

VERZEO

Cyber Security October Minor Project

Date: 25 November, 2022

Name: Nayan Acharya

NOTE: All the tasks are performed in local host, home network and virtual devices.

• **Problem Statements:**

- 1. Perform Foot printing on Microsoft Website and gather information about website by using online Websites (Whois / netcraft / Shodan / dnsdumpster., etc.) as much as possible and write report on gathered info along with screenshots.**

=

- Foot printing will allow the attacker to gather the information related to internal and external security architecture, attacker collects publicly available sensitive information.
- Collection of information also helps the attacker to identify the vulnerabilities in a system and which will in exploits to gain access.
- Getting more information about target reduces the focus area & bring attacker closer to the target to perform easier to attack.

Foot printing on Microsoft Website and gather information about website by using Whois, Shodan, dnsdumpster...

Here are some screenshots gathered using Whois: -

Name Servers: ns1-39.azure-dns.com
ns2-39.azure-dns.net
ns3-39.azure-dns.org
ns4-39.azure-dns.info



Registrant Contact

Name:	Domain Administrator
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	admin @domains.microsoft



Administrative Contact

Name:	Domain Administrator
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	admin @domains.microsoft

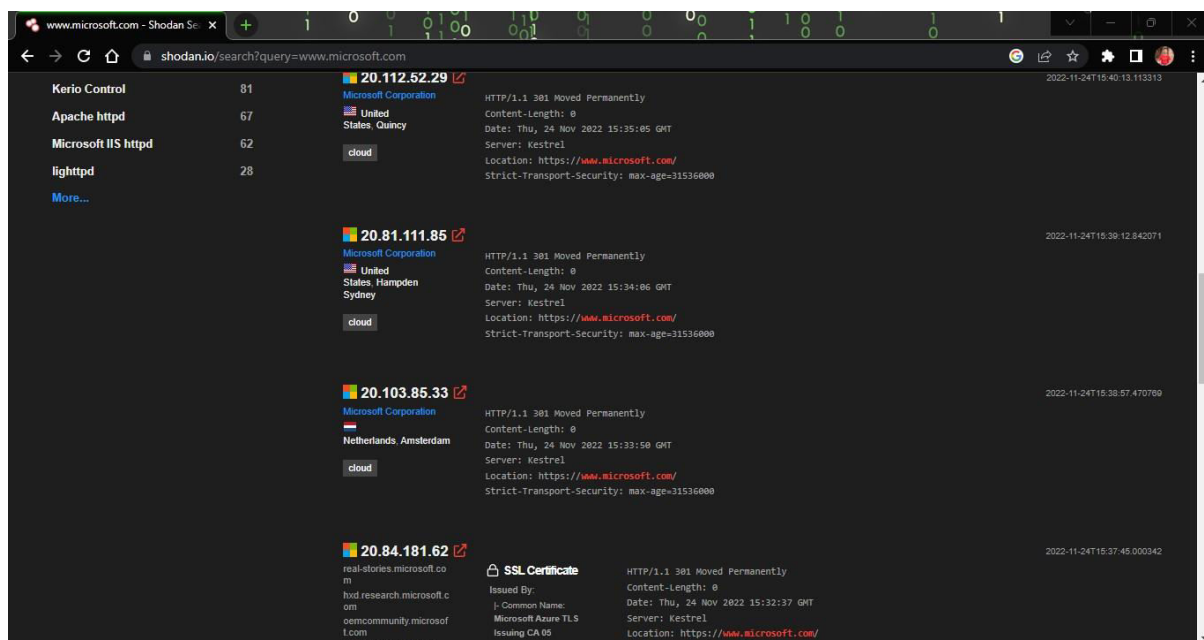


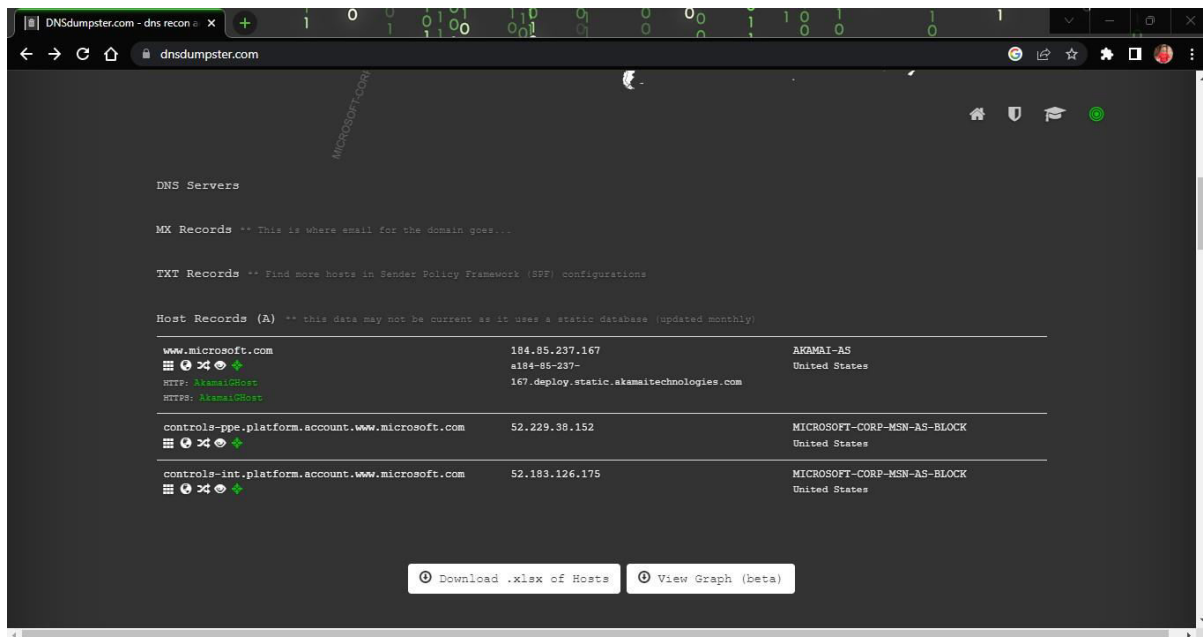
Technical Contact

Name:	MSN Hostmaster
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	nsnhst @microsoft.com

Raw Whois Data

Domain Name: microsoft.com
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2022-04-18T19:25:49+0000
Creation Date: 1991-05-02T04:00:00+0000
Registrar Registration Expiration Date: 2023-05-03T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: **abusecomplaints**@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (<https://www.icann.org/epp#clientUpdateProhib>)
Domain Status: clientTransferProhibited (<https://www.icann.org/epp#clientTransferPr>)
Domain Status: clientDeleteProhibited (<https://www.icann.org/epp#clientDeleteProhib>)
Domain Status: serverUpdateProhibited (<https://www.icann.org/epp#serverUpdateProhib>)
Domain Status: serverTransferProhibited (<https://www.icann.org/epp#serverTransferPr>)
Domain Status: serverDeleteProhibited (<https://www.icann.org/epp#serverDeleteProhib>)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way,
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
Registrant Country: US
Registrant Phone: +1.4258828080
Registrant Phone Ext:
Registrant Fax: +1.4259367329
Registrant Fax Ext:
Registrant Email: **admin**@domains.microsoft



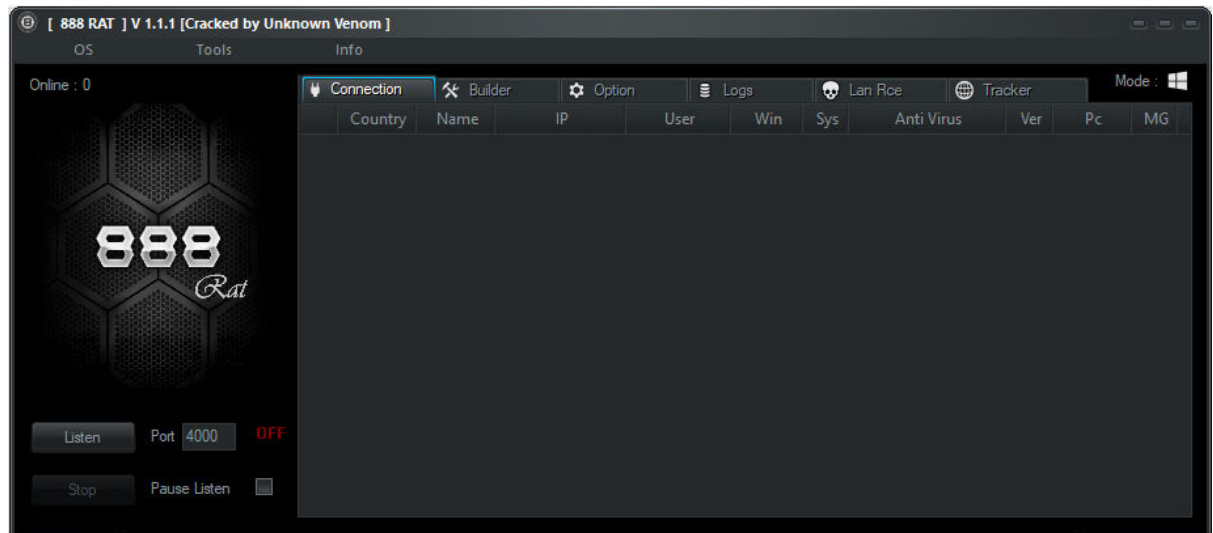


These all are the information gathered from different places like Whois, Shodan, dnsdumpster ... related to internal and external security architecture, attacker collects publicly available sensitive information which helps the attacker to identify the vulnerabilities in a system and which will in exploits to gain access. Getting such more information about target reduces the focus area & bring attacker closer to the target to perform easier to attack.

