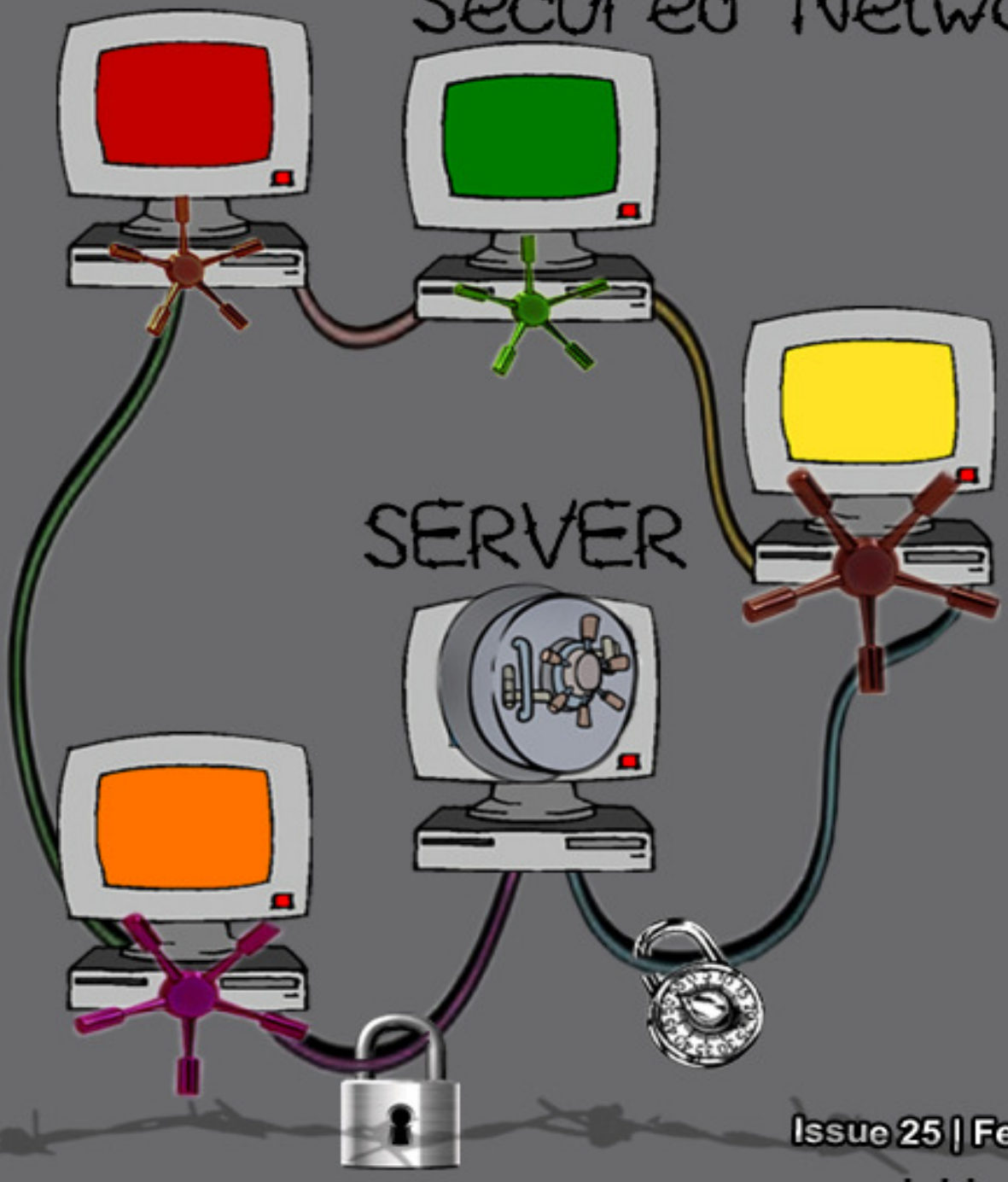
ClubHACK Mag

1st Indian "HACKING" Magazine



Issue 25 | Feb 2012

www.clubhack.com

TechGyan Exploiting Remote System without Being Online | **ToolGyan** Cain and Abel |

Mom's Guide Firewall 101 | **LegalGyan** Liability of Intermediaries under the IT Act |

It gives me immense pleasure to tell you that from 06-02-10 to 06-02-12 our magazine has completed two successful and rejoicing years. We at ClubHack are super excited! I hope you people are enjoying the magazine and would continue doing so it in the coming future too. We enjoy making this for you all.

It is said that "A lot can happen over a cup of coffee". We experienced this amazing moment over a cup of coffee when we had the idea of starting a hacking magazine and it now it has come all this way… :). 2 years looks small when we look back.

Rohit Srivastwa

For this incredible success we at ClubHack would like to thank all our readers, volunteers, and authors for giving us such unbelievable support. As we want to keep up the growth and progress therefore we request you all to keep throwing in articles, suggestions, support and your love!

ClubHACKMag

Issue 25, February 2012.

Team CHmag

Rohit Srivastwa
rohit@clubhack.com

Aarja Bhattacharyya
aarja@chmag.in

Abhijeet R Patil
abhijeet@chmag.in

Abhishek Nagar
abhishek@chmag.in

Pankit Thakkar
pankit@chmag.in

Sagar Nangare
sagar@chmag.in

Varun V Hirve
varun@chmag.in

www.chmag.in
info@chmag.in

CONTENTS

Exploiting Remote System without Being Online

Introduction

This paper demonstrates unique kind of communication technique between attacker machine and victim machine during the exploitation of any victim system. Usually, while an attacker exploits the remote system and gets the remote command prompt (remote shell), attacker is only able to execute commands till the session from the remote machine is opened (established). While exploiting the system in a normal way, attacker and the victim system both should be online, if attacker wants to execute some commands in remote machine (Victim Machine). This paper would demonstrate how an attacker can attack a remote victim without being online (attacker may or may be online AND victim may or may not be online).

History

During the exploitation of vulnerable remote system (victim system) by an attacker, after vulnerability injection, attacker sends payload and gets remote command prompt on his/her (attacker's) machine. In this case of normal payload, the limitation for an attacker is that, once the session is expired or shell is terminated, attacker can't execute commands in remote machine (victim computer).This white paper demonstrates new type of payload by using which attacker can execute command in remote machine (victim system) without actually directly connecting to victim machine and also fooling Antivirus, Firewalls etc.

