How Hackers Cover Their Tracks (Anti-forensics)

Anti-forensics is a term that contradicts Cyber Forensics. It attempts to negatively affect the existing amount and quality of evidence from a crime scene or make the analysis and examination of evidence difficult or impossible to conduct.

Anti-forensic techniques are actions whose goal is to prevent the proper investigation process or make it much harder. These actions are aimed at reducing the quality and quantity of digital evidence. These are deliberate actions of not only computer users but also of developers who write programs secured prior to the methods of Cyber forensics.

For the anti-forensic techniques, we can include activities such as the intentional deletion of data by overwriting them with new data or protection tools against forensics analysis. Anti-forensic techniques can be used to increase security for example erasing and overwriting data so that they cannot be read by unauthorized persons. These techniques can be misused by perpetrators of cybercrimes in order to protect against disclosure of their actions.

Users of anti-forensics tools can also become computer users who want to remove evidence of criminal activities such as hackers, terrorists, pedophiles, and counterfeiters. Anti-forensics tools can be used by users who will be using it to destroy any data indicating that they could steal valuable data to gain unauthorized access to the computer systems or capture secure information and passwords.

Goals of Anti forensics:

- Avoiding detection of compromising events that have taken place.
- Disrupting and preventing the collection of information.
- Increasing the time that an examiner needs to spend on a case.
- Casting doubt on a forensic report or testimony.
- Subverting the forensic tool (for example, using the forensic tool itself to attack the organization in which it is running).
- Leaving no evidence that an anti-forensic tool has been run.

Various fields to be used in Anti forensics:

Data Destruction: It is the destruction of any evidence before someone gets a chance to find it. The field used in anti-forensics in cyber security systems are as follows:

- **Wiping:** Securely deleting data so that it cannot be restored even with forensic software.
- **Changing MAC attributes:** The changing or deleting file attributes to avoid timeline analysis.

Data Contraception: It is a technique to limit the quantity and quality of forensic evidence by keeping forensically important data off the disk.

- **Syscall Proxying:** It is a technique where a local program transparently proxies a process's system call to the remote server.

- **Memory resident compiler/assemblers:** They are used when an attacker wants to send remote code fragments from a remote device to the compiler/ assembler residing in the local device.
    - **Direct Kernel Object Manipulation (DKOM):** It is a method that allows attackers to use drivers or loadable kernel modules to modify the memory associated with kernel objects.
    - **Data Hiding:** It provides an exploration into the present day and next generations of tools and techniques used in data concealment tactics and advanced malware methods.

Steganography: It is the art of writing hidden messages in such a way that no one apart from the sender and intended recipient, suspects the existence of the message.

Other Anti-Forensic Categories:

- Obfuscation and encryption.
- Data forgery
- Data Deletion and Physical Destruction
- Analysis Prevention
- Online anonymity

What is a Proxy Server?

A proxy server is an intermediary server that acts as a gateway between the user and the internet, preventing malware from accessing the server and network. It provides anonymous browsing, and security, bypassing geo-blocking, and regulating web requests, depending on the user's use case, needs, or company policy. By implementing a proxy server, users can protect their online privacy and avoid potential security threats.

Why use proxy server?

Proxies provide enhanced security and help organizations put certain restrictions on their employees. It can be used for personal purposes, such as hiding location while watching movies online, etc and for professional purposes like.

- To control internet usage by employees
- Bandwidth savings
- Improved speeds
- Improve security
- Balance internet traffic to prevent crashes
- Control the websites employees access in the office
- Save bandwidth by caching files

How does a proxy server work?

A proxy server is basically a computer on the internet with its own IP address that your computer knows. If you use a proxy server internet traffic flows through the proxy server on its way to the address you requested i.e When you send a web request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the web server, and forwards you the data. It can also block access to certain web pages, based on IP address.

