ESKRA

- THE INNOVATIVE SPARK -

CSE Dept. Campus Publication | RNGPIT | ISSUE:01| FEB 2020

It's all about Protect, Detect and respond.

Computer Science and Engineering

esKra

R.N.G.P.I.T.
CAMPUS PUBLICATION

Circulation:- ESKRA is published frequently by the students of Computer Science and Engineering department of R. N. G. Patel Institute of Technology, Bardoli-Navsari road, At:Isroli, Taluka:Bardoli-394620, District:Surat.

Phone: +91-9427527398, +91-9033707334, +91-9510427118 e-mail: eskra.cse@rngpit.ac.in

Editorial:- Unless otherwise stated articles,as well as images and description, reflect author's or firms opinion. Inclusion in ESKRA does not necessarily constitute endorsement by ESKRA or students of Computer Science and Engineering department of R.N.G.P.I.T. All submissions are subject to editing for style, clarity,and space.

Message from Editor-in-Chief

Dr. Madhavi B. Desai
(HoD, CSE, RNGPIT)
(Editor in Chief, Eskra)

Nowadays, security is one of the most important requirements for any computer device. Data being most valuable asset needs to be preserved and being a part of the computer department it is our priority to get the knowledge of it and spread it among others. This magazine gives us a brief knowledge about the cyber security, hacking, online frauds and safe internet usage. It will provide you with knowledge to use your device safely and keeping it secured from the potential threats.

Cloud is a widely used technique for computing in this generation of increasing data and to cope up with the expenses of the system which are not always feasible. To take the steps with this advancing technology and gain more knowledge about it, this magazine provides articles related to cloud computing, what is it, how it work, what services it provides and how people and use it. The more you explore this magazine, the interesting it gets and it will definitely boost your eagerness and willingness to learn more about this domain.

With this growing world, data handling and security, both are in great demand. This demand need to be managed efficiently. We have tried our best to impart our knowledge regarding these topics and enlighten with some current trends and technologies. So delve yourselves into the pool of information about cyber security and cloud computing.

Editorial

Mr. Dhaval J. Rana
(Asst. Professor CSE, RNGPIT)
(Faculty Advisor)

Mr. Ankit D. Prajapati
(Asst. Professor CSE, RNGPIT)
(Faculty Advisor)

Cyber Security is a way of protecting your data and identity from any potential threats or malware online. Online web portals are a new place to find any person's data with just few clicks and scrolls. Malicious activities such as Phishing, Hacking, Spamming, Packet Sniffing, etc. are used to get the user's data manipulatively. In today's world, it is almost impossible to keep one's information safe and sound. There are certain steps to protect user's information from getting it to hackers; also there are system softwares which protect user's information and privacy.

To use network and hardware resources online without having physical devices or servers, cloud computing is used. Cloud provides the feature of online servers which can be accessed from anywhere in the world with the help of internet service. These servers can help you run any application or provide storage facility. This is the main feature of cloud which reduces cost and system necessity for a company. Cloud computing provides us with many more facilities and services such as software, platform and infrastructure service.

Using cloud services along with online security is the new future. This magazine will provide you with ample knowledge about Cloud computing and safe online surfing which will enhance your skills. It will help brush up your brain with some cool technologies to lead the future.

About Authors

Bhagyesh Parmar

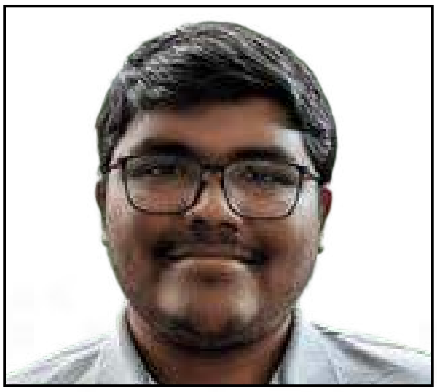
Bhagyesh is a ALUMNI student of CSE at R.N.G.P.I.T., whose goal is to obtain the title of Security Researcher. In addition, he provides assistance to his subordinates in the domain of cyber security. Considering what he knows about the matter his article demonstrates how Anonymity Tools are more effective at safeguarding data and maintaining privacy.

Article: "How to be completely Anonymous on the internet in 2020"

Kuldip Patel

Kuldip iis a ALUMNI student of CSE at R.N.G.P.I.T., His interest in Cyber Security led him to BountyCon 2020 presented by Facebook. He tried to cover every related topic of BountyCon 2020 in his article. Additionally, he explained how binary reverse engineering can be used to retrieve source code from a binary file.

Article: " BountyCon 2020 CTF — Anti What"

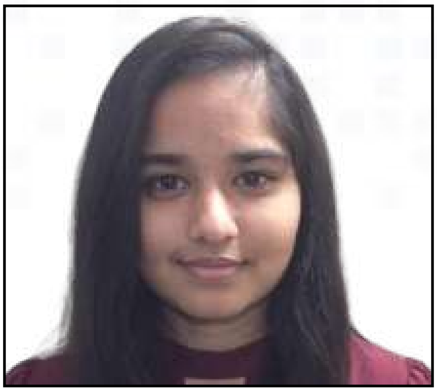


Anjali Biju

Anjali is a fourth-year CSE student at R.N.G.P.I.T. She wrote an article entitled "Invulnerability is a Delusion". She discussed a number of cybercrimes in her article, such as phishing, fraud, spam, and sniffing. In addition to the above-mentioned crimes, prevention methods were also be discussed.

Article: "Invulnerability is a Delusion"

About Authors



Palak Varu

Palak is a student at RNGPIT, pursuing a degree in Computer Science (CSE) in the fourth year. Her article's title 'Cloud computing- Let's be on cloud 9' is what would entice us to read her article. According to the article she wrote, she mentioned about Cloud Computing, its Benefits, Facts as well as the Future of Cloud Computing. It is likely that she will be able to pique our interest with this article and guide us in the process as well.

Article: "Cloud Computing- Let's be on cloud 9"

Parva Gurav

Parva is in his third year of computer science department at R.N.G.P.I.T., and in this article, he discussed about cloud connectivity and also explained cloud in terms of models like IaaS, PaaS, SaaS, and Cloud Types in greater detail. In order for every newbie to understand Cloud computing easily, he tried to explain it in the simplest terms possible.

Article: "Cloud Computing : The beginning"

Contents

1. How to be completely Anonymous on the internet in 2021

• *This Battle is for our online privacy…*

Figure-1.1 Online Privacy

A survey conducted last year discovered that 69% of data breaches were related to identity theft, and the tool that may be used to steal your identity is the internet. You can enjoy free Wi-Fi at coffee shops, at bars, at libraries, at airports, and other public places. It seems very dangerous to use free Wi-Fi in public places. And even if you are not using public Wi-Fi, you are still unsafe on your network. Let’s dig into this.

• *Top List of Firms Tracking You Online:*

During your regular browsing session, there are thousands of third-party trackers running and continuously trying to snatch your data or attack your device with malware. You are being tracked by companies even if you have never signed up for their services.

The names of the companies are

Figure-1.2 Companies [2]

Companies are everywhere, collecting and storing your data for their profits. Facebook is the most obvious example of information being collected via social media. Everything you post publicly or make some posts private is being stored and analyzed. They are not just having our social media data they are having our digital records too. They have records of everything, including where you shop, what you watch, where you go, what you search for on the internet, and what happens in your home. Even your physical movement is tracked by these giant companies.

They can create marketing strategies directly for you. The storage of this data is becoming a profitable enterprise on the planet. Always think before you post anything on social media. Also, it's almost impossible to know if user data is being misused within company bounds or in business-to-business interactions

Even if you use private mode on your browser, even a VPN can be easily identified and tracked. Your VPN provider knows the same information about you that your ISP does. A VPN only changes your IP address and makes it difficult for your ISP to see what you are visiting. VPNs are useful to bypass geo-blocking or throttling by your ISP, but they don't give you any anonymity. Modern trackers don't even need to know your IP address to track you and your identity.

Anonymity is not for criminals or any individual. It's important if you don't want a record of your online activities like your interests, preferences, searches, emails, messages, contacts, browsing history, and social media activity. Online anonymity gives you the highest level of privacy protection on the Internet. Most privacy tools are focused on encryption like VPN, and it is great, but encryption only protects the content, but in modern surveillance, it's the metadata that's the most valuable thing. Based on your metadata, whom you talk to when, where, for how long, how often on what device, and what software do you use?

In this article, you will learn what it means to be anonymous on the web, how to use essential anonymity tools, and you will learn some tips and habits to protect your online anonymity so nobody knows who you are. Let's talk about one by one those anonymity tools: **VPN, TOR, WHONIX, & TAILS.**

• *VPN:*

A Virtual Private Network (VPN) is an internet security service that allows users to access the Internet as though they were connected to a private network. A VPN creates a private "tunnel" from your device to the internet and hides your data by applying encryption techniques. Some of the most common reasons people use VPNs are to protect against snooping on public WiFi, to circumvent Internet censorship, or to connect to a business's internal network for remote work.

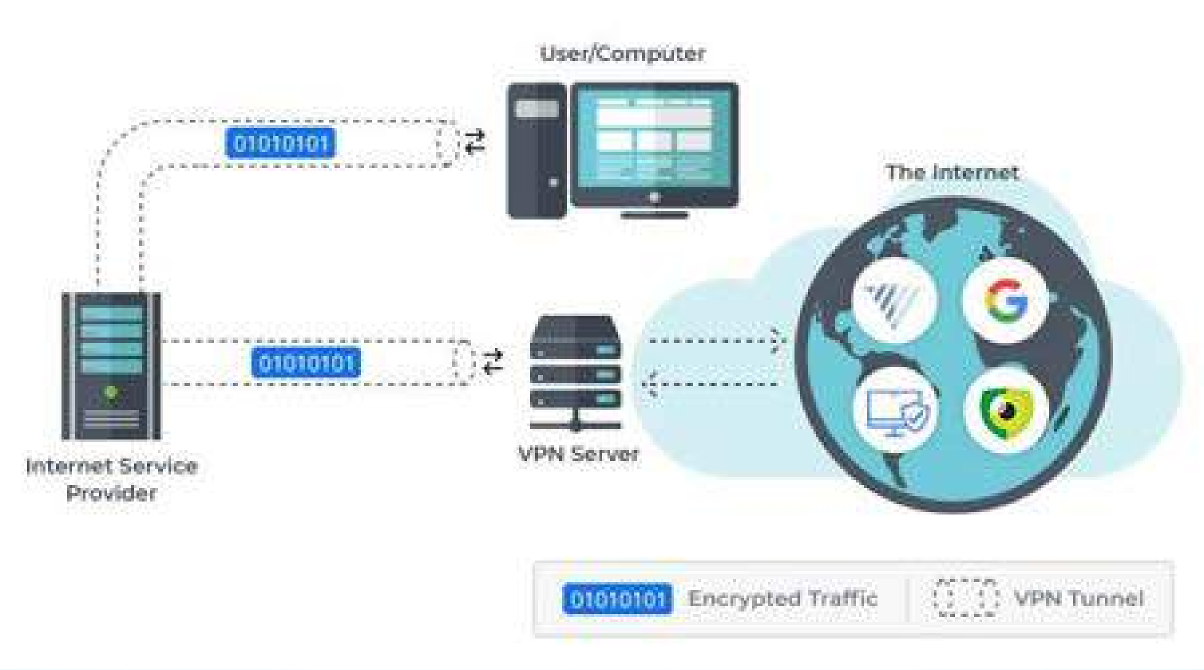


Figure-1.3 VPN [3]

Here are a few of the most common reasons for using a VPN.
1. Security when using public Wi-Fi
2. Remote work
3. Freedom from censorship in oppressive states
4. Location anonymity

What are the downsides of a VPN?

A VPN service provider doesn't guarantee your security. Users can only feel secure with a VPN if they trust the VPN provider. Many VPN providers could sell their users' personal information or leave them open to attacks. As a result, your communication is not entirely private and is being monitored by service providers.

• *TOR:*

The Onion Router (TOR) is a free and open-source software for enabling anonymous communication. It is designed to stop people from tracking your browsing habits, including government agencies and corporations. The name (The Onion Router) refers to the way that Tor protects your data by **wrapping it in multiple layers of encryption** like an onion.

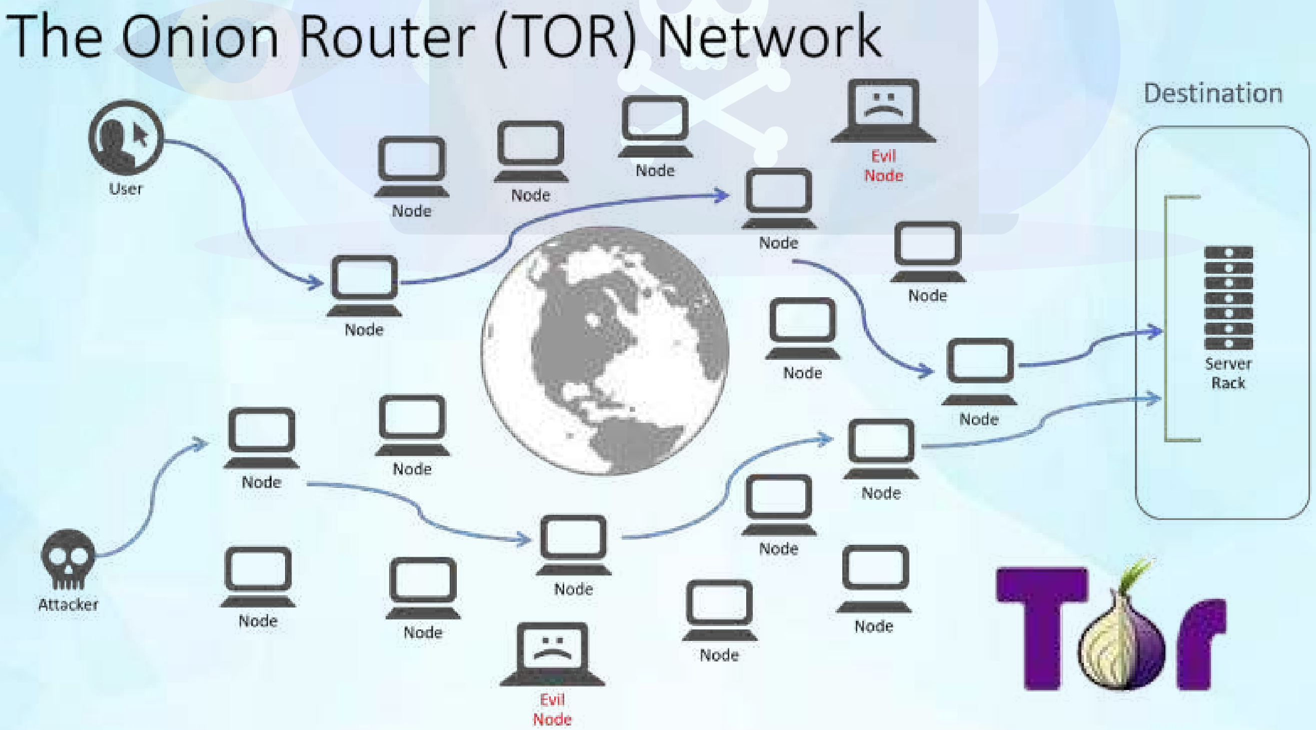


Figure-1.4 TOR [4]

• *What are the downsides of TORs?*

Slow speed: Since traffic goes through so many relays, there is often a delay in content. In particular, photos and videos have trouble loading even if you have fiber broadband.

