



CSC – Jordan Shield Special Edition
Powered By : Mohammed Kher Al-Khawaldeh.

Subnet Mask

IP : 192.168.1.10

Mask : 255.255.255.0

Network : **Whole** Network Address

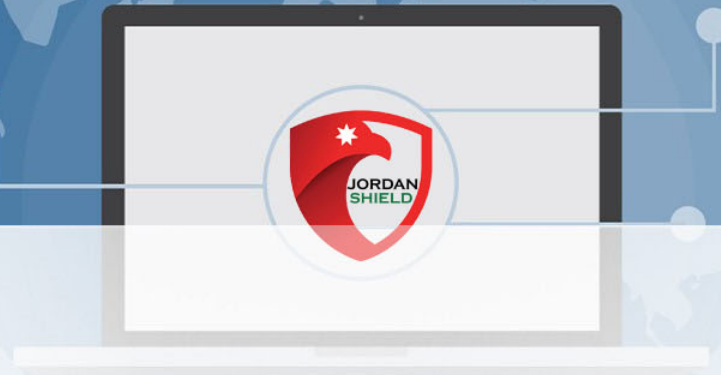
Host : **Devices** Inside Network

Broadcast : **Last Address** Inside The Network

Class **A** : 255.0.0.0

Class **B** : 255.255.0.0

Class **C** : 255.255.255.0



Subnet Mask



192.168.1.10/28

8+8+8+4

255.255.255.240

192.168.1.10/15

8+7+0+0

255.254.0.0

192.168.1.10/18

8+8+2+0

255.255.192.0

192.168.1.10/22

8+8+6+0

255.255.252.0

128

192

224

240

248

252

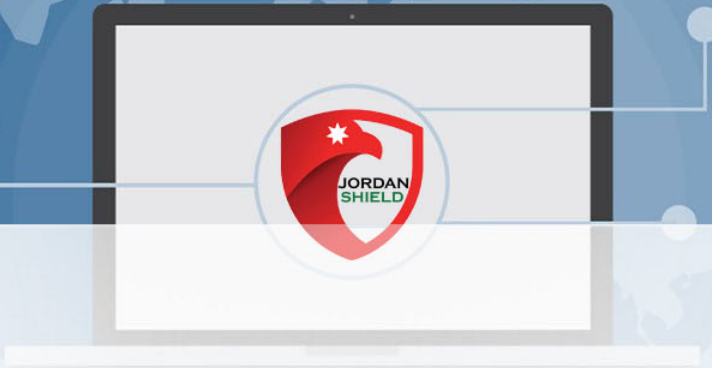
254

255

In Octet : 255 + 255 + 0 + 0
11111111.11111111.00000000.00000000

128	64	32	16	8	4	2	1

Subnet Mask



192.168.1.10/28

8+8+8+4

255.255.255.240

IP Address:	192.168.1.10
Network Address:	192.168.1.0
Usable Host IP Range:	192.168.1.1 - 192.168.1.14
Broadcast Address:	192.168.1.15
Total Number of Hosts:	16
Number of Usable Hosts:	14
Subnet Mask:	255.255.255.240

First IP

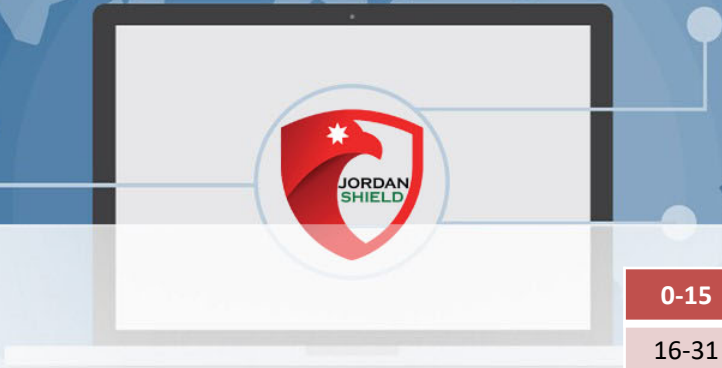
Last IP

Usable Host = Total - 2

128
192
224
240
248
252
254
255

128	64	32	16	8	4	2	1

Subnet Mask



192.168.1.50/28

8+8+8+4

255.255.255.240

IP Address:	192.168.1.50
Network Address:	192.168.1.48
Usable Host IP Range:	192.168.1.49 - 192.168.1.62
Broadcast Address:	192.168.1.63
Total Number of Hosts:	16
Number of Usable Hosts:	14
Subnet Mask:	255.255.255.240

First IP

Last IP

Usable Host = Total - 2

0-15	Network	128
16-31	Network	192
32-47	Network	224
48-63	Network	240
64-79	Network	248
80-95	Network	252
96-111	Network	254
112-127	Network	255

128	64	32	16	8	4	2	1

Subnet Mask



Prefix size	Network mask	Usable hosts per subnet
/1	128.0.0.0	2,147,483,646
/2	192.0.0.0	1,073,741,822
/3	224.0.0.0	536,870,910
/4	240.0.0.0	268,435,454
/5	248.0.0.0	134,217,726
/6	252.0.0.0	67,108,862
/7	254.0.0.0	33,554,430

Subnet Mask



Prefix size	Network mask	Usable hosts per subnet
Class A		
/8	255.0.0.0	16,777,214
/9	255.128.0.0	8,388,606
/10	255.192.0.0	4,194,302
/11	255.224.0.0	2,097,150
/12	255.240.0.0	1,048,574
/13	255.248.0.0	524,286
/14	255.252.0.0	262,142
/15	255.254.0.0	131,070

Subnet Mask



Prefix size	Network mask	Usable hosts per subnet
Class B		
/16	255.255.0.0	65,534
/17	255.255.128.0	32,766
/18	255.255.192.0	16,382
/19	255.255.224.0	8,190
/20	255.255.240.0	4,094
/21	255.255.248.0	2,046
/22	255.255.252.0	1,022
/23	255.255.254.0	510

