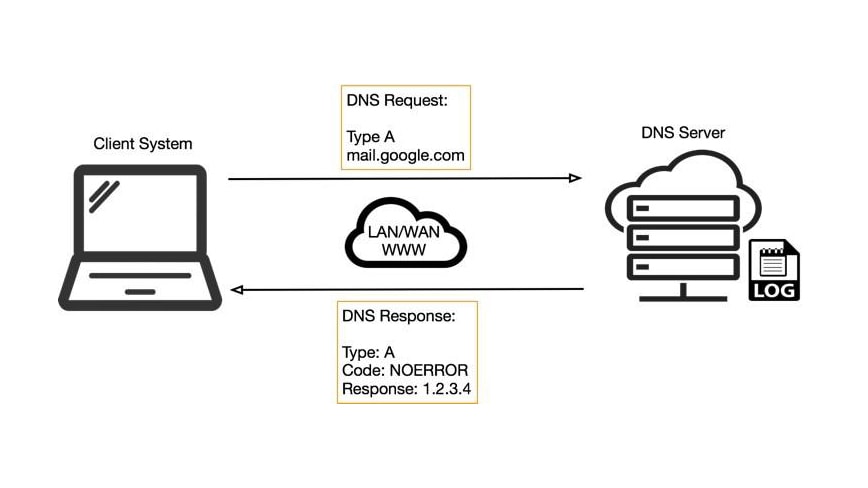
Domain name system, or DNS, is the protocol that translates human-friendly URLs, such as paloaltonetworks.com, into machine-friendly IP addresses, such as 199.167.52.137.

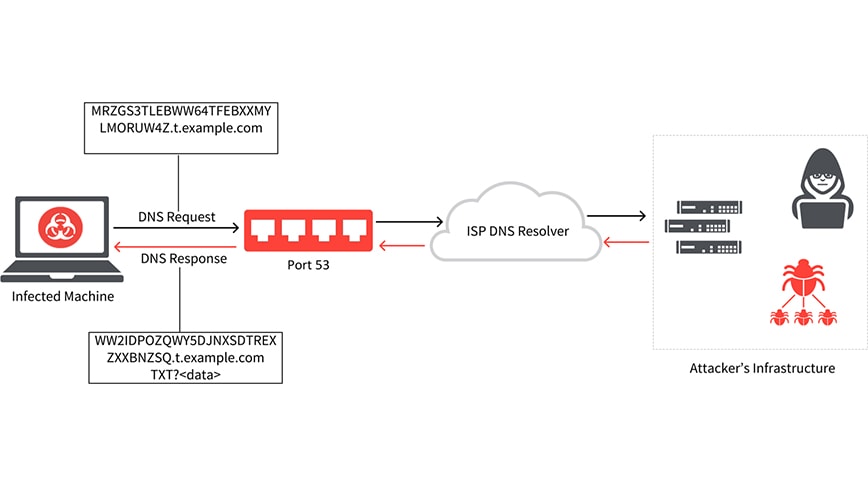
DNS is a critical and foundational protocol of the internet. It is often described as the “phonebook of the internet” because it maps domain names to IP addresses (and much more as described in the [core RFCs](https://tools.ietf.org/html/rfc1034.html) for [the protocol](https://tools.ietf.org/html/rfc1035.html)).



**How DNS Tunneling Works**

DNS tunneling attacks exploit the DNS protocol to tunnel malware and other data through a client-server model.

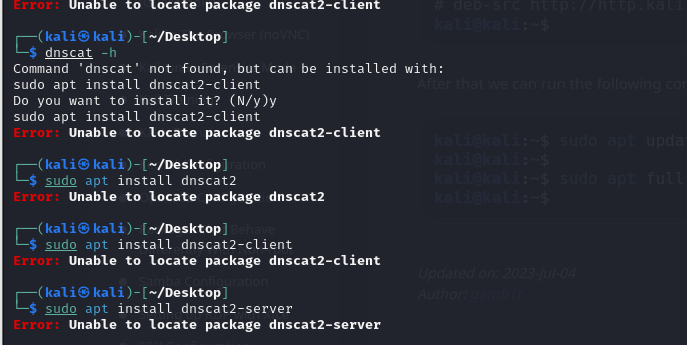
1. The attacker registers a domain, such as badsite.com. The domain’s name server points to the attacker’s server, where a tunneling malware program is installed.
2. The attacker infects a computer, which often sits behind a company’s firewall, with malware. Because DNS requests are always allowed to move in and out of the firewall, the infected computer is allowed to send a query to the DNS resolver. The DNS resolver is a server that relays requests for IP addresses to root and top-level domain servers.
3. The DNS resolver routes the query to the attacker’s command-and-control server, where the tunneling program is installed. A connection is now established between the victim and the attacker through the DNS resolver. This tunnel can be used to exfiltrate data or for other malicious purposes. Because there is no direct connection between the attacker and victim, it is more difficult to trace the attacker’s computer.



