Information security-IV

Prof. Vasan
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Module-18
Lecture - 18
Server Side Attacks (Cont)
Tools in Kali Linux

We are going to continue our discussions on the different tools that are there available for a penetration tester to do any kind of a server side attacks. So, on the previous session we had looked at a couple of tools for getting more details on a particular web server or a web portal by doing a crawling of that particular site.

So, in this session we are going to look at a proxy software tool and what kind of detail we could possibly get from using this particular tool. Now before we getting that we just need to do a quick recap on what we exactly mean by a proxy software and why does somebody use a proxy software.

So, a proxy software is typically used for some of the application protocols which will actually act as an intermediary between the client and the actual destined server. Now why should a proxy software be lying as an intermediary between the client and the server?

There are few reasons for it; one of the reasons that is very commonly used especially if you consider for example, the HTTP protocol is that if I use a HTTP proxy software application; using this proxy, I will be able to cache the contents from the server locally on this particular server where I am running the proxy software and thereby, get the response back for the clients who is actually asking for the contents very quickly as compared to trying to get fetch the content from a remote server every time.

So, for example, if I have a for example, a proxy software application running on one of my servers in my local network only the first instance where I do not have the content that has been requested right now over HTTP available locally as part of my cash; I need to really go all the way to the internet fetch the content and then, delivered to the client.

But having done that once, if I am basically able to service the next request that is coming for the same content from my local network from other clients, I will be able to have a quicker turnaround time for those request. Because my traffic need not be travelling all the way over the internet to reach the actual destined server and then come back.

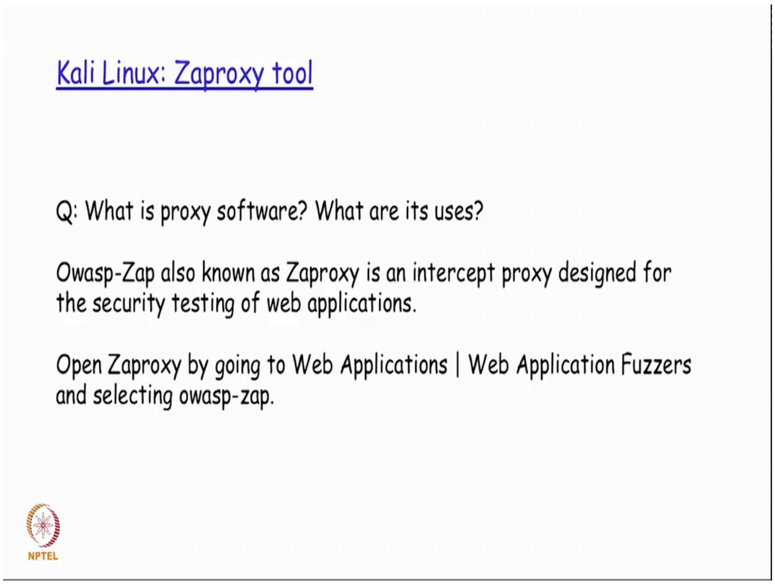
So, this is predominantly one reason why the administrators prefer to use a proxy software and another prominent reason is all also to do some sort of administration of either enabling or disabling access for different type of users. So, the different type of users here could actually mean based on the user ID or it could be based on IP addresses from which taxes being made and so on.

So, for example, if you might have actually come across some organisations, who do not allow access to some of the social engineering sites like Facebook or Twitter from their organisation network right. But this is not a common policy across all the employees in that organisation.

But there will be certain employees at a certain level who will be allowed access rights. So, again with something with tool like a proxy software, the administrator will be able to sort of differentiate between who is actually trying to access the particular URL site and by the policy defined as part of the software right now either allow or deny that particular request.

So, predominantly you will find the proxy software is actually used for these kind of a purposes. So, one is to basically improve the performance of the request a turnaround times and two, to sort of have it is an effective administration tool where by access policies can be very easily implemented. Now there is a call Zaproxy.

