ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse94952020.pdf
https://doi.org/10.30534/ijatcse/2020/94952020

Kerberos: Security Analysis of Authentication protocol

Dr. Dayanand Lal N[1], Nida Kousar G[2], Sahana D S[3], Dr. Brahmananda S H[4], Madhurya J A[5]
[1]Assistant Prof., Department of CSE, GITAM School of Technology, Bengaluru, India, dayanandlal@gmail.com
[2]Assistant Prof., Department of CSE, GITAM School of Technology, Bengaluru, India, knida@gitam.edu
[3]Assistant Prof., Department of CSE, GITAM School of Technology, Bengaluru, India, ssanthos@gitam.edu
[4]Professor, Department of CSE, GITAM School of Technology, Bengaluru, India, bsavadat@gitam.edu
[5]Assistant Prof., Department of CSE, GITAM School of Technology, Bengaluru, India, mambuja@gitam.edu

ABSTRACT

Communication over the internet is increasing with scientific advancements, which seeks the desires of surveillance and replaying attacks over the internet. To prevent unauthorized users from attempting to access data passed over the network, several authentic services have been created. Kerberos is a protocol intended to assure protection when working over a network which is not stable. The authentication protocol allows access to the intended services over the internet only for authorized customers. Kerberos was designed for a project named Athena by the Massachusetts Institute of Technology (MIT). Kerberos uses methods for symmetric key encryption and a key distribution center which is an additional-system that can be integrated for existing networks.

Key words: Kerberos, Silver tickets, Key Distribution Centre (KDC).

1. INTRODUCTION

Modern computer systems offer various users with service, a nd require the ability to successfully identify the requesting user. In conventional systems, the information of the person is examined by verifying a password that is typed when sign ing in; the program records the information and uses it to de cide what operations can be done[1]. Nowadays safe communication is becoming a crucial thing. So many more companies tend to run their company using network infrastructure. The main feature in maintaining connectivity over the distributed network is authentication-the method of assuring someone else's identity. Kerberos is a Network Authentication Protocol [2]. It is designed to include authentication methods for client / server applications using secret-key cryptography. This procedure is being applied by the Massachusetts Institute of Technology (MIT).The Internet is an insecure environment where it is used in several industrial products. Several of the protocols used on the Internet offer little protection. Devices to misuse passwords may take away network passwords are widely used by malicious hackers. Apps that transmit an

Unencrypted passwords over the network are also extremely vulnerable [3].With the simple example if we can consider, client / server programs depend on the client software to be "genuine" about the user identity that uses it. Many approaches depend on the client to limit their operations to what they are permitted to do, without any other server compliance. To overcome their network security problems, some websites make use of firewalls. But firewalls presume that "the malicious actors" will always be outside, which is often a very weak assumption. Many of the computer fraud cases that are particularly harmful are committed by insiders. Networking devices often have a big downside in that they limit how the users can access the Internet [4]. For example, say that firewalls are generally a less instance which is not more secure than a network which is not a connected device. They are clearly inefficient and unacceptable under many of the limitations. Using an encryption algorithm, the Kerberos protocol helps a user to demonstrate their uniqueness to a server over an unprotected internet access. After the user and server used the Kerberos to prove their identity, all of their messages can sometimes be encrypted while they go about their business to ensure privacy and information integrity.

At MIT, Kerberos is freely available, quite close to those used under copyright authorization for the Berkeley Software Distribution (BSD) operating system and the X Window System [5]. MIT will have management of the update to Kerberos so that anybody who wants to use it can search after themselves at the code and make sure the code is correct. Kerberos is also accessible from several different vendors as a product, but for those who choose to focus on a product that is highly supported. In short, Kerberos is an answer to your security problems with your network. It seems to provide the authorization tools and comprehensive security by applying cryptographic algorithms and techniques to make sure of securing information systems across your entire business [6]. Kerberos, the network protocol is commonly used to handle the part of authentication, and serves as a critical key component to ensure a stable networked

environment. Before running other protocols this protocol will run between two contact parties.