My Method

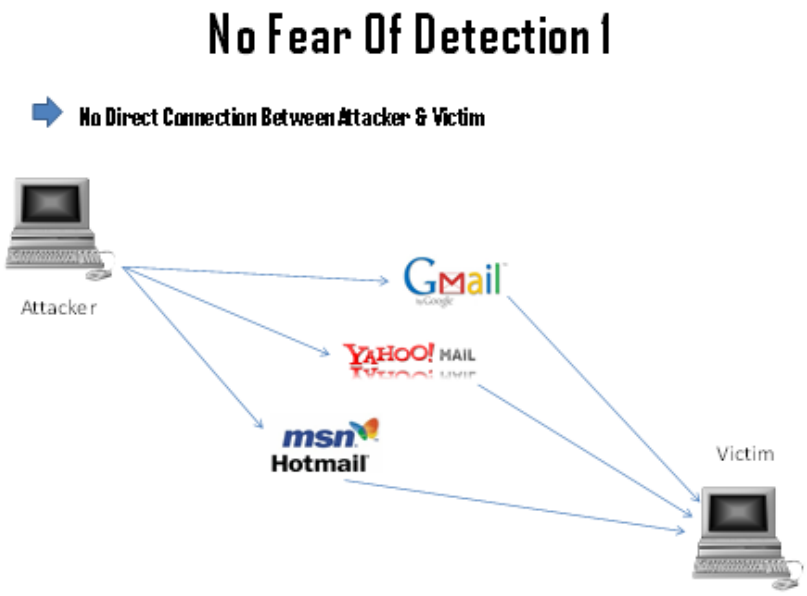
In general scenario, if attacker gets remote command prompt and execute command in the current session then there is direct communication (connection) between attacker and victim machine. But by using this paper's mechanism we can prevent direct communication (connection) between attacker and victim. For this, we use an intermediate server (zombie) that should be up and running all the time (24x7). In our case, we use this zombie as an email service like Gmail, Yahoo, msn etc. So the whole system works as explained below.

Attacker infects remote system with an Executable, which can be infected by one of the below mentioned methods:

1. By autorun.inf
2. During Metasploit Exploitation
3. Physical access of victim system

Now once Executable is up and running in the remote machine (Victim Machine), when the victim connects to the internet then it first checks the instruction set in Gmail inbox by an attacker. Now let's say if an attacker wants to execute command 'ipconfig' in remote machine (victim machine) then attacker has to send email with subject 'ipconfig' to his own email address . Because the username and password is already encrypted in the Executable file in the victim machine (remote machine), and as victim comes online , that executable file automatically logs in your Gmail account and reads all command instructions which is loaded by attacker.

It executes the commands of attacker's choice and attaches these results to the attacker's Gmail account. Attackers simply have to download that attachment which contains command output from victim machine. So there is an email service (Gmail) between attacker and victim machine. That shows, attacker can execute command in victim system but there is no direct connection between attacker and victim machine, and if an attacker uses Tor (The Onion Router Browser) or Anonymizers for accessing the Gmail account then attacker never can be caught (no reverse traces).It is something like Attacker <->email service <->Victim <->. So life cycle will be as shown below:



Attacker ←→Proxy ←→ Email Service ←→Victim

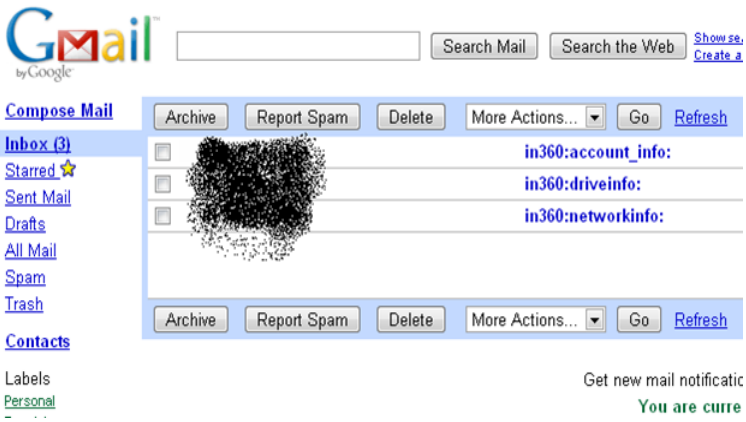
(Tor, Anonymizers) (Gmail, Yahoo, etc.)

(Proxy Case Scenario)

Hands-on-Approach

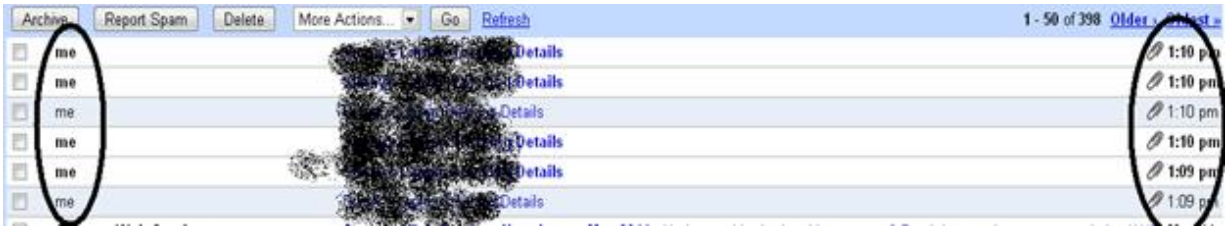
Stage I

Let's say you have infected remote system with this exe and you want account info, drive info and network info from the remote machine (victim machine) then you have to send email to your own account (note: which is also listened and shared by injected exe in remote victim machine) with subject containing account_info, driveinfo, networkinfo as shown in the figure on the next page.



Stage II

Now once the email with appropriate subject is sent to your account, now it's time for remote machine (victim machine) to be online and fetch the instruction given by intruder (in this approach, "Attacker"). As the victim system comes online, it executes appropriate commands of attacker's need, redirect command output to .data file and finally automatically attach this file to your email account. Hence, by simply downloading this file you will get all the cmd output in attached .data file as shown in below figure.



Here in the above figure you can clearly see that, all required outputs are attached in your email address!

Advantages

1. Advantages are that the attacker is never going to be caught if he/she is using the browser like TOR, Anononymizer, VPNs or Any PROXY.... For accessing the attacking Gmail account.
2. No Antivirus can detect the Instruction data because all traffic would come from HTTPS And Antivirus Softwares and Network Intrusion Detection Software Detects simply an outbound connection with GMAIL...!
3. Only a single Gmail account is required. Attacker and victim machine both would be connected to the same account but the attacker knows, and the victim doesn't!!

Disadvantages

Disadvantage is that, if the victim has a habit of checking the current connections using commands like 'netstat –n', then there is a possibility to detect Gmail connection when actually there is no browser activity. But still it is difficult to detectbecause process is running in Hidden mode.

Conclusion

So by using above technique, attacker has to send commands as a subject to his/her own email address and then it is fetched and executed in victim machine by executable file running in victim machine. And results of that commands are sent back to the attacker's email account as an attachment. So there is no need to be online for both attacker and victim. And Anti-viruses and Firewalls going to bypass using this technique because Av and Firewall notice that victim system connects to the Gmail (not actually connects to attacker machine for transferring data) and it uses HTTPS encryption of Gmail for transferring the data (no chance of signature based detection because of HTTPS), so they don't find any threats for victim machine, so no security alarms!

Merchant Bhaumik
backdoor.security@gmail.com

Merchant Bhaumik helps local law-enforcement as a Digital Forensics Investigator and is a Student Of Maharaja SayajiRao University (MSU) Vadodara. Bhaumik is the developer of "IND 360 Intrusion Detection System.

Cain and Abel: The Black Art of ARP Poisoning

Overview

Cain and Abel is windows based password recovery tool available as a freeware and maintained by MassimilianoMontoro. It supports wide features to recover passwords varying from Local Area Network to various routing protocols as well as provides intelligent capability to recover cached passwords and encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks.