Legal Trouble: -The Tor browser can be used by anyone. If someone is participating in illegal activity and you're the exit relay, the traffic will be tracked to you. Governments are also keeping a close eye on Tor users.

Many services directly block access to Tor or others. Some may allow access but you have to pass through CAPTCHA that is needed to enter the site.

Tor is running on your main operating system, and if you download something from the web and execute it on your host operating system, then it leads to compromising your data.

• *WHONIX OS:*

WHONIX is a Linux-based operating system made to run inside a virtual machine. That means you can keep your host system and run WHONIX inside it in a virtual environment. By default, every application you run inside it is connected to the TOR network. WHONIX is another security layer on top of the TOR browser that protects your main system. If a tracker or malware escapes the TOR browser, it will still be trapped inside the TOR network on your WHONIX machine, and it will not get access to your main host operating system or your real IP address. If you already know how to run VMware or VirtualBox, then it will be very easy for you to set up WHONIX OS.

Figure-1.5 WHONIX [5]

What are the downsides of the WHONIX OS?

1. It is complicated to set up and requires administrator or root privileges.
2. WHONIX needs modern hardware that supports visualization technologies.
3. If your host machine is ever compromised, all the stored personal information and your internet browsing activity could be easily discovered.

• *TAILS Linux OS (Incognito Live System)*

Figure-1.6 TAILS [6]

If your goal is to leave no trace of any activity, then choose Tails. Tail is a live operating system that runs separately from your host operating system. tails directly boot from a USB drive on a machine without the presence of the host operating system. The tails leave no trace on the device, and all traffic is routed through the Tor network, making the installation process even simpler than that of the WHONIX.

Tails have a lot of use cases, especially if you are using devices that you don't own, like in a library or on your friend's laptop. Tails give you an option to create persistent encrypted storage that is going to securely store files. If somebody obtains physical access to your USB drive, they will be able to see there is a tail persistent storage. They will not be able to decrypt your files. Tails reduce the attack surface over your host machine.

• *CONCLUSION:*

As we have seen, many techniques and tools are available to hide a person's identity while browsing the internet. We have also seen the pros and drawbacks of all the above-mentioned tools. And we can say that TAILS provides complete anonymity and security for data transmission, identity privacy, and physical security.

• *Some Important Tips:*

1. If you want to write an anonymous comment or blog post, don't directly type it into the website. Instead, write it into a notepad and then copy-paste it into the website because many scripts can easily identify your keystrokes in a similar way to the way you walk on the road. You should also change your writing style and speed as much as possible.
2. Clear your Internet browsing history after every use.
3. Always check the authenticity before you fill out any Google forms.
4. At least try one Linux distro before you die.
5. You can use the following extension to protect your privacy online Privacy Possum, Disable JavaScript, Privacy Badger, uBlock Origin, HTTPS Everywhere, and DuckDuckGo Privacy Essentials.
6. Privacytools.io protects your privacy against global mass surveillance. Here you find an alternative to your daily driver.
7. Mobile phone companies track your location by embedding spyware into their software, so the best alternative is the use of custom ROMs. The best thing about custom ROMs is that you can run them without any Google apps installed, giving you complete control over your phone. You can find more about custom ROMs on XDA Developers.

- Bhagyesh Parmar
(ALUMNI, CSE, R.N.G.P.I.T)

Image Source:-

[1] https://webcdn.bigpicture.one/kinsta-website/2021/02/18113833/Crunch-how-to-avoid-it-in-long-term-development-1024x576.png
[2] https://profit.pakistantoday.com.pk/wp-content/uploads/2021/07/logo2-696x464.jpg
[3] https://www.wpwhitesecurity.com/wp-content/uploads/2019/03/how-VPN-works.jpg
[4] https://miro.medium.com/max/828/1*bFE2V6Gz2bOgUefOONcniQ.png
[5] https://miro.medium.com/max/1400/1*MHwqc8p47c7ZupY5PnJUvw.jpeg
[6] https://miro.medium.com/max/1400/1*YnXRcX3zJEI5QmnlCaBQhQ.jpeg

2. BountyCon 2020 CTF-Anti What?

• *What is BountyCon?*

BountyCon is an invitation-only application security conference arranged by Facebook annually in Singapore for the BugBounty Community of the Asia-Pacific region and BountyCon2020 is the second edition of their conference.

Now, let us understand what is the significance of BugBounty.

• *What is BugBounty?*

A BUG BOUNTY is a reward (typically financial) provided by corporations to persons (outside the organization) who discover a bug or flaw (particularly those relating to security exploits and vulnerabilities) in software or an application.

To encourage bug reporting from the public and promote product improvement, several employers (businesses), particularly IT corporations, provide enticing Bug Bounty schemes.

> ***“ To encourage bug reporting from the public and promote product improvement, several employers (businesses), particularly IT corporations, provide enticing Bug Bounty schemes.”***

A BUG BOUNTY is a reward (typically financial) provided by corporations to persons (outside the organization) who discover a bug or flaw (particularly those relating to security exploits and vulnerabilities) in software or an application.

• *Challenge given in BountyCon 2020 CTF*

One of the challenges was Binary Reversing Challenge 'Anti What' which was the easier one. Challenge says that "What do you mean a debugger is already attached?" which means there could be an anti-debugging code, Anyways after downloading binary. I quickly fired up IDA Disassembler to disassemble it. Then I noticed the **main** function has a ptrace call which indicates anti-debugging.

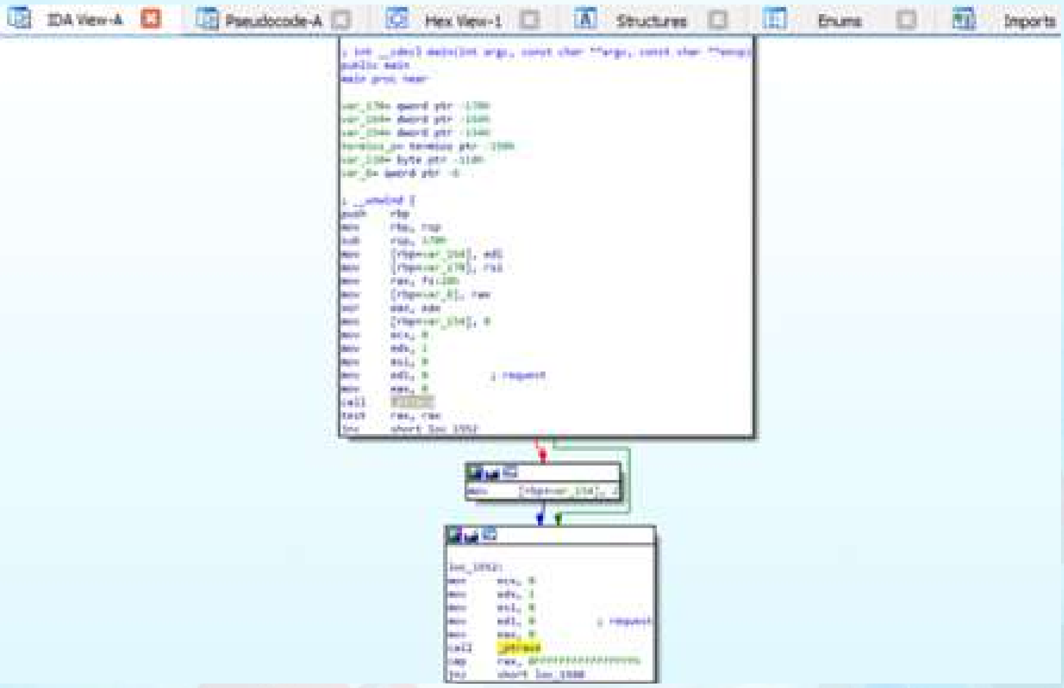
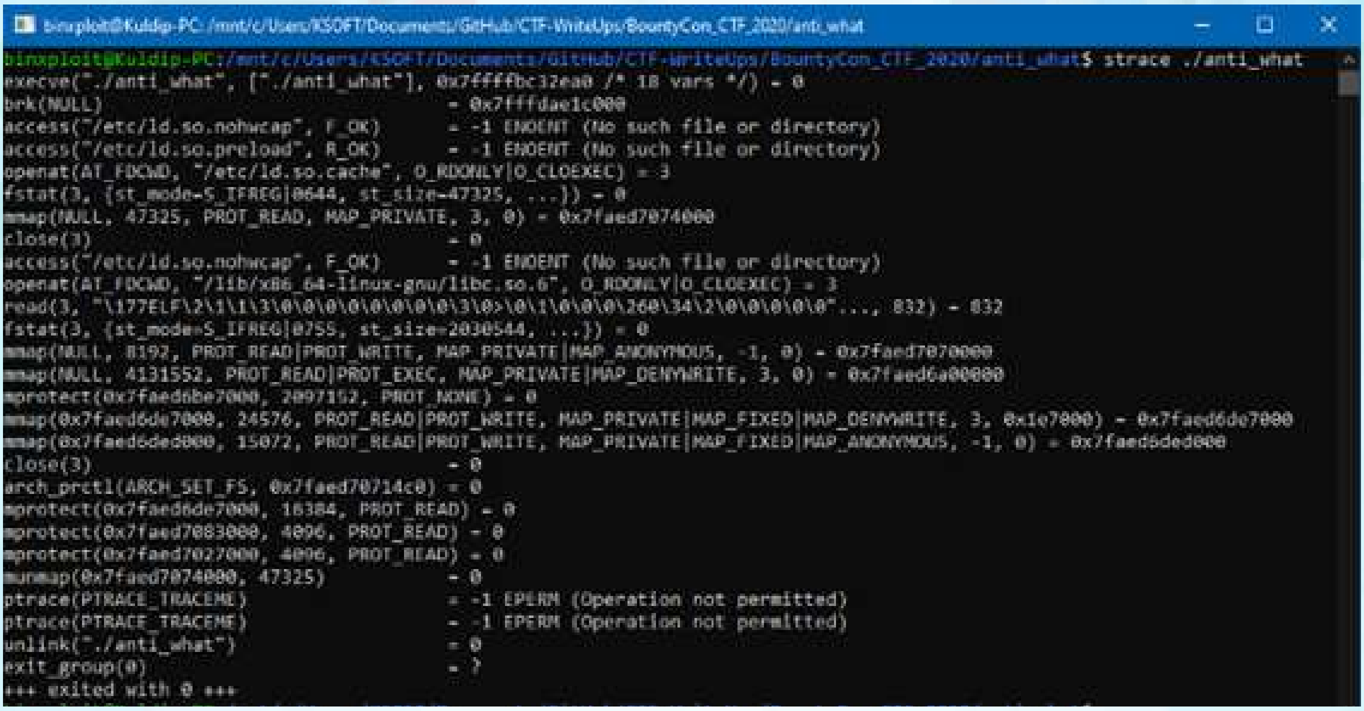


Figure-2.1 Main Function [1]

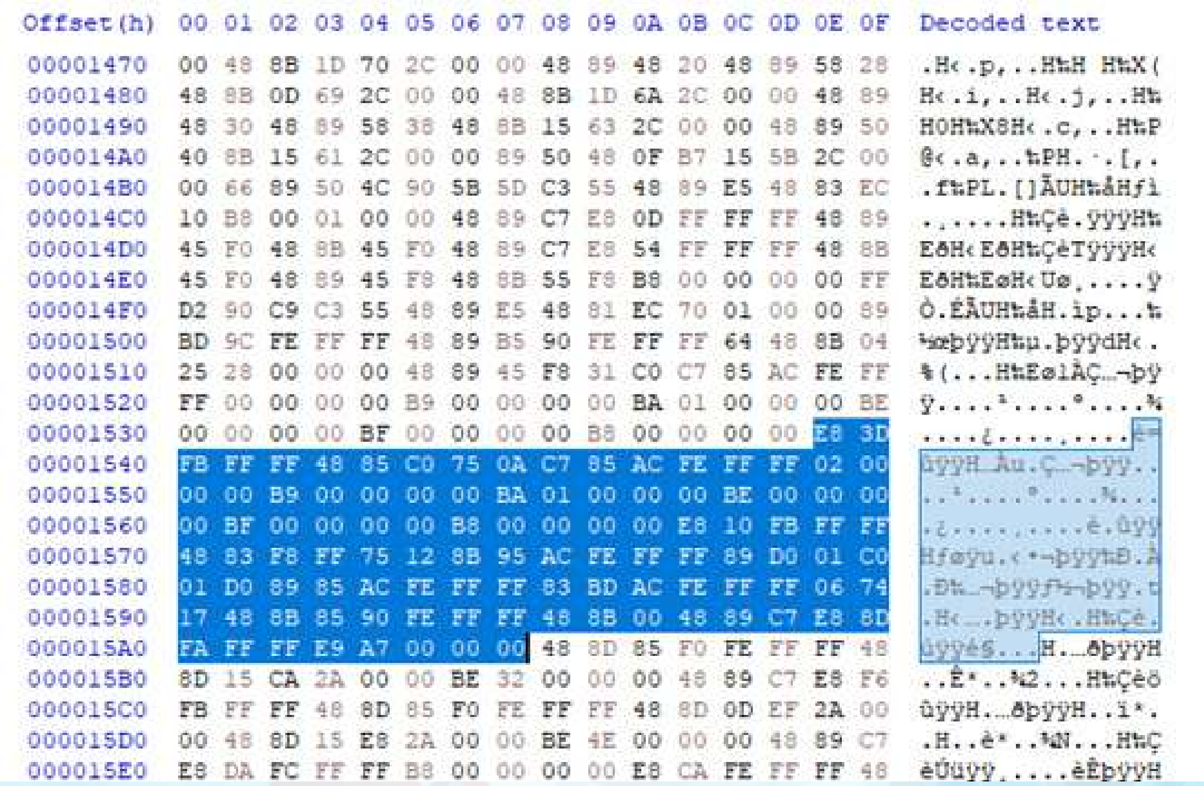


binxploit@Kuldip-PC: /mnt/c/Users/KSOFT/Documents/GitHub/CTF-WriteUps/BountyCon_CTF_2020/anti_what

```
binxploit@Kuldip-PC:/mnt/c/Users/KSOFT/Documents/GitHub/CTF-WriteUps/BountyCon_CTF_2020/anti_what$ strace ./anti_what
execve("./anti_what", ["./anti_what"], 0x7ffffbc32ea0 /* 18 vars */) = 0
brk(NULL)                               = 0x7fffdae1c000
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=47325, ...}) = 0
mmap(NULL, 47325, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7faed7074000
close(3)                                = 0
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\260\34\2\0\0\0\0\0"..., 832) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=2030544, ...}) = 0
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7faed7070000
mmap(NULL, 4131552, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7faed6a00000
mprotect(0x7faed6be7000, 2097152, PROT_NONE) = 0
mmap(0x7faed6de7000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x1e7000) = 0x7faed6de7000
mmap(0x7faed6ded000, 15072, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x7faed6ded000
close(3)                                = 0
arch_prctl(ARCH_SET_FS, 0x7faed70714c0) = 0
mprotect(0x7faed6de7000, 16384, PROT_READ) = 0
mprotect(0x7faed7083000, 4096, PROT_READ) = 0
mprotect(0x7faed7027000, 4096, PROT_READ) = 0
munmap(0x7faed7074000, 47325)           = 0
ptrace(PTRACE_TRACEME)                  = -1 EPERM (Operation not permitted)
ptrace(PTRACE_TRACEME)                  = -1 EPERM (Operation not permitted)
unlink("./anti_what")                   = 0
exit_group(0)                           = ?
+++ exited with 0 +++
```