(Refer Slide Time: 04:18)



Kali Linux: Zaproxy tool

Q: What is proxy software? What are its uses?

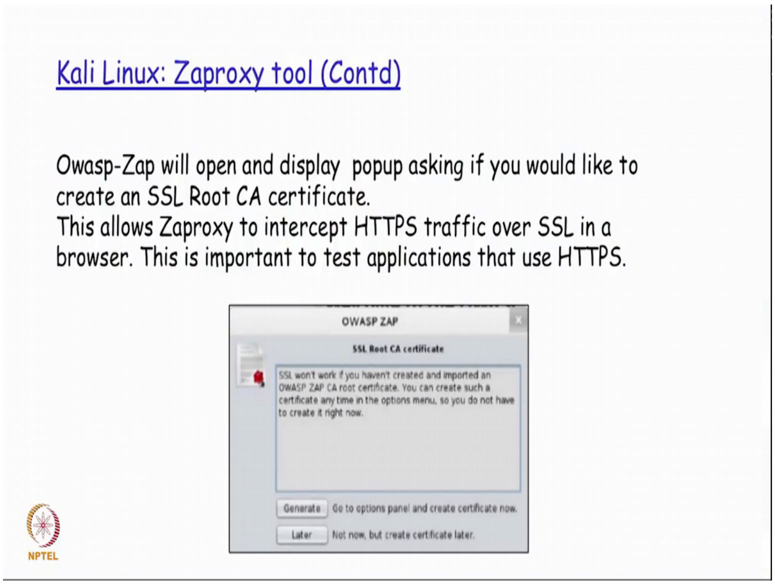
Owasp-Zap also known as Zaproxy is an intercept proxy designed for the security testing of web applications.

Open Zaproxy by going to Web Applications | Web Application Fuzzers and selecting owasp-zap.

That is actually available and very commonly used. It is basically intercept proxy which is really designed for security testing of publication. So, with this tool, being available in Kali Linux.

So, it is actually available under web applications sub menu and web application process grouping; you can really find out how the proxy server is actually working and what are the initial steps that are really required to actually have it started.

(Refer Slide Time: 04:57)



Kali Linux: Zaproxy tool (Contd)

Owasp-Zap will open and display popup asking if you would like to create an SSL Root CA certificate.
This allows Zaproxy to intercept HTTPS traffic over SSL in a browser. This is important to test applications that use HTTPS.

OWASP ZAP

SSL Root CA certificate

SSL won't work if you haven't created and imported an OWASP ZAP CA root certificate. You can create such a certificate any time in the options menu, so you do not have to create it right now.

Generate Go to options panel and create certificate now.

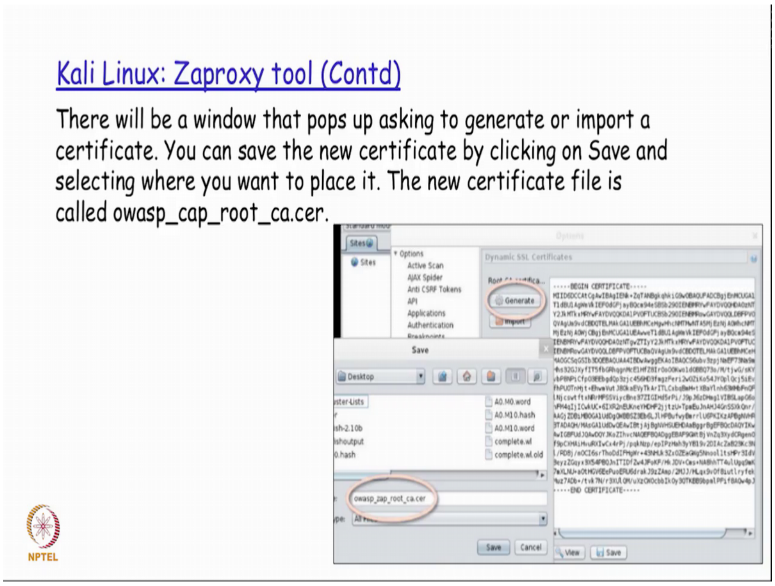
Later Not now, but create certificate later.