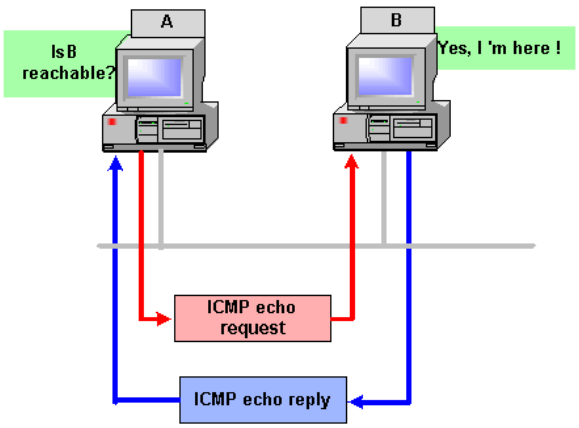
It is a two part program where Cain is the GUI of the program, and Abel is windows service that provides a remote console on the target machine.

An interesting feature of Cain & Abel is APR (ARP Poison Routing) which allows sniffing packets of various protocols on switched LAN's by hijacking IP traffic of multiple hosts concurrently. It can also analyze encrypted protocols such as SSH-1and HTTPS.

Basics of Address Resolution Protocol

Assume two computers, Computer A and Computer B are in a local area network connected by Ethernet cables and network switches. Computer A wants to send a packet to Computer B. Computer A determines that Computer B's IP address is 192.168.0.5.

In order to send the message, it also needs to know Computer B's MAC address. First, Computer A uses a cached ARP table to look up 192.168.0.5 for any existing records of Computer B's MAC address (00:24:56:e2:ac:05). If the MAC address is found, it sends the IP packet on the link layer to address (00:24:56:e2:ac:05).If the cache did not produce a result for 192.168.0.5, Computer A has to send a broadcast ARP message (destination FF:FF:FF:FF:FF:FF) requesting an answer for 192.168.0.5. Computer B responds with its MAC address (00:24:56:e2:ac:05).Computer B may insert an entry for Computer A into its own ARP table for future use. The response information is cached in Computer A's ARP table and the message can now be sent.



How ARP Poisoning Works

The attacker machine makes use of the stored ARP cache table to re-route or re-direct packets from a target, to an attacker machine, and then forward to the host, thus the attacker machine "sees" all traffic between target and host. First the target MAC address is established, and then the ARP Poison Routing feature "poisons" the cache of the target by forcing a cache update with the path re-routed so that the attacker machine forwards traffic to and from host and target. The attacker machine can also observe packets with a sniffer such as Wireshark.

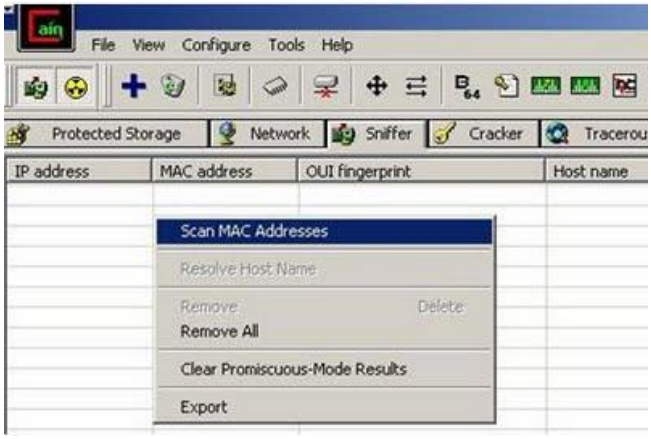
Now, I will discuss the steps to sniff password of remote computers in a Local Area Network.

Requirements:

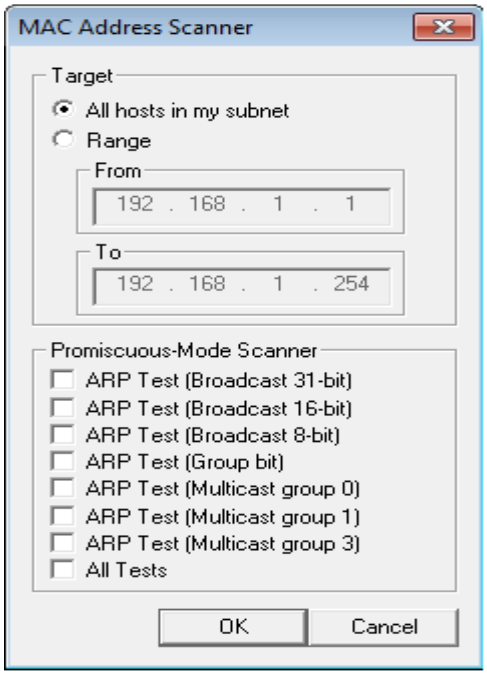
1. Download and install Cain & Abel from http://www.oxid.it/cain.html
2. Make sure WinPcap packet capture driver is installed properly.
3. Download and install Wireshark from http://www.wireshark.org/download.html.
4. At least 3 hosts must be present in a network to place an attack.

Working Steps:

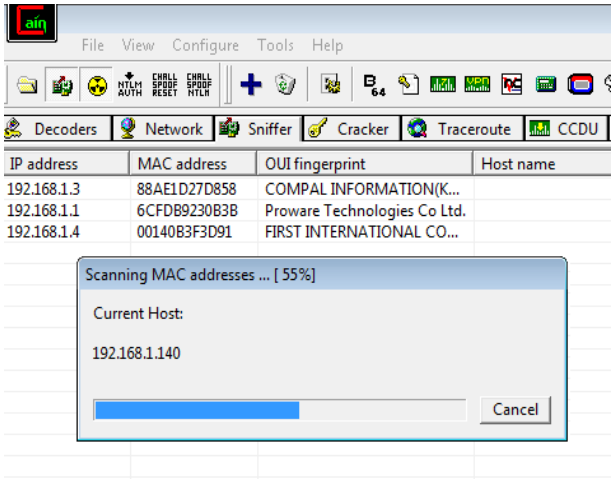
1. To start ARP Spoofing, you need to activate the sniffing daemon and the APR daemon. You can do this by clicking on both the "Sniff" and "APR" buttons at the top of the window.
2. Next go to the sniffer tab and right click anywhere inside the tab. You should see a "Scan MAC addresses" option. Click it.



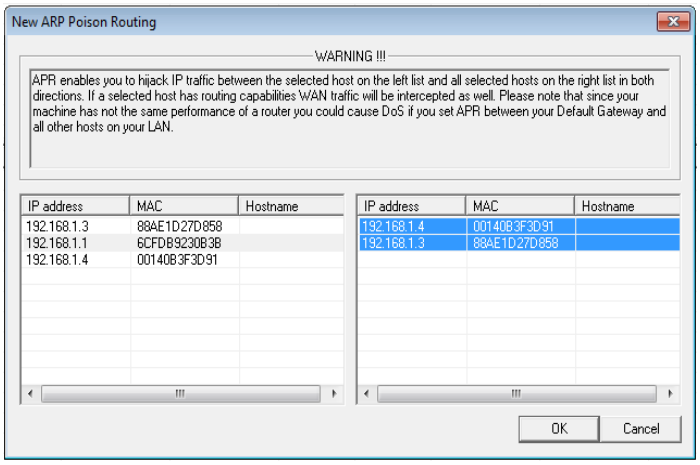
3. Select the IP range accordingly to your local area network and click on "OK".



