a directory called Social phish. In this directory you have to install the tool.

```
cd Desktop
```

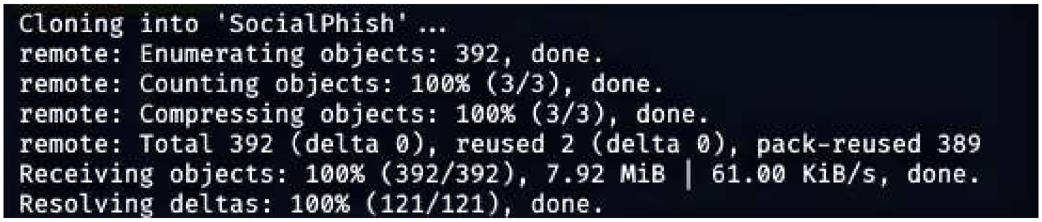
Step 2: Now you are on desktop. Here you have to create directory called Social phish. To create Mask phish directory use following command.

```
mkdir Socialphish
```

Step 3: You have created directory. Now use following command to move into that directory.

```
cd Socialphish
```

Step 4: Now you are in Socialphish directory. In this directory you have to download the tool means you have to clone the tool from GitHub. Use following command to clone the tool from GitHub.
git clone https://github.com/xHak9x/SocialPhish.git



```
Cloning into 'SocialPhish'...
remote: Enumerating objects: 392, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 392 (delta 0), reused 2 (delta 0), pack-reused 389
Receiving objects: 100% (392/392), 7.92 MiB | 61.00 KiB/s, done.
Resolving deltas: 100% (121/121), done.
```

Step 5: The tool has been downloaded in the directory Socialphish. Now to list out the contents of the tool that has been downloaded use following command.
ls

Step 6: When you listed out the contents of the tool you can see that a new directory has been generated by the tool that is Social Phish. You have to move in this directory to view the contents of the tool. To move in this directory, use following command.
cd SocialPhish

Step 7: To list out the contents of this directory use following command.
ls

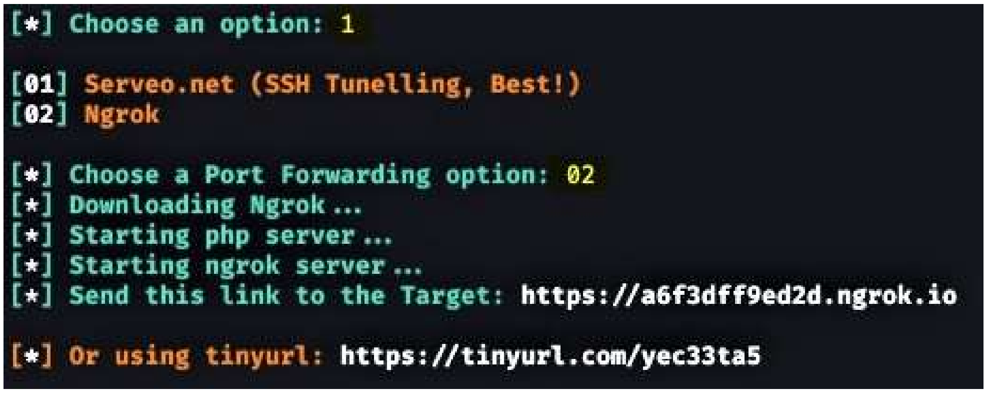
Step 8. Now you have to give the permission to the tool using following command.

chmod +x socialphish.sh

Step 9: Now you can run the tool using following command. This command will open help menu of the tool.
./socialphish.sh

For usage,

Type 01 and then for port forwarding 02



```
[*] Choose an option: 1

[01] Serveo.net (SSH Tunelling, Best!)
[02] Ngrok

[*] Choose a Port Forwarding option: 02
[*] Downloading Ngrok ...
[*] Starting php server ...
[*] Starting ngrok server ...
[*] Send this link to the Target: https://a6f3dff9ed2d.ngrok.io

[*] Or using tinyurl: https://tinyurl.com/yec33ta5
```

You can see the link has been generated by the tool that is instagram phishing webpage. Send this link to victim. once he/she open the link he/she will get an original look alike web page of instagram and once he/she fill the details in the webpage. It will be highlighted in the Socialphish terminal.

You can see here we have filled the login form we have given username as goosy and password as geesygoosy now once victim click on login all the details will be shown in social phish terminal.

You can see credentials has been found. Even you can perform this attack using yourself on to your target.

The tool is running successfully.

Solutions:

Steps to identifying and preventing phishing scams.

1. Know what a phishing scam looks like

New phishing attack methods are being developed all the time, but they share commonalities that can be identified if you know what to look for. There are many sites online that will keep you informed of the latest phishing attacks and their key identifiers. The earlier you find out about the latest attack methods and share them with your users through regular security awareness training, the more likely you are to avoid a potential attack.