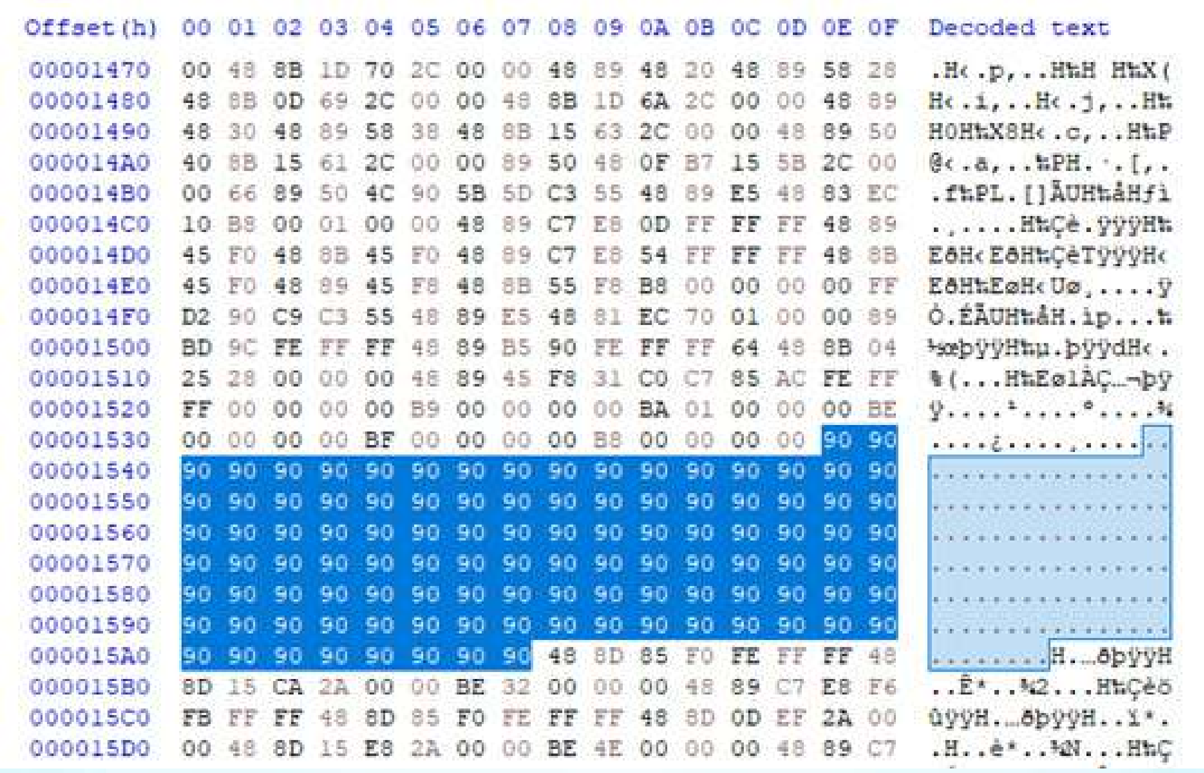
Figure-2.2 Strace Output [2]

So, when we try to debug this binary it simply close and delete(unlink) itself. Now we have to bypass it, Simplest way is a patch or modifies the binary. so We will replace from first _ptrace call to jmp before function **RC4_set_key** with NOP(No Operation) which is 0x90. I will use the HxD editor to modify it.



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00001470  00 48 8B 1D 70 2C 00 00 48 89 48 20 48 89 58 28  .H‹.p,..H‰H H‰X(
00001480  48 8B 0D 69 2C 00 00 48 8B 1D 6A 2C 00 00 48 89  H‹.i,..H‹.j,..H‰
00001490  48 30 48 89 58 38 48 8B 15 63 2C 00 00 48 89 50  H0H‰X8H‹.c,..H‰P
000014A0  40 8B 15 61 2C 00 00 89 50 48 0F B7 15 5B 2C 00  @‹.a,..‰PH.·.[,.
000014B0  00 66 89 50 4C 90 5B 5D C3 55 48 89 E5 48 83 EC  .f‰PL.[]ÃUH‰åHƒì
000014C0  10 B8 00 01 00 00 48 89 C7 E8 0D FF FF FF 48 89  .¸....H‰Çè.ÿÿÿH‰
000014D0  45 F0 48 8B 45 F0 48 89 C7 E8 54 FF FF FF 48 8B  EðH‹EðH‰ÇèTÿÿÿH‹
000014E0  45 F0 48 89 45 F8 48 8B 55 F8 B8 00 00 00 00 FF  EðH‰EøH‹Uø¸....ÿ
000014F0  D2 90 C9 C3 55 48 89 E5 48 81 EC 70 01 00 00 89  Ò.ÉÃUH‰åH.ìp...‰
00001500  BD 9C FE FF FF 48 89 B5 90 FE FF FF 64 48 8B 04  ½œþÿÿH‰µ.þÿÿdH‹.
00001510  25 28 00 00 00 48 89 45 F8 31 C0 C7 85 AC FE FF  %(...H‰Eø1ÀÇ…¬þÿ
00001520  FF 00 00 00 00 B9 00 00 00 00 BA 01 00 00 00 BE  ÿ....¹....º....¾
00001530  00 00 00 00 BF 00 00 00 00 B8 00 00 00 00 E8 3D  ....¿....¸....è=
00001540  FB FF FF 48 85 C0 75 0A C7 85 AC FE FF FF 02 00  ûÿÿH…Àu.Ç…¬þÿÿ..
00001550  00 00 B9 00 00 00 00 BA 01 00 00 00 BE 00 00 00  ..¹....º....¾...
00001560  00 BF 00 00 00 00 B8 00 00 00 00 E8 10 FB FF FF  .¿....¸....è.ûÿÿ
00001570  48 83 F8 FF 75 12 8B 95 AC FE FF FF 89 D0 01 C0  HƒøÿU.‹•¬þÿÿ‰Ð.À
00001580  01 D0 89 85 AC FE FF FF 83 BD AC FE FF FF 06 74  .Ð‰…¬þÿÿƒ½¬þÿÿ.t
00001590  17 48 8B 85 90 FE FF FF 48 8B 00 48 89 C7 E8 8D  .H‹….þÿÿH‹.H‰Çè.
000015A0  FA FF FF E9 A7 00 00 00 48 8D 85 F0 FE FF FF 48  úÿÿé§...H.…ðþÿÿH
000015B0  8D 15 CA 2A 00 00 BE 32 00 00 00 48 89 C7 E8 F6  ..Ê*..¾2...H‰Çèö
000015C0  FB FF FF 48 8D 85 F0 FE FF FF 48 8D 0D EF 2A 00  ûÿÿH.…ðþÿÿH..ï*.
000015D0  00 48 8D 15 E8 2A 00 00 BE 4E 00 00 00 48 89 C7  .H..è*..¾N...H‰Ç
000015E0  E8 DA FC FF FF B8 00 00 00 00 E8 CA FE FF FF 48  èÚüÿÿ¸....èÊþÿÿH
```

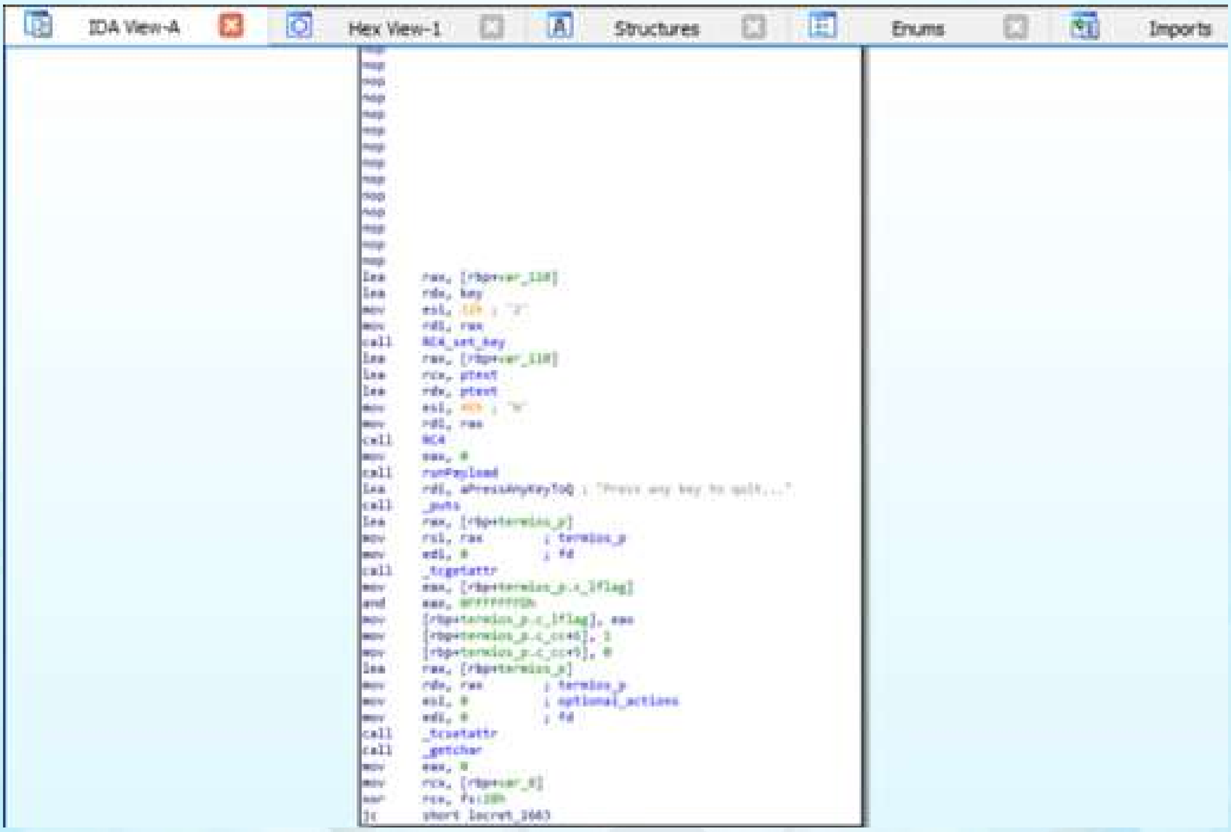
Figure-2.3 Before Patchig [3]



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00001470  00 48 8B 1D 70 2C 00 00 48 89 48 20 48 89 58 28  .H‹.p,..H‰H H‰X(
00001480  48 8B 0D 69 2C 00 00 48 8B 1D 6A 2C 00 00 48 89  H‹.i,..H‹.j,..H‰
00001490  48 30 48 89 58 38 48 8B 15 63 2C 00 00 48 89 50  H0H‰X8H‹.c,..H‰P
000014A0  40 8B 15 61 2C 00 00 89 50 48 0F B7 15 5B 2C 00  @‹.a,..‰PH.·.[,.
000014B0  00 66 89 50 4C 90 5B 5D C3 55 48 89 E5 48 83 EC  .f‰PL.[]ÃUH‰åHƒì
000014C0  10 B8 00 01 00 00 48 89 C7 E8 0D FF FF FF 48 89  .¸....H‰Çè.ÿÿÿH‰
000014D0  45 F0 48 8B 45 F0 48 89 C7 E8 54 FF FF FF 48 8B  EðH‹EðH‰ÇèTÿÿÿH‹
000014E0  45 F0 48 89 45 F8 48 8B 55 F8 B8 00 00 00 00 FF  EðH‰EøH‹Uø¸....ÿ
000014F0  D2 90 C9 C3 55 48 89 E5 48 81 EC 70 01 00 00 89  Ò.ÉÃUH‰åH.ìp...‰
00001500  BD 9C FE FF FF 48 89 B5 90 FE FF FF 64 48 8B 04  ½œþÿÿH‰µ.þÿÿdH‹.
00001510  25 28 00 00 00 48 89 45 F8 31 C0 C7 85 AC FE FF  %(...H‰Eø1ÀÇ…¬þÿ
00001520  FF 00 00 00 00 B9 00 00 00 00 BA 01 00 00 00 BE  ÿ....¹....º....¾
00001530  00 00 00 00 BF 00 00 00 00 B8 00 00 00 00 90 90  ....¿....¸......
00001540  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
00001550  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
00001560  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
00001570  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
00001580  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
00001590  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
000015A0  90 90 90 90 90 90 90 90 48 8D 85 F0 FE FF FF 48  ........H.…ðþÿÿH
000015B0  8D 15 CA 2A 00 00 BE 32 00 00 00 48 89 C7 E8 F6  ..Ê*..¾2...H‰Çèö
000015C0  FB FF FF 48 8D 85 F0 FE FF FF 48 8D 0D EF 2A 00  ûÿÿH.…ðþÿÿH..ï*.
000015D0  00 48 8D 15 E8 2A 00 00 BE 4E 00 00 00 48 89 C7  .H..è*..¾N...H‰Ç
```

Figure-2.4 After Patchig [4]

Now we can debug it without Problem and now if we check its IDA, a good NOP slide is created.