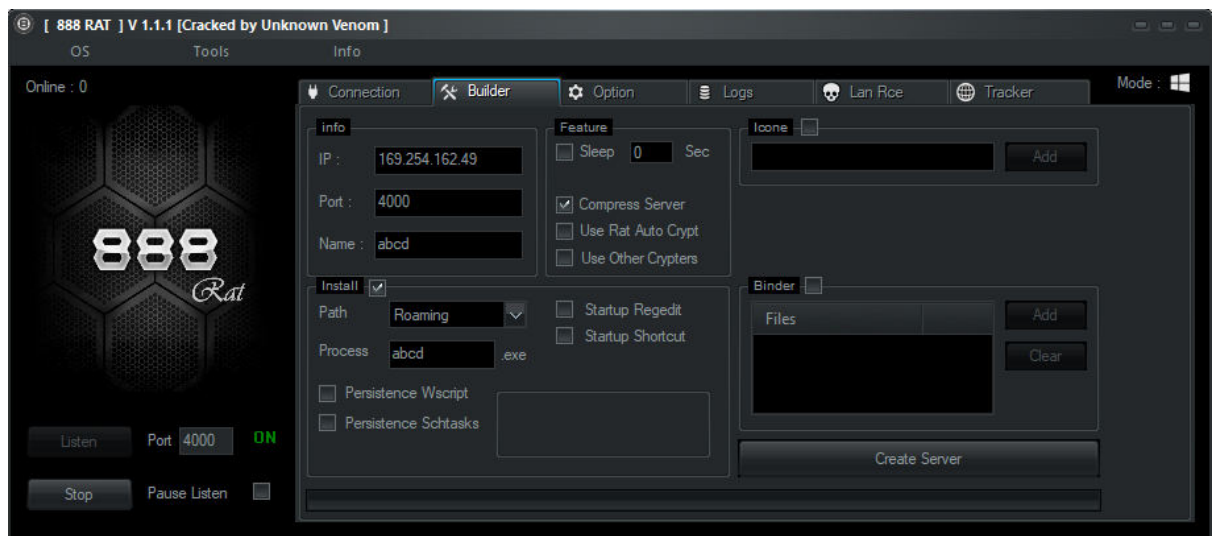
2. Test the System Security by using PRORAT / Darkcommet (Anyone Tool) Trojan by hacking virtual machine and try to take screenshots & Keystrokes along with change data in Desktop. Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these type of attacks Hacker Machine: Windows 7 / Windows 10 Victim machine: Windows XP / Windows 7.

=

I am testing the system security using 888 private RAT Trojan by hacking virtual machine.

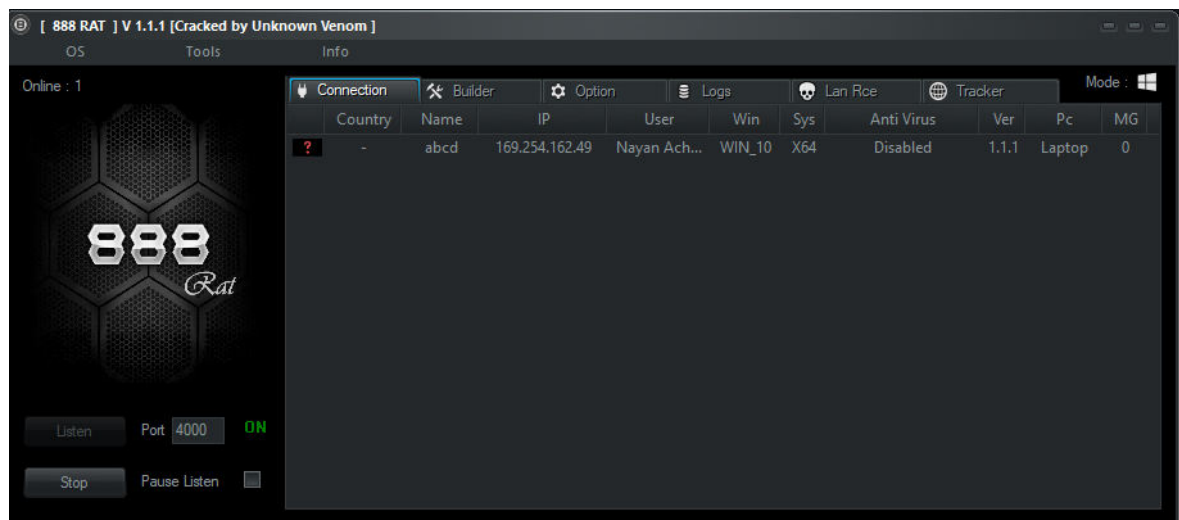


Creating Virus using 888 RAT:

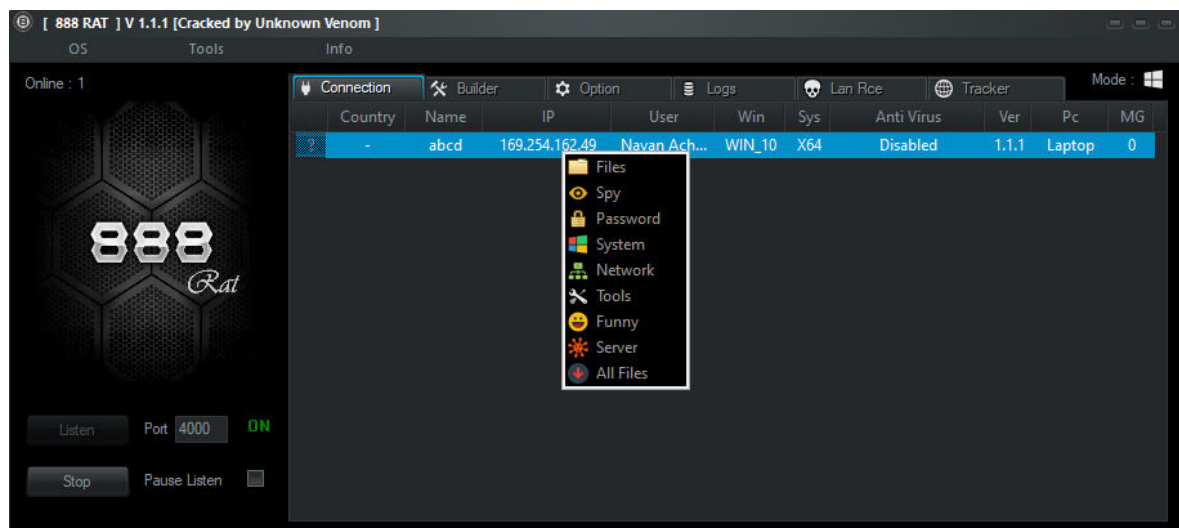


After creating virus, that virus is sent to victim computer, when he/she opens the .exe file the virus gets its job done. Then we have the full control of the victim device.

