Web Application Security

Dr. Digvijaysinh Rathod
Associate Professor
School of Cyber Security and Digital Forensics
National Forensic Sciences University

digvijay.rathod@nfsu.ac.in

Finding virtual hosts

Virtual Host

- ✓ The term Virtual Host refers to the practice of **running more than one web site (such as company1.example.com and company2.example.com) on a single machine.**
- ✓ Virtual hosts can be **"IP-based"**, meaning that you have a **different IP address for every web site**, or **"name-based", meaning that you have multiple names running on each IP address**. The fact that they are running on the same physical server is not apparent to the end user.

Virtual Host

- ✓ The concept of **virtual hosts allows more than one Web site on one system or Web server**.
- ✓ The servers are differentiated by their host name. Visitors to the Web site are routed by host name or IP address to the correct virtual host.
- ✓ Virtual hosting allows companies sharing one server to each have their own domain names. For example www.company1.com and www.company2.com can both be hosted on the same server.

Virtual Host

“Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers).

This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name.”

HTTP Server virtual host types

- ✓ There are three variations of virtual hosts on HTTP Server:

1. IP address-based virtual host

The IP address-based virtual host requires one **IP address per Web site (host name).**

This approach works very well, but requires a dedicated IP address for every virtual host. For more information on virtual hosts refer to the <VirtualHost> directive.

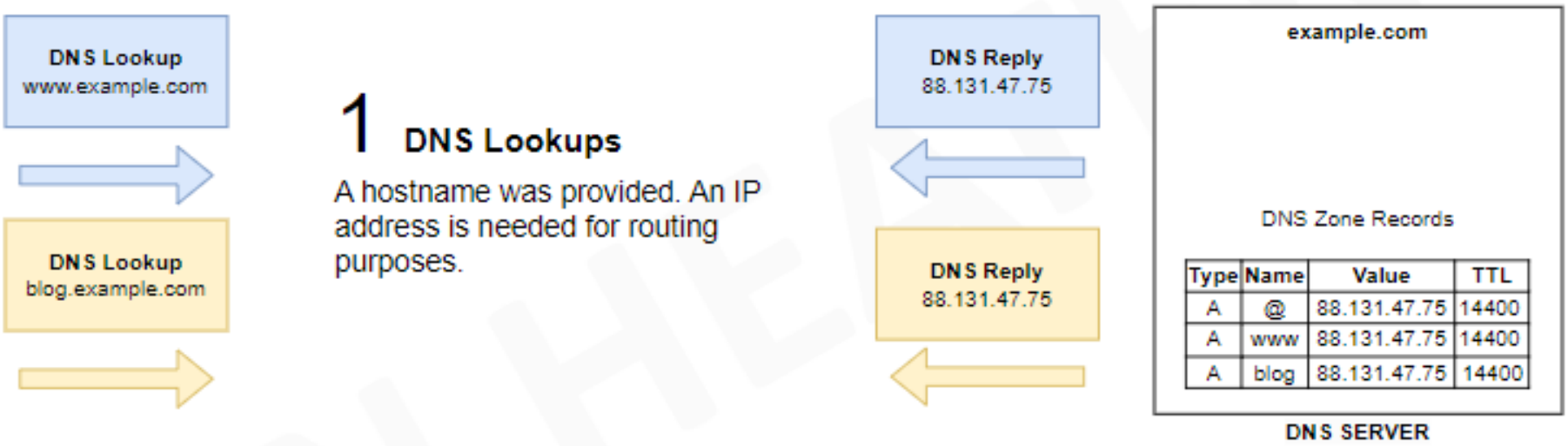
2. Name-based virtual host

- ✓ The name-based virtual host allows **one IP address to host more than one Web site (host name)**.
- ✓ This approach allows practically an unlimited number of servers, ease of configuration and use, and requires no additional hardware or software.
- ✓ The main disadvantage to this approach is that the **client must support HTTP 1.1** (or HTTP 1.0 with 1.1 extensions) that include the host name information inside the HTTP document requests.