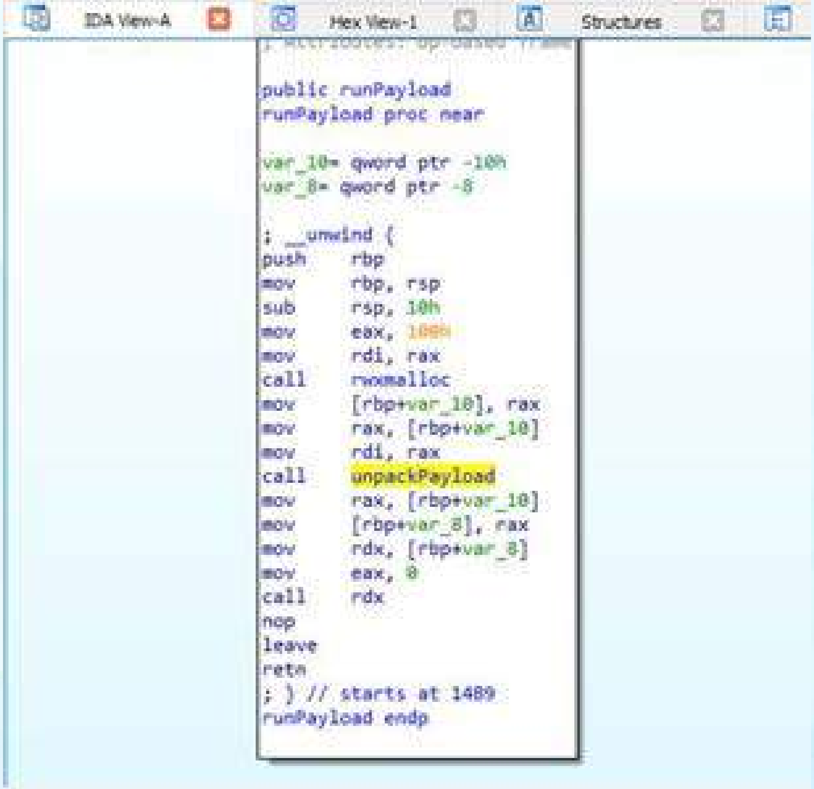


```
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
lea     rax, [rbp+var_110]
lea     rdx, key
mov     esi, [illegible] ; "[illegible]"
mov     rdi, rax
call    RC4_set_key
lea     rax, [rbp+var_110]
lea     rcx, ptext
lea     rdx, ptext
mov     esi, [illegible] ; "[illegible]"
mov     rdi, rax
call    RC4
mov     eax, 0
call    runPayload
lea     rdi, aPressAnyKeyToQ ; "Press any key to quit..."
call    _puts
lea     rax, [rbp+termios_p]
mov     rsi, rax        ; termios_p
mov     edi, 0          ; fd
call    _tcgetattr
mov     eax, [rbp+termios_p.c_lflag]
and     eax, 0FFFFFFF5h
mov     [rbp+termios_p.c_lflag], eax
mov     [rbp+termios_p.c_cc+6], 1
mov     [rbp+termios_p.c_cc+5], 0
lea     rax, [rbp+termios_p]
mov     rdx, rax        ; termios_p
mov     esi, 0          ; optional_actions
mov     edi, 0          ; fd
call    _tcsetattr
call    _getchar
mov     eax, 0
mov     rcx, [rbp+var_8]
xor     rcx, fs:28h
jz      short locret_1663
```

Figure-2.5 Pathed Binary with NOP Slide [5]

There is a function **RC4_set_key** which takes a global variable **key** as a parameter. which is an array of bytes. then it writes to memory location [rbp+0x110] from the first parameter, which looks like a c++ object. Now after that function **RC4** is called with the same object pointer and global variable **ptext** as a parameter and writes output to the location of ptext so replaces the encrypted text with decrypted one. Execution flow looks normal till now.

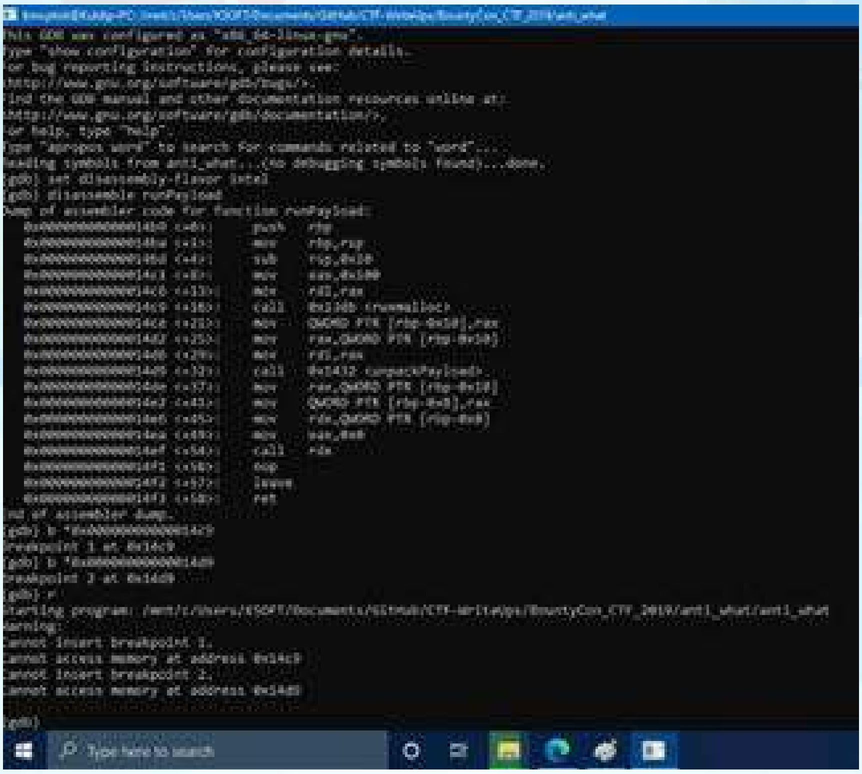
Then **runPayload** function is called, by looking into that function we can see that it dynamically allocates memory location into a heap by a custom wrapper function around mmap syscall named **rwxmalloc**. then one more function **unpackPayload** called, which jumbles bytes of plaintext ptext with bytes from other locations and writes the result onto the newly



```
; Attributes: bp-based frame

public runPayload
runPayload proc near

var_10= qword ptr -10h
var_8= qword ptr -8

; __unwind {
push    rbp
mov     rbp, rsp
sub     rsp, 10h
mov     eax, 100h
mov     rdi, rax
call    rwxmalloc
mov     [rbp+var_10], rax
mov     rax, [rbp+var_10]
mov     rdi, rax
call    unpackPayload
mov     rax, [rbp+var_10]
mov     [rbp+var_8], rax
mov     rdx, [rbp+var_8]
mov     eax, 0
call    rdx
nop
leave
retn
; } // starts at 14B9
runPayload endp
```

Figure-2.6 RunPayload function [6]

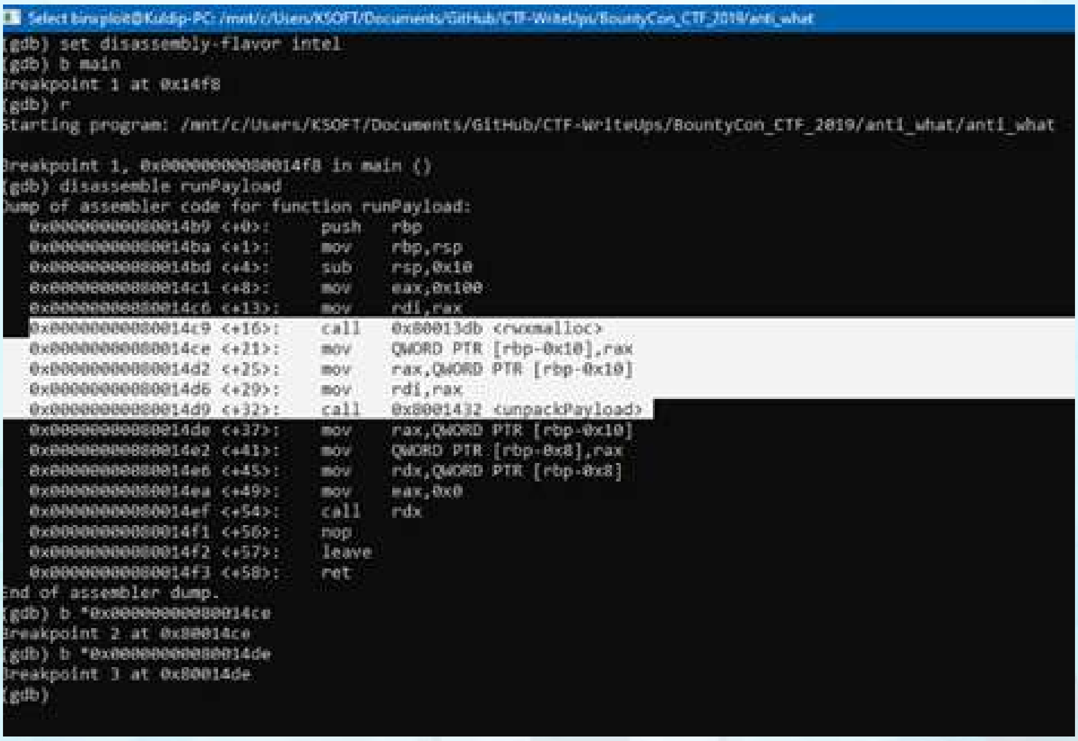
So It is clear that we have to use a debugger to look into that dynamically allocated memory address to find out the flag. So I started gdb on binary & set the first breakpoint after function **rwxmalloc** and 2nd after **unpackPayload.**



```
kmuyaol@Kuldip-PC: /mnt/c/Users/KSOFT/Documents/GitHub/CTF-WriteUps/BountyCon_CTF_2019/anti_what
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from anti_what...(no debugging symbols found)...done.
(gdb) set disassembly-flavor intel
(gdb) disassemble runPayload
Dump of assembler code for function runPayload:
   0x00000000000014b9 <+0>:     push   rbp
   0x00000000000014ba <+1>:     mov    rbp,rsp
   0x00000000000014bd <+4>:     sub    rsp,0x10
   0x00000000000014c1 <+8>:     mov    eax,0x100
   0x00000000000014c6 <+13>:    mov    rdi,rax
   0x00000000000014c9 <+16>:    call   0x12db <rwxmalloc>
   0x00000000000014ce <+21>:    mov    QWORD PTR [rbp-0x10],rax
   0x00000000000014d2 <+25>:    mov    rax,QWORD PTR [rbp-0x10]
   0x00000000000014d6 <+29>:    mov    rdi,rax
   0x00000000000014d9 <+32>:    call   0x1432 <unpackPayload>
   0x00000000000014de <+37>:    mov    rax,QWORD PTR [rbp-0x10]
   0x00000000000014e2 <+41>:    mov    QWORD PTR [rbp-0x8],rax
   0x00000000000014e6 <+45>:    mov    rdx,QWORD PTR [rbp-0x8]
   0x00000000000014ea <+49>:    mov    eax,0x0
   0x00000000000014ef <+54>:    call   rdx
   0x00000000000014f1 <+56>:    nop
   0x00000000000014f2 <+57>:    leave
   0x00000000000014f3 <+58>:    ret
End of assembler dump.
(gdb) b *0x00000000000014c9
Breakpoint 1 at 0x14c9
(gdb) b *0x00000000000014d9
Breakpoint 2 at 0x14d9
(gdb) r
Starting program: /mnt/c/Users/KSOFT/Documents/GitHub/CTF-WriteUps/BountyCon_CTF_2019/anti_what/anti_what
Warning:
Cannot insert breakpoint 1.
Cannot access memory at address 0x14c9
Cannot insert breakpoint 2.
Cannot access memory at address 0x14d9

(gdb)
```

Figure-2.7 Using a debugger for setting up breakpoints [7]

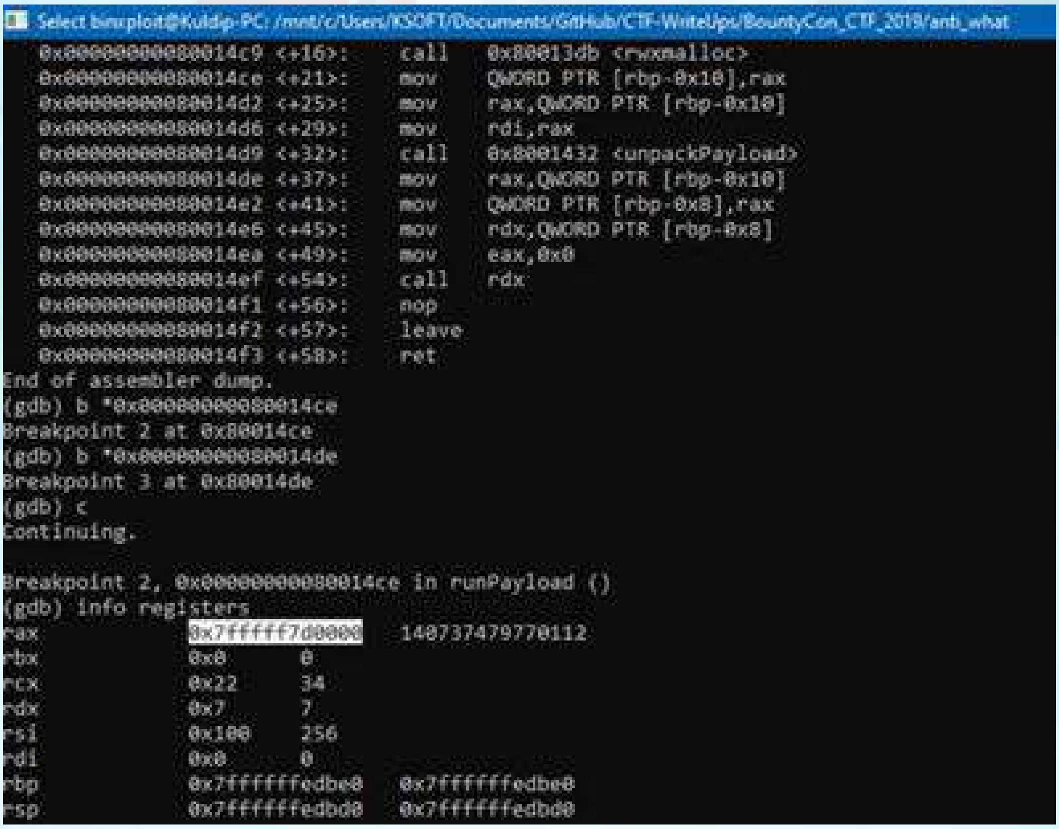
If we cannot insert a breakpoint then set a breakpoint on the main function first, then run binary which will stop execution at the main function now we can set a breakpoint to other instructions.