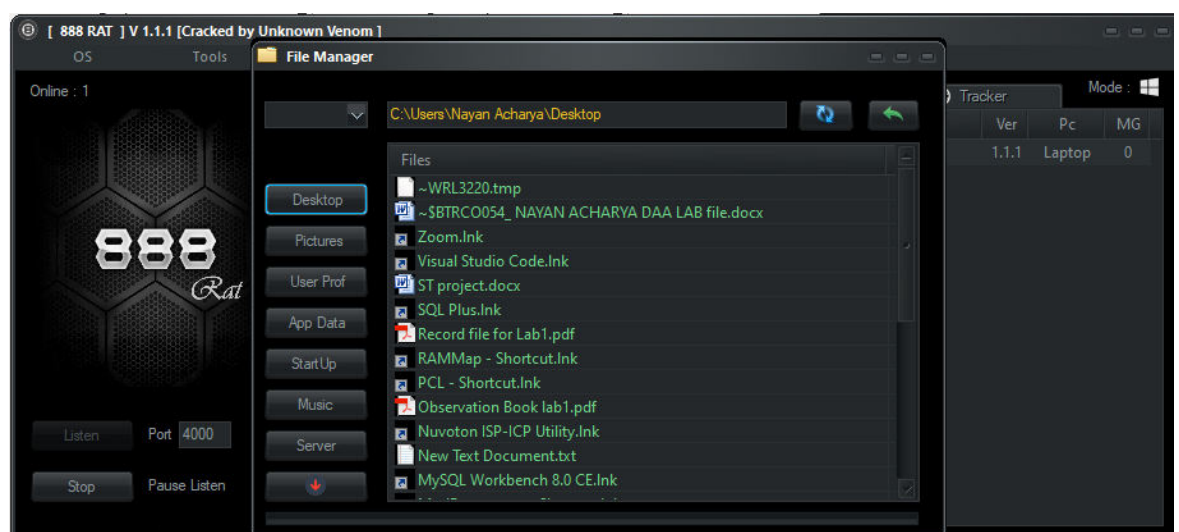
Here we can see the details of the victim computer.

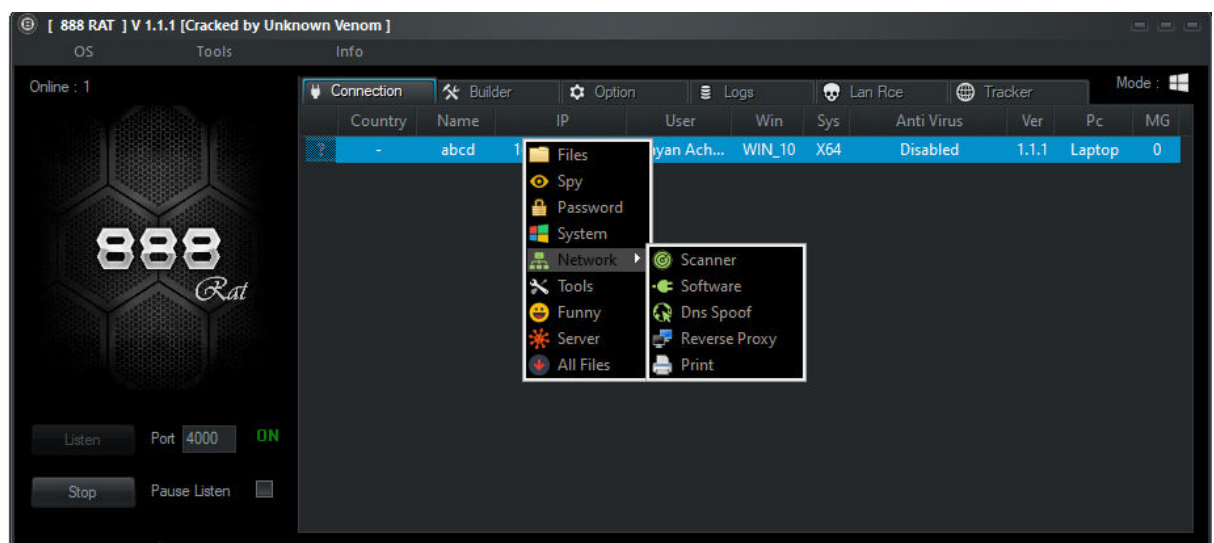
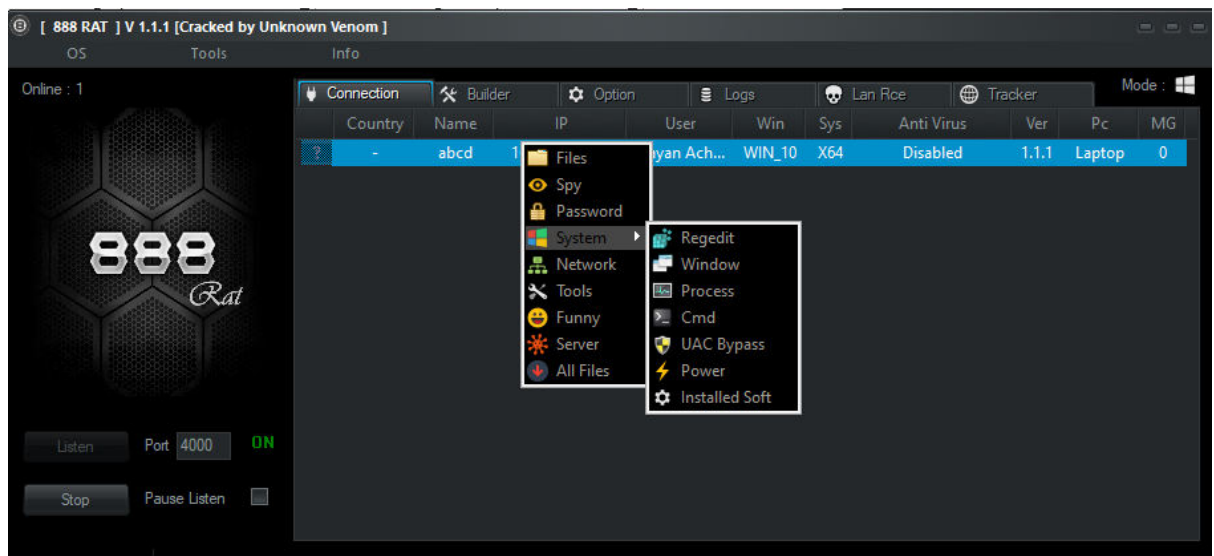
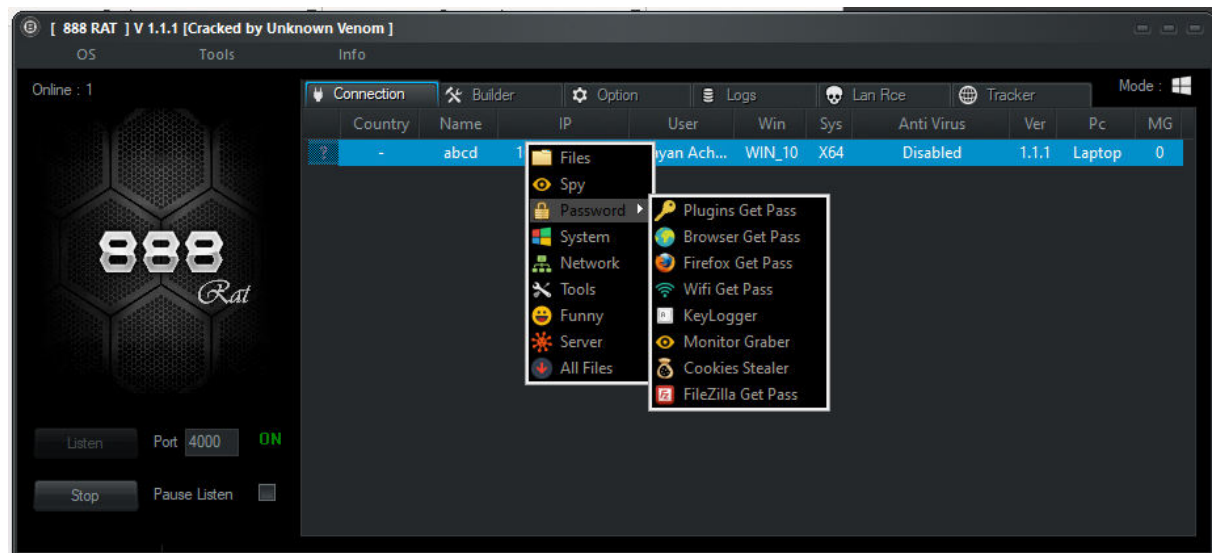