Assuming that a local authoritative server is present which in turn reaches out to the DNS servers to fetch the requested website this project has been demonstrated

We use dnscat2 tool to demonstate the DNS tunneling attack.   
dnscat2 has both the server and client there fore it used for the demonstration.

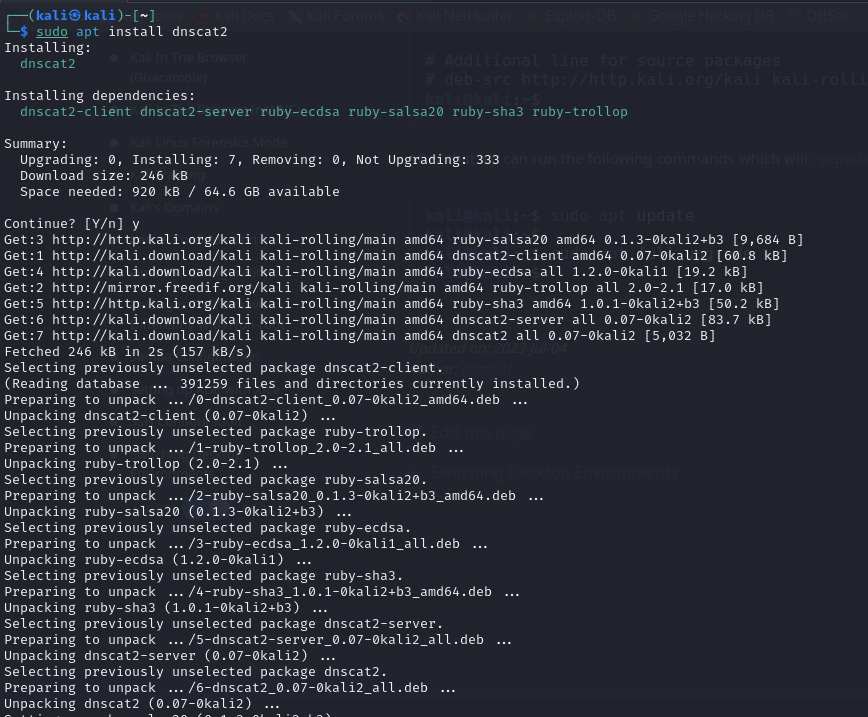
Step 1: using the command “sudo apt install dnscat2” install the package.



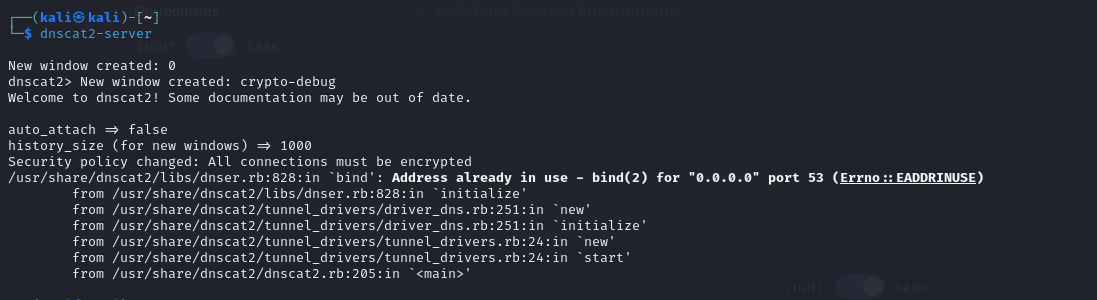
If the following error occurs update the kali and upgrade the packages installed using below command

Sudo apt update

After update retry installation command which will be resulting the below image



To check the whether the package is installed successful or not run dnscat2-server command resulting the following image

  
  
In the above image, the server cannot run as the OS is using port 53 to listen to the DNS resolvers, so use a different port but manually mention it or stop the DNS services. Stopping the DNS service can create problem for other programs to run.