4. The Progress bar scans and list all the MAC address present on the subnet.



5. After the scan, click on the APR sub-tab at the bottom of the window.Then click on the + icon on the top of the window to add host to attack.
6. A following dialog box appears on the screen. Select the host you wish to attack.



7. Wait for the victim host to enter his credentials. Click on the passwords sub-tab at the bottom of the window. There you can see all the captured passwords arranged in the group.

This was a basic tutorial on how you can use Cain and Abel for ARP Poisoning.

Happy Hacking ☺

Himanshu Kumar Das
me.himansu@gmail.com

Himanshu Kumar Das is a passionate security admirer. Himanshu, a do-it-yourself guy, is an electronic freak and imagines open source.

Firewall 101

Introduction

Today we are exposed to innumerable threats online. Firewalls act as the first line of defense for securing our network against these threats. Firewall could be a program or a device or group of devices used to control the traffic flow.

The basic principle that Firewall uses to control this communication is 'Access Rules'. It maintains an access rule table and every time a packet comes in or goes out, Firewall refers to this table. It only allows authorized traffic and blocks the unwanted packets.

Firewalls are of 2 types:

- Hardware Firewalls.
- Software Firewalls

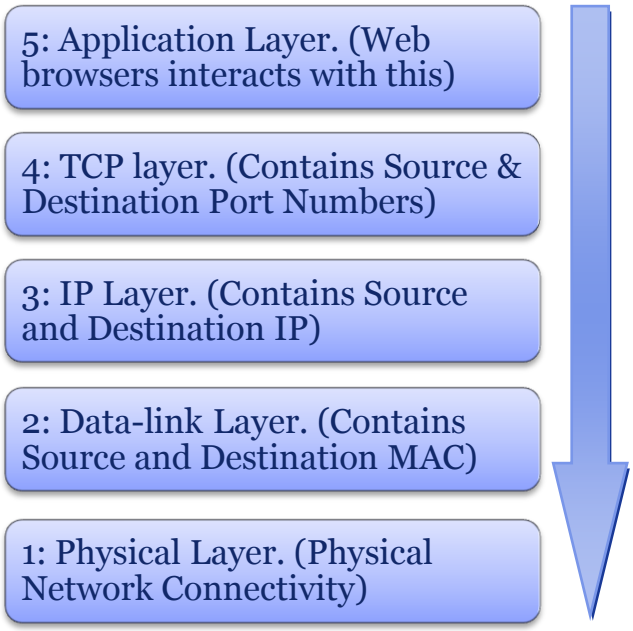
The basic characteristics of Firewalls include:

Hardware Firewall	Software Firewall
It's a standalone device	It's a software installed on your computer
Complex configurations involved	Relatively easy to configure
Consumes physical space	Consumes CPU utilization
More secured than software firewalls	Less expensive than hardware firewalls
Mainly uses packet filtering	Mainly looks at application characteristics
Mostly network based	Mostly host based
E.g.: Cisco ASA, SonicWall, etc	E.g.: Symantec EF, Checkpoint FW-1 etc

1. Traffic monitoring and reporting.
2. Intrusion detection and prevention.
3. Packet or Protocol filtering based on user defined rules.
4. Incorporate VPN gateways (Enterprise Level Firewalls).
5. Load balancing & Failover (Enterprise Level Firewalls).

Understanding Firewall operation:

Before we get in to how firewalls operate, let us understand the OSI layer and data flow
E.g.: When you type www.google.com this is what happens:



Before we get in to how firewalls operate, let us understand the OSI layer and data flow
E.g.: When you type www.google.com this is what happens:

Example of details at each layer:
Application: www.google.com

TCP: Source Port – 27785 Destination Port – 80

IP: Source IP – 21.22.23.24 Destination IP – 74.75.76.77

Data-link: Source MAC – aa:aa:aa:aa:aa:aa

Destination MAC – Router's MAC

Similarly when Google's server responds to the request, your response packet will look like this:
Application: www.google.com

TCP: Source Port –80 Destination Port – 27785

IP: Source IP –74.75.76.77 Destination IP – 21.22.23.24

Data-link: Source MAC – Router's MAC

Destination MAC –aa:aa:aa:aa:aa:aa

We see router's MAC because router acts as your gateway for interacting with the external world. So to communicate with any system outside your network, your destination MAC will be that of your router. There are several other things like sequence number etc, which are not mentioned to maintain the simplicity of the topic.

Firewalls can be categorized based on their filtering capabilities:

Packet Filtering

- Looks at IP address, Port Numbers & Protocol Type
- Does not pay attention to whether packet is a part of existing connection
- Makes decision solely based on ACLs

Stateful Filtering

- Does regular Packet Filtering
- Maintains info on all existing connections so only data from existing connection stream is allowed

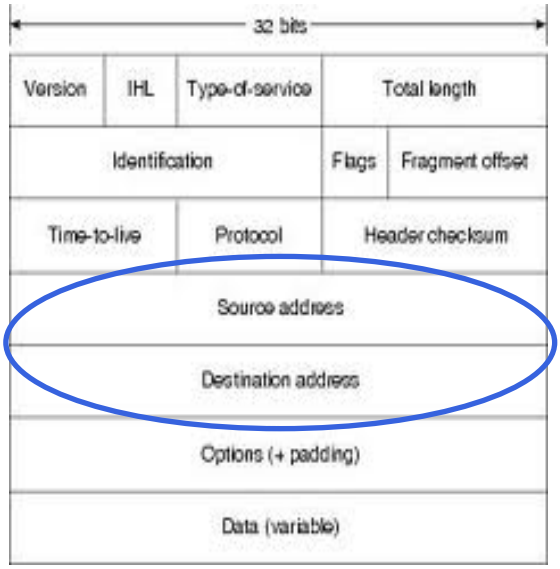
Application Filtering

- Possesses Deep Packet Inspection functionality
- Works in a similar manner to IPS
- Possesses ability to classify applications as well apart from packet and stateful filtering

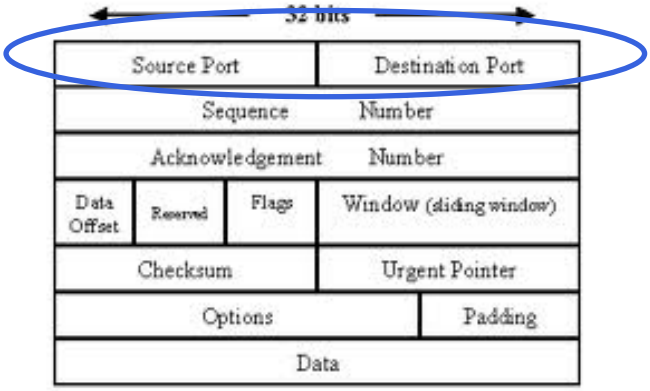
Packet Filtering:

As per the table above we understand how packet filtering works. However a TCP/IP packet will provide a clear picture on how packet filtering works

Provided below is an IP packet.