2. Name-based virtual host

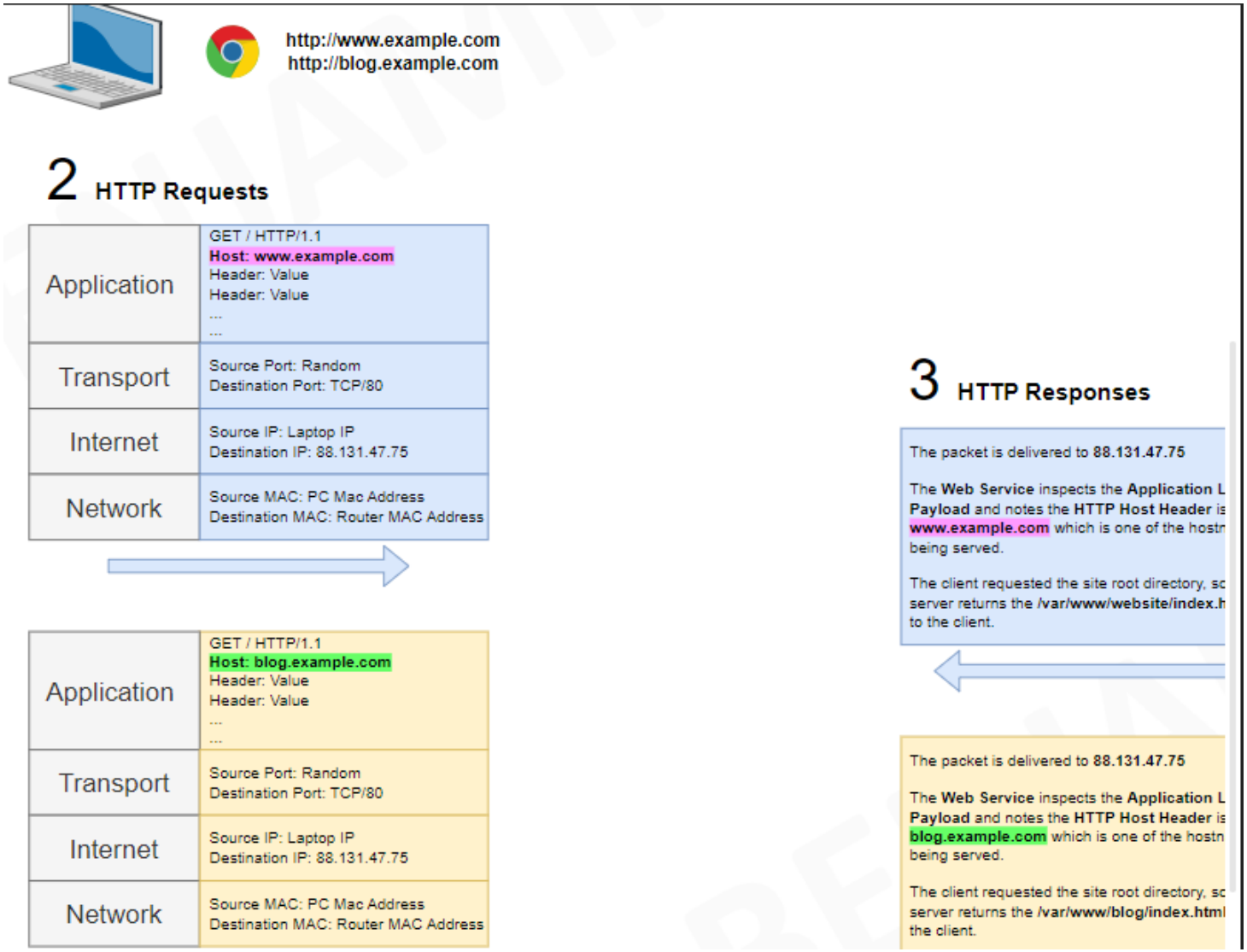
- ✓ The latest versions of most browsers support HTTP 1.1 (or HTTP 1.0 with 1.1 extensions), but there are still old browsers that only support HTTP 1.0. For more information on virtual hosts refer to the <VirtualHost> directive.