So, when you actually open up the there is a particular application you might actually have a popup asking if you would like to have a SSL Root certificate that is created specifically for you.

So, as you would have seen and learnt in the previous ISD code that as well as during the refresher part of this particular IS4 SSL is basically and encryption mechanism that is used between the browser and the server the web server typically to have your contents all encrypted before it is actually sent out onto the internet right.

So, this certificate will basically allow this creation on the certificate will basically allow the HTTPS traffic over SSL also to be sort of intercepted and then presented to you as a user of this particular tool.

(Refer Slide Time: 05:00).



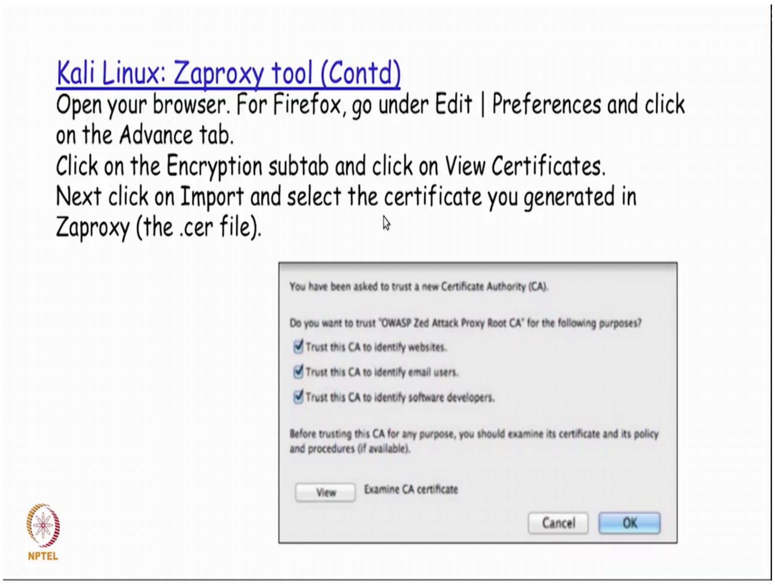
Kali Linux: Zaproxy tool (Contd)

There will be a window that pops up asking to generate or import a certificate. You can save the new certificate by clicking on Save and selecting where you want to place it. The new certificate file is called owasp_cap_root_ca.cer.

So, what exactly happens is first, one needs to generate this particular certificate. So, at the popup of that is there you will have a generate button that will be available. So, when one presses the generate button, the certificate will be generated that you see here. And then the certificate will actually be required to be saved by pressing the save button with the particular name available.

So, one possible example of a name could be something like this. So, whatever name that is actually been given as part of the save dialogue box, the file the certificate that is actually getting generated here will be saved in that particular name right.

(Refer Slide Time: 06:24)



Kali Linux: Zaproxy tool (Contd)

Open your browser. For Firefox, go under Edit | Preferences and click on the Advance tab.

Click on the Encryption subtab and click on View Certificates.

Next click on Import and select the certificate you generated in Zaproxy (the .cer file).

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "OWASP Zed Attack Proxy Root CA" for the following purposes?

☑ Trust this CA to identify websites.

☑ Trust this CA to identify email users.

☑ Trust this CA to identify software developers.