Authentication can be defined as determining an identity to the required level of assurance and Kerberos deals with the verification function that have been developed to support application level authentication[7][8]. Kerberos is an authentication protocol that helps to determine a user or host's identity. The authentication relies on tickets that are used as credentials, which allows communication and proving identity over a non-secure network in a secure condition [9][10].For further security, even the Kerberos protocol messages are protected against industrial espionage and replay attacks. Especially, Kerberos authentication uses a client-server model: a Kerberos user submits an authentication request to a Kerberos request. Kerberos is a protocol for computer network authentication that allows people to verify once authenticated on the network and access services [11]. Kerberos serves as a trusted third-party server called the Main Distribution Centre (KDC).

Kerberos uses either the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP), which sends plain text data. Because of this Kerberos is liable for the availability of encryption. On physically insecure networks, Kerberos provides strong protection. So it offers a structured server for authentication. The tickets are the principal structures managed by Kerberos. In addition to be used by them to perform multiple acts in the Kerberos domain, these tickets are supplied to the users. A forged service authentication ticket is a silver ticket. By breaching a computer username and password and using it to create a fake authentication ticket, a hacker can create a Silver Ticket. Before double checking that their token is actually legitimate, Kerberos enables services (low-level operating system programs) to log in, which hackers have exploited to build Silver Tickets. It is more difficult to detect Silver Tickets than Golden Tickets because there is no contact between the service and the Domain Controller and the targeted machine is local to any logging[12].

2. LITERATURE REVIEW

According to Michael Schneider [13], Kerberos is the authentication protocol that is used for user authentication in Microsoft Windows. The authors explained that the purpose used by Kerberos to award a ticket and summarized it in five stages. Authentication Service Request (AS-REQ): A customer requests a Ticket Granting Ticket (TGT) and requests a Key Distribution Centre (KDC) service. As in original request, a Long Term Key (normally the user's password) is used to encode the UTC timestamp. Authentication Service Response (AS-REP): The query is reviewed by the KDC, and the decryption is performed using the Active Directory (AD) Long Term Key. The KDC grants the TGT if this review is successful. Ticket-Granting Service Request (TGS-REQ): In order to access a random resource, the customer requests another ticket called Ticket-Granting Service (TGS) from the KDC Ticket-Granting Service Request (TGS-REP): The TGT sent over the request TGS-REQ is decrypted by the KDC and the information is copied into the TGS for the service. The consumer forwards the ticket to the target server in the Application Server Request.

Author Paul Roberts [14] explained how silver ticket attack works and called as post-exploitation attacks. That means that a threat actor must already have compromised a target system in the environment before they can generate a Kerberos Silver Ticket. According to Author Paul if once an attacker has a foothold on a single network system, they can start laying the groundwork for forging a Kerberos Silver Ticket. And author Paul outlined on offline cracking of credentials is a key component of Silver Ticket attacks; ensure that local user, administrator and service accounts use strong, unique passwords. In addition, organizations should make sure that credentials are not shared across accounts on the local system or with other network services and resources.

Author Mochan [15] has demonstrated that while Kerberos is a very protocol and possibly the best protocol for inner authentication, it has a wide attack surface for attackers. He listed all the key attacks on Kerberos, how to list them and finally how to use a wide variety of tool sets to exploit them. The author also tried to describe how to execute these attacks from both a Windows domain box and an external Linux VM , platform of an attacker. Kerberos is a protocol for network authentication that operates on the concept of handing out tickets to nodes to give access based on privilege level to services / resources. Kerberos is commonly used in Active Directory environments, and often in Linux, but mostly in Active Directory environments.

According to author Jeff petters [16], to check the identities of Active Directory entities, Kerberos utilizes authentication tokens or tickets. This comprises customers, accounts for the service, domain administrators, and systems. The author clarified that by breaching a computer account password and using it to create a fake authentication ticket; a hacker can produce a Silver Ticket. Without double checking that their token is actually legitimate, Kerberos allows services (low-level operating system programs) to log in, which hackers have used to build Silver Ticket

The Kerberos transfer protocol allows[17] a Kerberos service (i.e. a service configured to just use Kerberos authentication features) to receive a Kerberos principle service ticket on its own since no user token is needed for the transfer to occur. Authorization data for Windows will easily surpass over 1500 bytes. Since only computers with a Windows operating system need Windows authorization data, Windows-specific data is excluded from tickets on computers with other operating systems. Messages containing tickets to PCs with other working frameworks are well inside the restrictions of

UDP transport, so that is the means by which they are communicated. Messages containing tickets for PCs running Windows are probably going to surpass the breaking point, so those messages are sent utilizing the Transmission Control Protocol (TCP), which has a lot more noteworthy limit.