2. Don’t click on that link

It’s generally not advisable to click on a link in an email or instant message, even if you know the sender. The bare minimum you should be doing is hovering over the link to see if the destination is the correct one. Some phishing attacks are fairly sophisticated, and the destination URL can look like a carbon copy of the genuine site, set up to record keystrokes or steal login/credit card information. If it’s possible for you to go straight to the site through your search engine, rather than click on the link, then you should do so.

3. Get free anti-phishing add-ons

Most browsers nowadays will enable you to download add-ons that spot the signs of a malicious website or alert you about known phishing sites. They are usually completely free so there’s no reason not to have this installed on every device in your organization.

4. Don’t give your information to an unsecured site

If the URL of the website doesn’t start with “https”, or you cannot see a closed padlock icon next to the URL, do not enter any sensitive information or download files from that site. Site’s without security certificates may not be intended for phishing scams, but it’s better to be safe than sorry.

5. Rotate passwords regularly

If you've got online accounts, you should get into the habit of regularly rotating your passwords so that you prevent an attacker from gaining unlimited access. Your accounts may have been compromised without you knowing, so adding that extra layer of protection through password rotation can prevent ongoing attacks and lock out potential attackers.

6. Don't ignore those updates

Receiving numerous update messages can be frustrating, and it can be tempting to put them off or ignore them altogether. Don't do this. Security patches and updates are released for a reason, most commonly to keep up to date with modern cyber-attack methods by patching holes in security. If you don't update your browser, you could be at risk of phishing attacks through known vulnerabilities that could have been easily avoided.

7. Install firewalls

Firewalls are an effective way to prevent external attacks, acting as a shield between your computer and an attacker. Both desktop firewalls and network firewalls, when used together, can bolster your security and reduce the chances of a hacker infiltrating your environment.

8. Don't be tempted by those pop-ups

Pop-ups aren't just irritating; they are often linked to malware as part of attempted phishing attacks. Most browsers now allow you to download and install free ad-blocker software that will automatically block most of the malicious pop-ups. If one does manage to evade the ad-blocker though, don’t be tempted to click! Occasionally pop-ups will try and deceive you with where the “Close” button is, so always try and look for an “x” in one of the corners.

9. Don’t give out important information unless you must

As a general rule of thumb, unless you 100% trust the site you are on, you should not willingly give out your card information. Make sure, if you have to provide your information, that you verify the website is genuine, that the company is real and that the site itself is secure.

10. Have a Data Security Platform to spot signs of an attack

If you are unfortunate enough to be the victim of a successful phishing attack, then it’s important you are able to detect and react in a timely manner. Having a data security platform in place helps take some of the pressure off the IT/Security team by automatically alerting on anomalous user behavior and unwanted changes to files. If an attacker has access to your sensitive information, data security platforms can help to identify the affected account so that you can take actions to prevent further damage.

Conclusion:

Overall, phishing is real and dangerous. Everyone needs to watch out for it because it happens to everybody; and getting scammed can be costly. Thus, be careful, follow this advice; and always keep your eyes and ears open to anything that even remotely sounds off because it may very well be scammers looking for their next victim.

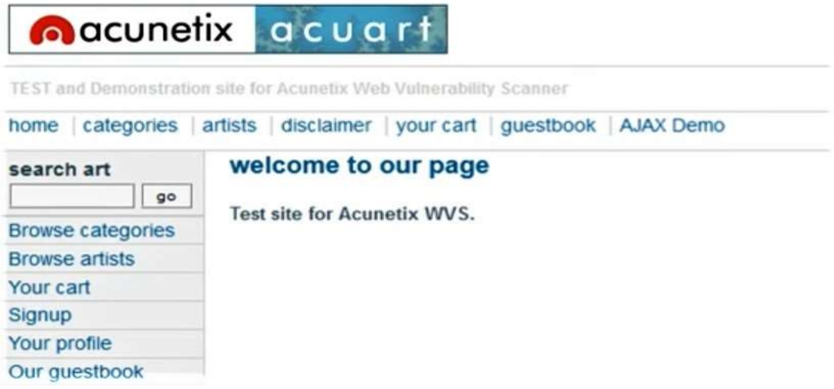
5. SQL Injection

Objective: To perform SQL injection Manually on http://testphp.vulnweb.com Write a report along with screenshots and mention preventive steps to avoid SQL injections

Keywords: Kalilinux, Windows 7, http://testphp.vulnweb.com, SQL map

Theory: SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. Hackers use injections to obtain unauthorized access to the underlying data, structure, and DBMS. This information may include any number of items, including sensitive company data, user lists or private customer details.