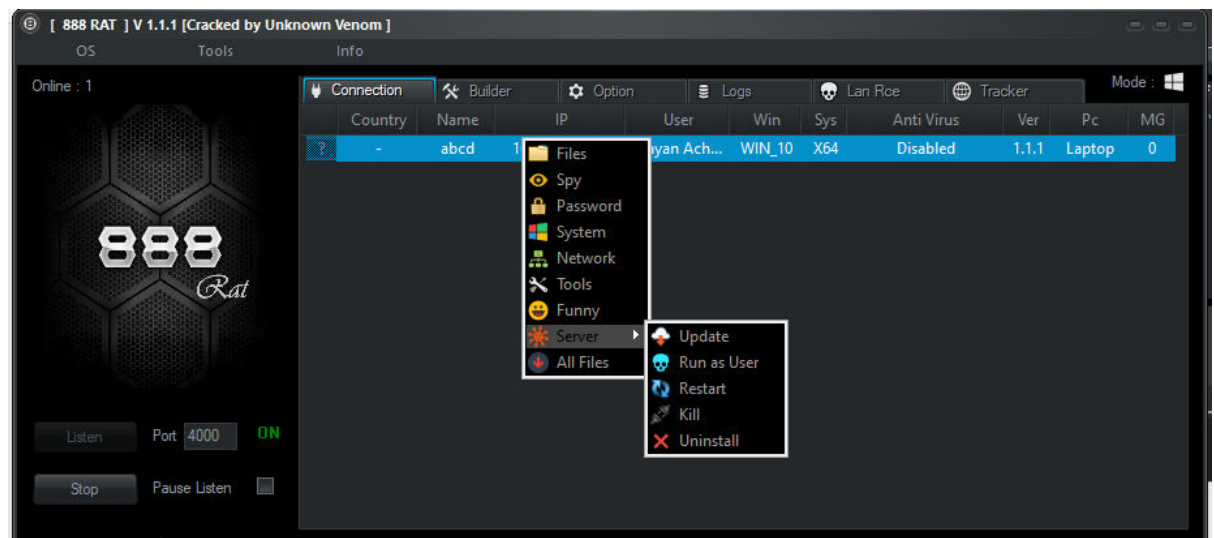
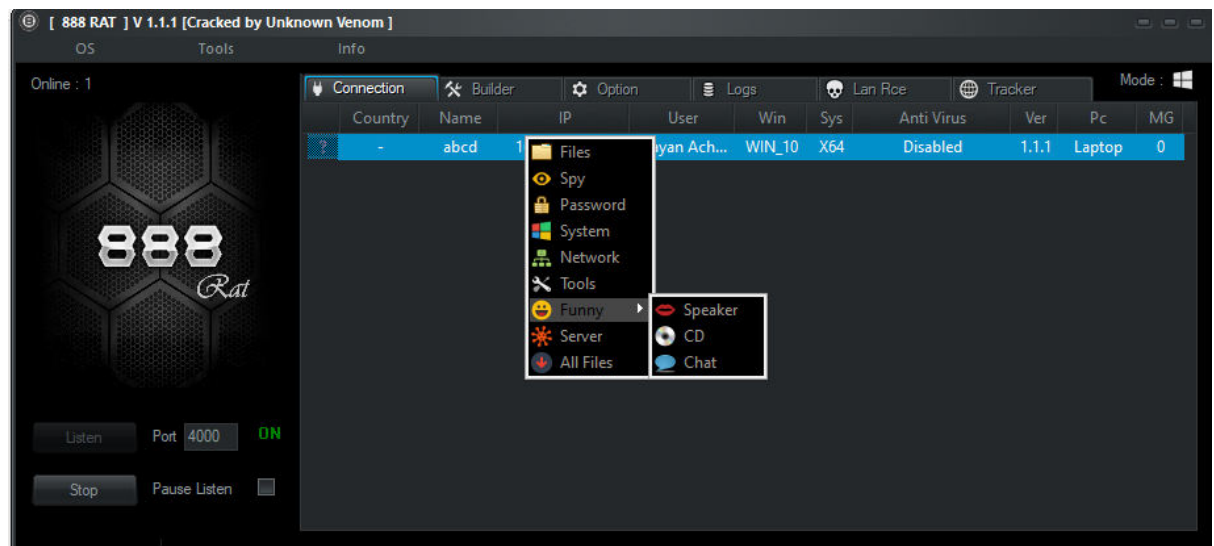
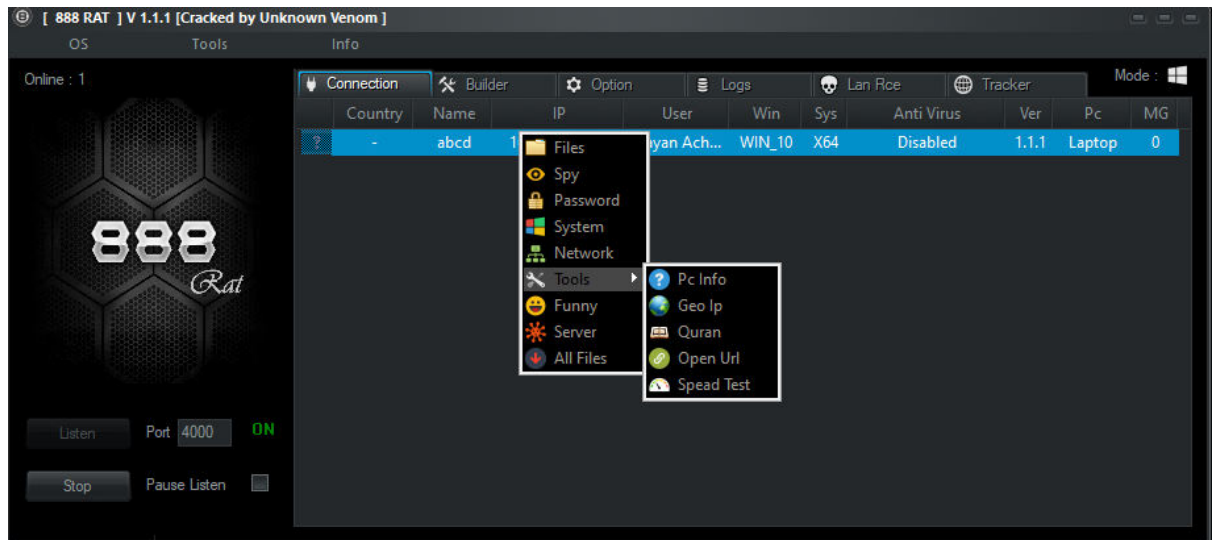
There are many things we can do using this 888 RAT. Like we can access all the files, spy, keylogger etc...



From file option we can access all files in victim's computer.







By using the 888 RAT we can see the real time camera and desktop screen. We can read write and delete any file and folders using this RAT and many more as shown in above screenshots.

How to secure your computer from hackers:

Despite the prevalence of computer hackers, most businesses rely on the internet to track their financials, order and maintain inventory, conduct marketing and PR campaigns, connect with customers, engage in social media, and perform other critical operations. Yet we continue to hear about massive computer breaches, even at giant corporations with robust security measures in place.

Small businesses are often targeted as well, especially because they may underestimate the risk of cybercrime and may not have the resources to employ expensive cybersecurity solutions. Follow these tips to protect your devices and safeguard your sensitive data:

1. Use a firewall.

Windows and macOS have built-in firewalls – software designed to create a barrier between your information and the outside world. Firewalls prevent unauthorized access to your business network and alert you to any intrusion attempts.

Make sure the firewall is enabled before you go online. You can also purchase a hardware firewall from companies such as Cisco, Sophos or Fortinet, depending on your broadband router, which also has a built-in firewall that protects your network. If you have a larger business, you can purchase an additional business networking firewall.

2. Install antivirus software.

Computer viruses and malware are everywhere. Antivirus programs such as Bitdefender, Panda Free Antivirus, Malwarebytes and Avast protect your computer against unauthorized code or software that may threaten your operating system. Viruses may have easy-to-spot effects – for example, they might slow your computer or delete key files – or they may be less conspicuous.

Antivirus software plays a major role in protecting your system by detecting real-time threats to ensure your data is safe. Some advanced antivirus programs provide automatic updates, further protecting your machine from the new viruses that emerge every day. After you install an antivirus program, don't forget to use it. Run or schedule regular virus scans to keep your computer virus-free.

3. Install an anti-spyware package.

Spyware is a special kind of software that secretly monitors and collects personal or organizational information. It is designed to be hard to detect and difficult to remove and tends to deliver unwanted ads or search results that are intended to direct you to certain (often malicious) websites.

Some spyware records every keystroke to gain access to passwords and other financial information. Anti-spyware concentrates exclusively on this threat, but it is often included in

major antivirus packages, like those from Webroot, McAfee and Norton. Anti-spyware packages provide real-time protection by scanning all incoming information and blocking threats.

4. Use complex passwords.

Using secure passwords is the most important way to prevent network intrusions. The more secure your passwords are, the harder it is for a hacker to invade your system.

More secure often means longer and more complex. Use a password that has at least eight characters and a combination of numbers, uppercase and lowercase letters, and computer symbols. Hackers have an arsenal of tools to break short, easy passwords in minutes.

Don't use recognizable words or combinations that represent birthdays or other information that can be connected to you. Don't reuse passwords, either. If you have too many passwords to remember, consider using a password manager, such as Dash lane, Sticky Password, LastPass or Password Boss. [See related article: [How to Create a Strong Password](#)]

5. Keep your OS, apps and browser up-to-date.

Always install new updates to your operating systems. Most updates include security fixes that prevent hackers from accessing and exploiting your data. The same goes for apps. Today's web browsers are increasingly sophisticated, especially in privacy and security. Be sure to review your browser security settings in addition to installing all new updates. For example, you can use your browser to prevent websites from tracking your movements, which increases your online privacy. Or, use one of these private web browsers.