Proxy servers provide you with overall better network performance and are also used for keeping data away from unauthorized access, maintaining anonymity, assessing the blocked content maintaining a valuable layer of security. There are a variety of available servers on the internet. Here we have reviewed some available proxy servers based on the above functionalities to filter out some top servers:

List of Best Proxy Servers:

1. IPROYAL

IPRoyal Proxy Manager is a free extension that allows you to easily control all your proxies in Google Chrome. With IPRoyal, you can get a genuine, ethically sourced IP address anywhere in the world. Web scraping, sneaker copping, social media automation, gathering SERP data, market research, avoiding geo-restrictions, IP-based blocks, bans, and more – everything with just a click. It's a great option if you need fast, reliable, and affordable residential proxies with excellent customization. They offer various plans with different pricing:

- Residential proxies starting from $4
- Datacenter proxies starting from $1.3 per proxy
- Sneaker proxies at $0.8 per proxy
- static residential proxies starting from $2.5 per month (unlimited bandwidth)

Features:

- Import different proxy types in seconds
- Great targeting options(country,state, or city)
- Pay-as-you-go model
- API support and additional tools
- Instantly switch between different profiles
- 24/7 support
- Set up your bypass list for issue-free surfing

2. Oxylabs

Oxylabs is a proxy service provider offering a diverse proxy network that includes residential, datacenter, mobile proxies, rotating ISP and SOCKS5 proxies. Oxylabs can cater to you if you are looking for services like brand protection and SEO monitoring, adverification, web scraping etc where maintaining anonymity and avoiding detection is crucial. They have a large network of IP addresses in over 195 countries, and they offer a variety of features that make them a good choice for a variety of use cases. It offers various services like web crawler that lets you collect only relevant data from target websites.

It sources its residential proxies from real devices, making them more reliable and less likely to be detected as proxies. It offers advanced features like session control, sticky sessions, and proxy rotation options that enhance your proxy usage.

Features:

- Enterprise-grade solution
- Large proxy pool across 195 countries
- Intelligent web scraping technologies
- Service Level Agreement (SLA) Management
- Referral Source Tracking
- High Volume Processing and data quality control

3. Kproxy

KProxy is unique, as it offers Chrome and Firefox extensions to make surfing simpler. Kproxy connects via a regular HTTP protocol. Its user’s HTTP connection will be seen as a standard connection and KProxy’s extension filters all internet traffic, as it turns the computer into a proxy server itself. It offers unlimited downloads, no ads, and access to premium servers and also allows you to hide the top menu. Different subscription plans are available to suit the user.

Features:

- Compatibility
- IP Masking
- Unlimited Access
- Great speed
- Kill switch to start/stop the proxy

4. Smartproxy

Smartproxy is a public data access platform that offers over 40 million residential and shared or dedicated data center proxies that helps you shoot unlimited connection requests concurrently. With Smartproxy's comprehensive documentation setting up proxies becomes exceptionally simple. This lets you access a plethora of web pages in no time. You can set up a separate proxy user with its own login credentials for each task. Smartproxy offers a flexible pricing plan starting from $12.5 for 1 GB for small projects to a 100 GB enterprise plan starting from $700/month.

Features:

- Unlimited connections
- Qualitative Analysis
- Data Security
- Facilitate simultaneous proxy connections.
- Allows access to geo-blocked services.
- 195 data centers spread across 8 cities worldwide.
- Social Media Monitoring

5. CroxyProxy

CroxyProxy is a free and secure web proxy with advanced capabilities. You can visit video hosting sites, search engines, social networks, etc. with Croxyproxy protecting your privacy. It changes your location and makes you invisible when you surf the Internet. It encrypts all data before it gets transferred to you. It works as a proxy browser. It is very easy to use, you don't need to download any application or configure your browser. Its basic version is free. Its ad-free premium access will cost you $3.50 per month.