Select binxploit@Kuldip-PC: /mnt/c/Users/KSOFT/Documents/GitHub/CTF-WriteUps/BountyCon_CTF_2019/anti_what

```
(gdb) set disassembly-flavor intel
(gdb) b main
reakpoint 1 at 0x14f8
(gdb) r
tarting program: /mnt/c/Users/KSOFT/Documents/GitHub/CTF-WriteUps/BountyCon_CTF_2019/anti_what/anti_what

reakpoint 1, 0x00000000080014f8 in main ()
(gdb) disassemble runPayload
ump of assembler code for function runPayload:
   0x00000000080014b9 <+0>:     push   rbp
   0x00000000080014ba <+1>:     mov    rbp,rsp
   0x00000000080014bd <+4>:     sub    rsp,0x10
   0x00000000080014c1 <+8>:     mov    eax,0x100
   0x00000000080014c6 <+13>:    mov    rdi,rax
   0x00000000080014c9 <+16>:    call   0x80013db <rwxmalloc>
   0x00000000080014ce <+21>:    mov    QWORD PTR [rbp-0x10],rax
   0x00000000080014d2 <+25>:    mov    rax,QWORD PTR [rbp-0x10]
   0x00000000080014d6 <+29>:    mov    rdi,rax
   0x00000000080014d9 <+32>:    call   0x8001432 <unpackPayload>
   0x00000000080014de <+37>:    mov    rax,QWORD PTR [rbp-0x10]
   0x00000000080014e2 <+41>:    mov    QWORD PTR [rbp-0x8],rax
   0x00000000080014e6 <+45>:    mov    rdx,QWORD PTR [rbp-0x8]
   0x00000000080014ea <+49>:    mov    eax,0x0
   0x00000000080014ef <+54>:    call   rdx
   0x00000000080014f1 <+56>:    nop
   0x00000000080014f2 <+57>:    leave
   0x00000000080014f3 <+58>:    ret
nd of assembler dump.
(gdb) b *0x00000000080014ce
reakpoint 2 at 0x80014ce
(gdb) b *0x00000000080014de
reakpoint 3 at 0x80014de
(gdb)
```

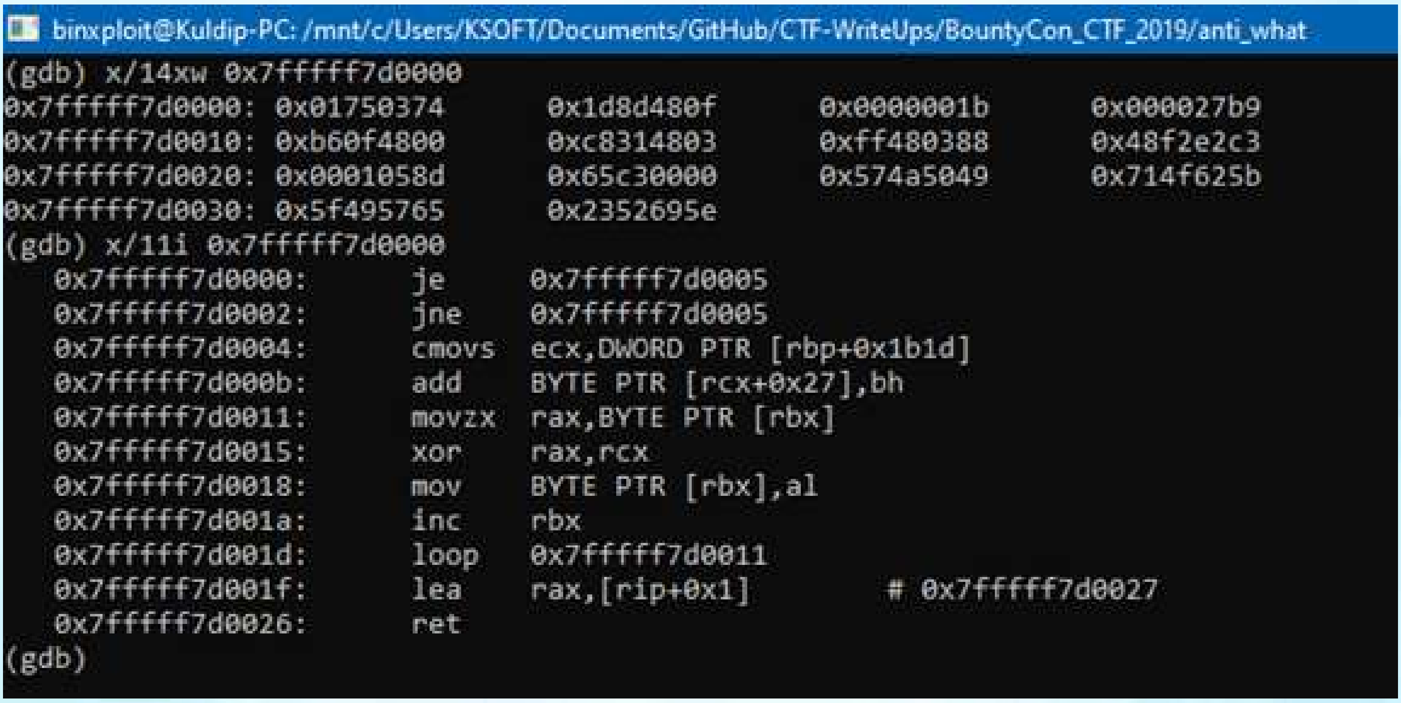
Figure-2.8 Breakpoint set [8]



Select binxploit@Kuldip-PC: /mnt/c/Users/KSOFT/Documents/GitHub/CTF-WriteUps/BountyCon_CTF_2019/anti_what

```
   0x00000000080014c9 <+16>:    call   0x80013db <rwxmalloc>
   0x00000000080014ce <+21>:    mov    QWORD PTR [rbp-0x10],rax
   0x00000000080014d2 <+25>:    mov    rax,QWORD PTR [rbp-0x10]
   0x00000000080014d6 <+29>:    mov    rdi,rax
   0x00000000080014d9 <+32>:    call   0x8001432 <unpackPayload>
   0x00000000080014de <+37>:    mov    rax,QWORD PTR [rbp-0x10]
   0x00000000080014e2 <+41>:    mov    QWORD PTR [rbp-0x8],rax
   0x00000000080014e6 <+45>:    mov    rdx,QWORD PTR [rbp-0x8]
   0x00000000080014ea <+49>:    mov    eax,0x0
   0x00000000080014ef <+54>:    call   rdx
   0x00000000080014f1 <+56>:    nop
   0x00000000080014f2 <+57>:    leave
   0x00000000080014f3 <+58>:    ret
End of assembler dump.
(gdb) b *0x00000000080014ce
Breakpoint 2 at 0x80014ce
(gdb) b *0x00000000080014de
Breakpoint 3 at 0x80014de
(gdb) c
Continuing.

Breakpoint 2, 0x00000000080014ce in runPayload ()
(gdb) info registers
rax            0x7ffff7d00000   140737479770112
rbx            0x0      0
rcx            0x22     34
rdx            0x7      7
rsi            0x100    256
rdi            0x0      0
rbp            0x7ffffffedbe0   0x7ffffffedbe0
rsp            0x7ffffffedbd0   0x7ffffffedbd0
```

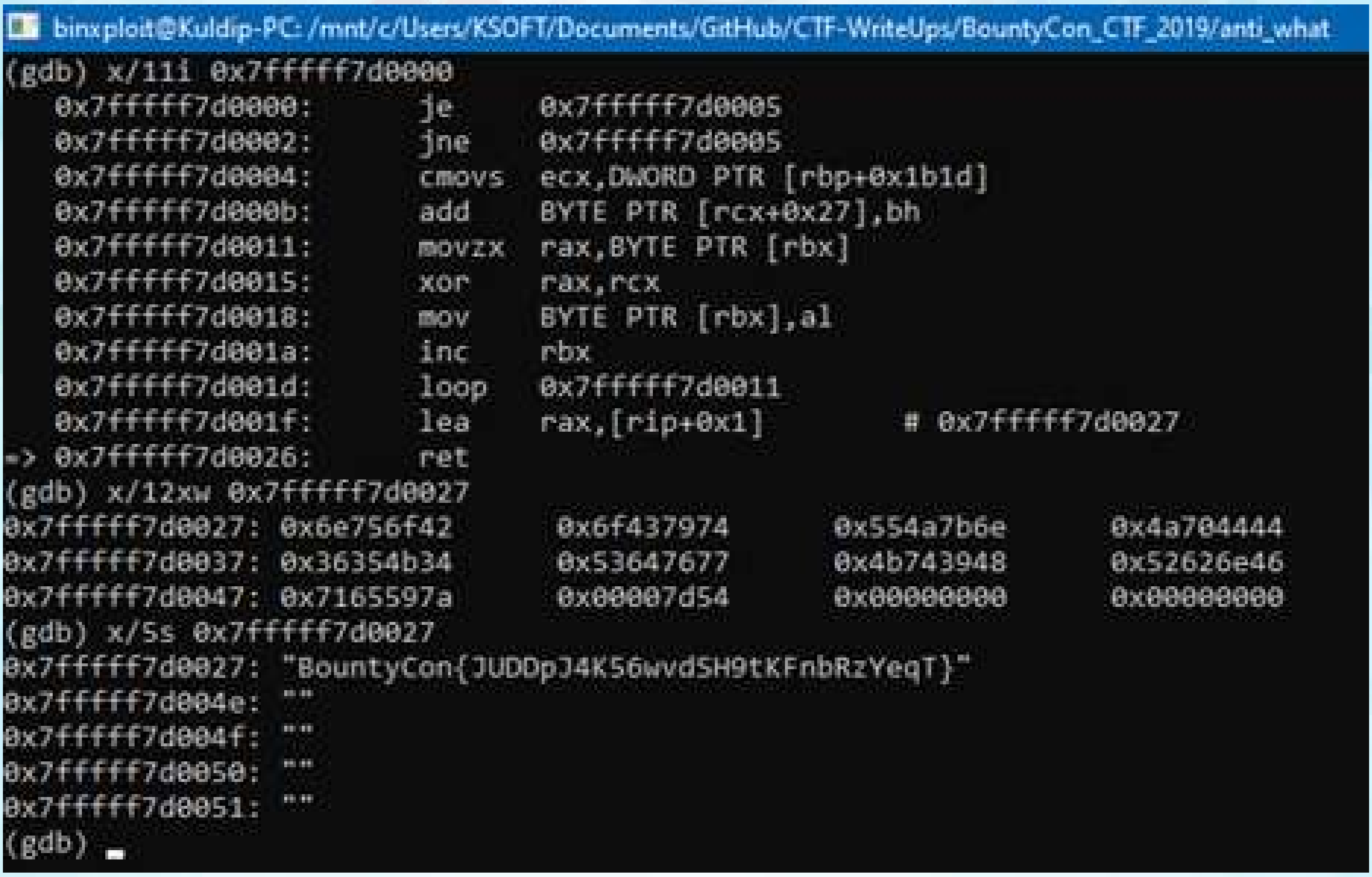
Figure-2.9 Allocated Memory Address Returned by rwxmalloc [9]



```
binxploit@Kuldip-PC: /mnt/c/Users/KSOFT/Documents/GitHub/CTF-WriteUps/BountyCon_CTF_2019/anti_what
(gdb) x/14xw 0x7fffff7d0000
0x7fffff7d0000: 0x01750374      0x1d8d480f      0x0000001b      0x000027b9
0x7fffff7d0010: 0xb60f4800      0xc8314803      0xff480388      0x48f2e2c3
0x7fffff7d0020: 0x0001058d      0x65c30000      0x574a5049      0x714f625b
0x7fffff7d0030: 0x5f495765      0x2352695e
(gdb) x/11i 0x7fffff7d0000
   0x7fffff7d0000:      je     0x7fffff7d0005
   0x7fffff7d0002:      jne    0x7fffff7d0005
   0x7fffff7d0004:      cmovs  ecx,DWORD PTR [rbp+0x1b1d]
   0x7fffff7d000b:      add    BYTE PTR [rcx+0x27],bh
   0x7fffff7d0011:      movzx  rax,BYTE PTR [rbx]
   0x7fffff7d0015:      xor    rax,rcx
   0x7fffff7d0018:      mov    BYTE PTR [rbx],al
   0x7fffff7d001a:      inc    rbx
   0x7fffff7d001d:      loop   0x7fffff7d0011
   0x7fffff7d001f:      lea    rax,[rip+0x1]        # 0x7fffff7d0027
   0x7fffff7d0026:      ret
(gdb)
```

Figure-2.10 Machine instructions unpacked [10]

It unpacks raw machine instructions and calls instruction transfers Program Counter to that address. These instructions perform an XOR operation to decrypt data. So we can now quickly set a breakpoint on ret instruction and look into the returned address & we have successfully found the Flag.



```
binxploit@Kuldip-PC: /mnt/c/Users/KSOFT/Documents/GitHub/CTF-WriteUps/BountyCon_CTF_2019/anti_what
(gdb) x/11i 0x7fffff7d0000
   0x7fffff7d0000:      je     0x7fffff7d0005
   0x7fffff7d0002:      jne    0x7fffff7d0005
   0x7fffff7d0004:      cmovs  ecx,DWORD PTR [rbp+0x1b1d]
   0x7fffff7d000b:      add    BYTE PTR [rcx+0x27],bh
   0x7fffff7d0011:      movzx  rax,BYTE PTR [rbx]
   0x7fffff7d0015:      xor    rax,rcx
   0x7fffff7d0018:      mov    BYTE PTR [rbx],al
   0x7fffff7d001a:      inc    rbx
   0x7fffff7d001d:      loop   0x7fffff7d0011
   0x7fffff7d001f:      lea    rax,[rip+0x1]        # 0x7fffff7d0027
=> 0x7fffff7d0026:      ret
(gdb) x/12xw 0x7fffff7d0027
0x7fffff7d0027: 0x6e756f42      0x6f437974      0x554a7b6e      0x4a704444
0x7fffff7d0037: 0x36354b34      0x53647677      0x4b743948      0x52626e46
0x7fffff7d0047: 0x7165597a      0x00007d54      0x00000000      0x00000000
(gdb) x/5s 0x7fffff7d0027
0x7fffff7d0027: "BountyCon{JUDDpJ4K56wvdSH9tKFnbRzYeqT}"
0x7fffff7d004e: ""
0x7fffff7d004f: ""
0x7fffff7d0050: ""
0x7fffff7d0051: ""
(gdb) _
```

Figure-2.11 Flag revealed at returned address [11]

I hope you have learnt something from this. Thanks for reading & happy learning!

-Kuldip Patel
(ALUMNI, CSE, R.N.G.P.I.T)

Image Source:-

[1] https://miro.medium.com/max/720/1*E_Gm6NsbUGJox-psVp3LFg.png

[2] https://miro.medium.com/max/720/1*oF-4tVcYZ-lXcp2SqOXl6A.png

[3] https://miro.medium.com/max/640/1*moEv-Z8xa8qGGIPCaQRB7g.png

[4] https://miro.medium.com/max/720/1*jSdGKQM7wbHSLJOEq3bmmw.png

[5] https://miro.medium.com/max/720/1*sP6VAJDJF9RpctoASSngiA.png

[6] https://miro.medium.com/max/640/1*7QAaOgUPSoLpK15rRqR4Ew.png

[7] https://miro.medium.com/max/720/1*wQAEp5D9N58aBUzFb_WDZA.png

[8] https://miro.medium.com/max/720/1*hcczjWtFiXJWs22rFajmZw.png

[9] https://miro.medium.com/max/720/1*Y82s7d0ylNK_5wbGn3kZeQ.png

[10] https://miro.medium.com/max/720/1*ZiJF92Nkpky0Sdimu0QYvQ.png

[11] https://miro.medium.com/max/640/1*jbJ0ebzbyELGLKcax684uQ.png

3. Cloud Computing
Let's be on cloud 9

Figure-3.1 Cloud Computing [1]

• *Basic Interesting Facts about Digital Data:*

In 2019, there were 4.4 Zettabytes (ZB) of data in the digital world. By the end of this year, it will reach 44 ZB and will grow to 174 ZB by 2025. And to be more clear let's analyze how much is 1 Zettabyte.