6. Ignore spam.

Beware of email messages from unknown parties, and never click on links or open attachments that accompany them. Inbox spam filters have gotten pretty good at catching the most conspicuous spam. But more sophisticated phishing emails that mimic your friends, associates and trusted businesses (like your bank) have become common, so keep your eyes open for anything that looks or sounds suspicious.

7. Back up your computer.

If your business is not already backing up your hard drive, you should begin doing so immediately. Backing up your information is critical in case hackers do succeed in getting through and trashing your system.

Always be sure you can rebuild as quickly as possible after suffering any data breach or loss. Backup utilities built into macOS (Time Machine) and Windows (File History) are good places to start. An external backup hard drive can also provide enough space for these utilities to operate properly.

8. Shut it down.

Many businesses, especially those operating a web server, are "all systems go" all the time. If you're not operating a complex internet-based company, however, switch off your machine overnight or during long stretches when you're not working. Always being on makes your computer a more visible and available target for hackers; shutting down breaks the

connection a hacker may have established with your network and disrupts any possible mischief.

9. Use virtualization.

Not everyone needs to take this route, but if you visit sketchy websites, expect to be bombarded with spyware and viruses. While the best way to avoid browser-derived intrusions is to steer clear of unsafe sites, virtualization allows you to run your browser in a virtual environment, like Parallels or VMware Fusion, that sidesteps your operating system to keep it safer.

10. Secure your network.

Routers don't usually come with the highest security settings enabled. When setting up your network, log in to the router, and set a password using a secure, encrypted setup. This prevents intruders from infiltrating your network and messing with your settings.

11. Use two-factor authentication.

Passwords are the first line of defence against computer hackers, but a second layer boosts protection. Many sites let you enable two-factor authentication, which boosts security because it requires you to type in a numerical code – sent to your phone or email address – in addition to your password when logging in.

12. Use encryption.

Even if cybercriminals gain access to your network and files, encryption can prevent them from accessing any of that information. You can encrypt your Windows or macOS hard drive with BitLocker (Windows) or File Vault (Mac), encrypt any USB flash drive that contains sensitive information and use a VPN to encrypt web traffic. Only shop at encrypted websites; you can spot them immediately by the “https” in the address bar, accompanied by a closed-padlock icon.

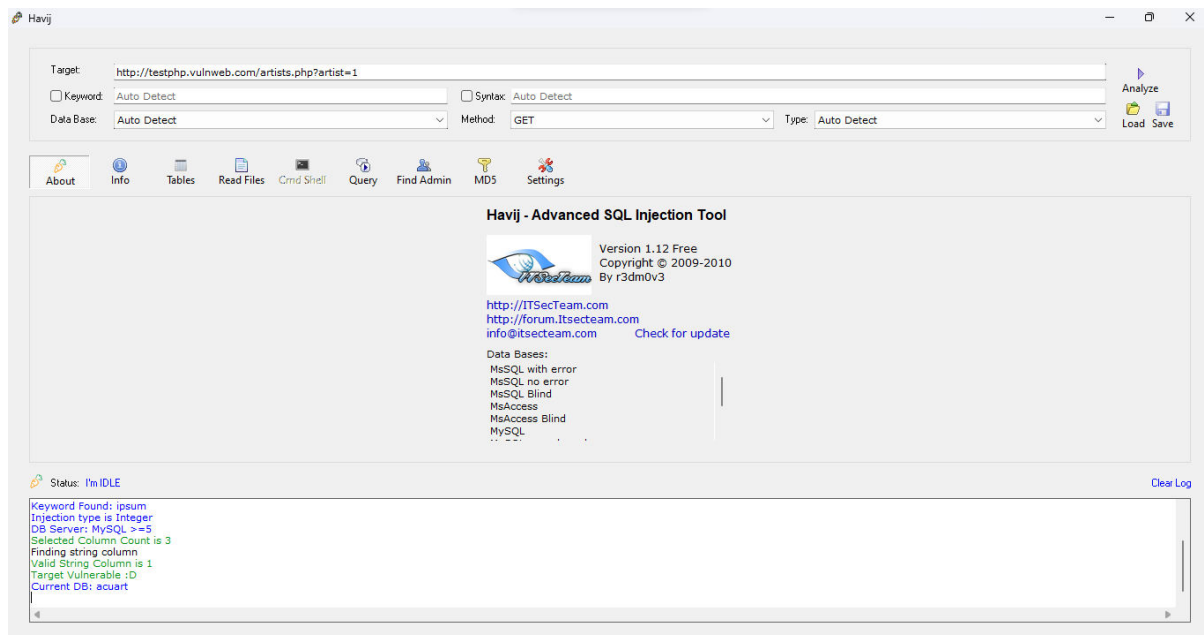
3. Perform SQL injection on by using Havij Tool (Download it from Internet) on <http://testphp.vulnweb.com> Write a report along with screenshots and mention preventive steps to avoid SQL injections.

=

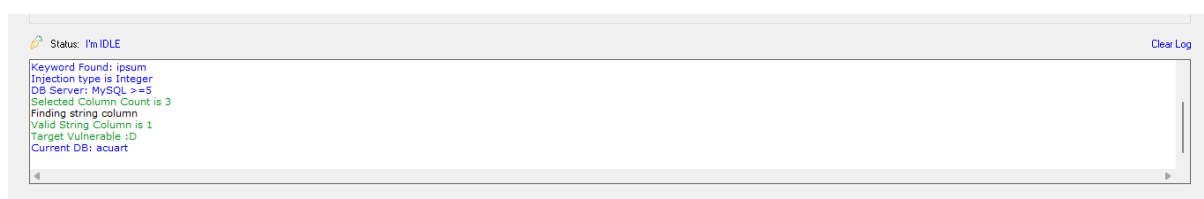
Havij is an automated SQL injection tool. To say in the own words of its creators, “Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page. It can take advantage of a vulnerable web application. By using this software, user can perform back-end database fingerprinting, retrieve DBMS

login names and password hashes, dump tables and columns, fetch data from the database, execute SQL statements against the server, and even access the underlying file system and execute operating system shell commands.”

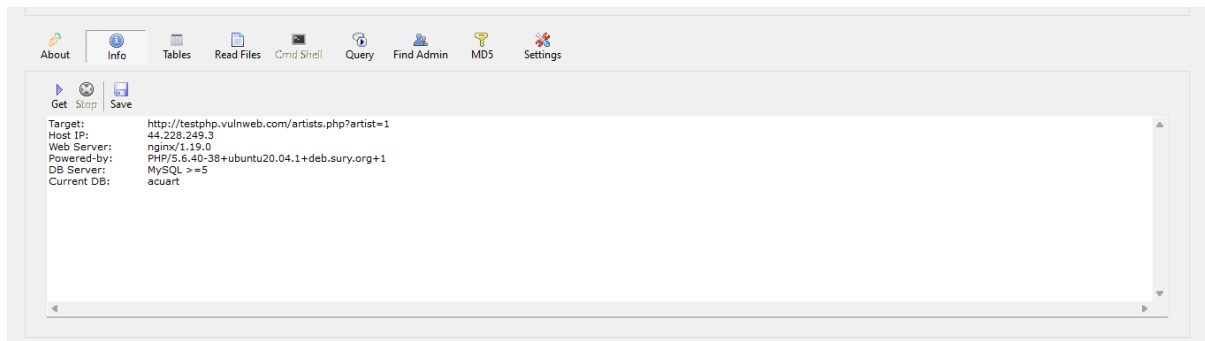
It is available both in free and commercial versions. Today we are going to see how to dump the contents of a database using Havij. For this I am going to use the free version. First download Havij from here and install it. Then open it and enter the vulnerable page URL in the target column (for this I am using <http://testphp.vulnweb.com>).