Experiment and result analysis:



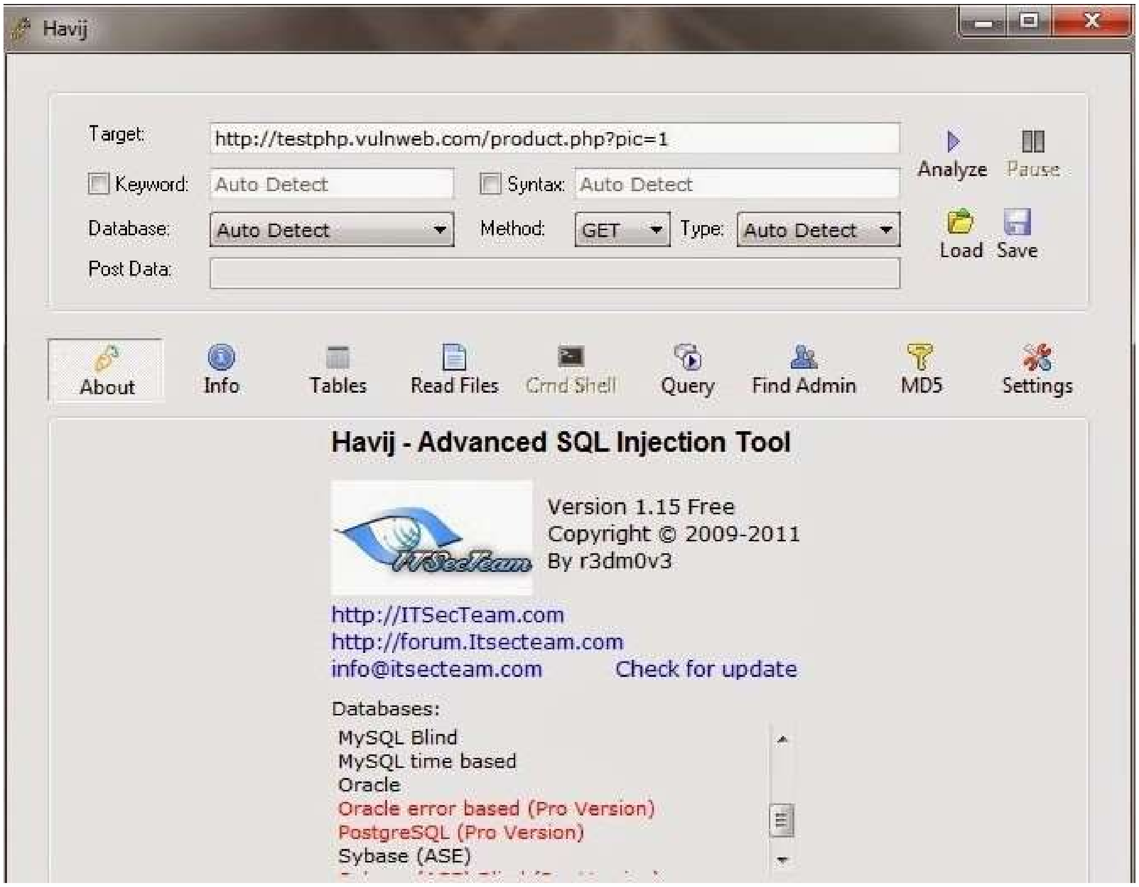
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

welcome to our page

Test site for Acunetix WVS.

- Find **SQL injection Vulnerability** in tour site and insert the string (like http://testphp.vulnweb.com) of it in Havij**.** Now click on the Analyze button

- Now click on the Tables button and then click Get Tables button from below column



Target: http://testphp.vulnweb.com/product.php?pic=1

□ Keyword: Auto Detect

□ Syntax: Auto Detect

Database: Auto Detect

Method: GET

Type: Auto Detect

Post Data:

Havij - Advanced SQL Injection Tool

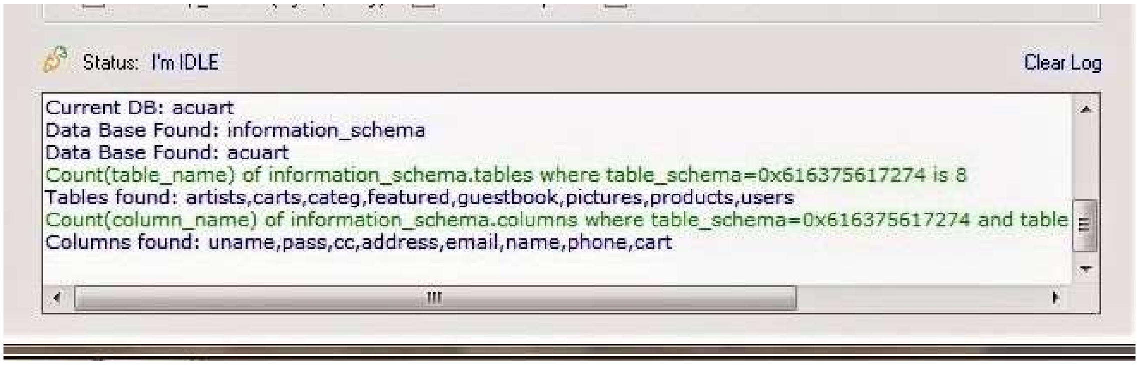
Version 1.15 Free
Copyright © 2009-2011
By r3dm0v3