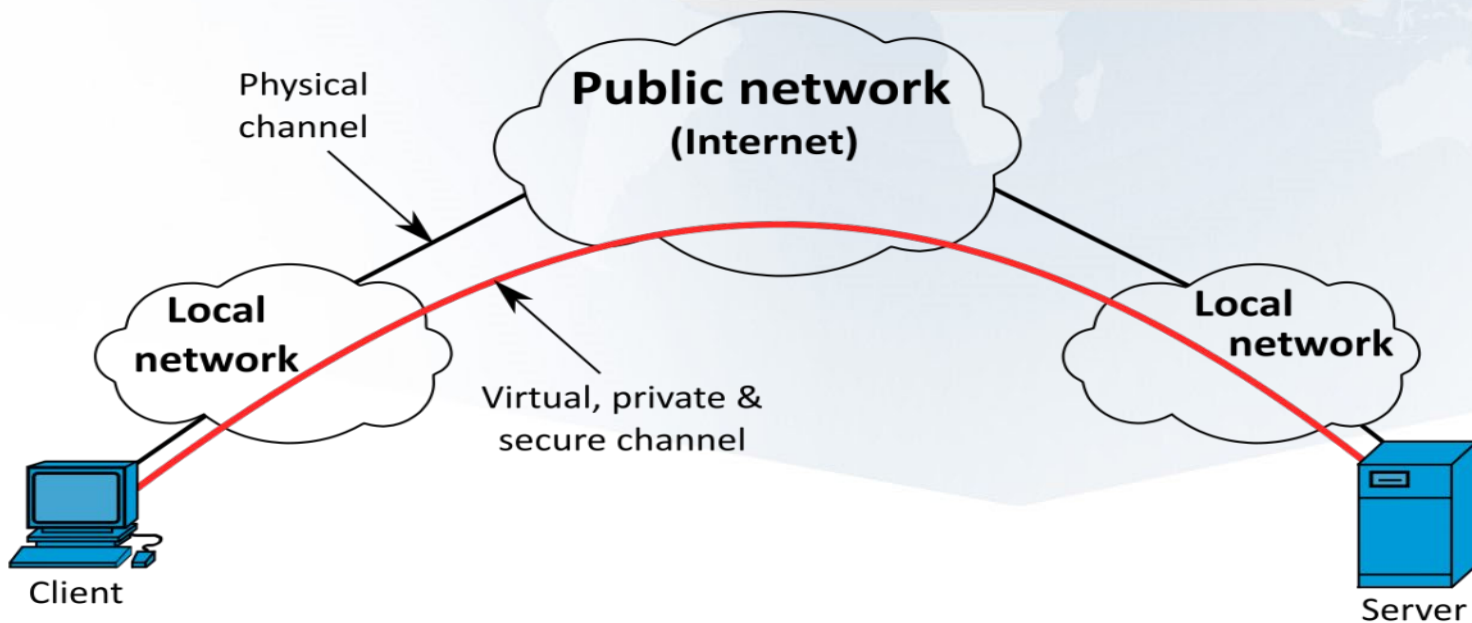
Subnet Mask



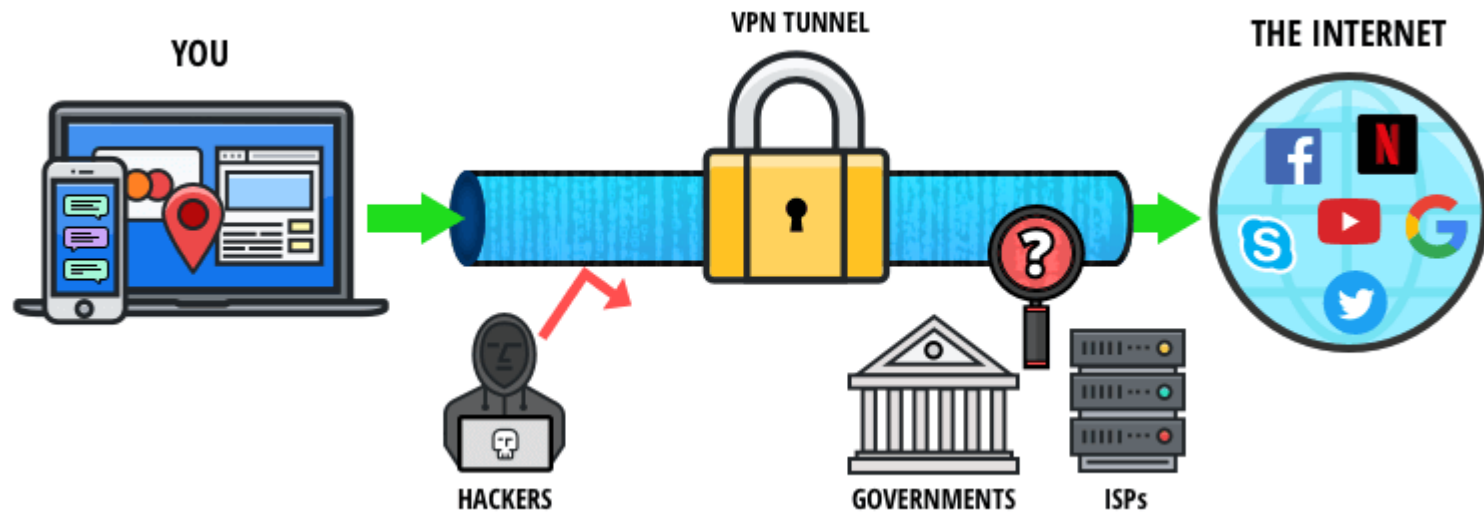
Prefix size	Network mask	Usable hosts per subnet
Class C		
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14
/29	255.255.255.248	6
/30	255.255.255.252	2
/31	255.255.255.254	0
/32	255.255.255.255	0

VPN vs Proxy

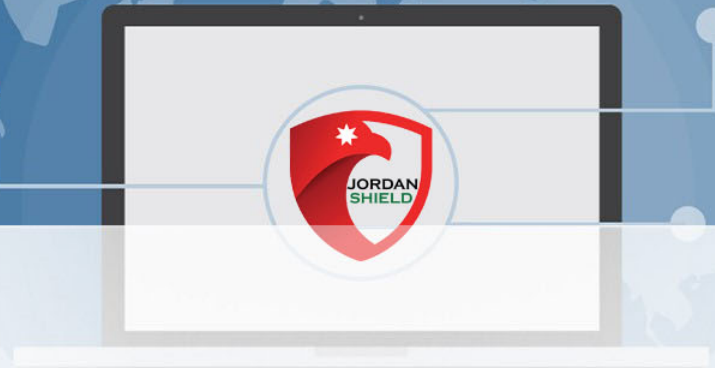
VPN : **V**irtual **P**rivate **N**etwork