3. METHODOLOGY

3.1 Entities in Kerberos flow:

a) Client: Begins the contact of a request for a service. Works on the user's behalf.

b) Server: The server that holds the resource that the user wishes to access.

c) Authentication Sever (AS): Provides authentication for clients. The AS offers a ticket called TGT (Ticket Awarding Ticket) if the client is effectively authenticated. For other servers, TGT proves that the user has been authorized.

d) Key Distribution Centre (KDC): Authentication severs are divided into three parts in the Kerberos environment: database, authentication server (AS) and ticket granting server (TGS). In a single server, all these sections are present and are referred to as the Key Distribution Centre, which is defined in Figure 1.

e)Ticket Granting Server (TGS): An application server that acts as a service for the allocation of service tickets.

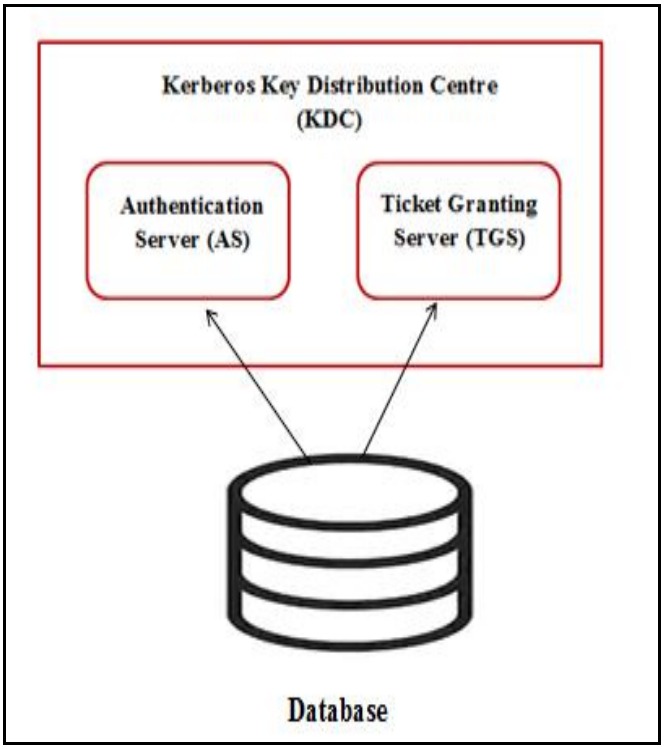

Figure 1: Components of key distribution center

There are 3 major secret keys in Kerberos Flow. For clients / users, TGS and servers that are shared with the AS, there is a special secret key.

a. Client / server secret key: Hash extracted from the password of the server.

b. TGS Secret Key: The password hash that is used to evaluate TGS.

c. Server secret key: The password hash that is used to evaluate the server that provides the service.

3.2 Operation of Kerberos authentication protocol.

Users have to log in to their account initially. The client's secret key will be determined by using the user's password. It accompanied the real flow of Kerberos. The procedure will normally be taken out and outlined in Figure 2 below with the steps below.

Stage 1: Service request from TGS.

Step 2: Access permissions rights in the Authentication Server checked in database, after which TGT and Session key are given. The results are then secured using the user's password.

Step3: The message is decrypted using a password, followed by the ticket being submitted to the Ticket Granting Server. Authenticated information, such as user name and network address, is included in the ticket.

Stage 4: TGS decrypts the ticket that the user / client sent from the authenticator, by verifying the request and then produces a server request ticket.

Stage 5: The sender transmits an authenticator and a ticket to the server.

Step-6: The server checks the ticket, and authenticators provide service access. The user / client will use the services there for a while.

3.3 Silver Ticket Attacks

A Silver Ticket is a forged authentication service ticket, also referred to as a Ticket Granting Service (TGS) ticket (this may be a user account or a computer account). There is no interaction with the Domain Controller (AS-REQ / AS-REP and TGS-REQ / TGS-REP) while using Silver Tickets, as seen in figure 3, since a Silver Ticket is a forged TGS. It is more difficult to detect Silver Tickets than Golden Tickets because there is no contact between the service and the domain controller and any logging to the targeted device is local. Hence it's very useful to use this attack as a persistence

technique. Silver Ticket Attacks are post-exploitation attacks. That means that a threat actor must already have compromised a target system in the environment before they can generate a Kerberos Silver Ticket.