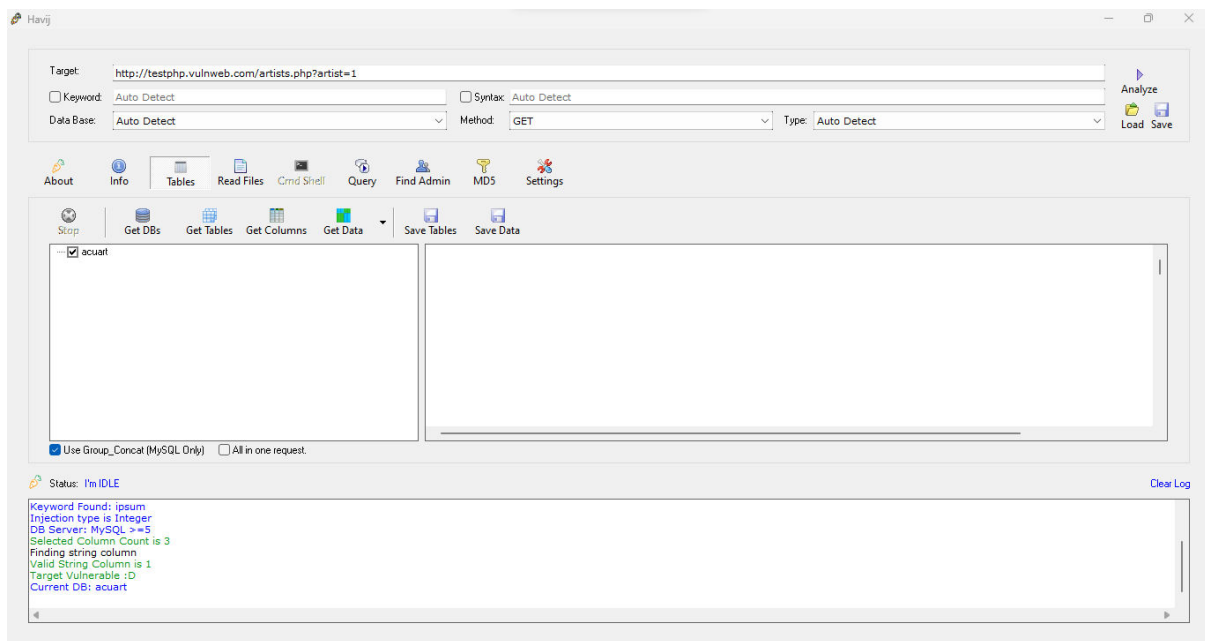
Set the database option to ‘*auto detect*’ and hit analyse. This should show you the current database name as shown below.



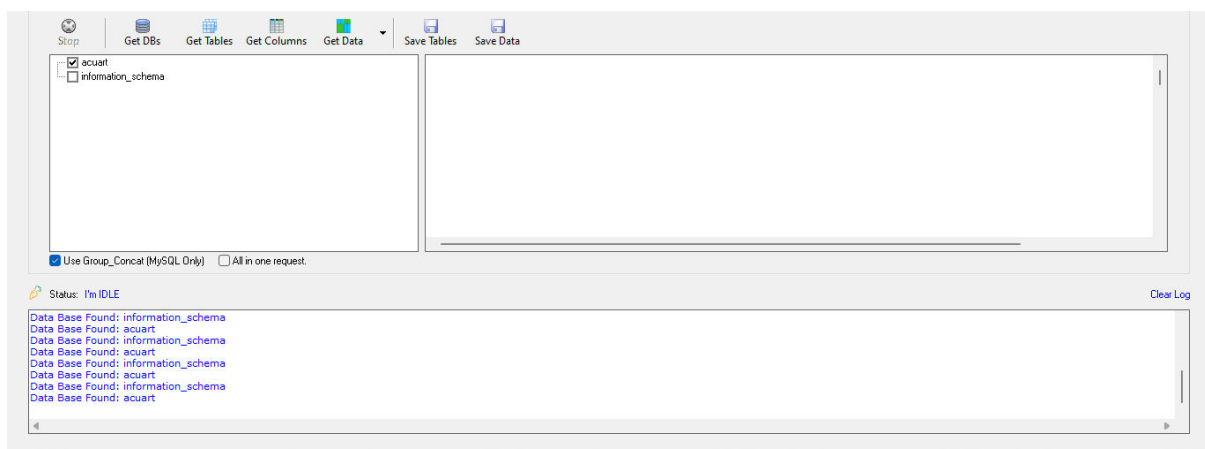
Click on the “*info*” tab. This will show you information about the victim’s system. We can see information like Host IP address, web server version etc.



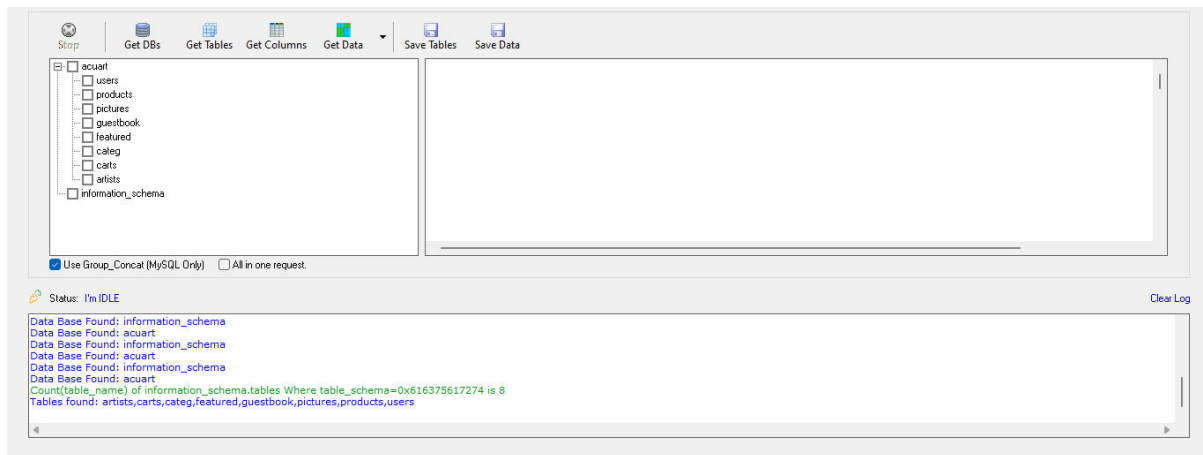
Click on the “*Tables*” tab.



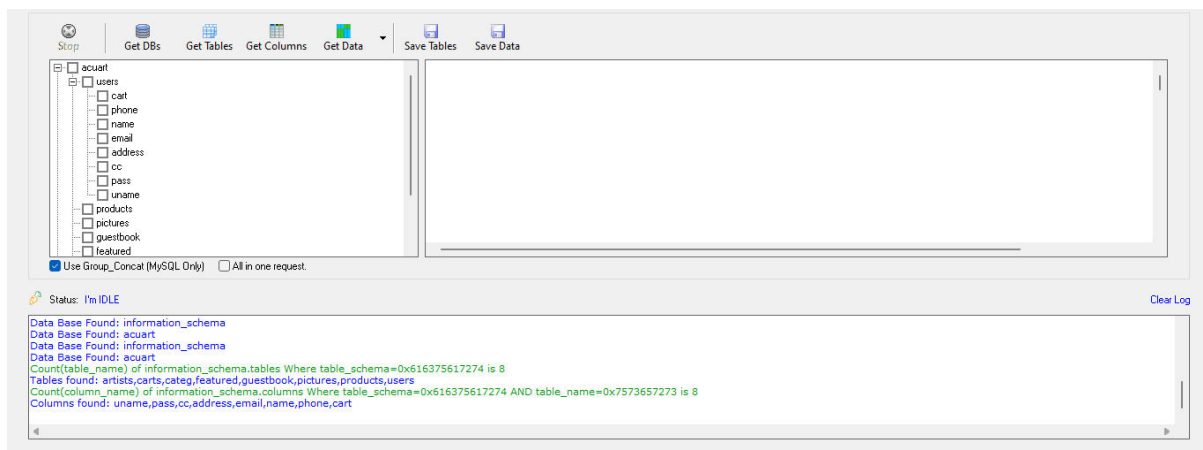
Click on “*Get DBs*” option. This will list all the databases as shown below.



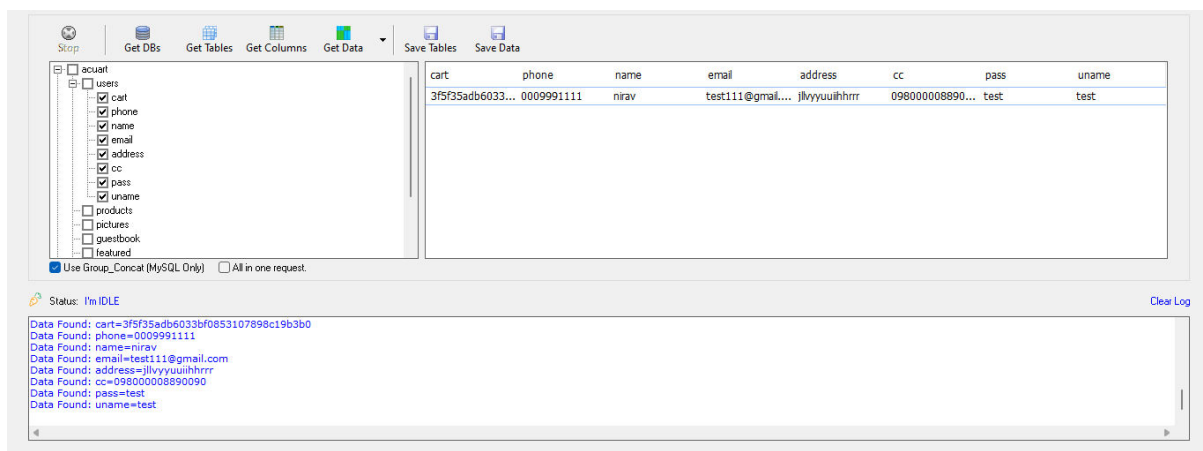
To get tables in a specific database, select the database and click on “*Get Tables*”. This will list all the tables present in the selected database. I selected database “*acuart*” here.