http://ITSecTeam.com
http://forum.Itsecteam.com
info@itsecteam.com Check for update

Databases:

MySQL Blind
MySQL time based
Oracle
Oracle error based (Pro Version)
PostgreSQL (Pro Version)
Sybase (ASE)

- Now select any one Table and then click Get columns button
- Now select desired columns and click on get data to get the result



Status: I'm IDLE

```
Current DB: acuart
Data Base Found: information_schema
Data Base Found: acuart
Count(table_name) of information_schema.tables where table_schema=0x616375617274 is 8
Tables found: artists,carts,categ,featured,guestbook,pictures,products,users
Count(column_name) of information_schema.columns where table_schema=0x616375617274 and table
Columns found: uname,pass,cc,address,email,name,phone,cart
```

Solutions:

1. Install a security plugin
2. Only use trusted themes and plugins
3. Delete any pirated software on your site
4. Delete inactive themes and plugins
5. Update your website regularly
6. Change the default database name
7. Control field entries and data submissions
8. Harden your WordPress website

Conclusion:

SQL injection is one of the more common and more effective forms of attack on a system. Controlling the malicious SQL code/script on the web application and maintaining the end privacy is still a key challenge for the web developer. These issues must be considered seriously by the web developers involved in developing websites using databases.

6. Mobile tracker free

Objective: To use Mobile tracker free (online tool) to install in android mobile phone and try to execute the commands and taken live webcam streams and screenshots and WhatsApp messages. Write a report on that attack and provide solutions to avoid android hacking.

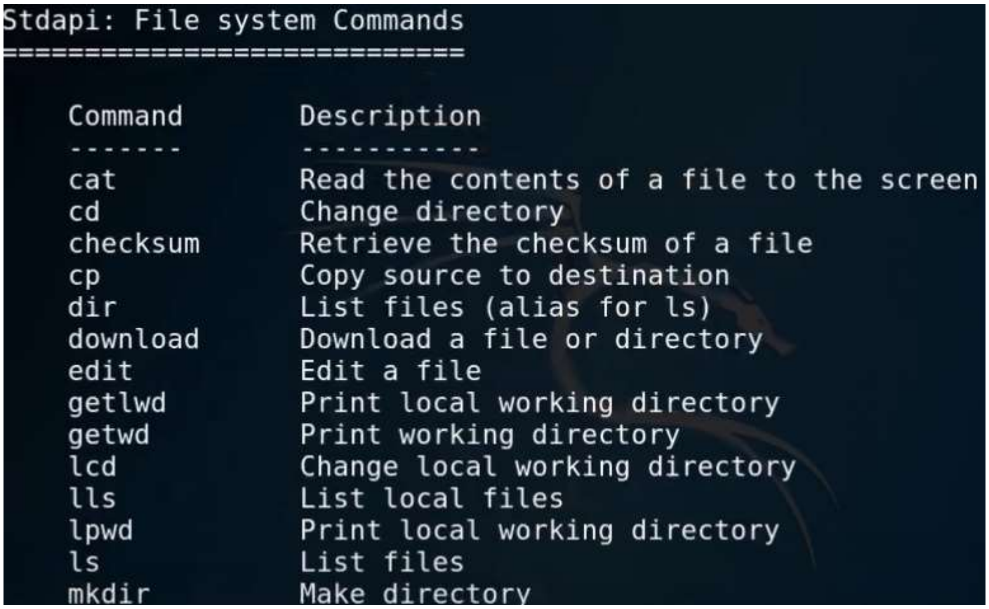
Keywords: Mobile tracker free, Android Mobile

Theory: There are many software applications for hacking phones. You can use them that are free. However, if you are serious and do the hacking for a legitimate purpose the best thing is to buy a good quality phone Spy App.