VPN vs Proxy



VPN vs Proxy



Types of VPN technologies :

PPTP : Point-to-Point Tunneling Protocol

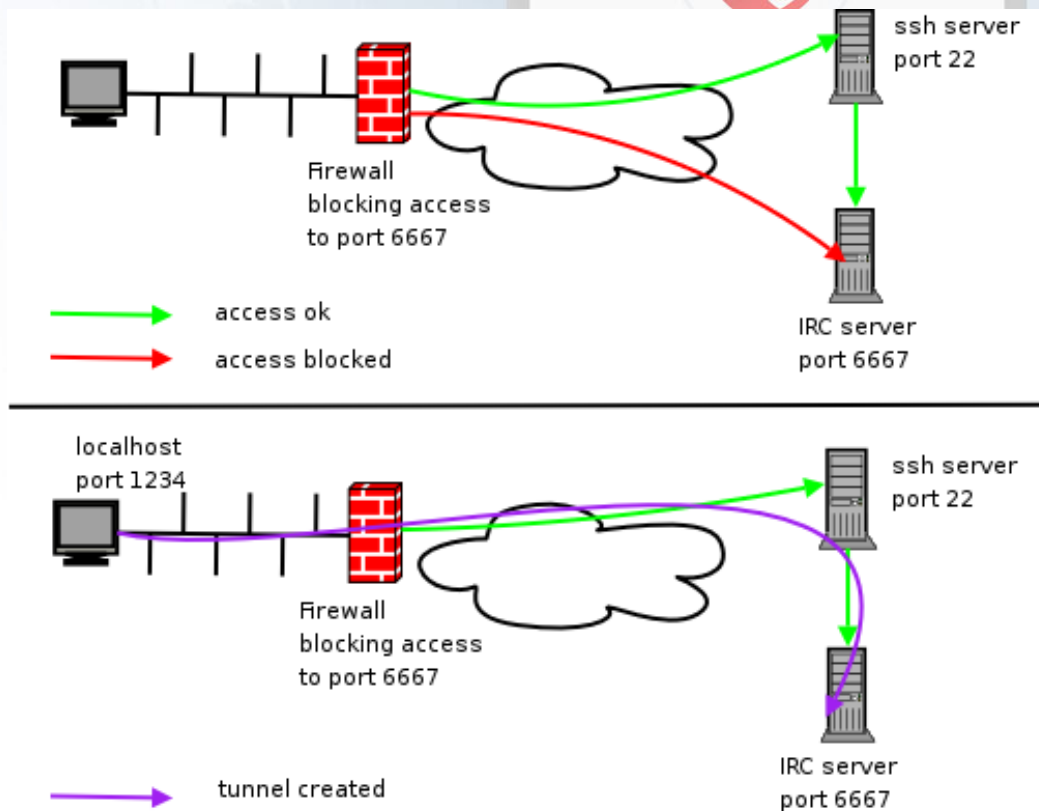
IPsec: Internet Protocol Security

L2TP : Layer 2 Tunneling Protocol

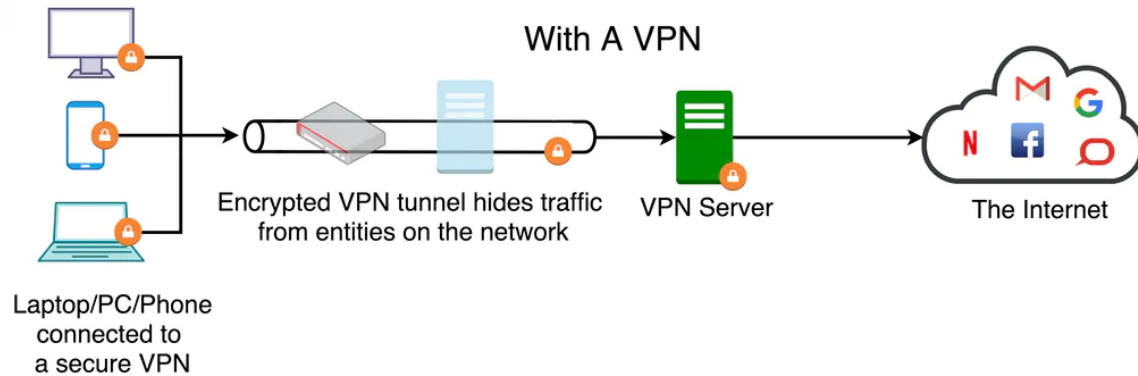
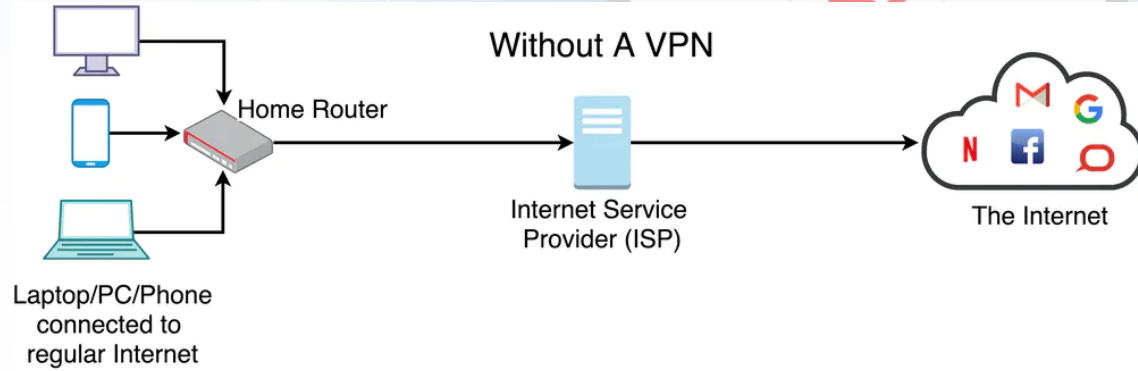
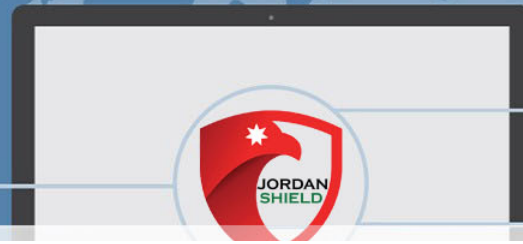
SSH : Secure Shell