- A gigabyte is 1,024 megabytes
- A terabyte is 1,024 gigabytes
- A petabyte is 1,024 terabytes
- An exabyte is 1,024 petabytes
- A zettabyte is 1,024 exabytes (1,125,899,910,000,000 megabytes!)

• *What is Cloud Computing?*

Cloud computing is a growing area of computer technology where data and programs are stored on servers that are accessed over the internet instead of on a computer's hard drive or local server. Cloud computing can also be referred to as Internet-based computing, or (IBC).

• *How does Cloud Computing work?*

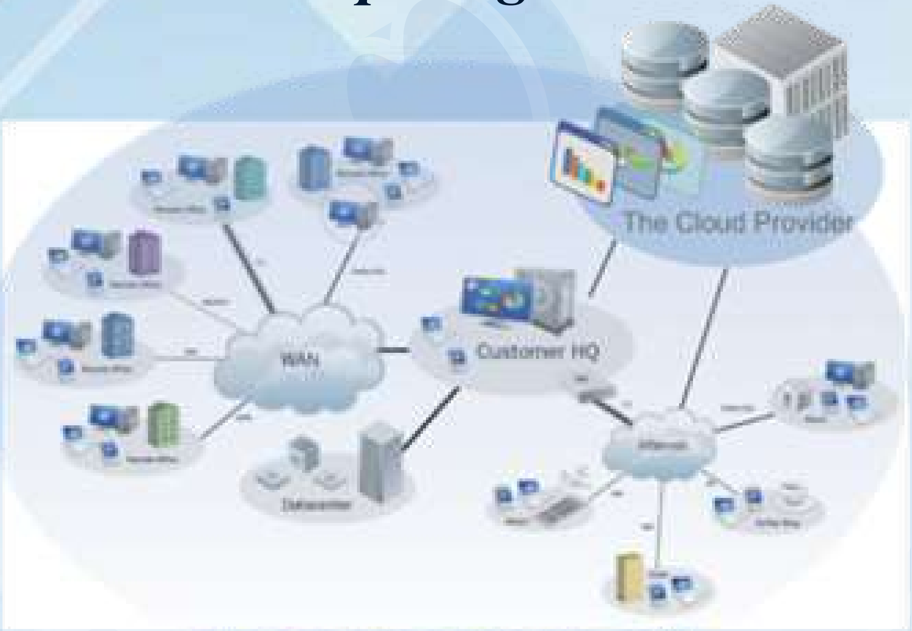


Figure-3.2 Cloud Computing Work [2]

• The way cloud computing operates is by allowing users to upload and download the stored data. The information is available to us everywhere. The initial amount of storage will be provided to a user at a very low cost.

• There are two different cloud computing systems. The first is the front end, whereas the second is the back end. An internet connection is used to establish a connection between the two endpoints.

• The system is the cloud's back end, while a computer user or client is its front end. The application that is used to access the cloud system is on the system's front end. The cloud is made up of numerous computers, pieces of hardware, servers, and data storage systems on the backend.

• The central server is in charge of all these features and operations. The main server makes sure that everything functions flawlessly and without a hitch. It is accomplished with the use of middleware, a piece of software that also enables network computers to connect.

• *Benefits:*

1. Scalability: This scaling may be completed rapidly, which is excellent for a business that is expanding swiftly. Without spending money on physical components, a company can easily extend its cloud-based infrastructure as demand rises.

2. Cost: The majority of firms experience cost reductions in employing cloud services right away, even if the initial migration of current infrastructure may need planning, resources, and time. Businesses never pay for more than they need since cloud computing resources may be scaled to meet their needs. Pay-as-you-go is the method used.

3. Speed: Software development has sped up thanks to cloud computing, which has also reduced costs and saved time. With a few mouse clicks, a new development environment or virtual machine may be set up on a cloud in a matter of seconds. In a conventional data center, you would need to buy, set up, and maintain all the necessary gear.

4. Security: Cybersecurity is a big concern for any business. Data breaches can damage an enterprise's revenue, reputation, and even its clients. Cloud services resolve this by managing permissions and access to the services and resources they provide. For example, you could restrict access to an important file to a specific set of users.

5. Productivity: Cloud computing improves productivity in many ways:

- As we mentioned before, by removing the requirement for infrastructure maintenance, your IT personnel can concentrate on duties that are related to your company's operations.
- It speeds up and simplifies the processes of software creation, testing, and deployment. It provides a worldwide network of services that can be easily accessed by remote employees.

6. Maintenance: The system maintenance is handled by cloud service providers, and access is provided via APIs that do not require application installations onto PCs, thereby lowering the need for maintenance. The cloud provider carries out a variety of duties to guarantee the effective use of cloud resources, as depicted in the diagram below.

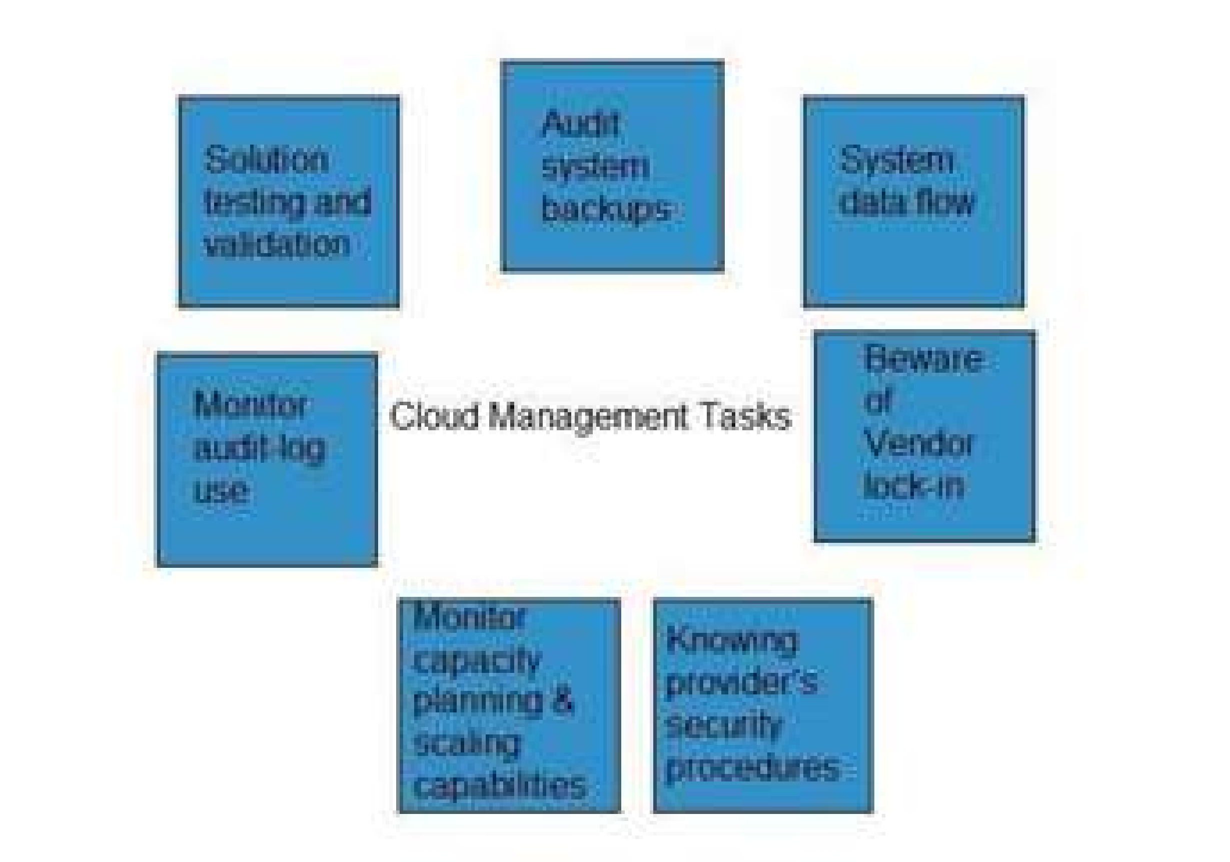

Solution testing and validation
Audit system backups
System data flow
Monitor audit-log use
Cloud Management Tasks
Beware of Vendor lock-in
Monitor capacity planning & scaling capabilities
Knowing provider's security procedures

Figure-3.3 Cloud Management Task [3]

• *Basic Consumer Cloud Services:*

Cloud computing is the foundation of a huge variety of services. That includes commercial services that enable big businesses to host all of their data and run all of their apps in the cloud, as well as consumer services like Gmail or the cloud backup of the images on your smartphone. In addition to many other businesses, Netflix depends on cloud computing technologies to run its video streaming service and other business operations.

• *Types Of Cloud:*

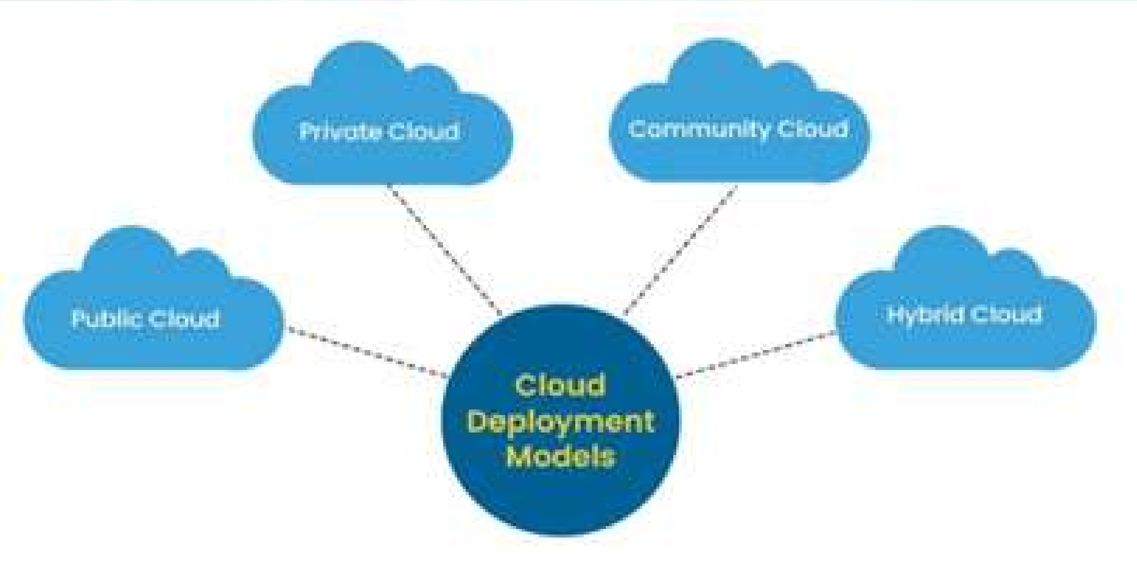


Figure-3.5 Types of cloud [5]

(1) Public Cloud: The general public can access the cloud infrastructure on a cloud service provider on a for-profit basis. As a result, a customer can Create and deploy a service on the cloud for very little money. Compared to the capital investment needs typically connected with alternative deployment options.
Example: Microsoft Azure, Amazon web services, Google Cloud

(2) Private Cloud: For a particular organization, the cloud infrastructure has been set up, is being maintained, and is being run. The operation could take place on-site or with a third party.
Example: Amazon VPC, Microsoft ECi data center, Ubuntu Enterprise Cloud

(3) Community Cloud: Several organizations with comparable needs and interests share the cloud infrastructure. Because the expenditures are split among the organizations, this may help decrease the capital expenditure costs for its establishment. The operation could take place on-site or with a third party.
Example: Google Apps for Government, Microsoft Government Community Cloud

(4) Hybrid Cloud: The cloud infrastructure consists of several clouds of any type, but the clouds have the ability through their interfaces to allow data and/or applications to be moved from one cloud to another. This can be a combination of private and public clouds that support the need to provide cloud services as well as the desire to retain some data in an organization.
Example: On-demand self-service, Resource Pooling, Rapid Elasticity

• *Types of Cloud Service:*

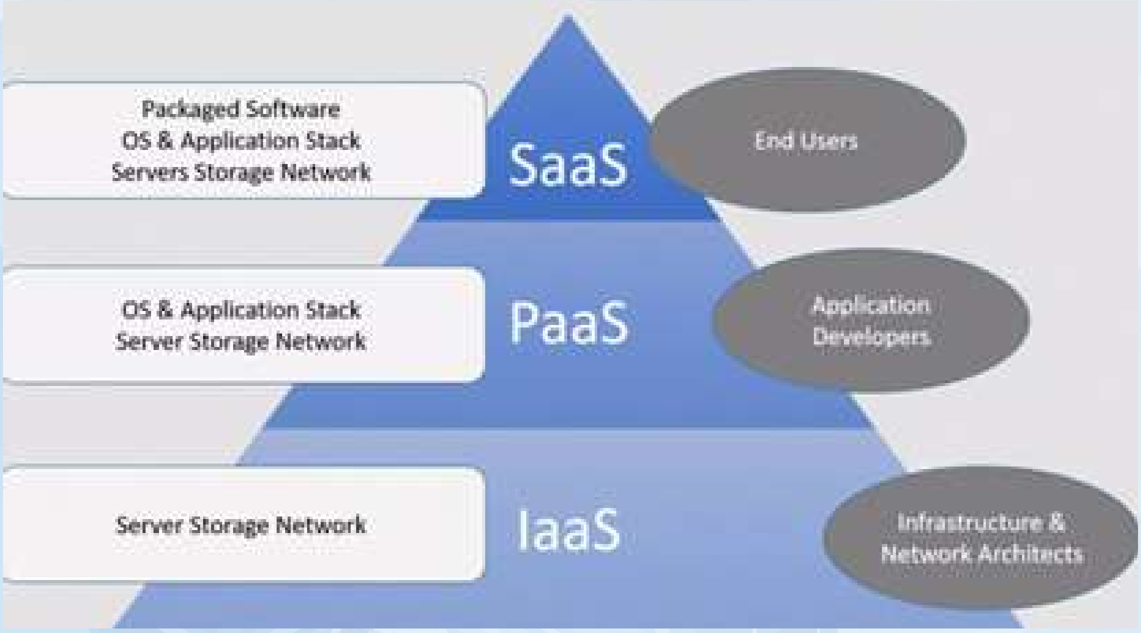


Figure-3.6 Types of Cloud Service [6]

1. Software as a Service (SaaS): The consumer is given the option to use the provider's applications that are hosted on a cloud infrastructure. Through a program interface or a thin client interface like a web browser (for example, web-based email), the programs can be accessed from a variety of client devices. With the possible exception of a small number of user-specific application configuration options, the user does not manage or control the underlying cloud infrastructure, which includes the network, servers, operating systems, storage, or even specialized application capabilities.