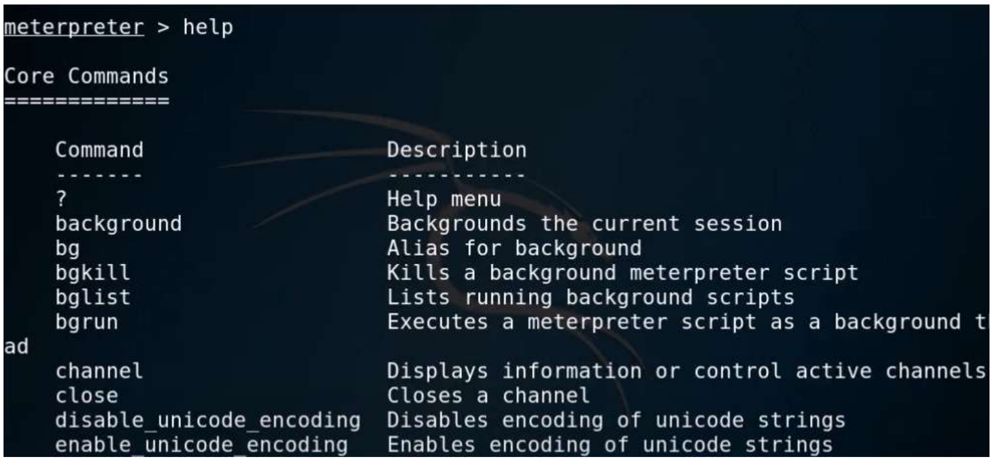
You have to install the software on the target phone manually.
Hackers can install a phone spying software on your phone, without even and Moon and Moon and accessing your phone physically.
And, even you cannot know that you are being spied by a hacker as the spying app is not visible to you.
It is hidden inside the phone.

Experiment and result analysis:

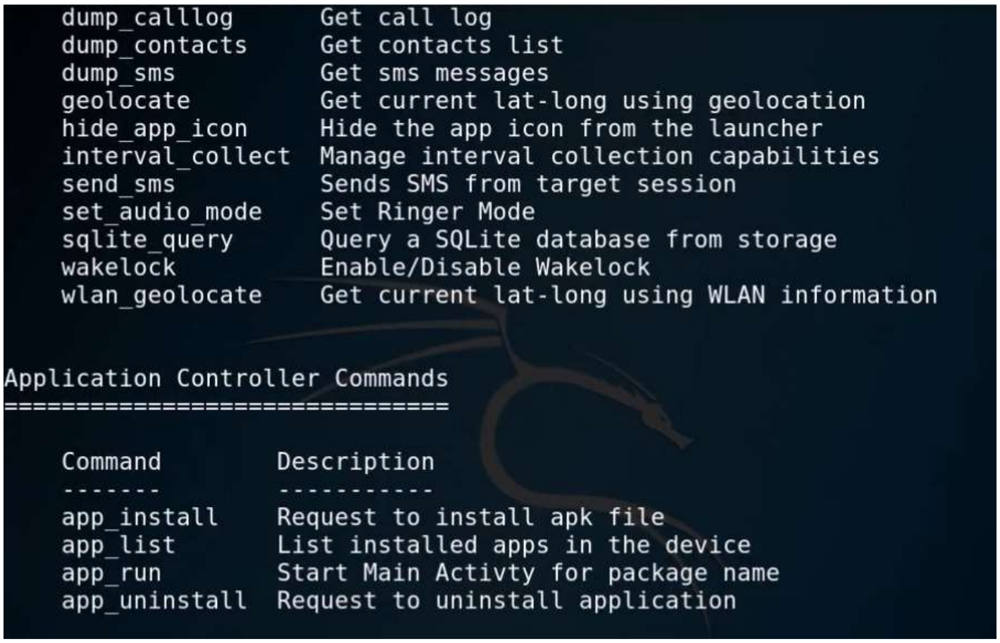
For executing commands and taken live streams



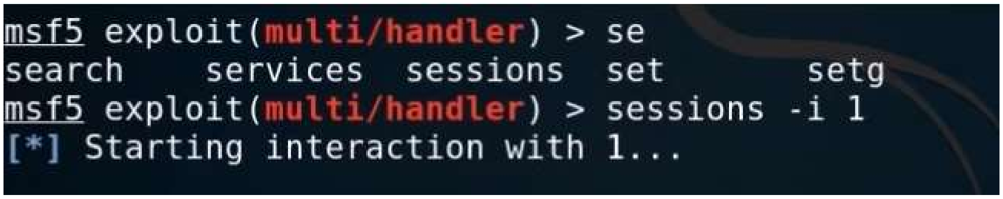
```
Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    checksum      Retrieve the checksum of a file
    cp            Copy source to destination
    dir           List files (alias for ls)
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
    lls           List local files
    lpwd          Print local working directory
    ls            List files
    mkdir         Make directory
```