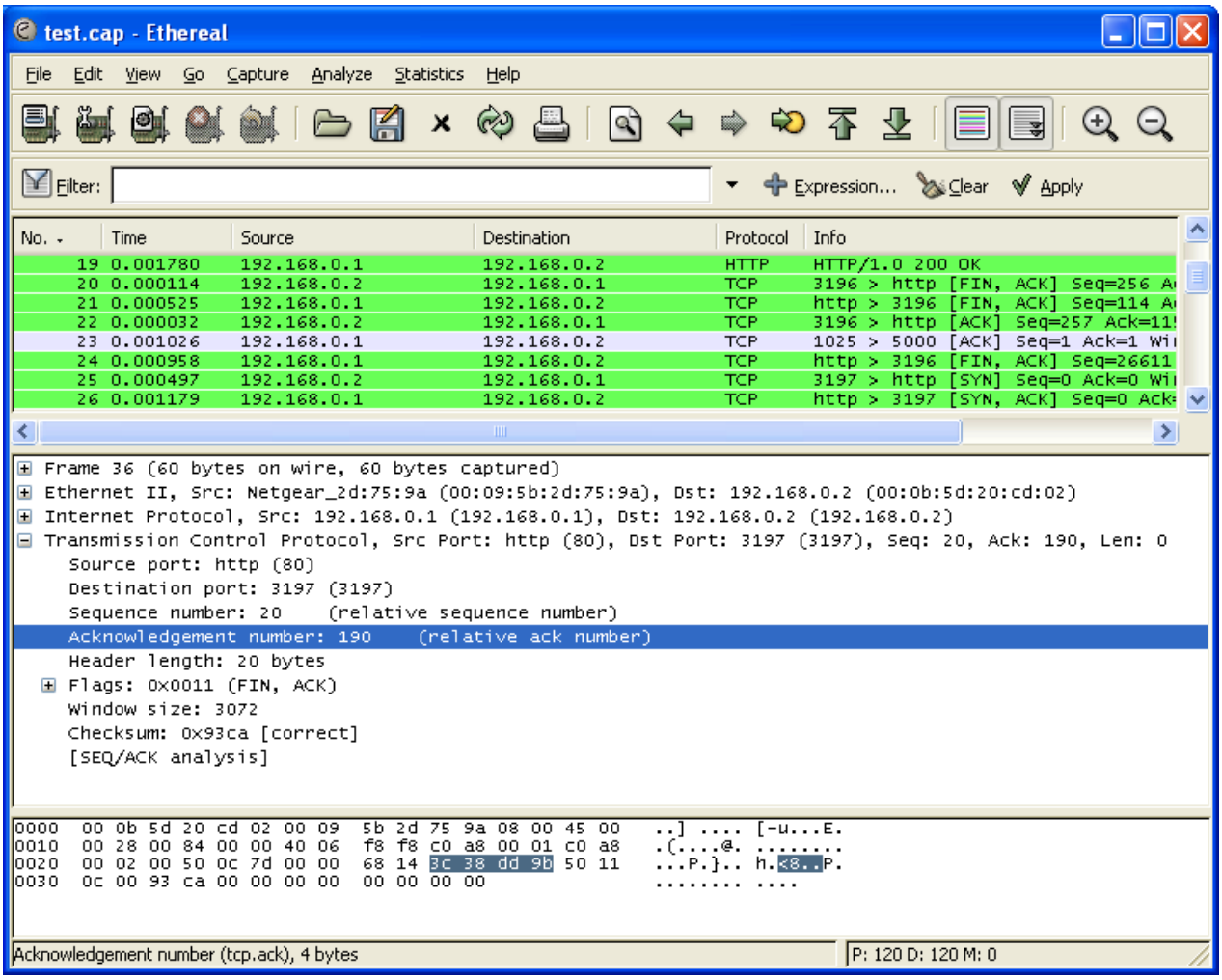


This is what packet filtering will focus on when looking at an IP header. To grant access or not will depend on the Access List table.



This is what packet filtering will focus on when looking at a TCP header. To grant access or not will depend on the Access List table.

[Screenshot below is captured from Ethereal. It displays TCP & IP details]



Packet filtering will act in the following manner:

1. Block or Accept IP addresses (e.g. A subnet – 192.168.10.0 / 24)
2. Block or accept a particular port (e.g. Port 23 or 445)
3. Block or accept a particular protocol (e.g. TCP or UDP or ICMP)

Blocking a protocol is never recommended. E.g. if you block UDP, then you may end up blocking DNS requests too.

Overall this method of filtering proved to be ineffective due to the following reasons:

1. Cannot keep a track of state of existing connections (Stateless)
2. Cannot check the payload (data). This makes application filtering impossible.

This gave rise to the need of Stateful Filtering.

Stateful Filtering:

It records the state of all the existing connections i.e. data streams and stores it in the memory. Therefore the basis of dropping packets is the connection state.

Following are the features of Stateful Filtering:

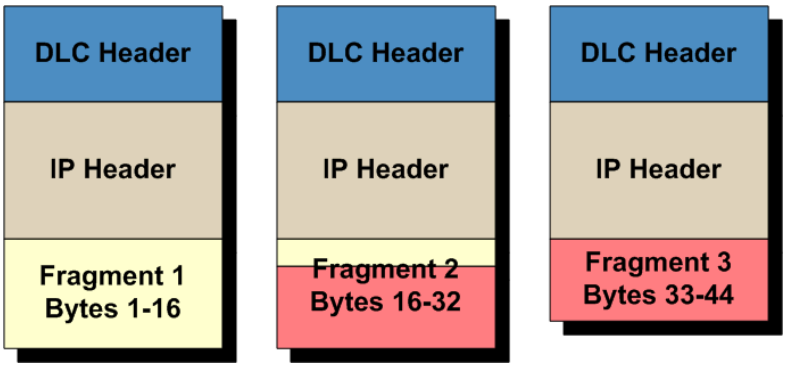
1. It looks at the state table – Unlike packet filtering which has no track of connections, this method looks at

the data stream and only packets which are a part of the stream are allowed. The rest are discarded.

2. It clears entries from the state table once the TCP session closes or after a few minutes to ensure that the table is clean and does not unnecessarily waste its memory

Again, this is not the perfect solution. Fragmentation causes trouble to stateful filtering.

Fragmentation was allowed to break large packets in to small fragments for the routers or firewalls that do not support large packets.



This is a fragmented packet. Every fragmented packet has its own IP header and is not reassembled until all the fragments arrive at the destination host.

TCP or UDP is in the 0th fragment (Fragment 1). So setting fragment number to 1 instead of 0 will help packet bypass the Stateful Firewall. Some older firewalls used to filter only well-known port numbers i.e. the ones below 1024.

One more drawback is that Trojan Horses can defeat these firewalls if they use NAT (Network Address Translation)

Application Filtering:

This concept is similar to HIPS (Host based Intrusion Prevention System). Application is the top most layers of TCP/IP model (and even OSI model). Usually, anti-virus acts in at this layer.

The mode of operation is looking for information in the payload section of the header which other firewalls fail to do.