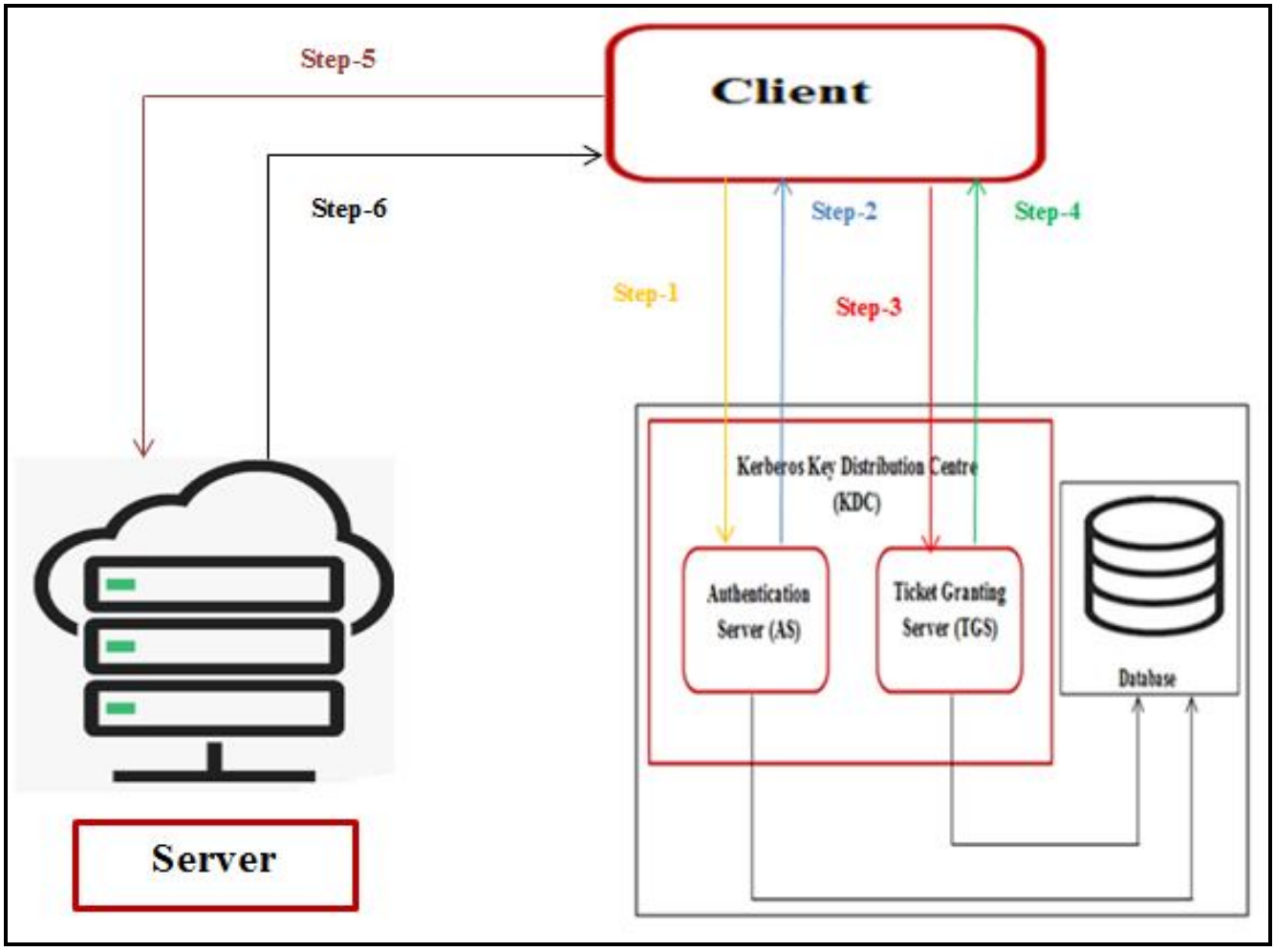

Figure 2: Operation of Kerberos authentication protocol

3.3 Silver Ticket Attacks

A Silver Ticket is a forged authentication service ticket, also referred to as a Ticket Granting Service (TGS) ticket (this may be a user account or a computer account). There is no interaction with the Domain Controller (AS-REQ / AS-REP and TGS-REQ / TGS-REP) while using Silver Tickets, as seen in figure 3, since a Silver Ticket is a forged TGS. It is more difficult to detect Silver Tickets than Golden Tickets because there is no contact between the service and the domain controller and any logging to the targeted device is local. Hence it's very useful to use this attack as a persistence technique. Silver Ticket Attacks are post-exploitation attacks. That means that a threat actor must already have compromised a target system in the environment before they can generate a Kerberos Silver Ticket.

3.3.1 Working of silver ticket attack:-

Step 1: Generate the password hash of the Network Technology LAN Manager (NTLM) by either a server account