VPN vs Proxy

SSH :

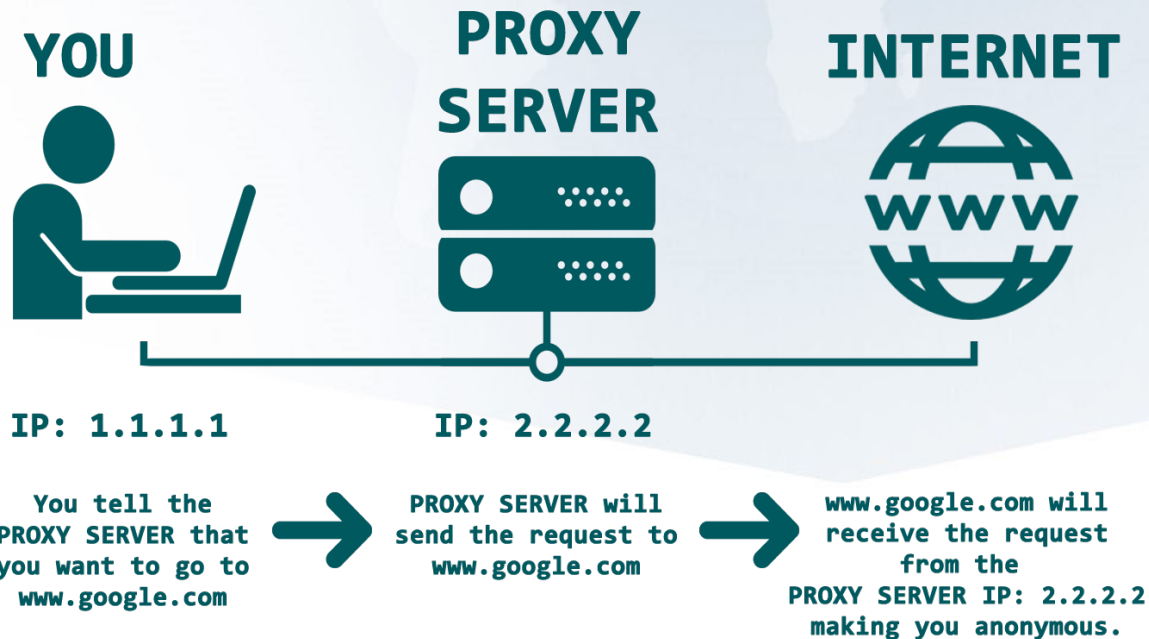


VPN vs Proxy

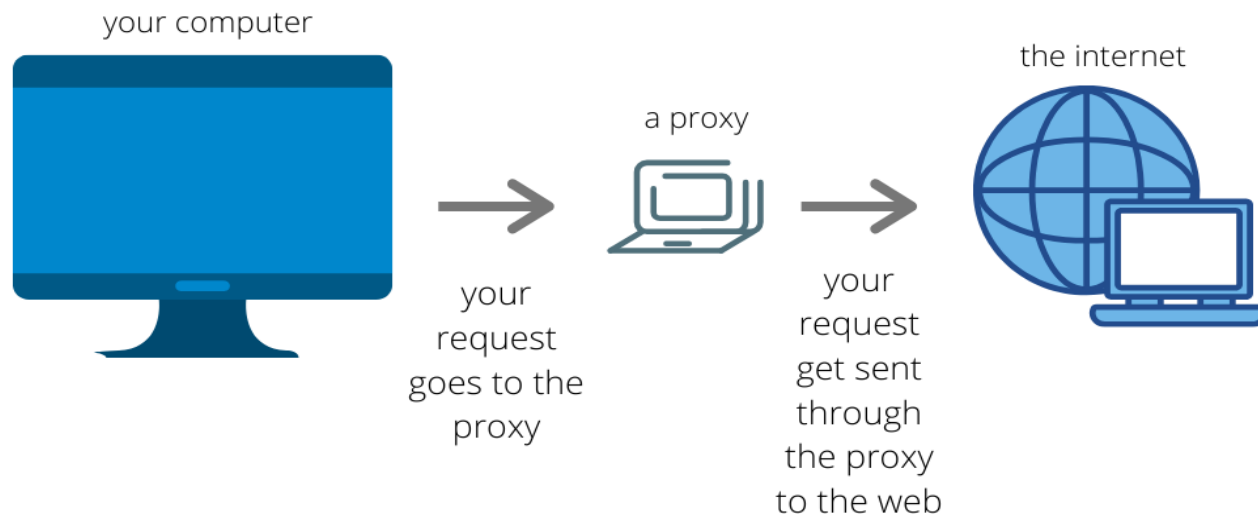
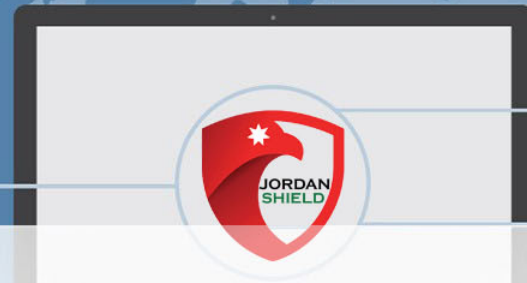


VPN vs Proxy

Proxy :