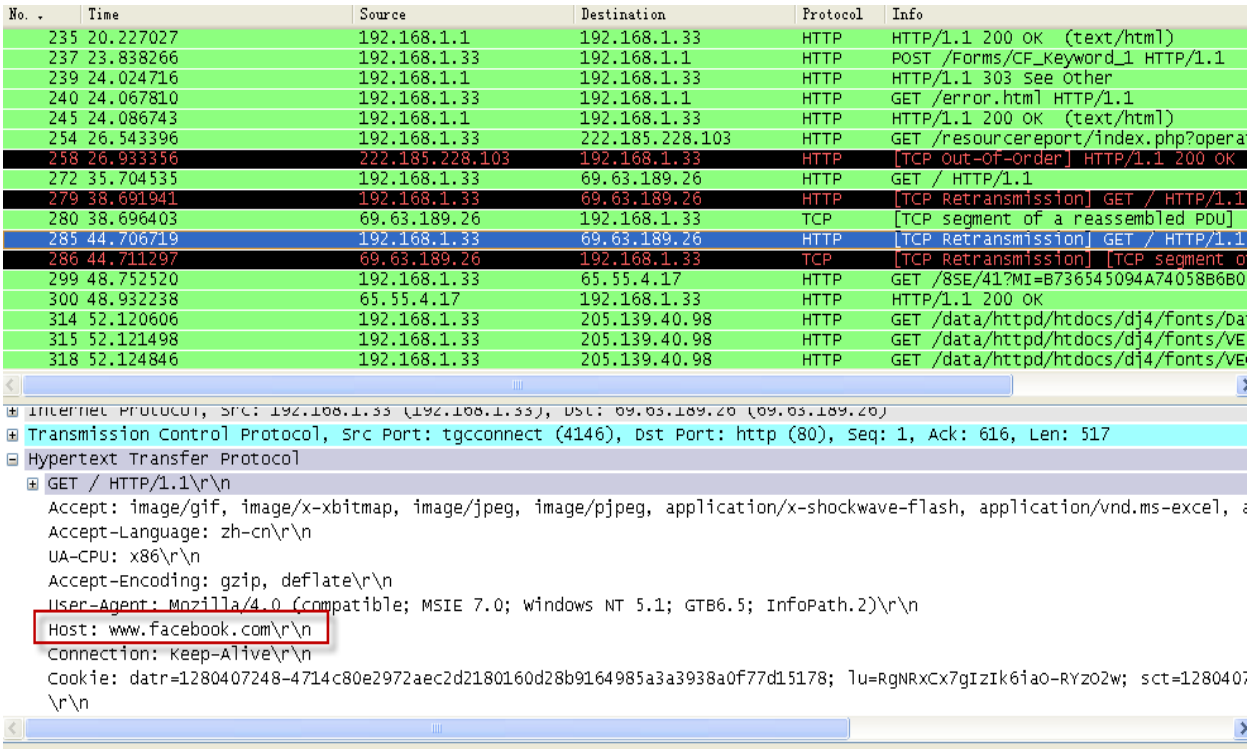
The basis of blocking or allowing application depends on the following factors:

1. Cross check with existing database of signatures
2. Look for abnormal behavior of a particular file type (size modification or registry edits etc.)

In short Application filtering is an intelligent technology that looks for abnormal information within the payload (data) and can block unwanted or suspicious data (application).

These firewalls can prevent attacks like:

- ✓ DNS buffer overflows
- ✓ HTTP based web server attacks
- ✓ Code hidden within SSL tunnels (https websites) and many more
- ✓ E.g. You can allow access to Facebook, but block games.



No.	Time	Source	Destination	Protocol	Info
235	20.227027	192.168.1.1	192.168.1.33	HTTP	HTTP/1.1 200 OK (text/html)
237	23.838266	192.168.1.33	192.168.1.1	HTTP	POST /Forms/CF_Keyword_1 HTTP/1.1
239	24.024716	192.168.1.1	192.168.1.33	HTTP	HTTP/1.1 303 See Other
240	24.067810	192.168.1.33	192.168.1.1	HTTP	GET /error.html HTTP/1.1
245	24.086743	192.168.1.1	192.168.1.33	HTTP	HTTP/1.1 200 OK (text/html)
254	26.543396	192.168.1.33	222.185.228.103	HTTP	GET /resourcereport/index.php?opera
258	26.933356	222.185.228.103	192.168.1.33	HTTP	[TCP Out-Of-Order] HTTP/1.1 200 OK
272	35.704535	192.168.1.33	69.63.189.26	HTTP	GET / HTTP/1.1
279	38.691941	192.168.1.33	69.63.189.26	HTTP	[TCP Retransmission] GET / HTTP/1.1
280	38.696403	69.63.189.26	192.168.1.33	TCP	[TCP segment of a reassembled PDU]
285	44.706719	192.168.1.33	69.63.189.26	HTTP	[TCP Retransmission] GET / HTTP/1.1
286	44.711297	69.63.189.26	192.168.1.33	TCP	[TCP Retransmission] [TCP segment o
299	48.752520	192.168.1.33	65.55.4.17	HTTP	GET /8SE/41?MI=B736545094A74058B6B0
300	48.932238	65.55.4.17	192.168.1.33	HTTP	HTTP/1.1 200 OK
314	52.120606	192.168.1.33	205.139.40.98	HTTP	GET /data/httpd/htdocs/dj4/fonts/Da
315	52.121498	192.168.1.33	205.139.40.98	HTTP	GET /data/httpd/htdocs/dj4/fonts/VE
318	52.124846	192.168.1.33	205.139.40.98	HTTP	GET /data/httpd/htdocs/dj4/fonts/VE

```
Internet Protocol, Src: 192.168.1.33 (192.168.1.33), Dst: 69.63.189.26 (69.63.189.26)
Transmission Control Protocol, Src Port: tgcconnect (4146), Dst Port: http (80), Seq: 1, Ack: 616, Len: 517
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, a
    Accept-Language: zh-cn\r\n
    UA-CPU: x86\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; GTB6.5; InfoPath.2)\r\n
    Host: www.facebook.com\r\n
    Connection: Keep-Alive\r\n
    Cookie: datr=1280407248-4714c80e2972aec2d2180160d28b9164985a3a3938a0f77d15178; lu=RgNRxCx7gIzIk6iaO-RYzO2w; sct=128040
    \r\n
```

This screenshot shows HTTP packet capture. HTTP works at application layer of TCP/IP model

Application filtering in conjunction with lower layer protection is by far the best combination to safeguard your network. All the Enterprise class firewalls possess these capabilities.

SagarDawda
Sagard31@gmail.com

SagarDawda is Network Security student. Sagar handles Sonicwall firewalls for the company he works for. Sagar's ultimate aim is to learn as much as he can about IT security and get in to Forensics (Network Forensics to start with). His dream is to join an intelligence agency and help them solve cases where computers/network was used a part of the crime.

Liability of Intermediaries under the Information Technology Act

Introduction

Recently Delhi high court has summoned Google, Facebook and Twitter to remove objectionable content from their website within the prescribed time period failing to which may result into blocking of the websites in India. So the question which triggers is*What is the liability of the intermediaries like Google, Facebook and Twitter under Indian law?*

Who is an Intermediary?

"Intermediary" under Section 2(1) (w). It reads as –

"intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, webhosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;'.

Liability of Intermediaries

Section 79 of the IT Act exempts intermediaries from liability in certain cases. The Section reads as –

Sec. 79

1. Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.
2. The provisions of sub-section (1) shall apply if—
    a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
    b) the intermediary does not—
        I. initiate the transmission,
        II. select the receiver of the transmission, and
        III. select or modify the information contained in the transmission;

c) The intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

3. The provisions of sub-section (1) shall not apply if—
   a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;
   b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation

For the purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

This provision arises two questions –

- What is the meaning of "observing due diligence"?
- What is the time frame to remove objectionable material from resource?