HTTP Server virtual host types

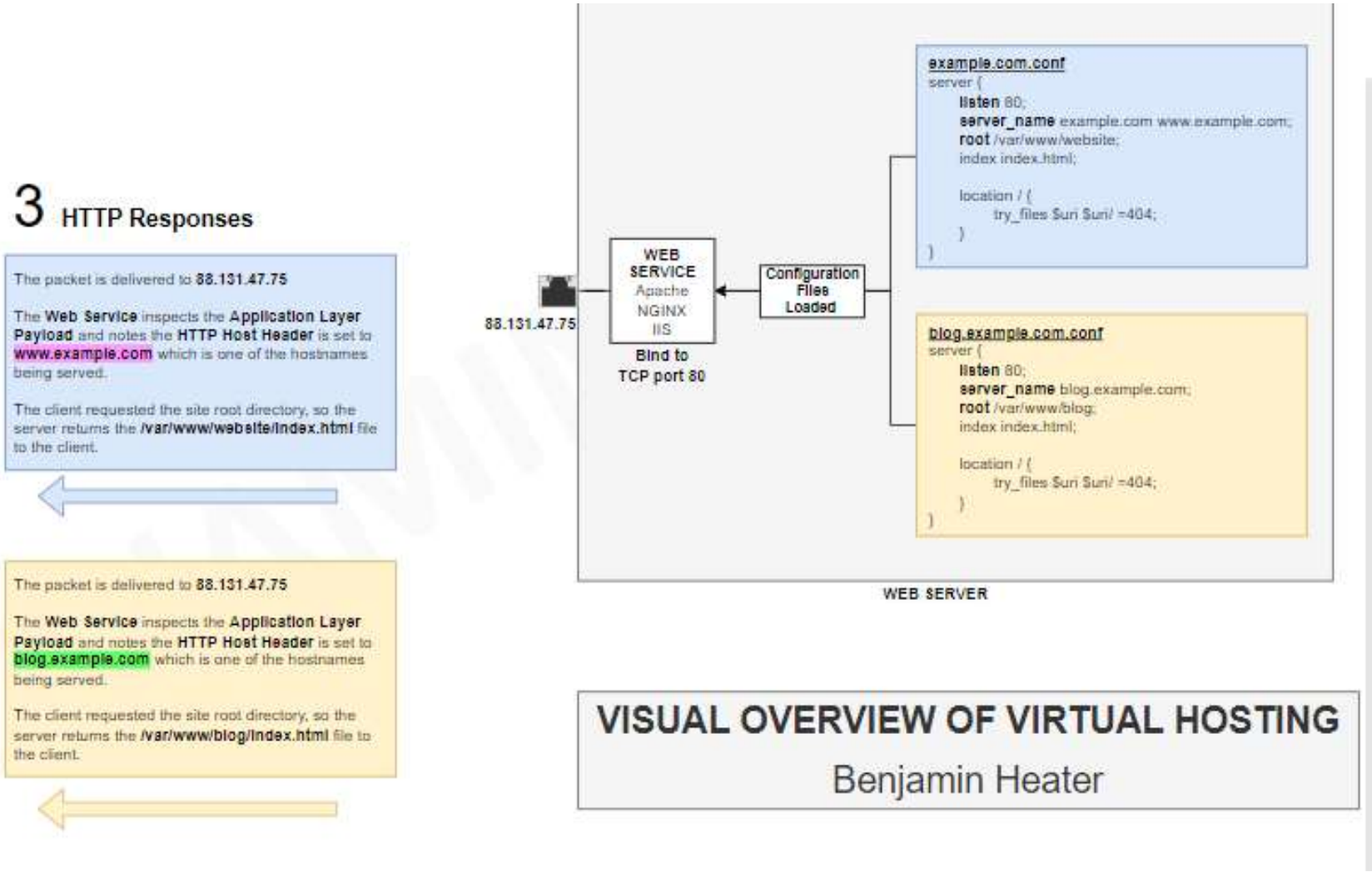


https://notes.benheater.com/books/web/page/virtualhost-enumeration#bkmrk-virtualhosts-example