Features:

- Permanent link generation.
- It supports any OS and device, and most web browsers.
- The basic version is free.
- Allows anonymous surfing
- Supports cross-platforms
- HTML5 videos and audio playback is supported

Conclusion:

There are several functions that a proxy server can provide, including anonymous browsing, security measures, bypassing geographical restrictions, and regulating web requests. In previous discussions, we have explored various proxy server providers that offer features such as web scraping, automating social media, accessing blocked services, anonymous browsing, and hiding IP addresses. Depending on your requirements and preferences, you can choose one from the list and enjoy a safer browsing environment.

Tunneling

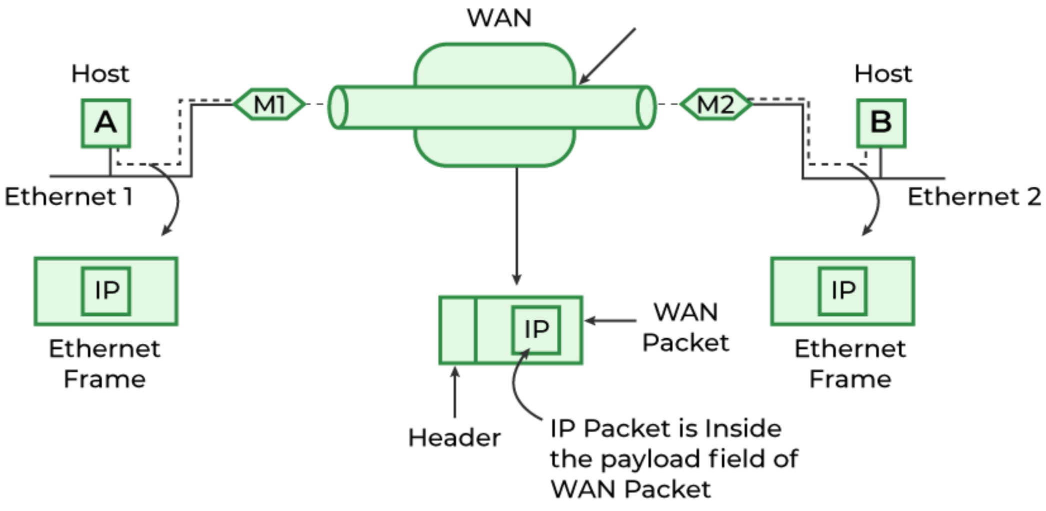
Last Updated : 13 Apr, 2023

-
-
-

A technique of inter-networking called **Tunneling** is used when source and destination networks of the same type are to be connected through a network of different types. Tunneling uses a layered protocol model such as those of the OSI or TCP/IP protocol suite.

So, in other words, when data moves from host A to B it covers all the different levels of the specified protocol (OSI, TCP/IP, etc.) while moving between different levels, data conversion (Encapsulation) to suit different interfaces of the particular layer is called tunneling.

For example, let us consider an Ethernet to be connected to another Ethernet through a WAN as:



Tunneling

The task is sent on an IP packet from host A of Ethernet-1 to host B of Ethernet-2 via a WAN.

Steps

- Host A constructs a packet that contains the IP address of Host B.
- It then inserts this IP packet into an Ethernet frame and this frame is addressed to the multiprotocol router M1
- Host A then puts this frame on Ethernet.
- When M1 receives this frame, it removes the IP packet, inserts it in the payload packet of the WAN network layer packet, and addresses the WAN packet to M2. The multiprotocol router M2 removes the IP packet and sends it to host B in an Ethernet frame.

How Does Encapsulation Work?

Data travels from one place to another in the form of packets, and a packet has two parts, the first one is the header which consists of the destination address and the working protocol and the second thing is its contents.

In simple terminology, Encapsulation is the process of adding a new packet within the existing packet or a packet inside a packet. In an encapsulated packet, the header part of the first packet is remain surrounded by the payload section of the surrounding packet, which has actual contents.

Why is this Technique Called Tunneling?