To address these and other issues the Information Technology (Intermediary guidelines) Rules, 2011 are introduced. They are applicable from 11th April, 2011.

Features of the rules are as follows

Observing Due Diligence - Rule 3

Of the said rules has given circumstances which if complied satisfies the criteria of observing *Due Diligence*. It reads as –

1. The intermediary shall publish the rules and regulations, privacy policy and user agreement for access-or usage of the intermediary's computer resource by any person.
2. Such rules and regulations, terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —
   a) belongs to another person and to which the user does not have any right to;
   b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, pedophilic, libelous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;
   c) harm minors in any way;
   d) infringes any patent, trademark, copyright or other proprietary rights;
   e) violates any law for the time being in force;
   f) deceives or misleads the addressee about the origin of such messages or communicates any information which is

grossly offensive or menacing in nature;

g) impersonate another person;

h) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource;

i) threatens the unity, integrity, defense, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting any other nation

- The intermediary, on whose computer system the information is stored or hosted or published, upon obtaining knowledge by itself or been brought to actual knowledge by an affected person in writing or through email signed with electronic signature about any objectionable information as mentioned above, shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention.
- Further the intermediary shall preserve such information and associated records for at least ninety days for investigation purposes.
- The intermediary shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable security practices and procedures and sensitive personal Information) Rules, 2011.
- The intermediary shall publish on its website the name of the Grievance Officer and his contact details as well as mechanism by which users or any victim who suffers as a result of access or usage of computer resource by any person in violation of rules can notify their complaints against such access or usage of computer resource of the intermediary or other matters pertaining to the computer resources made available by it. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint.

Note: -

These are just features of the rules; full copy of the rules is available at: http://mit.gov.in/content/cyber-laws

SagarRahurkar

contact@sagarrahurkar.com

SagarRahurkar is a Law graduate. He is a techno-legal consultant and a Senior Faculty at Asian School of Cyber Laws. Sagar specializes in Cyber Law, Cyber Crime Investigation, Computer Forensics and Intellectual Property Laws. Sagar teaches and provides consultancy to corporates, law enforcement agencies and education institutes across India.

Introduction to Skipfish

Skipfish is an active web application security reconnaissance tool written and maintained by Michal Zalewski (@lcamtuf). Skipfish is one of the fastest webscanners available which spiders using the wordlists, a very powerful web scanning tool with a simple implementation. In MatriuxSkipfish can be found in the arsenal under Arsenal →Framework →Skipfish

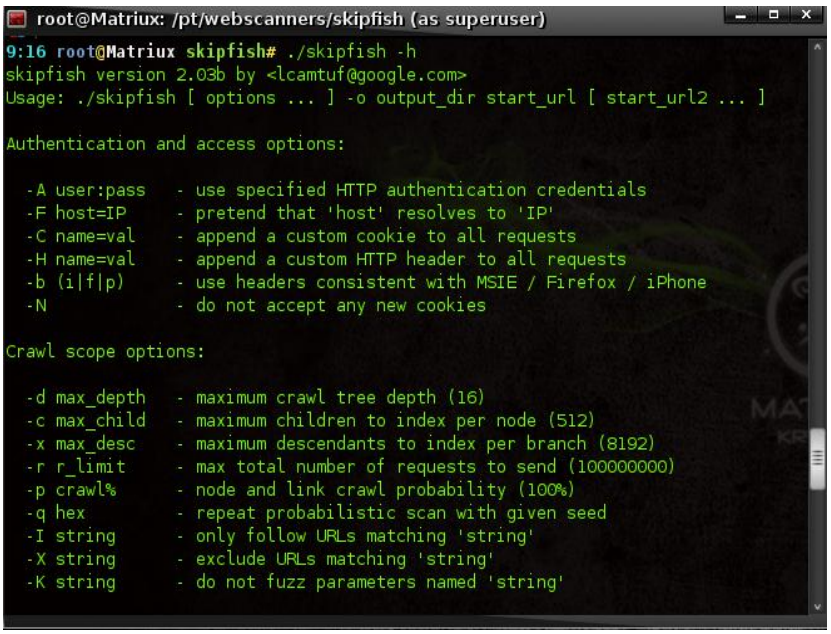
Why Skipfish?

Skipfish fast and easy to implement can perform a robust scan of any website providing a lot of security tests, like php injection, XSS, format string vulnerabilities, overflow vulnerabilities, file inclusions and lot more categorized into high risk, medium risk and low risk issues. Skipfish also provides summary overviews of document types and issue types found; and an interactive sitemap, with nodes discovered through brute-force denoted in a distinctive way.

Getting started

Before starting skipfish make sure you provide a skipfish.wl wordlist file from the dictionaries directory found at `/pt/webscanners/skipfish/dictionaries/` (to put it simple copy a file from dictionaries/ to the directory of skipfish into skipfish.wl).

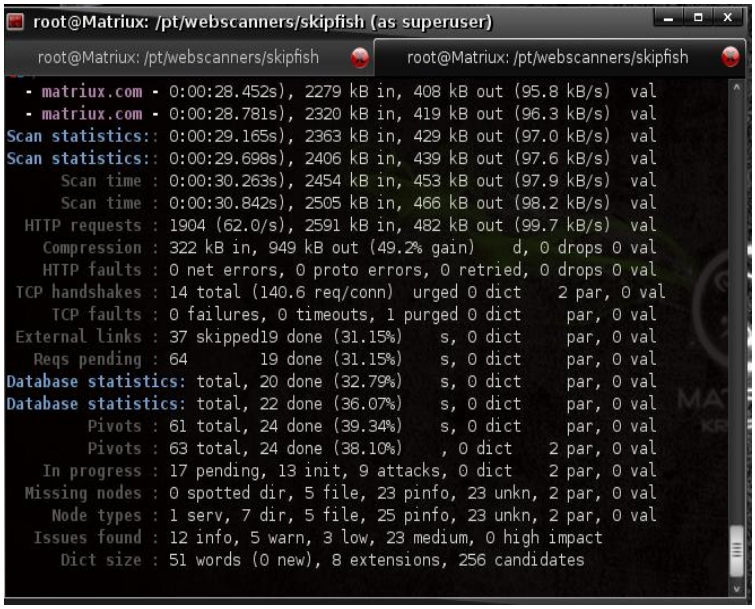
Start skipfish from Arsenal or move to directory `/pt/webscanners/skipfish/` and run `./skipfish –h` for help.



A simple way to perform a scan is by using the following command:-

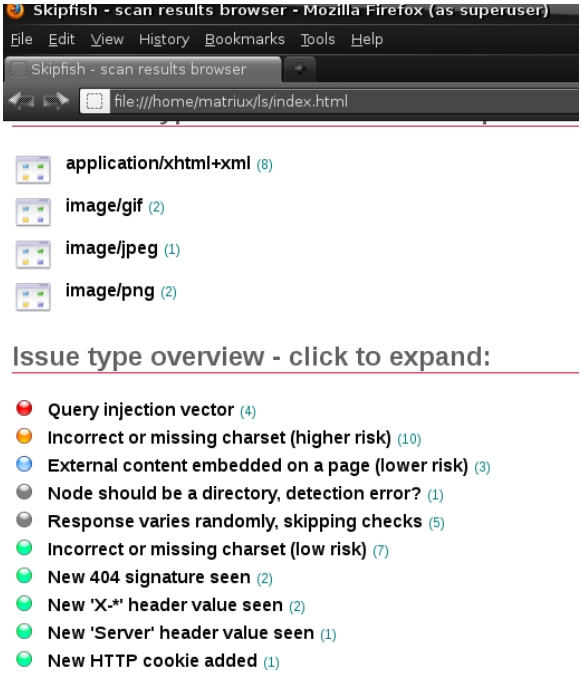
```
./skipfish –o /home/matriux/path
http://www.example.com/
```

You can replace `/home/matriux/path` with other desired locations you want.