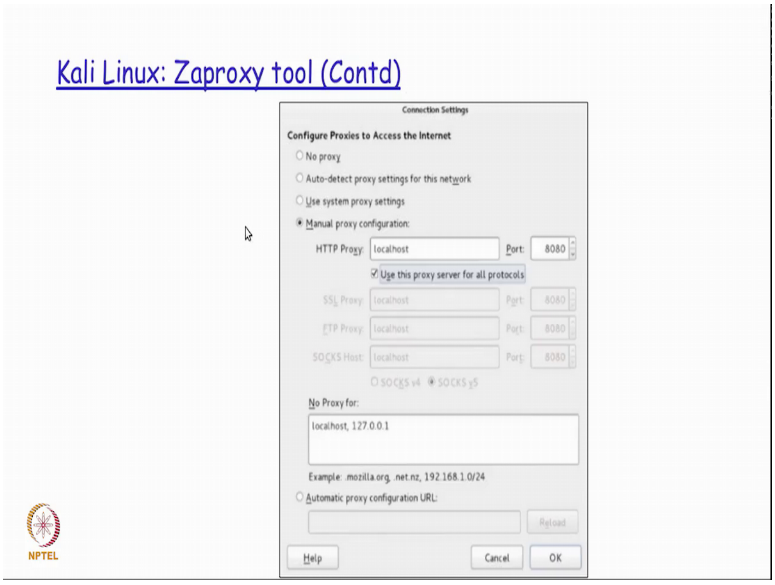
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Once, this particular file is actually generated and then, saved this needs to be imported as a valid certificate right. Now why is this needs to be imported is a valid certificate is that because the certificate is actually used for the exchange of what he has to be used by the client browser and the actual web server on the server side to be used for encryption and decryption.

So, depending on what browser you have the menu options could be slightly different. So, assuming that we are actually making use of the Firefox browser, we really going into edit preferences and then, on the advanced tab you will have an encryption sub tab in which we could we could see view certificate right.

So, there you could actually have a import button and then choose that particular certificate that you have generated and then, saved in the previous dialogue and give that as the file to be imported right. So, whatever is a dot cer file that was actually saved as part of the generational certificate and these the savings process.

(Refer Slide Time: 07:42)



Kali Linux: Zaproxy tool (Contd)

Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: localhost Port: 8080

☑ Use this proxy server for all protocols

SSL Proxy: localhost Port: 8080

FTP Proxy: localhost Port: 8080

SOCKS Host: localhost Port: 8080

○ SOCKS v4 ● SOCKS v5

No Proxy for:

localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

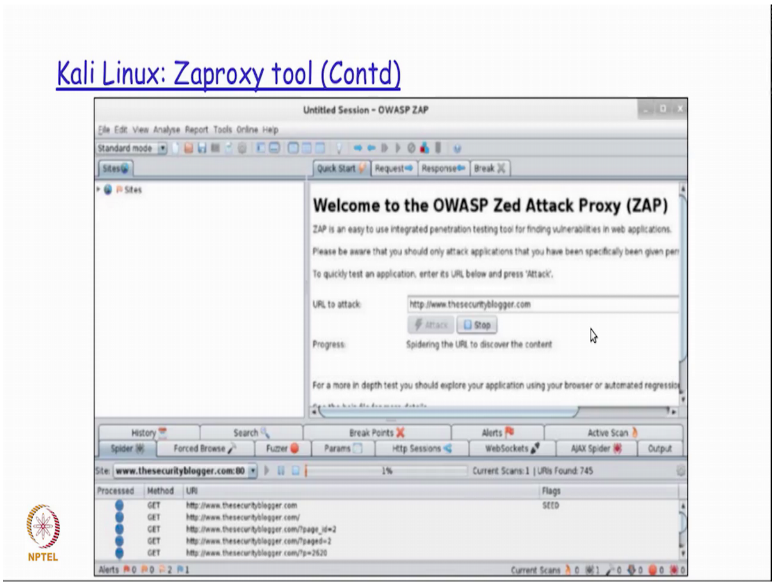
That cer file is right now given here as part of importing after which this, certificate file will be also used by the browser for exchanging of the key required for doing encryption or decryption between the browser and the server side right. So, as we had seen before this key needs to be exchanged between the 2 sides or the SSL mechanism to be successful.

And using this particular certificate the key could potentially we getting exchange between the between the 2 ends on the clients and the on the on the server side right. Now before we actually go ahead and use a Zaproxy tool, we also need to do one more setting on the browser side where we actually need to configure the proxy configuration right.