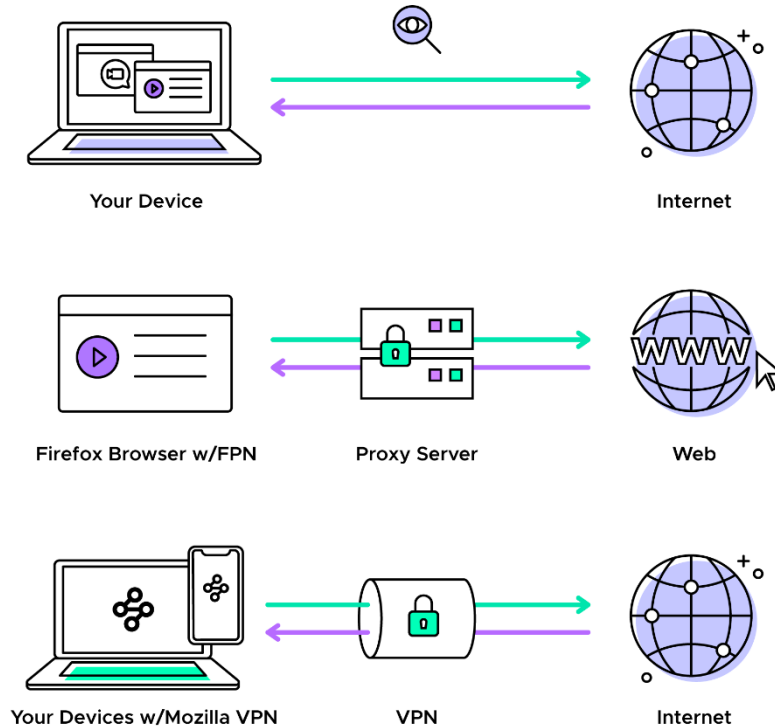


VPN vs Proxy



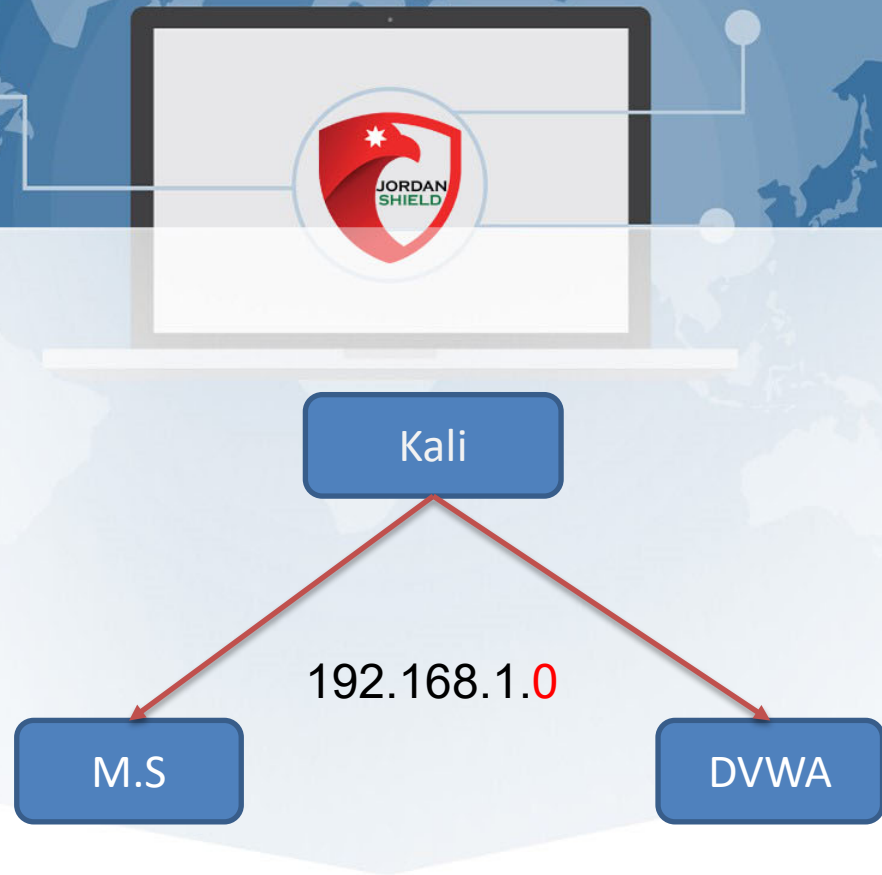
VPN vs Proxy

VPN vs Proxy

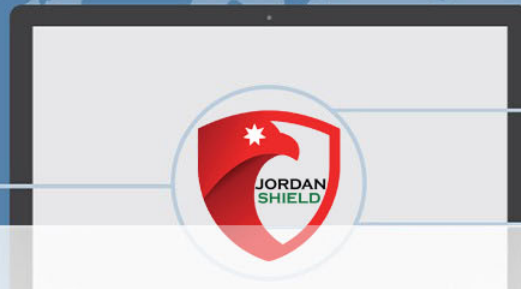


Web Attack

- 1- Metasploitable
- 2- Angry IP
- 3- NMAP
- 4- DVWA
- 5- Apache System

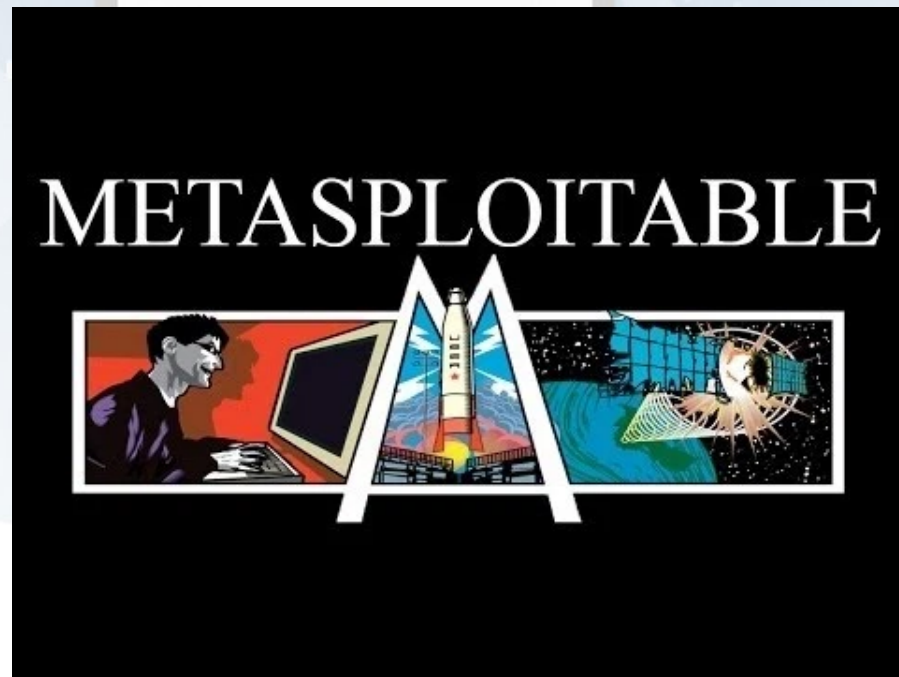


Web Attack

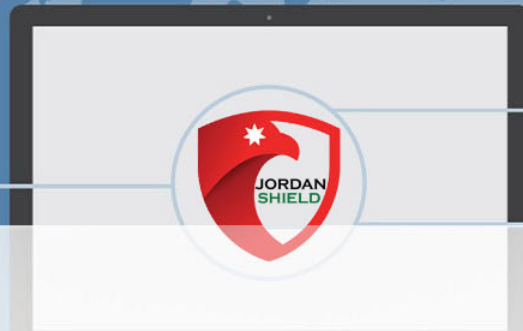


1- Metasploitable

Metasploitable is an intentionally vulnerable Linux virtual machine that can be used to conduct security training, test security tools, and practice common penetration testing techniques. The VM will run on any recent VMware products and other virtualization technologies such as VirtualBox