In this particular example, the IP packet does not have to deal with WAN, and the host's A and B also do not have to deal with the WAN. The multiprotocol routers M1 and M2 will have to understand IP and WAN packets. Therefore, the WAN can be imagined to be equivalent to a big tunnel extending between multiprotocol routers M1 and M2 and the technique is called Tunneling.

Types of Tunneling Protocols

1. Generic Routing Encapsulation
2. Internet Protocol Security
3. Ip-in-IP
4. SSH
5. Point-to-Point Tunneling Protocol
6. Secure Socket Tunneling Protocol
7. Layer 2 Tunneling Protocol
8. Virtual Extensible Local Area Network

1. Generic Routing Encapsulation (GRE)

Generic Routing Encapsulation is a method of encapsulation of IP packets in a GRE header that hides the original IP packet. Also, a new header named delivery header is added above the GRE header which contains the new source and destination address.

GRE header act as a new IP header with a Delivery header containing a new source and destination address. Only routers between which GRE is configured can decrypt and encrypt the GRE header. The original IP packet enters a router, travels in encrypted form, and emerges out of another GRE-configured router as the original IP packet as they have traveled through a tunnel. Hence, this process is called GRE tunneling.

2. Internet Protocol Security (IPsec)

IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted, and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

3. IP-in-IP

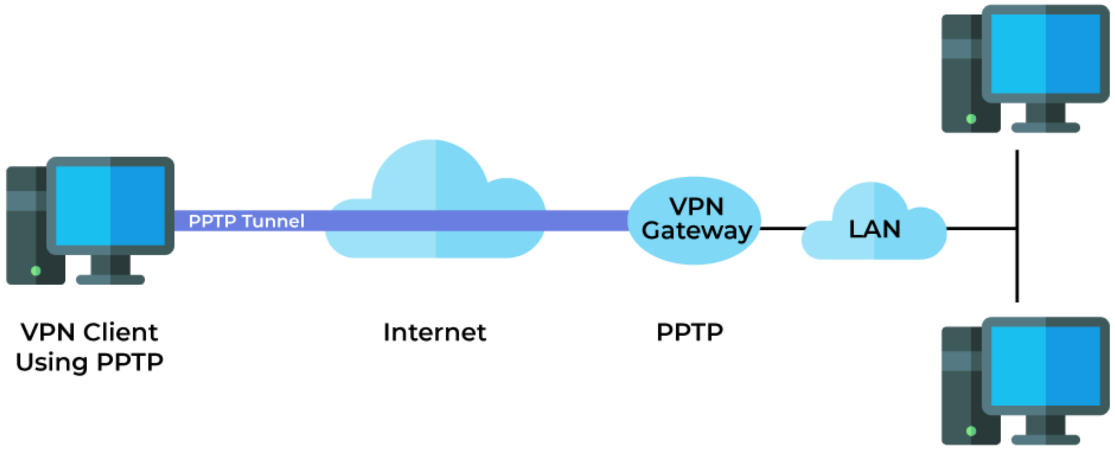
IP-in-IP is a Tunneling Protocol for encapsulating IP packets inside another IP packet.

4. Secure Shell (SSH)

SSH(Secure Shell) is an access credential that is used in the SSH Protocol. In other words, it is a cryptographic network protocol that is used for transferring encrypted data over the network. It allows you to connect to a server, or multiple servers, without having to remember or enter your password for each system which is to log in remotely from one system to another.

5. Point-to-Point Tunneling Protocol (PPTP)

PPTP or Point-to-Point Tunneling Protocol generates a tunnel and confines the data packet. Point-to-Point Protocol (PPP) is used to encrypt the data between the connection. PPTP is one of the most widely used VPN protocols and has been in use since the early release of Windows. PPTP is also used on Mac and Linux apart from Windows.



Point-to-Point Tunneling Protocol (PPTP)

6. Secure Socket Tunneling Protocol (SSTP)

A VPN protocol developed by Microsoft that uses SSL to secure the connection, but only available for Windows.