So, the proxy configuration we specify where is the proxy going to be available. So, in this particular case it is local host which is essentially nothing but the same server, the same mission on which we are right now running the browser also. And then, what is the port number on which is actually going to be running right. So, this is basically the well known port number that is typically used for a proxy server. So, some of the other ports port numbers that are used for proxy server could be either 8000 or 80000 and so on.

But in this case, we will actually have this running on port number 80 80. So, we specify the proxy local host because the proxy is going to be running on the same machine as the browser that is currently run browser is currently running on and we specify 80 80 as a port number on which the proxy is going to be as we listening and running.

(Refer Slide Time: 09:21)



Kali Linux: Zaproxy tool (Contd)

Untitled Session - OWASP ZAP

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given per

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://www.thesecurityblogger.com

Progress: Spidering the URL to discover the content

For a more in depth test you should explore your application using your browser or automated regressio

Site: www.thesecurityblogger.com:80 1% Current Scans:1 | URIs Found: 745

Processed	Method	URI	Flags
●	GET	http://www.thesecurityblogger.com	SEED
●	GET	http://www.thesecurityblogger.com/	
●	GET	http://www.thesecurityblogger.com/?page_id=2	
●	GET	http://www.thesecurityblogger.com/?paged=2	
●	GET	http://www.thesecurityblogger.com/?p=2620	

So, after this is actually said, you just press the button here which would have completed the configuration of all the required things to be done as far as a browser is concerned.

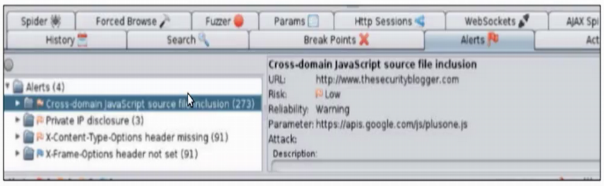
So, after this is actually said in the Zaproxy in the tool that I would open up from the Kali Linux menu option that we saw, I basically give the URL that I need to basically have the a make an attempt to sort of do the penetration testing right now right.

So, we go head press the URL that is there and then, after some point in time we find out the different URL that is actually getting access at the below frame there right.

(Refer Slide Time: 10:04)

Kali Linux: Zaproxy tool (Contd)

To see the vulnerabilities, click on the Alerts tab.



Alerts (4)
- Cross-domain JavaScript source file inclusion (273)
- Private IP disclosure (3)
- X-Content-Type-Options header missing (91)
- X-Frame-Options header not set (91)

Cross-domain JavaScript source file inclusion

URL: http://www.thesecurityblogger.com
Risk: Low
Reliability: Warning
Parameter: https://apis.google.com/js/plusone.js
Attack:
Description:

So, in each of these frames you could potentially have an attack that the penetration tester could be making use of and all those possible vulnerabilities are available as part of the Alert tab in this particular tool.

So, if you look at it here for the specific attempt that was made on this on that particular URL that is given as an input , there has been four different alerts that has actually been generated right. So, one alert is a cross domain JavaScript source file inclusion. Another could be a private IP disclosure and so on and so forth.

So, each of these Alerts again, has the possibility of it either being a very serious alert that needs the attention of the administrator to be immediately addressing it or alternatively it could also be a something which is just information purposes which could which would not possibly be a very serious issued to be looked at or addressed immediately.

So, depending on whether it is a security administrator who is actually running this tool to find out the different vulnerabilities or the penetration tester who is actually trying to get more and more details of this particular site that is trying to a target for attacking; appropriately, each of the alerts that is actually getting listed here will be handled the differently. If it is an administrator the administrator will try to actually resolvers those alerts as quickly as possible.

And similarly, if it is basic is a penetration tester who was run this tool and got these details, before the administrator basically sorts of get alerted with these alerts; the penetration tester who try to make use of these loopholes and then penetrate the system successfully.

Thank you.