Web Attack

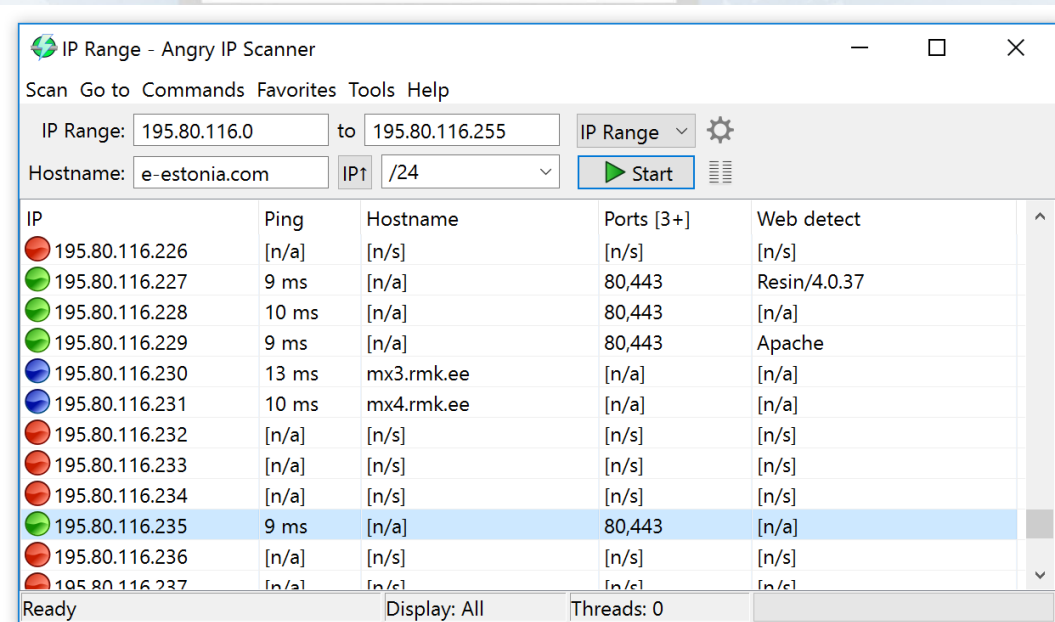


2- Angry IP

Angry IP Scanner (or simply ipscan) is an open-source and cross-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports as well as has

Features

- Scans local networks as well as Internet
- IP Range, Random or file in any format
- Exports results into many formats
- Extensible with many data fetchers
- Provides command-line interface



Web Attack



3- NMAP

Nmap, short for **N**etwork **M**apper, is a free, open-source tool for vulnerability scanning and network discovery.

Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.