7. Layer 2 Tunneling Protocol (L2TP)

L2TP stands for Layer 2 Tunneling Protocol, published in 2000 as proposed standard RFC 2661. It is a computer networking protocol that was designed to support VPN connections used by an Internet service provider (ISP) to enable VPN operation over the Internet. L2TP combines the best features of two other tunneling protocols- PPTP(Point-to-Point Tunneling Protocol) from Microsoft and L2F(Layer 2 Forwarding) from Cisco Systems.

8. Virtual Extensible Local Area Network (VXLAN)

Virtual Extensible Local Area Network is short called VXLAN. It is a network virtualization technology that stretches layer 2 connections over layer 3 networks by encapsulating Ethernet frames in a VXLAN packet which includes IP addresses to address the scalability problem in a more extensible manner.

What is SSL Tunneling?

SSL Tunneling involves a client that requires an SSL connection to a backend service or secures a server via a proxy server. This proxy server opens the connection between the client and the backend service and copies the data to both sides without any direct interference in the SSL connection.

What is the Difference Between Smishing and Vishing

Both smishing and vishing are carried out by cyber criminals to steal personal information from the victim. These can include their credit card numbers and bank details. However, these two approaches differ in how they are carried out.

Smishing is done via text or instant messaging apps like WhatsApp and Telegram. The scammer provides their victim with a link, which, when clicked, will help them steal personal information or upload malware.

Vishing, on the other hand, uses phone calls and voicemail to reach the victim. They will pretend to be representatives of a bank or other institution to retrieve personal information. AI has also made vishing more possible, with AI tools used to mimic a person's voice and trick the victim into sending them money or sharing data.

Fast Flux and Advanced Fast Flux in Cyber Security

Last Updated : 27 Jan, 2023

-
-
-

Fast flux is a DNS technique used by botnets to phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies. It can also be referred to as peer-to-peer networking, distributed command and control, web-based load, and balancing proxy redirection used to make malware networks more resistant to delivery and countermeasures. The Storm Worm is the most recent malware variant to make use of this technique.

Advanced Fast Flux

The basic idea behind advanced fast flux is to have numerous IP addresses associated with a single fully qualified domain name, where the IP addresses are swapped in and out with extremely high frequency through changing DNS records. Internet users may see fast flux used in phishing attacks linked to criminal organizations, including attacks on social networking services.

Types of Fast Flux

1. Single Fast Flux
2. Double Fast Flux

1. Single Fast Flux: It is the simplest type of fast flux characterized by multiple individual nodes within the registering and de-registering of their addresses as a part of the DNS A (address) record list for a single DNS name. This combines with round-robin DNS with very short- usually less than 5 minutes. TTL (Time to Leave) values to create a constantly changing list of the destination address for that single DNS name, The list can be hundreds or thousands of entries long.

2. Double Fast Flux: It is the sophisticated type of fast flux referred to as Double fast flux characterized by multiple nodes within the network registering and de-registering their addresses as part of the DNS name server record list for the DNS Zone. This provides an additional layer for redundancy and survivability within the malware network.

In fast-flux hosting the **fast-flux service networks are used for two purposes**:

1. To host referral websites: Bots in this service network typically do not host the fast flux customer's content but will redirect the web traffic to the web server where the fast flux customer host unauthorized or illegal activities. When this is the only network operated for fast flux hosting, the term single flux hosting is applied here.

2. To host name servers: Bots in this service network run name server referrers for the fast flux customers. These name servers forward DNS requests to hidden name servers that host zones containing DNS A resource records for a set of referral websites. The hidden name server does not relay responses back through the referring name server but replies directly to the querying host. When this second network is operated with a conjunction that enhances deception the term used is "Double flux".

Example

Fast Flux Watch is a mechanism for the online detection of fast flux agents. It is envisioned to exist as a software agent at leaf routers that connect stub networks to the internet.

The core mechanism of the fast flux watch is based on the inherent features of the fast flux network: flux agents within stub networks take the role of relaying client requests to point-of-sale websites of spam campaigns.