We can see that there is on table 'users' in our database 'acuart'. To get columns , select the table ' users' and click on “*Get Columns*”.



This will list all the columns in the table. We can see that we have five columns in the table 'users'. All the columns. It's time to dump the values of columns. Select the columns whose data we want to dump and click on “*Get data*”. Here I selected all the columns.



We got all the data including usernames, passwords, cart, phone, name, email, address, cc.

How to Prevent SQL Injection Attacks?

Preventing or mitigating SQL injection attacks is a lot about ensuring that none of the fields are vulnerable to invalid inputs and application execution. yours is manually impossible to actually to check every page and every application on the website, especially when updates are frequent and user-friendliness is the top priority. Nonetheless, security analysts and seasoned developers recommend a number of the subsequent points guarantee your database square measure well protected inside the confinement of the server.

1) Continuous Scanning and Penetration Testing:

The automated web application scanner has been the best choice to point out vulnerabilities within the web applications for quite some time now. Now, with SQL injections getting smarter in exploiting logical flaws, website security professionals should explore manual testing with the help of a security vendor.

They can authenticate user inputs against a set of rules for syntax, type, and length. It helps to audit application vulnerabilities discreetly so that you can patch the code before hackers exploit it to their advantage.

2) Restrict Privileges:

It is more of a database management function, but enforcing specific privileges to specific accounts helps prevent blind SQL injection attacks. Begin with no privileges account and move on to 'read-only', 'edit', 'delete' and similar privilege levels.

Minimizing privileges to the application will ensure that the attacker, who gets into the database through the application, cannot make unauthorized use of specific data.

3) Use Query Parameters:

Dynamic queries create a lot of troubles for security professionals. They have to deal with variable vulnerabilities in each application, which only gets graver with updates and changes. It is recommended that you prepare parameterized queries.

These queries are simple, easy to write, and only pass when each parameter in SQL code is clearly defined. This way, your info is supplied with weapons to differentiate between code and information inputs.

4) Instant Protection:

A majority of organizations fail the problems like outdated code, scarcity of resources to test and make changes, no knowledge of application security, and frequent updates in the application. For these, web application protection is the best solution.

A managed web application firewall can be deployed for immediate mitigation of such attacks. It contains custom policies to block any suspicious input and

deny information breach instantly. This way, you do not have to manually look for loopholes and mend problems afterward.

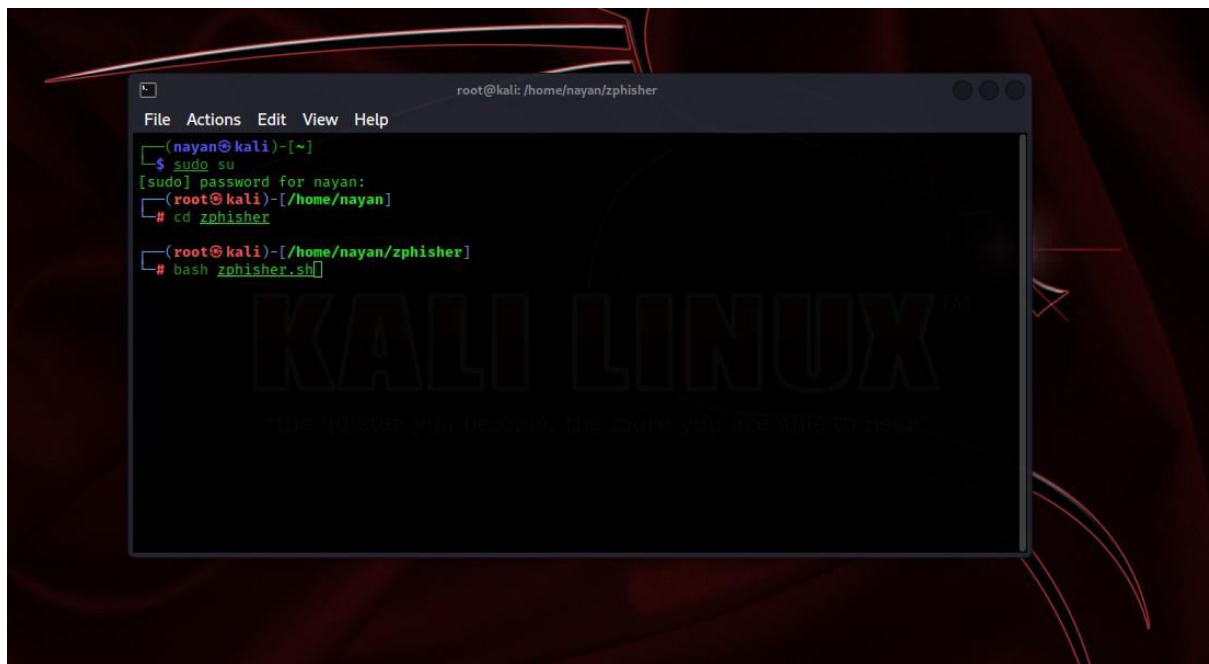
4. Clone a Facebook page and try to perform Desktop Phishing in your local machine and capture the credentials and write the document along with screenshots and suggest the solution to avoid from phishing.

=

Phishing may be a sort of social engineering attack often want to steal user data, including login credentials and Mastercard numbers. It occurs when attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, the recipient is then tricked into clicking a malicious link.

Here are some screenshots of process of cloning using zphisher in Kali Linux and the login page of Facebook:

Running the zphisher tool: -



```
root@kali: /home/nayan/zphisher
File Actions Edit View Help
(nayan@kali)-[~]
└─$ sudo su
[sudo] password for nayan:
(root@kali)-[/home/nayan]
# cd zphisher
(root@kali)-[/home/nayan/zphisher]
# bash zphisher.sh
```

The screenshot shows a terminal window with a dark background and red highlights. The window title is 'root@kali: /home/nayan/zphisher'. The terminal output shows the user 'nayan' running 'sudo su' to become root, then navigating to the 'zphisher' directory and running 'bash zphisher.sh'. The background of the terminal window features the 'KALI LINUX' logo and the tagline 'The quieter you become, the more you are able to hear.'

```
Kali linux x
root@kali: /home/nayan/zphisher

File Actions Edit View Help

ZPHISHER
Version : 2.3.4

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch          [21] DeviantArt
[02] Instagram     [12] Pinterest       [22] Badoo
[03] Google         [13] Snapchat         [23] Origin
[04] Microsoft     [14] LinkedIn         [24] DropBox
[05] Netflix       [15] Ebay            [25] Yahoo
[06] Paypal        [16] Quora           [26] Wordpress
[07] Steam         [17] Protonmail      [27] Yandex
[08] Twitter       [18] Spotify         [28] StackoverFlow
[09] Playstation  [19] Reddit          [29] VK
[10] Tiktok        [20] Adobe           [30] XBOX
[31] Mediafire     [32] Gitlab          [33] Github
[34] Discord

[99] About        [00] Exit

[-] Select an option : █
```