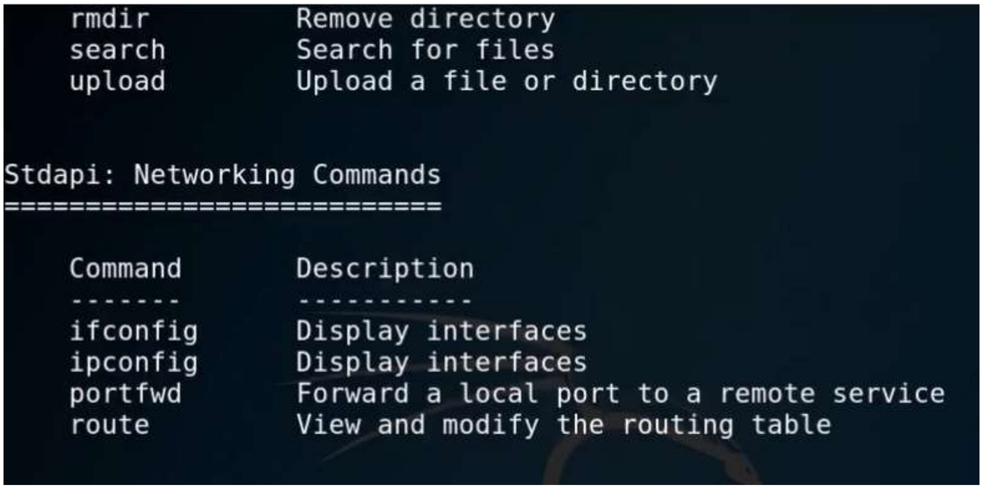
```
meterpreter > help

Core Commands
=============

    Command                    Description
    -------                    -----------
    ?                          Help menu
    background                 Backgrounds the current session
    bg                         Alias for background
    bgkill                     Kills a background meterpreter script
    bglist                     Lists running background scripts
    bgrun                      Executes a meterpreter script as a background t
ad
    channel                    Displays information or control active channels
    close                      Closes a channel
    disable_unicode_encoding   Disables encoding of unicode strings
    enable_unicode_encoding    Enables encoding of unicode strings
```



```
    dump_calllog       Get call log
    dump_contacts      Get contacts list
    dump_sms           Get sms messages
    geolocate          Get current lat-long using geolocation
    hide_app_icon      Hide the app icon from the launcher
    interval_collect   Manage interval collection capabilities
    send_sms           Sends SMS from target session
    set_audio_mode     Set Ringer Mode
    sqlite_query       Query a SQLite database from storage
    wakelock           Enable/Disable Wakelock
    wlan_geolocate     Get current lat-long using WLAN information


Application Controller Commands
===============================

    Command          Description
    -------          -----------
    app_install      Request to install apk file
    app_list         List installed apps in the device
    app_run          Start Main Activty for package name
    app_uninstall    Request to uninstall application
```



```
msf5 exploit(multi/handler) > se
search     services   sessions   set        setg
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
```

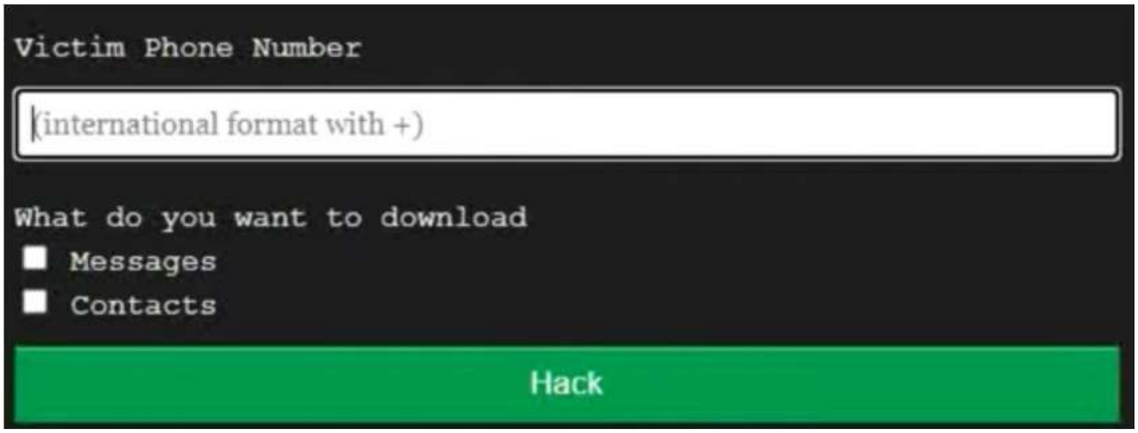


```
    rmdir          Remove directory
    search         Search for files
    upload         Upload a file or directory


Stdapi: Networking Commands
===========================

    Command        Description
    -------        -----------
    ifconfig       Display interfaces
    ipconfig       Display interfaces
    portfwd        Forward a local port to a remote service
    route          View and modify the routing table
```