2. Platform as a Service (PaaS): The ability to deploy consumer-created or acquired applications made using programming languages, libraries, services, and tools supported by the provider on the cloud infrastructure is a feature offered to the customer. The consumer has control over the deployed apps and possibly the configuration options for the application-hosting environment but does not manage or control the underlying cloud infrastructure, including the network, servers, operating systems, or storage.

3. Infrastructure as a Service (IaaS): The consumer is given the power to set up processing, storage, networks, and other basic computer resources so that they can deploy and run any software, such as operating systems and apps. Although the consumer has no management or control over the underlying cloud infrastructure, they do have some limited influence over some networking components, operating systems, storage, and deployed applications (e.g., host firewalls).

• *Where next for the cloud?*

Big Data : Big data, a current buzzword, is poised to change how the cloud will seem in the future since handling and analyzing such a large number of data will be difficult.

AI and Machine Learning : A wave of AI and ML emerges from big data. It takes a lot longer to prepare hundreds of terabytes of huge data for analysis, thus ML will be used to manage it effectively and aid in the development of future cloud-based applications.

Quantum Computing : Quantum computing is more quickly becoming a reality while being rather exotic in nature. Quantum computing will soon replace conventional computing paradigms as the future unfolds. When this occurs, anticipate a new AI progression and hence the immediate access to cloud data.

• Interesting Facts About Cloud Computing:

- 90% of businesses use the cloud.
- With a 32% market share, Amazon Web Services is the most popular cloud provider.
- In 2021, cloud data centers will handle 94% of the workloads.
- The largest public cloud market is in the US, where spending is expected to reach $124.6 billion in 2019.
- By 2023, it is anticipated that the global cloud computing market would be worth $623.3 billion.

-93% of new users in the cloud choose AWS and Azure as their vendors.

-Palak Varu
(FOURTH Year, CSE, R.N.G.P.I.T)

Image Source:-

[1] https://securecdn.pymnts.com/wp-content/uploads/2020/06/cloud-computing-IBM-investing.jpg
[2] https://www.engineersgarage.com/sites/default/files/Cloud-Storage-vs-Cloud-Computing.png
[3] https://www.codecademy.com/resources/blog/7-benefits-of-cloud-computing/
[4] https://www.tutorialspoint.com/cloud_computing/images/cloud_computing-cloud_management_tasks.jpg
[5] https://www.esds.co.in/blog/wp-content/uploads/2021/01/Cloud-Computing-types-Cloud-1.jpg
[6] https://theisozone.com/wp-content/uploads/2020/03/cloud-scaled.jpg

4. Cloud Computing The Beginning

• *What is cloud computing?*

Cloud computing is a general term for various hosted services delivered over the internet. It is the use of remote, rented servers to store and manage data, rather than the use of a local, privately maintained server.

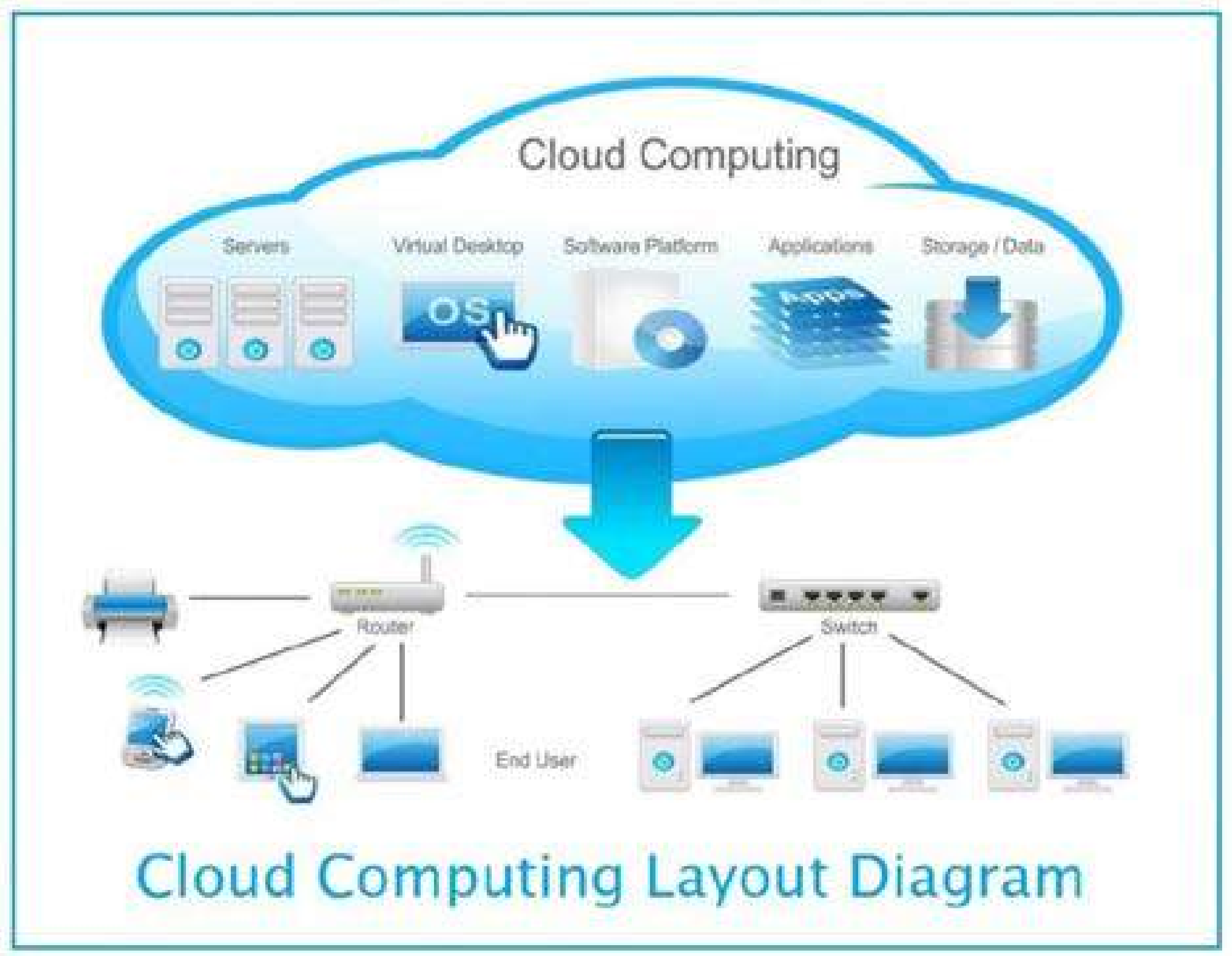


Figure-4.1 Cloud Computing Layout Diagr am[6]

• *So how can the cloud help us?*

In the cloud, we have a shared pool of computer resources(server, storage, applications, etc). When you need more resources all you need to do is to ask. Provisioning resources immediately is a piece of cake for the cloud. You can free resources when they are not needed. In this way, you only need to pay for what you use. The Cloud provider will take care of maintenance.

• *The biggest question that arises is where is the cloud?*

The shared pool of computer resources exists in a physical location called data centers. Cloud provider has multiple data centers around the world. So the data in the cloud are replaced in multiple sites. And if the data center gets clashed due to any reason the data remains safe.

• *Cloud computing services*

Cloud computing services can be divided into 3 models:
IaaS(Infrastructure as a service), PaaS(Platform as a service), and SaaS(System as a service).

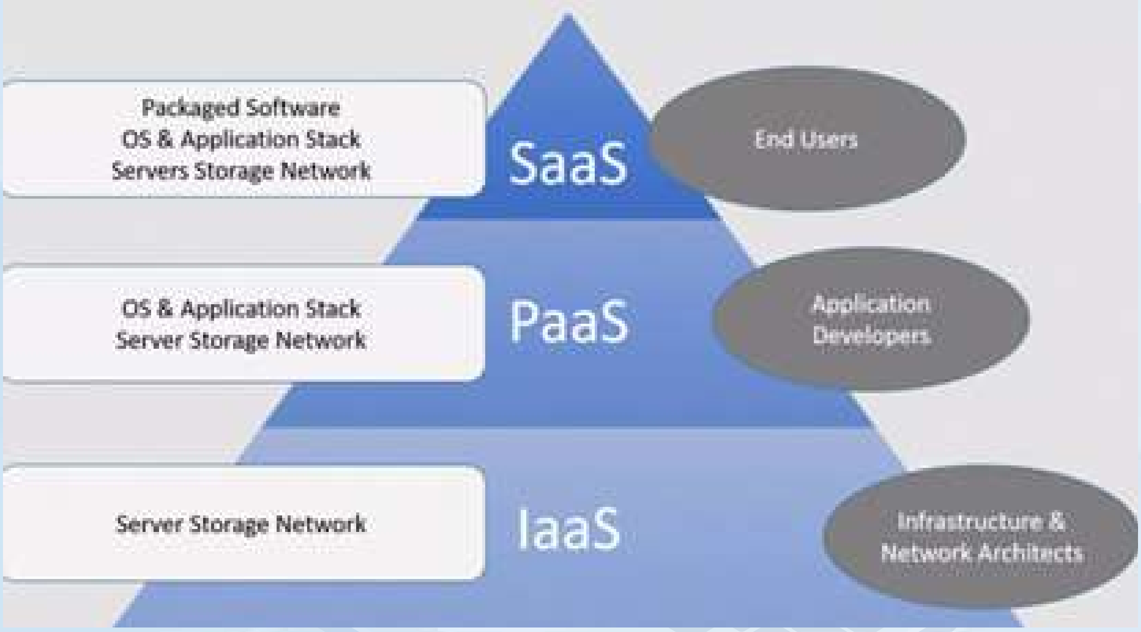


Figure-4.2 Types of Cloud Service [2]

Infrastructure as a Service (IaaS) refers to the fundamental building blocks of computing that can be rented as physical or virtual servers, storage, and networking. IaaS is one of the main components of cloud computing along with PaaS and SaaS. IaaS is completely provisioned and managed over the internet.

Platform as a Service(PaaS) is the next layer up of Iaas which also includes the tools and software that the developer needs to build the application. Core PaaS services are middleware, database management, operating systems, and development tools

Software as a Service(SaaS) is the delivery of application as a service, which is a version of cloud computing that most people use on their day to day basis. It can be managed and owned by one or many providers. A SaaS provider delivers the software based on a set of common code and data definitions. In simple words, SaaS is software that is leased and maintained by its creator based on the metrics. SaaS is a key component of cloud computing technology.

The three models of cloud computing are PaaS(Platform as a Service), SaaS (Software as a Service), and IaaS (Infrastructure as a Service). IaaS refers to cloud computing infrastructure servers, storage, etc. managed by a cloud vendor, while SaaS refers to full applications that are hosted in the cloud and maintained by the SaaS vendor. So let's take an example if SaaS is a customer, IaaS is the source renting a house, then PaaS is the one who supplies the heavy equipment that is needed to place in the house. This is how it relates to a house owner, customer, and the one with supplies of equipments.

• *Types of the cloud:*

There are three fundamental development models of cloud Public cloud, Private cloud, and Hybrid cloud.

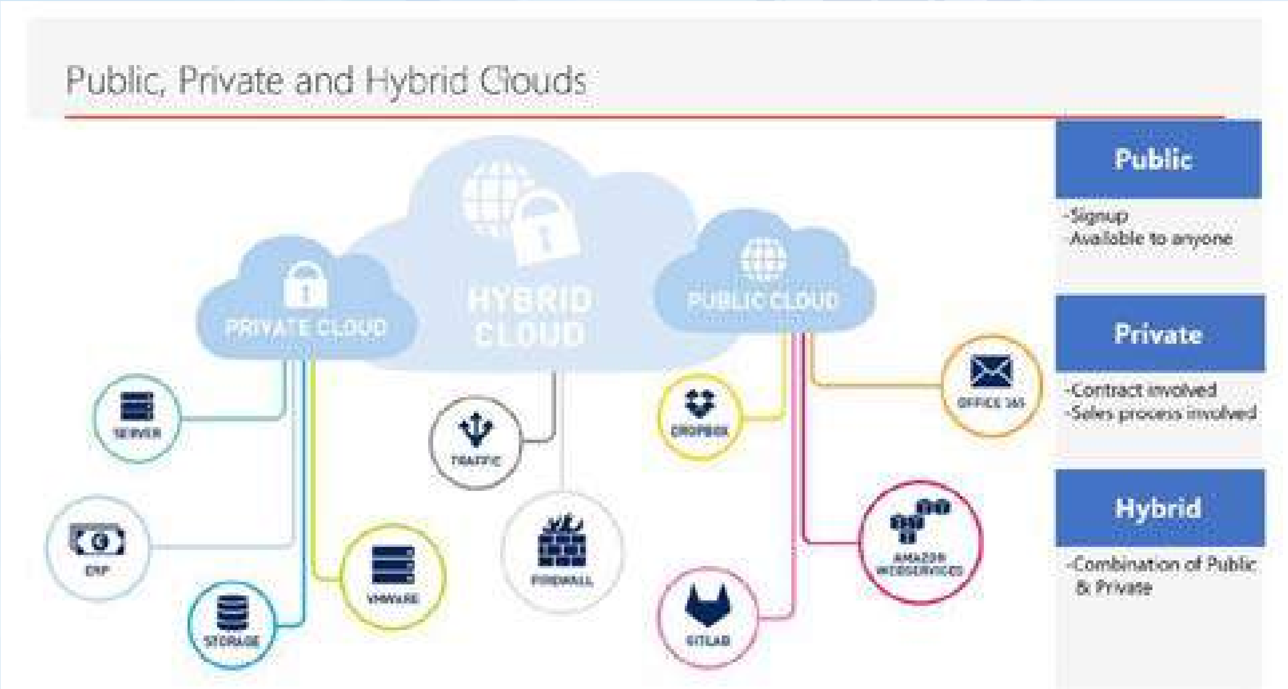


Figure-4.3 Types of Cloud [3]

Public Cloud: When a cloud provider hosts services and infrastructure off-site, shares them across the clients, and, makes them accessible to them via public networks such as the internet, it is called a public cloud.

Private Cloud: A pooled service and infrastructure that is stored and maintained on a private network (physical or virtual), and is accessible by a single client is called a private cloud.

Hybrid Cloud: A combination of public and private cloud elements is called a hybrid cloud. The public cloud can be used for non-sensitive operations while the private cloud can be used for sensitive or mission-critical operations, allowing the companies to maximize their efficiencies.