running a server on a device or a device account itself (e.g. by Kerberoasting, or by hosting local administrator accounts).

Step 2: Utilize the Mimikatz command 'kerberos::golden' to build a Silver Ticket by passing the Domain SID, Target Host Name, Service Name, User Name and Group Information.

Step 3: Insert the fake number into your memory and enable the target service remotely**.**

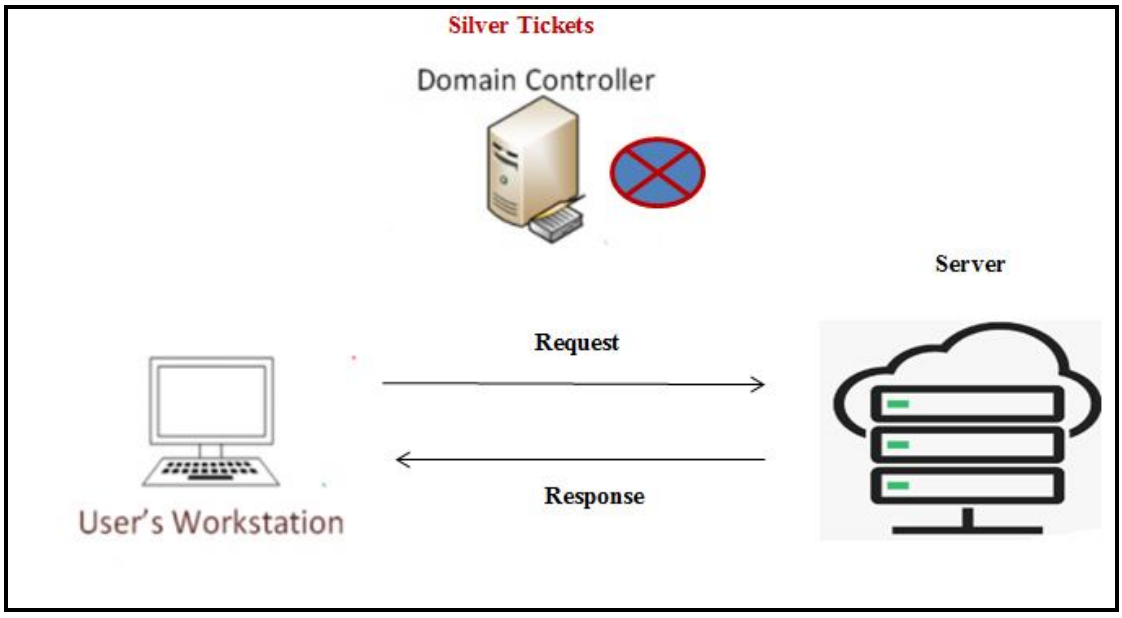

Figure 3: Silver ticket process do not communicate with Domain Controller

3.4 Attack Demonstration

The aim is to focus on the demonstration of the attack that is illustrated in figure 4. Assuming that the NTLM (Rivest Cipher 4 - RC4) of target server2 account during the post-exploitation. However, the demonstration of this attack from (server1.abc.local) and trying to achieve a command execution on (server2.abc.local). First step was to collect some information using PowerView.ps1 or Active Directory PowerShell module, and already compromised with server1 and got a domain user (any user) who has local admin privilege on server1[18].