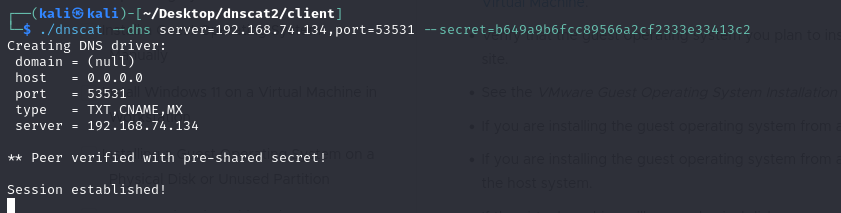
Run the following command to start the server  
sudo dnscat2-server – dns host=x.x.x.,port= xxx, domain=evilhacker.com

Evilhacker.com is the opensource domain used for learning hacking techniques



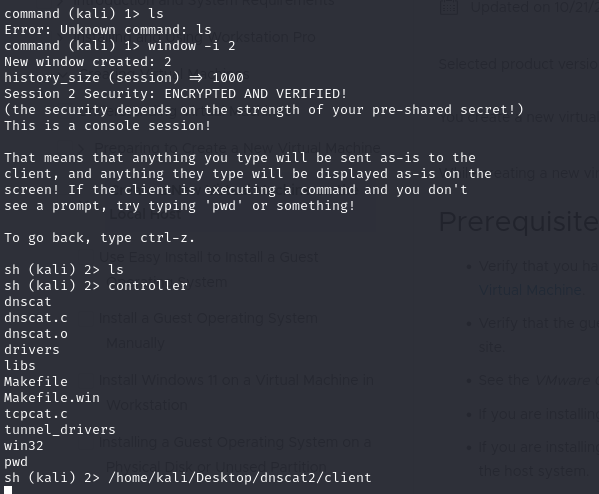
Running the command would result in the above image. This shows that the DNS server of the attacker is up and running, now on Any DNS requests by the client would be taken to this server, and the attacker can respond as required.

For the demonstration puporse, we run the client in the next and once the connection is established the attacker can pass commands to the client system and execute commands

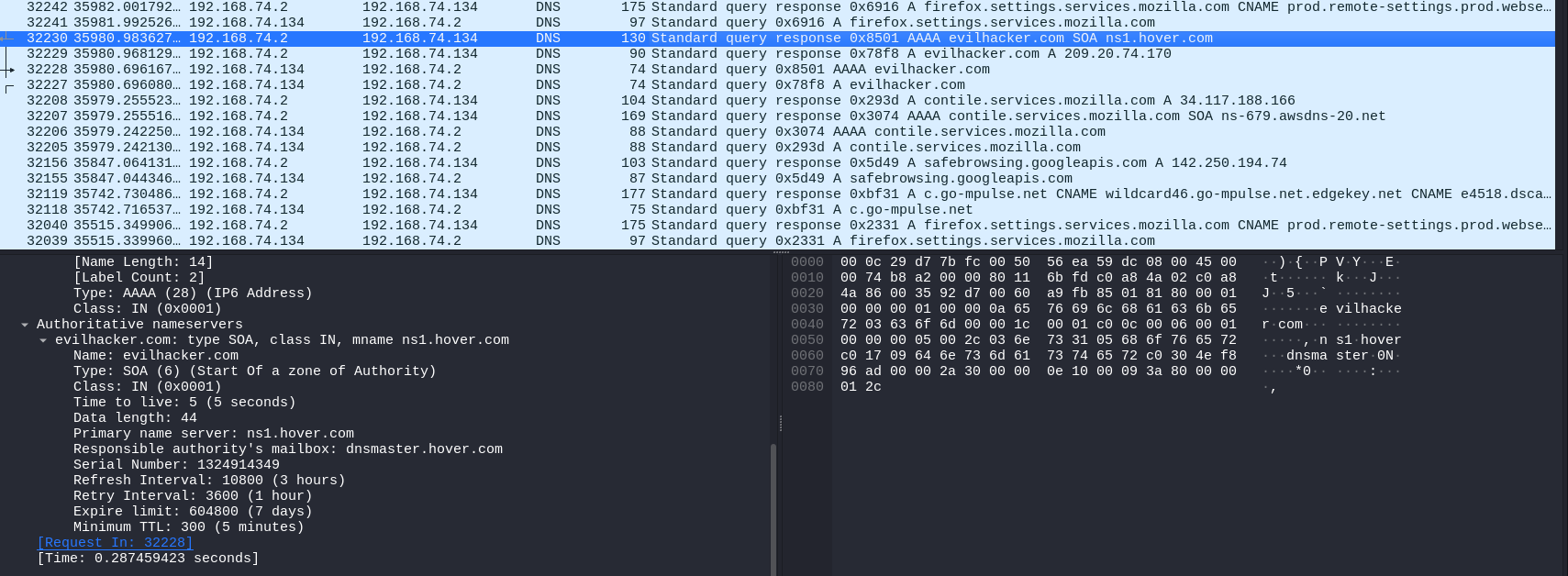


As the connection established the above image is the result of it.