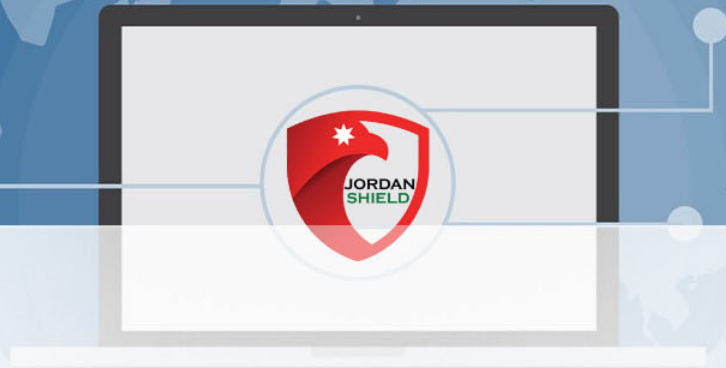
```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC Bind 9.2.1
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Serv-U ftpd 4.0
25/tcp    open  smtp     IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http     Microsoft IIS webserver 5.0
110/tcp   open  pop3     IMail pop3d 7.15 931-1
135/tcp   open  mstask   Microsoft mstask (task server - c:\winnt\system32\
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  msrpc    Microsoft Windows RPC
5800/tcp  open  vnc-http Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

Web Attack



4- DVWA

DVWA is a **DAMN VULNERABLE WEB APP** coded in *PHP/MYSQL*.

Seriously it is too vulnerable.

In this app security professionals, ethical hackers test their skills and run this tools in a legal environment.

It also helps web developer better understand the processes of securing web applications

and teacher/students to teach/learn web application security in a safe environment.

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerability, with various difficulty levels, with a simple straightforward interface.

General Instructions

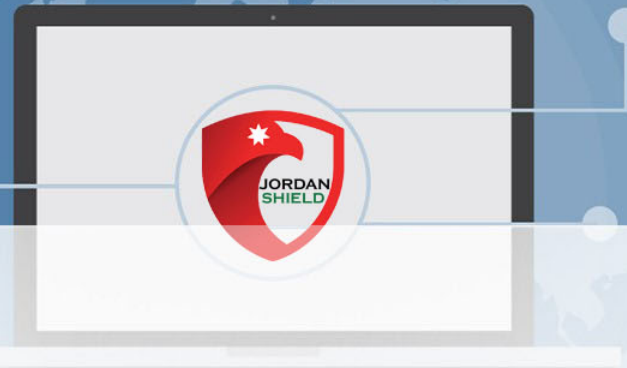
It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advance users)

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

VPN vs Proxy



5- Apache System

The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.



Web Attack



[3 Way Handshake]

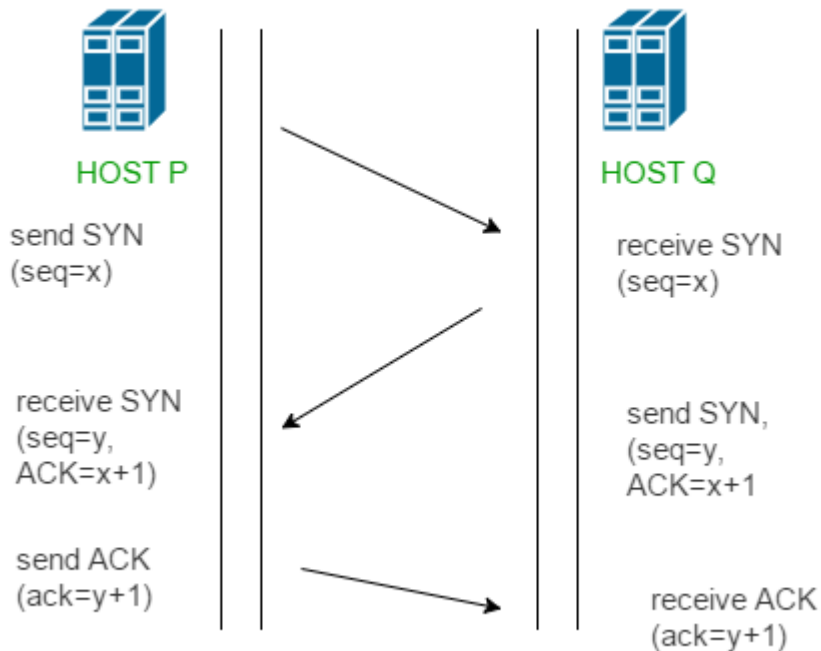
X = Random

Y = Random

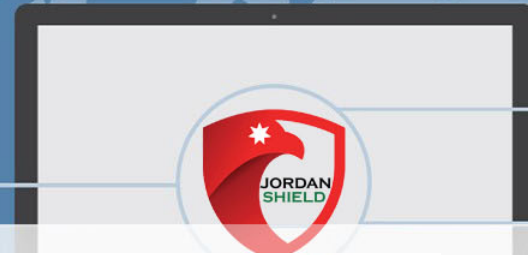
X = 100

y = 150

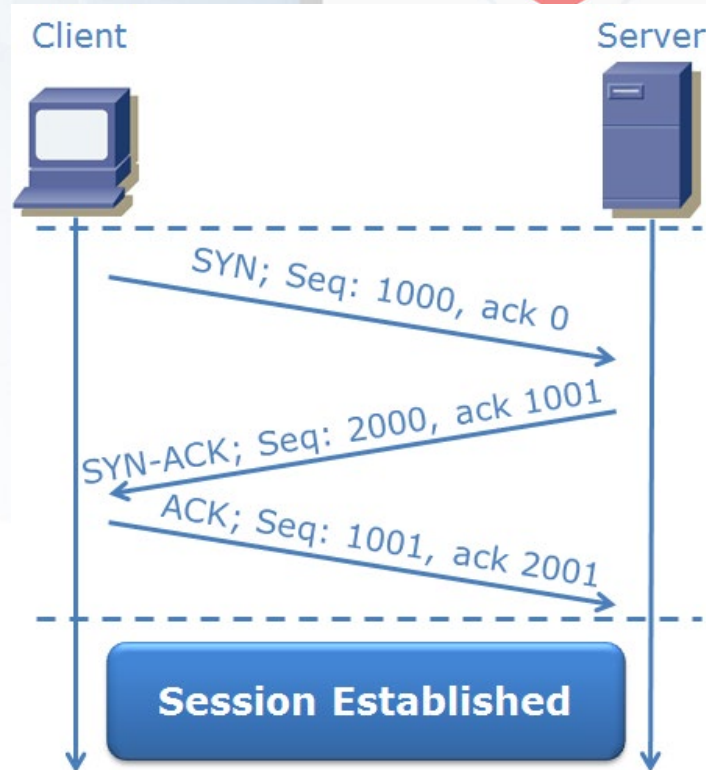
Full Connect TCP



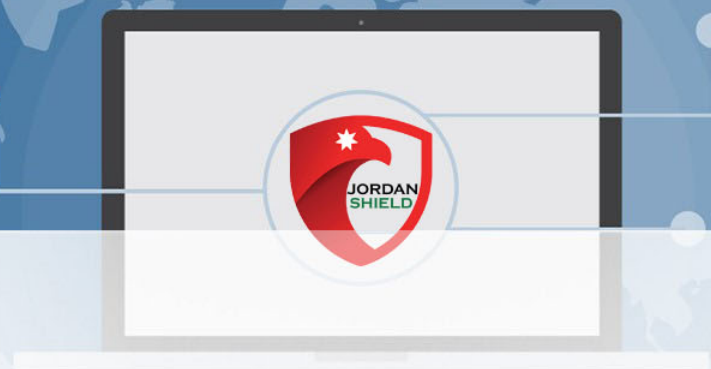
Web Attack



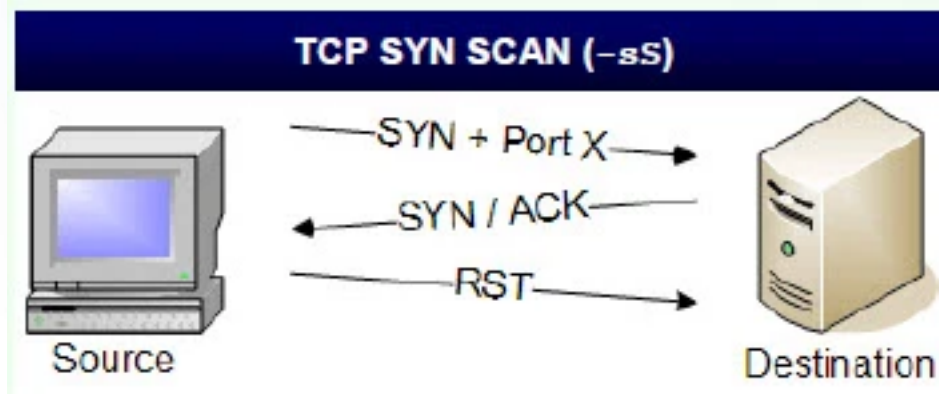
[3 Way Handshake]



Web Attack

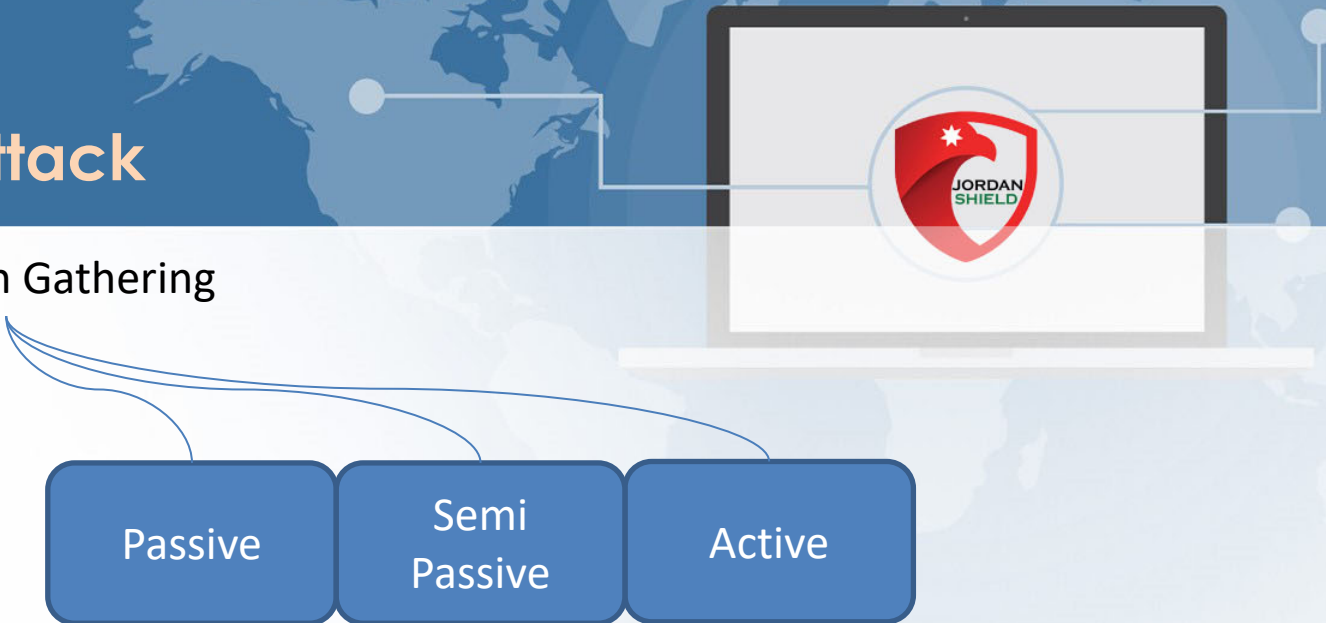


[3 Way Handshake]



Web Attack

Information Gathering

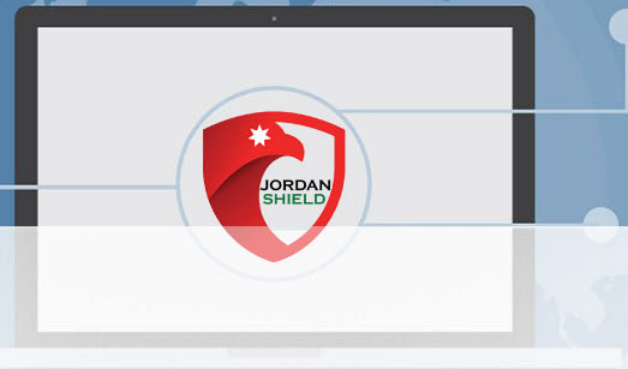