Current user (any user) does not have any privileges or access to the target server (server2).As mentioned earlier, already have the NTLM (RC4) of server2 account, so no need to get to domain's SID to complete the attack requirement. Next, objective was to choose the *Service principal name* (SPN) , which is a name of service for which TGS is to be created, this service must be existing in the targeted server. Since all the required information, can be used to Invoke-Mimikatz.ps1 to proceed attack.

Case-1: A Command Execution using PowerShell Remoting

PowerShell Remoting uses some set of services to work like HOST, HTTP, OR WSMAN RPCSS(Windows Remote Server Administration Tools) which are dependent on OS, there is a need to create a silver ticket for these services and make them to use against target server (server2.abc.local). Note that (real domain user) is a normal domain user with no access to server2.abclab.local server. Forging of a two silver tickets for HOST & HTTP services which are required for PowerShell Remoting service on a remote system (server2.abc.local).Then the execution commands on server2.abc.local have used to Invoke-Command, which give us an ability to execute PowerShell commands on Remote system as shown in figure 5.

Figure 4: Local admin access on server1

```
C:\Users\anyuser\abc>klist

Current LogonId is 0:0*21eb18

Cached Tickets : (2)

#0>     Client : realdomainuser  @ abclab.local
        Server :HTTP/Server2.abclab.local @ abclab.local
      KerbTicket Encryption Type :RSADSI RC4-HMAC(NT)
      Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
      Start Time : 06/08/2020 4:32:49 (local)
      End Time : 06/04/2030 4:32:49 (local)
      Renew Time : 06/04/2030 4:32:49 (local)
      Session Key Type : RSADSI RC4-HMAC(NT)
      cache Flags : 0
      kdc called :

#1>   Client : realdomainuser  @ abclab.local
      Server : HOST/Server2.abclab.local @ abclab.local
      KerbTicket Encryption Type :RSADSI RC4-HMAC(NT)
      Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
      Start Time : 06/08/2020 4:32:49 (local)
      End Time : 06/04/2030 4:32:49 (local)
      Renew Time : 06/04/2030 4:32:49 (local)
      Session Key Type : RSADSI RC4-HMAC(NT)
      cache Flags : 0
      kdc called :
```

Figure 5: Command execution access on server2 using Invoke-command after using host tickets

Case-2: Command Execution using Scheduled Tasks

Similar to PowerShell Remoting process, the process starts by creating a silver ticket for one service, which is HOST so scheduling a Task with SYSTEM Privileges can happen (server2.abclab.local). Entering HOST ticket to session done by Invoke-Minikatz.ps1. Then carried with scheduling a task to make it run on remote server (server2.abc.local) with SYSTEM privilege. The PowerShell command gives us a reverse shell using Invoke- PowerShellTcp.ps1which has been described in figure 6. Finally, the same approach can be used with the other services like WMI, WinRM. Some services can give more than command execution like Lightweight Directory Access Protocol (LDAP) service which allows you to gain and use DC Sync rights.

```
Client : realdomainuser  @ abclab.local
 Server : HOST/Server2.abclab.Local @ abclab.local
 KerbTicket Encryption Type :RSADSI RC4-HMAC(NT)
Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
Start Time : 06/08/2020 4:32:49 (local)
End Time : 06/04/2030 4:32:49 (local)
Renew Time : 06/04/2030 4:32:49 (local)
Session Key Type : RSADSI RC4-HMAC(NT)
cache Flags : 0
kdc called :
C:\Users\anyuser\abc > schtasks / create / S server2.abclab.local / SC Weekly / RU "NT Authority/System"/
TN"pwntask"/ TR "powershell.exe -C iex(New-objectnet.Webclient).Download String ("http://10.10.10.10.2 / Invoke -Powershell
TCP.ps1") : Invoke -PowershellTCP-Reverse-IP Address 10.10.10.2-port 443".

SUCCESS : The Scheduled task "pwntask" has successfully been created.
C:\Users\anyuser\abc > schtasks / Run / S server2.abclab.local / TN "pwntask"
C:\Users\anyuser\abc>
```

Figure 6: Scheduling task on and running it on remote target server2.abclab.loc

4. CONCLUSION

Kerberos was designed to support network applications that can safely identify their peers. Kerberos is particularly concerned with authentication; the relevant protection does not concern directly regarding authorization and accounting roles. Supporting incorporation of these relevant functions by other resources, Kerberos offers a tamper-proof transmission system for authorization. This paper gives overview of steps involved in operation of Kerberos authentication protocol, overview and working of silver tickets and considered with two cases of attack demonstration which shows Command Execution using PowerShell Remoting and command execution using scheduled tasks by performing a security check on the attacks.