HTTP Server virtual host types



HTTP Server virtual host types



3. Dynamic virtual host

- ✓ The dynamic virtual host allows you to dynamically add Web sites (host names) by adding directories of content.
- ✓ This approach is based on automatically inserting the IP address and the contents of the Host: header into the pathname of the file that is used to satisfy the request.

3. Dynamic virtual host

The advantages of a dynamic virtual host are:

- ✓ A smaller configuration file so that the server starts faster and uses less memory.
- ✓ Adding virtual hosts does not require the configuration to be changed or the server to be restarted.
- ✓ **The disadvantage** of a dynamic virtual host is that you cannot have a different log file for each virtual host

Description

Gobuster is a tool used to brute force URLs (directories and files) from websites, DNS subdomains, Virtual Host names and open Amazon S3 buckets. It can be particularly useful during CTF challenges that require you to brute force webserver data, but also during pentest engagements.

Installation on Linux (Kali)

Sudo apt-get install gobuster

Gobuster - Cheatsheet

 # Syntax

gobuster [mode] -u [target ip] -w [wordlist]

Gobuster can run in multiple scanning modes, at the time of writing these are: dir, dns and vhost.

It is recommended to download the worldlist from gethub for the Vhost, DNS and Dir.

The world list is available in the kali at /usr/share/wordlist

But you did not find for the Vhost, DNS and Dir

Ref: https://sohvaxus.github.io/content/gobuster.html

DIR mode - Used for directory/file bruteforcing

Syntax

gobuster dir -u [target ip] -w [wordlist]

 # Example

gobuster dir -u http://192.168.0.1:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt# **Example which excludes pages with a certain length**

gobuster dir -u http://192.168.0.1:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt --exclude-length 9265

DNS mode - Used for DNS subdomain bruteforcing

Syntax

gobuster dns -d [target site] -w [wordlist]

Standard example

gobuster dns -d example.com -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt #

Example with show ip

gobuster dns -d example.com -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

Example of force processing of a domain that has wildcard entries

gobuster dns -d 0.0.1.example.com -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt --wildcard

VHOST mode - Used for VHOST bruteforcing

Syntax

gobuster vhost -u [target site] -w [vhost list]

Example

gobuster vhost -u https://example.com -w common-vhosts.txt

Gobuster - Cheatsheet

VHOST mode flags

-h : (--help) Print the VHOST mode help menu.

-r : (--followredirect) Follow redirects.

-H : (--headers [stringArray]) Specify HTTP headers, -H 'Header1: val1' -H 'Header2: val2'.

-c : (--cookies [string]) Cookies to use for the requests.

-k : (--insecuressl) Skip SSL certificate verification.

-U : (--username [string]) Username for Basic Auth.

-P : (--password [string]) Password for Basic Auth.

-u : (--url [string]) The target URL.

-p : (--proxy [string]) Proxy to use for requests [http(s)://host:port].

-a : (--useragent [string]) Set the User-Agent string (default "gobuster/3.0.1").

--timeout [duration] : HTTP Timeout (default 10s).

References

- ✓ https://sohvaxus.github.io/content/gobuster.html
- ✓ https://httpd.apache.org/docs/2.4/vhosts/
- ✓ https://httpd.apache.org/docs/2.4/vhosts/name-based.html
- ✓ https://www.ibm.com/docs/en/i/7.3?topic=concepts-virtual-hosts
- ✓ https://notes.benheater.com/books/web/page/virtualhost-enumeration#bkmrk-virtualhosts-example

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor
School of Cyber Security and Digital Forensics
National Forensic Sciences University

digvijay.rathod@nfsu.ac.in