Cloud Computing is an emerging technology that almost every company is being switched from its on-premise technologies. Whether it is public, private, or hybrid, Cloud Computing has become an essential factor for companies to rise to the competition.

• *Benefits of cloud computing :*

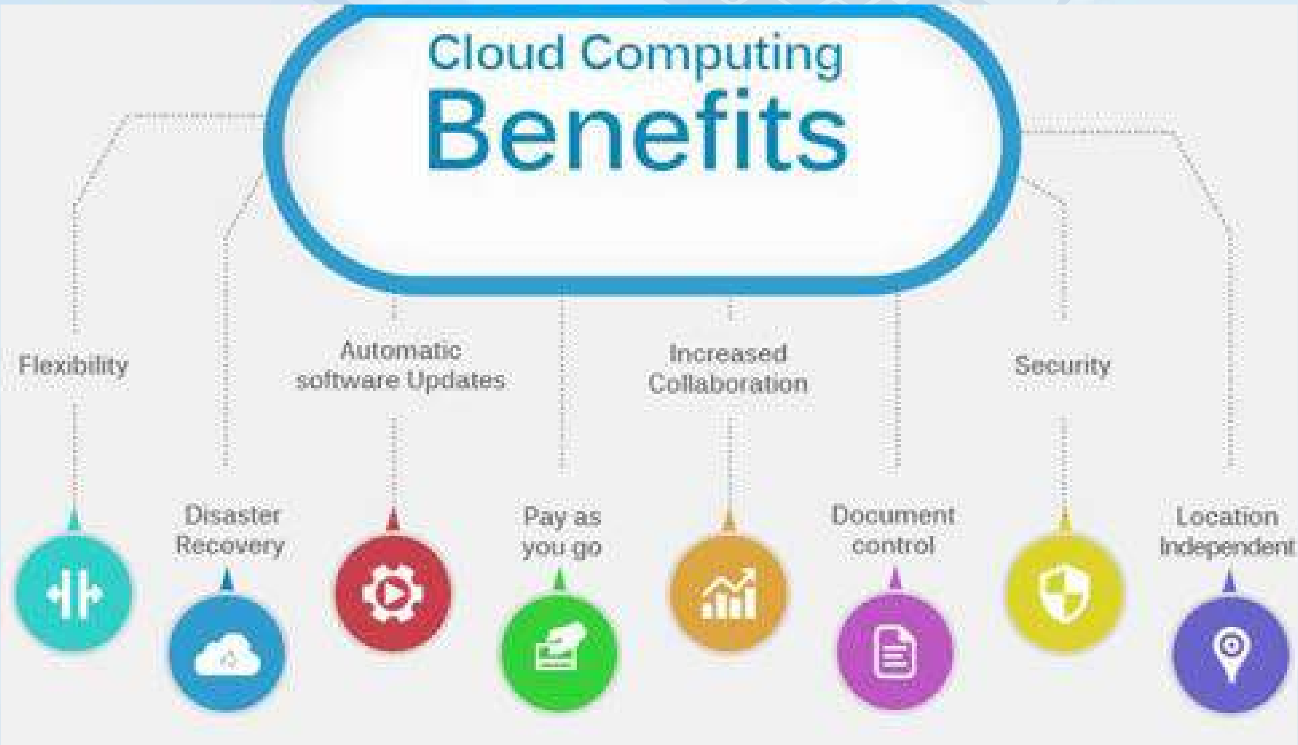


Figure-4.4 Benefits of Cloud Computing [4]

Knowledge Shared = Knowledge ^{2}.

Here I’ve shared basic concepts of cloud computing technology that might be useful for beginners.

-Parva Gurav
(THIRD Year, CSE, R.N.G.P.I.T)

Image Source:-

[1] https://i2.wp.com/www.informationq.com/wp-content/uploads/2015/04/cloud-computing-layout-diagram.jpg?resize=1024%2C796&ssl=1
[2] https://www.uniprint.net/wp-content/uploads/2017/05/Cloud-service-models-diagram.png
[3] https://www.tech-quantum.com/wp-content/uploads/2020/04/042520_1308_PublicPriva1.png
[4] https://2.bp.blogspot.com/-Gb6qwblxmnY/WVvjhb-5JDI/AAAAAAAAUIo/FYylt6eMObsHmLCqQOnb-RPAWt5PvFmogCLcBGAs/s1600/cloud-computing-benefit.png

5. Invulnerability is a Delusion

Figure-5.1 Image by master1305 on Freepik [1]

"I believe we will all be responsible for our own security – no vendor, service provider, or even government entity will save us."

-Sean Martin

With an increasing number of people going online for various purposes like downloading software, online gaming, and chatting on various social media platforms, it also opens multiple doors for hackers to get into your system and cause you trouble.

• *What is a Cyber Crime?*

Cybercrime is expanding quickly in the modern world. Cybercrime is defined as any criminal activity in which a computer is either the target of the crime or a tool used to carry it out. This offense involves using a user's private information, public information, or secret information. Additionally, it is used to tamper with data that is made available online as well as to sell data. Cyber crimes can be generally divided into two categories:

1) Crimes that target networks or devices
(Virus, Malware, or DoS Attacks)
2) Crimes using devices to participate in criminal activities
(Phishing Emails, Cyber Stalking, or Identity Theft)

Here, are the Top 5 popular forms of Cyber Crimes in India.

• *Phishing :*

When questioned about the effects of successful phishing attacks, 60% of security leaders said that their company lost data, 52% had credential breach issues, and 47% had ransomware problems. Phishing is the second most expensive attack vector to deal with, costing enterprises an average of $4.65 million to remediate, according to IBM's 2021 Cost of a Data Breach Report.

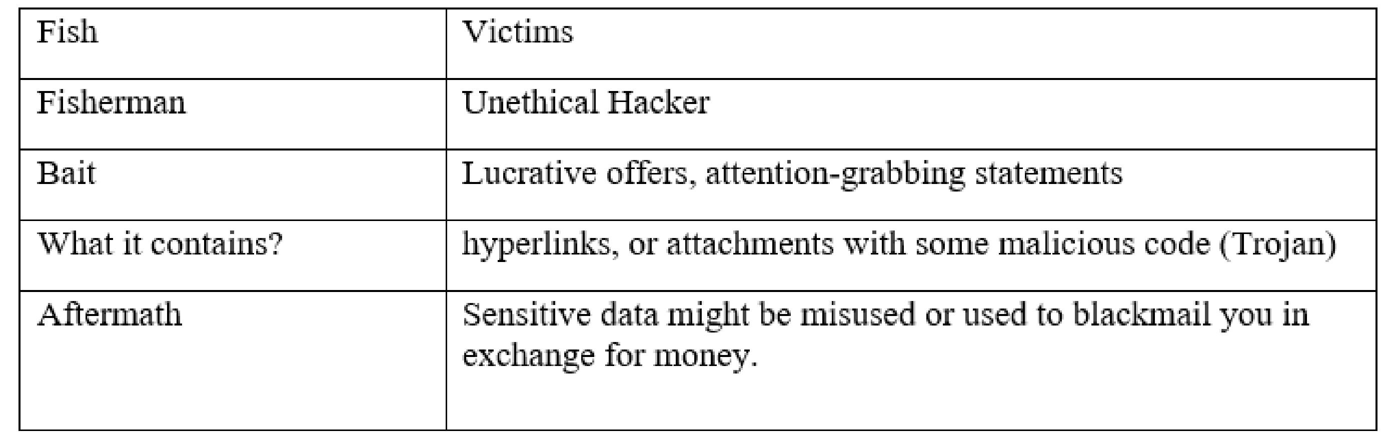
The Zoom application was targeted by cybercriminals during the COVID-19 epidemic. For the most popular platforms, phishing websites were created, including the fake versions of classroom.google.com (googloclassroom.com and googieclassroom.com).

• *What is phishing?*

Figure-5.2 Image by storyset on Freepik [2]

Phishing seems to be like same as “fishing”, where the bait is placed to attract fish (and that is the victims)! And these fishes are targeted via email, text message, or telephone (also known as Vishing i.e. voice phishing) by posing as a legitimate institution /organization to lure people into providing information or data that is sensitive.

• *How does it work?*



Fish	Victims
Fisherman	Unethical Hacker
Bait	Lucrative offers, attention-grabbing statements
What it contains?	hyperlinks, or attachments with some malicious code (Trojan)
Aftermath	Sensitive data might be misused or used to blackmail you in exchange for money.

• *How to prevent Phishing attacks?*

Generally, emails sent by a criminal are protected so they appear to be sent by a legitimate service.

1. You should be more cautious when opening emails that might not be relevant, such as those offering a loan from a bank that you haven’t yet applied for (an easy task!). Do not rely on the spam feature of your email. It is not 100% accurate.

2. Place a web filter to stop nefarious websites.

3. All sensitive information should be encrypted.

4. Install an antivirus that may give a warning before you enter a fake website.

• *ATM Frauds*

Customers of Bank of the West were victimized by an ATM skimmer attack in June 2022, the bank reports, compromising debit card numbers and associated PINs.[4]

Some of the types of ATM fraud are given by:

1. Card Skimming

2. Card Trapping

3. ATM Malware

Figure-5.3 Image by fanjianhua on Freepik [3]

• *How does it work?*

ATM fraud is done by tampering with the card and the device, as well as online transactions. Now, someone attempting to hack your online transactions via phishing emails and messages may gain access to your device's message section, allowing him to obtain one-time passwords. Card tampering and ATM device tampering are accomplished through the use of electronic devices that read the information on your card.

• *How to prevent ATM Fraud?*

1. The only way to avoid ATM fraud is to be aware of and have knowledge about ATMs. The machines should be checked once whether the numbers have been tampered with or not.
2. Avoid frequent visits to the ATM.
3. Never, knowingly or unknowingly, provide the One-time-password (OTP) to anyone.

• *Social Media Hack & Spamming*

Figure-5.4 Photo by Magnus Mueller [4]

In September 2022, a hacker going by the alias ‘teapotuberhacker’ compromised both Uber and Rockstar Games by hacking and taking control of the Slack account of one of the employees and collecting their important data. Uber’s breach appears to have been comprehensive, compromising source code, internal databases, and more. The Rockstar breach may have been more limited, but it did include Grand Theft Auto 6 leaked footage.

• *How does it work?*

So, here the hacker observes the behavior of the target and tries to obtain the password and the easy ones can be cracked just by guessing. Moreover, if the hacker has your phone number or mail, he can easily change the password of your account by using due to password recovery options.

• *How to prevent Social Media Hacking?*

1. The most important thing to remember is to change your password at least once a month.

2. Enable two-factor authentication where the user’s identity can be confirmed via logging into the account.

3. Be cautious while selecting third-party applications.

4. Password should be strong that contains special characters and numbers.

Any how if you become a victim, social media platforms have a facility to report the account.

- **Packet Sniffing :** Packets contain information such as destination, source, and so on. The data we want to send is contained in one section of the information. Capturing the packet in Packet Sniffing allows you to access the data.

- **How does it work?**

When you install packet sniffing software, the network interface card (NIC) — the interface between your computer and the network must be set to promiscuous mode. This instructs the computer to capture and process all network traffic using the packet sniffer.
Here's a type of Packet Sniffing.

- **Honeypot (Computing) :** A honeypot is a network-connected system that is set up as a decoy to help attract cyber attackers and detect, deflect, or study attempts to gain unauthorized access to information systems. A honeypot's function is to represent itself on the internet as a potential target for attackers typically a server or other high-value target and to gather information and notify defenders of any unauthorized user attempts to access the honeypot.

- **How to prevent packet sniffing?** : Initially, packet sniffing was used for administrative purposes such as penetration testing. However, hackers are now employing them to steal information and data from victims.

1. Using HTTPS, the secure version of HTTP will prevent packet sniffers from seeing the traffic on the websites you are visiting.
2. One effective way to protect yourself is to use a Virtual Private Network(VPN); which encrypts the traffic being sent between your computer and destination.

3. A router which includes VPN-ready; can protect your home network's traffic data from packet sniffers.
4. Privacy applications are available that protect your data (it's a third-party application, and it is risky).

- **DDoS Attacks:** A Distributed Denial of Service attack, as the name implies, occurs when multiple systems flood the bandwidth or resources of a targeted system, typically one or more web servers. As we know servers serve to the client's request. So basic idea is to flood the server with so many requests that it is unable to serve the user's important request.

- **How does it work?**

A DDoS attack occurs when multiple computers in a botnet send simultaneous requests to slow down and eventually stop the web server. A basic DDoS attack involves sending a large amount of traffic to a specific IP address. It is like intentionally choking up the server with so many requests that when the user requests, Service is denied and hence the names Denial of Service attack.

- **How to prevent DDoS attacks?**

You are not alone if you become a victim of a DDoS attack. High-profile victims of DDoS attacks in 2018 include organizations like Google, Amazon, PlayStation, and GitHub (Big parties!).
Recent attacks include In April, DDoS attacks were launched against the Israeli Airports Authority's and Health Ministry's websites that couldn't log in to their services for the same reason.

1. Recognize the DDoS attack as soon as possible: When you have problems with your server, it is because of a DDoS attack. Most DDoS attacks begin with sharp spikes in traffic, and this is the primary distinction between a sudden surge of legitimate visitors and the beginning of a DDoS attack. More Bandwidth may not avoid the attack, but it may give you some time to act before the attack takes place.

2. If nothing else works, the last thing you can do is shut down the server and restart the entire system.

-Anjaly Biju Ezhava
(FOURTH Year, CSE, R.N.G.P.I.T)

Image Source:-

[1] https://www.freepik.com/free-photo/hooded-computer-hacker-stealing-information-with-laptop_6779117.htm#query=cyber%20security&position=31&from_view=search
[2] https://www.freepik.com/free-vector/phishing-account-concept-illustration_8239218.htm#query=phishing&position=1&from_view=search
[3] https://www.freepik.com/free-photo/atm-operation-bank_1286422.htm#query=atm&position=19&from_view=search
[4] https://www.pexels.com/photo/photo-of-hand-holding-a-black-smartphone-2818118/

Student Coordinators

: Batch :
2016 - 2020

Mahendra Sharma

Dhiren Jummani

Saurabh Jha

Aadil Shaikh

Kuldip Patel

: Batch :
2019 - 2023

Urvi

Rushil

Manan

Navpreet

Dhairya

Vinit

Krishna

Dhruv

Computer Science and Engineering

esKra

R.N.G.P.I.T.
CAMPUS PUBLICATION

www.eskra.rngpit.ac.in

A Magazine by:
ESKRA - Campus publication
Computer Science and Engineering,
R.N.G. Patel Institute of Technology,
Surat

You can provide feedback on
eskra.cse@rngpit.ac.in

✉ eskra.cse@rngpit.ac.in

cserngpit

cserngpit

☎ +91-9427527398
+91-9033707334
+91-9510427118