For WhatsApp messages,

- Type www.whazzak.com
- whazzak main page appears, click on the main website
- whazzak main page asks for the victim’s phone number,

add victim’s phone number



Victim Phone Number

(international format with +)

What do you want to download

□ Messages

□ Contacts

Hack

- Click on Hack

Solutions:

- **Avoid unsecured public Wi-Fi.** Hackers often target important locations such as bank accounts via public Wi-Fi that can often be unsecured due to relaxed safety standards or even none at all.
- **Turn off your autocomplete feature.** By doing this, you can prevent stored critical personal data from being accessed.
- **Regularly delete your browsing history, cookies, and cache.** Removing your virtual footprint is important in minimizing the amount of data that can be harvested by prying eyes.

Conclusion:

Ethical hacking is a tool for data protection and prevention. Due to the proliferation of mobile devices, tablets and smartphones and the large number of applications, the phenomenon of computer insecurity has increased considerably and therefore these are highly vulnerable, because of the above, what is intended with this article is to be constantly ahead of those who try to attack us by doing their own tests and attacks with the help of computer experts. A new device is not that it is so remotely vulnerable, if the user makes an adequate handling of the phone without connecting to insecure networks, much less entering passwords on sites that do not handle encryption security that make the device an attack target for the attacker can steal information, however the beginning of the attacks is due to the bad manipulation of the user, nor does it serve to have port blocking by default or the deletion of permissions to install unknown applications if the user gives permissions without reading or having knowledge of what is which is installing making the phone's security vulnerable.

7. SAM file usage and Ophcrack tool

Objective: To create password for the windows machine by using ophcrack tool in virtual machine on windows 7, and try to get the password, along with mention the path of SAM file in windows and explain about the SAM file usage, and how it can be cracked by tool.

Keywords: SAM file, windows 7, ophcrack tool

Theory: **Ophcrack** is a free open-source (GPL licensed) program that cracks Windows log-in passwords by using LM hashes through rainbow tables. The program includes the ability to import the hashes from a variety of formats, including dumping directly from the SAM files of Windows. On most computers, ophcrack can crack most passwords within a few minutes.

Security Account Manager (SAM) is a database used to store user account information, including password, account groups, access rights, and special privileges in Windows operating system. In the registry, all of the users include the general users and the administrators cannot read the SAM file except the users who gain the system privileges. So, if the general user and administrator want to read the SAM file, they have to gain read access by changing the access control list of those registry keys with the permission of the administrative privileges.

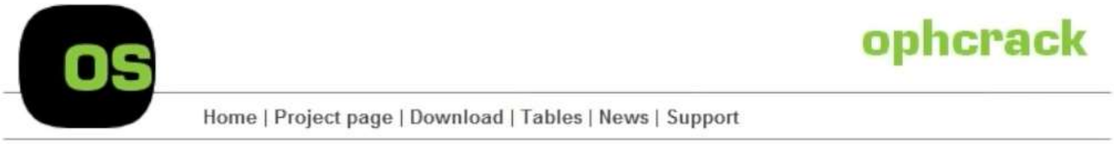
SAM uses cryptographic measures to prevent unauthenticated users accessing the system.

The user passwords are stored in a hashed format in a registry hive either as a LM hash or as an NTLM hash. This file can be found in %SystemRoot%/system32/config/SAM and is mounted on HKLM/SAM.

Experiment and result analysis:

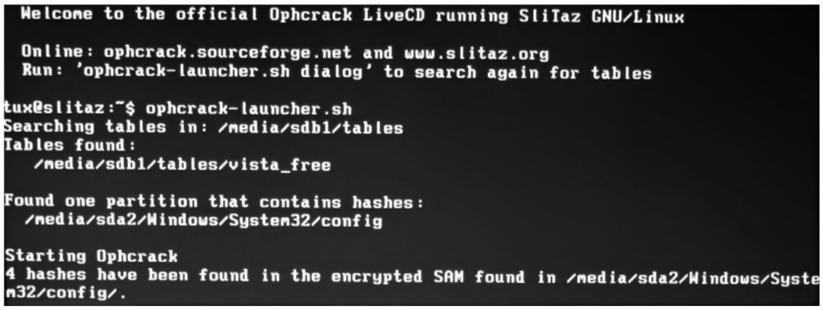
Step 1: Since we are assuming that your Windows PC is locked and you do not know the password, the first step needs to be carried out on a different PC with internet access and administrator privileges.

Step 2: Download the correct version of Ophcrack Live CD from the official website to the second PC.



Step 3: Burn the ISO file to a USB or CD. To do this, you will need an ISO burning application. Now proceed to the next step of the password reset process.