We use dnscat2 command window to create windows to execute commands on the client side.  
below is the image of the basic commands excuted on the client side.



To confirm communication between server and client we used wireshark to capture the packets and results are as follows



We see that the client is requesting for the evilhacker.com to the attacker set dns server which is running on 192.168.74.134

## Preventing DNS Tunneling

DNS is a very powerful tool used almost everywhere, allowing applications and systems to look up resources and services with which to interact. DNS provides a communication foundation enabling higher level and more powerful protocols to function but can mean it’s overlooked from a security point of view, especially when you consider how much malware is delivered via email protocols or downloaded from the web using HTTP.

For these reasons, DNS is the perfect choice for adversaries who seek an always-open, overlooked and underestimated protocol to leverage for communications from and to compromised hosts.

Organizations can defend themselves against DNS tunneling in many different ways, whether using [Palo Alto Networks Network Security Platform](https://www.paloaltonetworks.com/network-security) or open source technology. Defense can take many different forms, such as but not limited to, the following:

* Blocking domain-names (or IPs or geolocation regions) based on known reputation or perceived danger.
* Rules around “strange looking” DNS query strings.
* Rules around the length, type or size of both outbound and inbound DNS queries.
* General hardening of the client operating systems and understanding the name resolution capabilities as well as their specific search order.
* User and/or system behavior analytics that automatically spot anomalies, such as new domains being accessed especially when the method of access and frequency are abnormal.
* Palo Alto Networks recently introduced a new [DNS security service](https://www.paloaltonetworks.com/resources/datasheets/dns-security-service) focused on blocking access to malicious domain names.

## DNS Security Best Practices

* **Train and educate your security staff**  
  Implement a security education and awareness program to train your staff to identify malicious threats. Encourage them to take precautions when following links to avoid installing [malware](https://www.paloaltonetworks.com/cyberpedia/what-is-malware). [Phishing](https://www.paloaltonetworks.com/cyberpedia/what-is-phishing) training can help them learn to recognize, avoid and report email-based attacks.
* **Implement a threat intel program**  
  Understand the threat landscape and set up a threat intelligence program to be aware of the different types of threats and techniques attackers are using today. With this knowledge, you can ensure you have the right technology stack to keep your network safe.
* **Learn what DNS data can tell you**  
  Don’t just look at DNS traffic. Collecting DNS data logs has little value unless you understand what you’re looking at. By understanding the data, you can successfully prevent your organization from never-before-seen, DNS-layer threats.
* **Don’t delay on a DNS resolver**  
  If a DNS server is compromised, it may feed you false responses meant to direct your traffic to other compromised systems or enable a man-in-the-middle attack.
* **Plan for the risk of remote work**  
  Develop a strategy for your [remote workforce](https://www.paloaltonetworks.com/sase) as they can put sensitive company data at risk. Warn them against using unsecured, free or public Wi-Fi as adversaries can easily put themselves between employees and the connection point. Integrate multifactor authentication and prepare for the risk of devices being lost or stolen.
* **Approach network security holistically**  
  Take a holistic approach to network security and ensure you have the right capabilities that can address various threat vectors in your network and be easily integrated within your entire security stack. When evaluating vendor solutions, it’s important to make direct comparisons in proofs of concept. Every environment is different, and independent vendor-neutral testing for DNS-layer security has not yet been established.
* **Automate responses and not just alerts**  
  To successfully protect your organization, you need automated responses and not just alerts. The speed at which threats are carried out makes alerts and signals ineffective. By the time a threat has been identified, it may already be too late. Your security team needs to be able to automatically determine threats and quarantine potentially infected systems before more damage is done. In order to ensure your organization is following best practices and optimizing Palo Alto Networks DNS Security service, take a [Best Practice Assessment](https://www.paloaltonetworks.com/services/bpa).