Passive : The target couldn't detect your identity – There is no packet sent .

Semi-Passive : The target may detect your packet as normal visitor – Normal Traffic .

Active : The target detect you as non-normal user – As non published servers , etc ..

Web Attack



Information Gathering

,,,, Red Hawk

Site Title

IP
Address

CMS

Cloudflare
Detection

Robots.txt
Scanner

Whois
Lookup

Geo-IP
Lookup

Grab
Banners

DNS
Lookup

Subnet
Calculator

NMAP
Port Scan

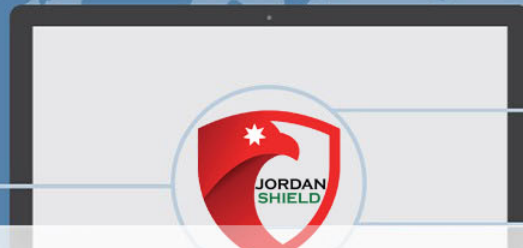
Subdomain
Scanner

Reverse
IP

SQLi
Scanner

Bloggers
View

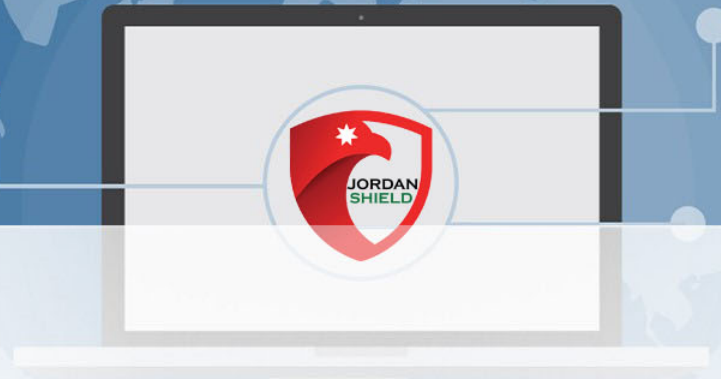
Web Attack



intitle:	intitle:"tesla vs edison" Search only in the page's title for a word or phrase. Use exact-match (quotes) for phrases.
allintitle:	allintitle: tesla vs edison Search the page title for every individual term following "allintitle:". Same as multiple intitle:'s.
inurl:	tesla announcements inurl:2016 Look for a word or phrase (in quotes) in the document URL. Can combine with other terms.
allinurl:	allinurl: amazon field-keywords nikon Search the URL for every individual term following "allinurl:". Same as multiple inurl:'s.
intext:	intext:"orbi vs eero vs google wifi" Search for a word or phrase (in quotes), but only in the body/document text.
allintext:	allintext: orbi eero google wifi Search the body text for every individual term following "allintext:". Same as multiple intext:'s.
filetype:	"tesla announcements" filetype:pdf Match only a specific file type. Some examples include PDF, DOC, XLS, PPT, and TXT.
related:	related:nytimes.com Return sites that are related to a target domain. Only works for larger domains.
AROUND(X)	tesla AROUND(3) edison Returns results where the two terms/phrases are within (X) words of each other.

Web Attack

Information Gathering



Web Attack

Information Gathering

site:*.jo

inurl:admin.php