Step 4: Remove the bootable media from the second PC and insert it into your locked Windows machine. Let the computer boot up from this media instead of the native Windows installation. This is made possible by the fact that Ophcrack itself contains a small operating system that can run independently of your Windows OS. In a few moments, you will see the Ophcrack interface on your computer.



```
 Welcome to the official Ophcrack LiveCD running SliTaz GNU/Linux

 Online: ophcrack.sourceforge.net and www.slitaz.org
 Run: 'ophcrack-launcher.sh dialog' to search again for tables

tux@slitaz:~$ ophcrack-launcher.sh
Searching tables in: /media/sdb1/tables
Tables found:
   /media/sdb1/tables/vista_free

Found one partition that contains hashes:
  /media/sda2/Windows/System32/config

Starting Ophcrack
4 hashes have been found in the encrypted SAM found in /media/sda2/Windows/Syste
m32/config/.
```

Step 5: You will now see a menu with 4 options. Leave it on the default option, which is automatic. After a few seconds, you will see the Ophcrack Live CD loading and then the disk partition information being displayed as Ophcrack identifies the one with the SAM file.

Step 6: Once the process has been complete, you will see a window with several user accounts and their passwords displayed in column format. Against the previously locked username, look for an entry in the NT Pwd column.

Step 7: This will be your recovered password, so note it down. You can now remove the Live CD from the drive and restart your computer. You will be able to login to your user account using the password that was recovered by Ophcrack

Conclusion:

The structure of SAM and discusses the encryption algorithm used in Windows. Then, makes an experiment to show how to obtain the user account information from SAM database and crack the account password. By using the method what I mentioned above, we can crack almost all the Windows account passwords including Windows 7, Windows 8 and Windows 10 which is the latest operating system of Microsoft.

8. Write an article on cyber security

Cyber Security

Cybersecurity is the protection of Internet-connected systems, including hardware, software, and data from cyber-attacks. It is made up of two words one is cyber and other is security. Cyber is related to the technology which contains systems, network and programs or data. Whereas security related to the protection which includes systems security, network security and application and information security. It is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access.

Every business, regardless of its size, is a potential target of cyber-attack. That is because every business has key assets criminals may seek to exploit. Sometimes that is money or financial information. At other times, it may be personal information of staff and customers, or even the business' infrastructure. Most often, cyber-attacks happen because criminals want one's business' financial details, customers' financial details, sensitive personal data, customers' or staff email addresses and login credentials, customer databases, clients lists, IT infrastructure, IT services (eg the ability to accept online payments), intellectual property (eg trade secrets or product designs).

Cyber-attacks can cause electrical blackouts, failure of military equipment and breaches of national security secrets. They can result in the theft of valuable, sensitive data records. They can disrupt phone and computer networks or paralyze systems, making data unavailable. Data breaches can have a direct effect on individuals when criminals get hold of enough information to steal their identity and carry out various fraudulent activities. I didn't face any direct cyber-attack recently but I was going to get attacked but I got alert. Some days ago, I was seeing a website, I clicked on it and immediately a pop-up menu appeared in which it was written,"3 viruses have been detected on your device". I got shocked, as my device was very clean. But then I noticed that the pop-up menu was a pop-up menu only, it was not at all a virus detector, though I didn't click further. May be it was any web developer's trick. I narrated this incident as hackers sometimes make these types of pop-up menus through some hacking tools and as soon as if people click on those, then their devices may get hacked. In this course, I learnt about foot printing, testing vulnerability system through ProRat, batch programming, SQL injection, cryptography, Scanning module and mobile free tracker.

Regularly changing your password and not using the same one for multiple accounts can prevent hackers gaining access in the event of a breach. Familiarising yourself with how fraudsters might try to 'phish' for information and being wary of any requests to change or confirm passwords is also key. If you own smart devices, ensure that you change any default usernames or passwords they have, so they can't be easily accessed. A netizen should take certain precautions while operating the internet and should follow certain preventive measures for cybercrimes. Identification of exposures through education will assist responsible companies and firms to meet these challenges. One should avoid disclosing any personal information to strangers via e-mail or while chatting. One must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day. An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination. A person should never send his credit card number to any site that is not secured, to guard against frauds. It is always the parents who have to keep a watch on the sites that your children are accessing, to prevent any kind of harassment or deprivation in children. Web site owners should watch traffic and check any irregularity on the site. Web servers running public sites must be physically separately protected from internal corporate network. It is better to use a security programmed by the body corporate to control information on sites. Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens. IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.

Cyber-attack is now an international concern and has given many concerns that hacks and other security attacks could endanger the global economy. Organizations transmit sensitive data across the networks and to other devices in the course of doing businesses, and cybersecurity describes to protect that information and the systems used to process or store it.