After the successful scan a report is generated and stored in the output directory you specified, open the index.html in a browser to view the report generated.

Following is how a sample report looks like.



In certain cases where the certain URLs may logout your session where you can use commands like :-

```
$ ./skipfish -X
/logout/logout.aspx ...other
parameters...
```

There are also other options with HTTP cookies, authentication which you can find in the skipfish doc or the README file present in the installation directory.

Overall skipfish is a very light tool for webscanning and security testing, which provides a lot of features and scan options in a faster way.

References

http://code.google.com/p/skipfish/wiki/SkipfishDoc

Happy Hacking ☺

Team Matriux

http://matriux.com/

ClubHACKMag
1st Indian "HACKING" Magazine

Testimonials

Here are few testimonials from experts, contributors and readers.

"Club Hack is a journal which is in a league of its own... Started in 2010 by a handful of committed members of the ethical hacker community, it has grown to be a mature publication with in-depth analysis on the most useful subjects which are of interest to domain professionals. It has a great range in coverage too - from hard core coding to cyber law."

- **Lt. Col (Retd) Deepak Rout**

  India Privacy Lead, Microsoft Corp

I am happy to note that our ClubHack magazine has completed two years today. I am proud to be associated with ClubHack and glad that members of ClubHack are innovative in thinking and hard working which reflected in the magazine. Working together is our strength.

- **Ashis K Mitra**

  Assistant Commandant / CISF
  Delhi International Airport
  India

"For colleagues and information security researchers around the world, ClubHack magazine is the face of the growing information security and hacking community in India and the place to be familiar with other professionals in India.
For Indian readers this is the entry point and door to get into the information security field and hacking scene".

- **EladShapira**

  Security Researcher, Developer & Reverse Engineer

"Long live the CHMag magazine!! :) I really love this mag and the team which works on this."

- **SamvelGevorgyan,**

  Managing Director, CYBER GATES

"The effort, organization and teamwork of professionals has made the best Indian Hacking Magazine named: ClubHACK Magazine. Woldwide recognized with large assorted content, following an attractive subject for the reader. It is a pleasure work with the talented guys behind ClubHACK and share knowledge with everyone. For many more Editions and Keeping Rocking!"

- **MaximilianoSoler**

  Security Researcher & Enthusiast

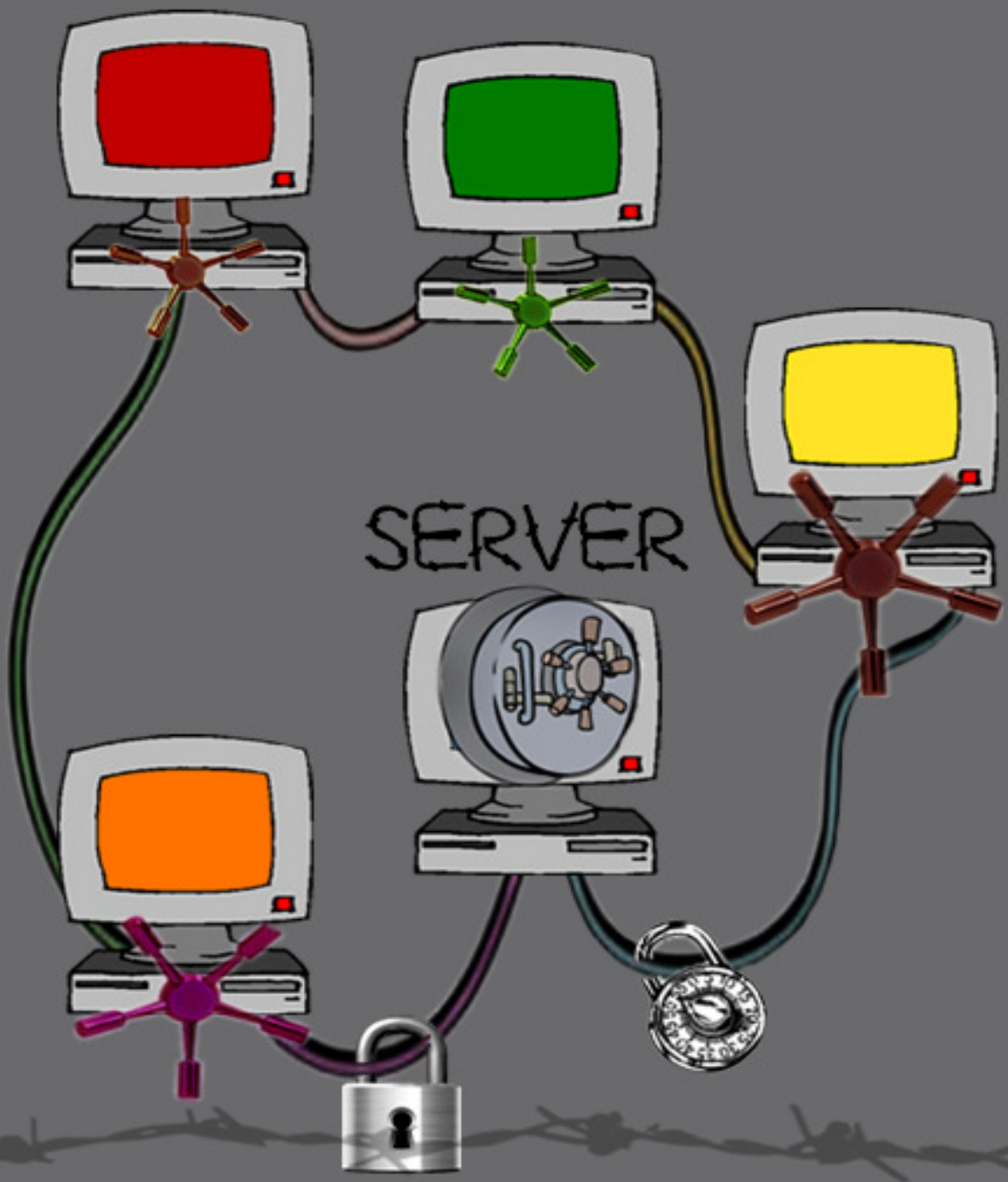
"Over the years, ClubHack Magazine has been doing phenomenal job in spreading security awareness, with the young guns behind the screen pulling complex chords to a melodic song. On this occasion of 2nd birthday, we heartily congratulate entire team and hope that they continue to illuminate the world with a greater light in the coming days."

- **NagareshwarTalekar**

  Founder and Independent Security Consultant at SecurityXploded

ClubHACK

Secured Network



Issue 25 | Feb 2012

www.clubhack.com

Design: @pankit_thakkar