REFERENCES

[1] Mr. Parikshith Nayaka S K, Mrs. Shobha Rani, Dr. Dayanand Lal, Dr. M Anand. (2020). "**Convert Channel and Information Hiding in TCP/IP"** . *International Journal of Control and Automation*, *13*(02), 582 - 591. Retrieved fromhttp://sersc.org/journals/index.php/IJCA/article/view/11199

[2] John T. Kohl, B. Clifford Neuman, Theodore Y. Ts'o ," **The Evolution of the Kerberos Authentication Service "** .

[3] Chandni Grover, Manpreet Kaur Aulakh, **"Big Data Authentication and Authorization in HDP (Hadoop Distributed platform) using Kerberos and Ranger".**

[4] Kashefi, Iman & Kassiri, Maryam & Shahidinejad, Ali, **"A Survey on Security Issues in Firewalls: A New Approach for Classifying Firewall Vulnerabilities".**

[5] Jennifer G. Steiner,Clifford Neuman, Jeffrey I. Schiller, **"Kerberos: An Authentication Service for Open Network Systems".**

[6] Min Li, Xin Lv, Wei Song, Wenhuan Zhou, Rongzhi Qi, Huaizhi Su, "**A Novel Identity Authentication Scheme of Wireless Mesh Network Based on Improved Kerberos Protocol"**, Distributed Computing and Applications to Business Engineering and Science (DCABES) 2014 13th International Symposium on, pp. 190-194, 2014.

[7] S. T. F. Al-Janabi and M. A. Rasheed, "**Public-Key Cryptography Enabled Kerberos Authentication,"** 2011 Developments in E-systems Engineering, *Dubai, 2011, pp. 209-214, doi: 10.1109/DeSE.2011.16.*

[8] , Shobharani D, Parikshith Nayaka S K, Swasthika Jain T, Dr. Dayanand Lal ," **Effective and Secure Approach for Multi-Keyword Quest Graded over Authenticated Data",** International Journal of Advanced Trends in Computer Science and Engineering, 2020, volume 9, number 2, pages 2278-3091

[9] Cheng Xiao-rong, Feng Qi-yuan, Dong Chao and Zhang Ming-quan, "**Research and realization of authentication technique based on OTP and Kerberos**," Eighth International Conference on High-Performance Computing in Asia-Pacific Region (HPCASIA'05), Beijing, 2005, pp. 5 pp.-416, doi: 10.1109/HPCASIA.2005.86.

[10] A. H. Harbitter and D. A. Menasce, "**Performance of public-key-enabled Kerberos authentication in large networks,"** Proceedings 2001 IEEE Symposium on Security and Privacy. S&P 2001, Oakland, CA, USA, 2001, pp. 170-183, doi: 10.1109/SECPRI.2001.924297.

[11] N. T. Abdelmajid, M. A. Hossain, S. Shepherd and K. Mahmoud, "**Location-Based Kerberos Authentication Protocol,**" 2010 IEEE Second International Conference on Social Computing, Minneapolis, MN, 2010, pp. 1099-1104, doi: 10.1109/SocialCom.2010.163.

[12] Dr. Brahmananda S.H, Dr. Dayanand Lal N, Mrs. Sahana D S, Mrs. Chaitanya B N, Mrs. Veena R C," **Investigation On Domain Controller Synchronization Attacks "**.

[13] Michael Schneider, Marc Ruef **," Kerberos under Attack".**

[14]https://www.qomplx.com/qomplx-knowledge-silver-ticket-atta

[15]https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc772815(v=ws.10)?redirectedfrom=MSDN

[16]https://m0chan.github.io/2019/07/31/How-To-Attack-Kerberos-101.html

[17]https://www.varonis.com/blog/kerberos-attack-silver-ticket/

[18] Jacob, I. Jeena. (2020). "**Ensuring Network Security using Secured Privileged Accounts".** International Journal of Emerging Trends in Engineering Research. 8. 1959-1963. 10.30534/ijeter/2020/80852020.