Setting server and port using ngrok: -

```
Kali linux x
root@kali: /home/nayan/zphisher

File Actions Edit View Help

ZPHISHER 2.3.4

[01] Localhost
[02] Ngrok.io [Account Needed]
[03] Cloudflared [Auto Detects]
[04] LocalXpose [NEW! Max 15Min]

[-] Select a port forwarding service : 2

[?] Do You Want A Custom Port [y/N]:

[-] Using Default Port 8080 ...

[-] Initializing ... ( http://127.0.0.1:8080 )

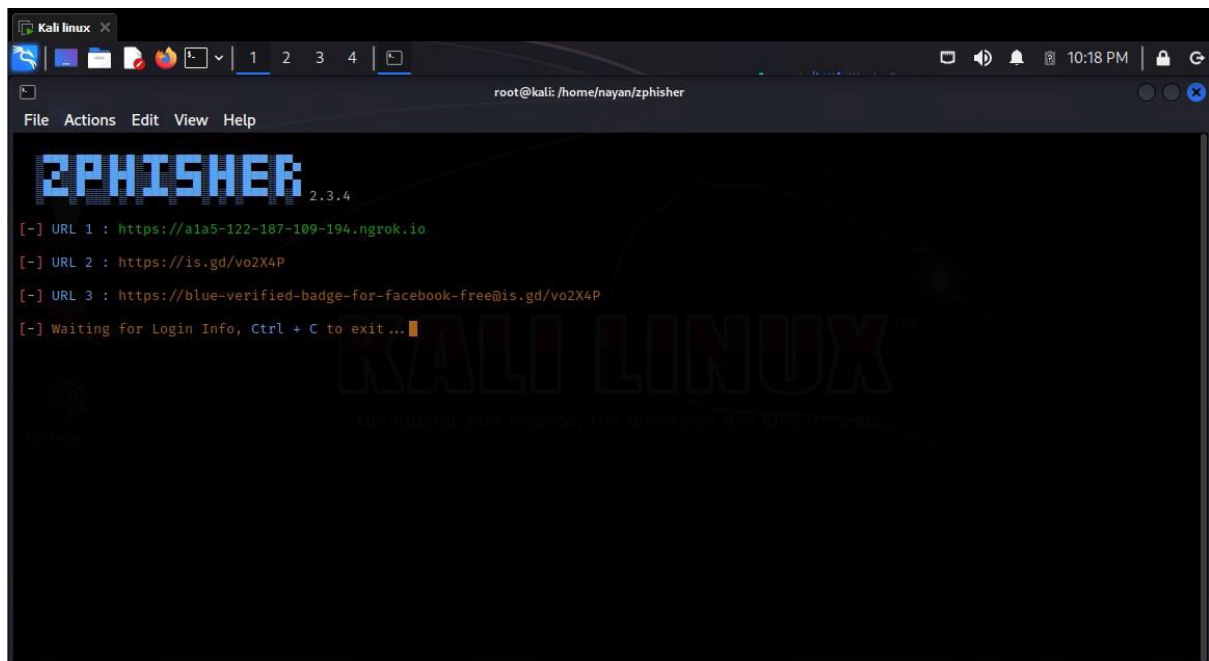
[-] Setting up server ...

[-] Starting PHP server ...

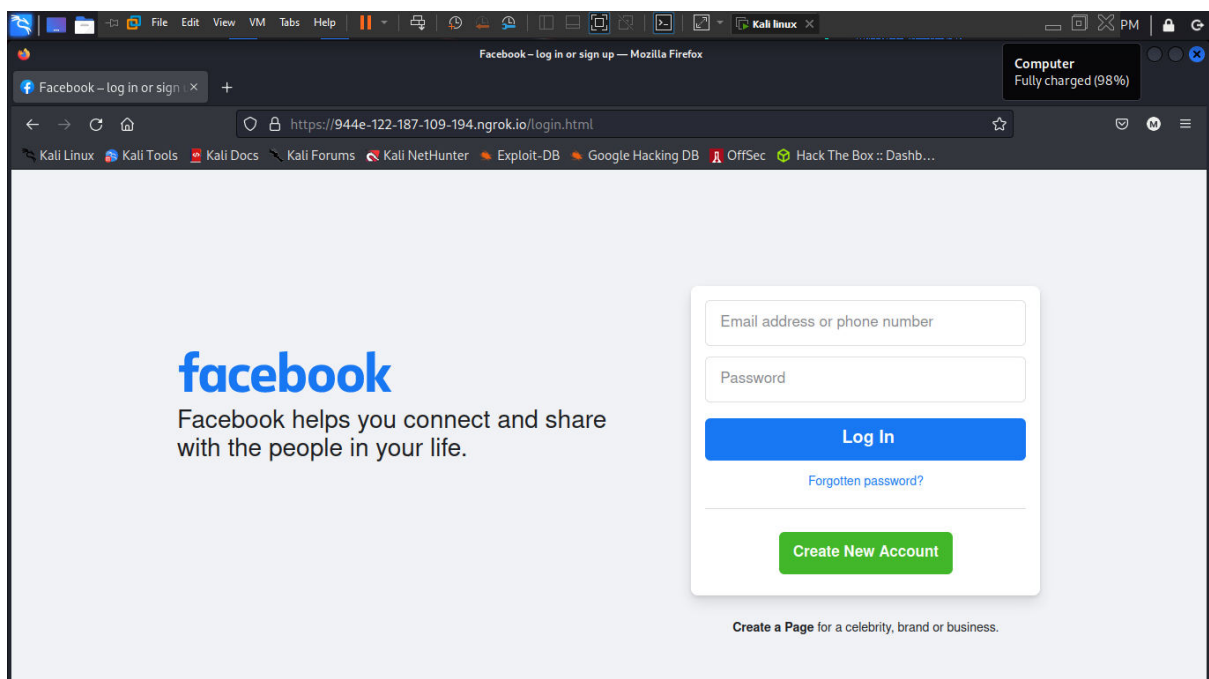
[-] Change Ngrok Server Region? [y/N]:

[-] Launching Ngrok ...
```

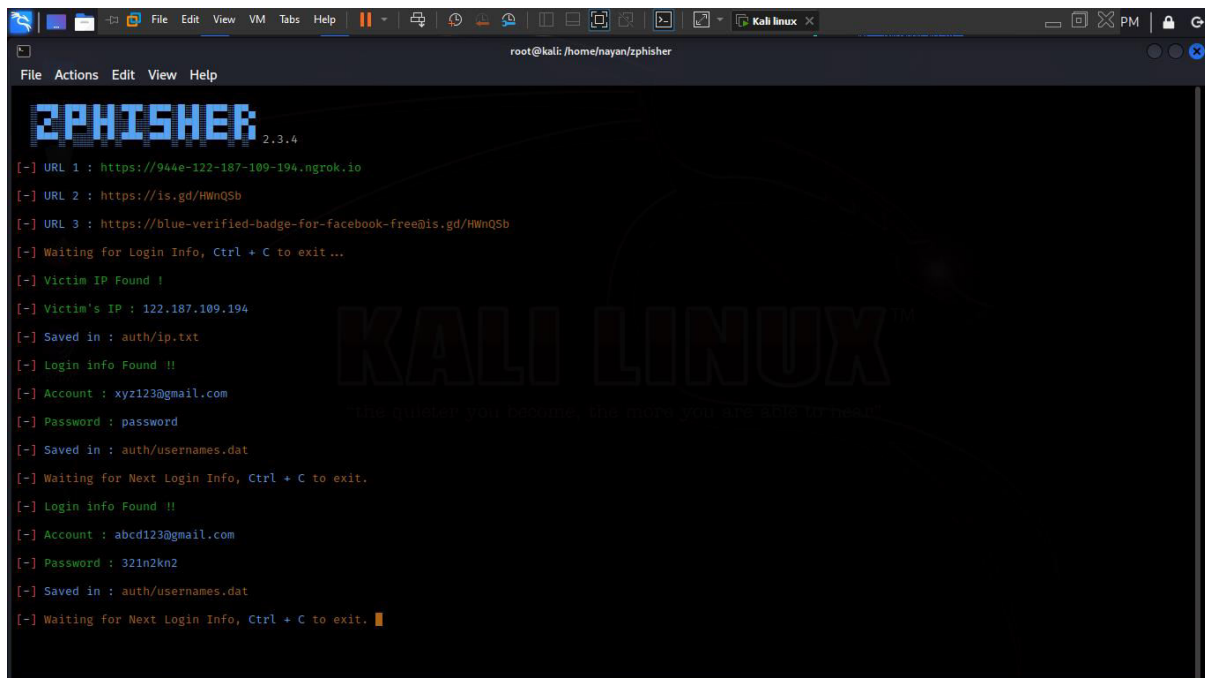
Clone Facebook login page link, which can be shared to any devices: -



Cloned Facebook login page: -



Captured credentials from this page: -



```
root@kali: /home/nayan/zphisher
File Actions Edit View Help
ZPHISHER 2.3.4
[-] URL 1 : https://944e-122-187-109-194.ngrok.io
[-] URL 2 : https://is.gd/HWnQsb
[-] URL 3 : https://blue-verified-badge-for-facebook-free@is.gd/HWnQsb
[-] Waiting for Login Info, Ctrl + C to exit ...
[-] Victim IP Found !
[-] Victim's IP : 122.187.109.194
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : xyz123@gmail.com
[-] Password : password
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.
[-] Login info Found !!
[-] Account : abcd123@gmail.com
[-] Password : 321n2kn2
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. █
```

Phishing scams are one of the most common methods of attack you're likely to come across. They are a hugely profitable attack method for cybercriminals, as thousands fall victim to them every year. Fortunately, due to their commonplace nature, phishing scams are avoidable if you know how to correctly identify and prevent them.

Here are 10 simple tips for 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. Sites 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 behaviour 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 action to prevent further damage.

THANK YOU