Possible attacks and countermeasures:

0) Preamble

The general idea would be:

After IG has found all the potential vulnerabilities (if any) of the web service, by countermeasures and possible attacks that can be carried out for each of them.

1) When the web-site is UP or hasn’t any type of Reverse Proxy

1-2 Check DOMAIN and IP

A) If the site is not protected by Reverse Proxy and fortnight can get the IP address, it is of great help to hackers who can start the "treasure hunt" on the site targeted.

B) In some cases it is also useful to analyse the HTML code offline, looking for comments in particular. Many elements that are not directly available to the public are listed in the HTML comment tags. It is faster to analyse the code offline than online, so you need to mirror the site. Mirroring tools include: Wget and Teleport Pro.

Wget=<https://www.gnu.org/software/wget/>

Telepro= <http://www.tenmax.com/teleport/pro/home.html>

3 GEO IP LOOKUP:

Location details.

A physical address can be useful for a specific hacker, representing the cue for attacks based on not very computerized techniques, such as implementing surveillance plans, social engineering, etc. In addition, a physical address can also lead to unauthorized access to a building, to wired and wireless networks. In fact, it is interesting to note that when Google's car travels the various roads with the camera, it doesn't just list visual data for Street View, but tracks any Wi-Fi network with associated MAC addresses.

4 WHOIS:

Another source of information is given to us by the Whois command or by extract public email (research number 17).

Contact names and email addresses are particularly useful data. In most organizations, real employee names are processed to form user names and email addresses. Knowing one of these addresses is easy to imagine the others. This information is used to access some reserved area or for social engineering. Hackers can rust phone numbers to trace a person's physical address with sites like phonenumber.com,411.com (United States), or blank pages, yellow pages, and clearly social networks. Another source of information is in the myriad of resumes available online.

Today the professions in the IT world are so vast and diverse that finding the right person for a specific position is very difficult. One of the best ways to facilitate the matching of supply and demand is to provide very detailed and sometimes even sensitive information in job advertisements and resumes. If, for example, a company posts an advertisement to look for a professional with, for example, 5 years of experience in using CheckPoint and IDS Snort firewalls, what type of firewall and IDS will that company use? Another threat may come from unhappy employees who also want some kind of revenge. Because the world is interconnected, it may not be difficult to tell whether an employee of such a company who has stayed at home is dissatisfied or not. The Hacker can pretend to be a new employee of that company and through the carrier of this former employee get even very sensitive information about the company in question.

5 URL HISTORY WEB SERVICES:

On the Internet it is possible to retrieve archived copies of information no longer available from the original source. These archives may allow the hacker to access information that has been deliberately removed for security reasons. Examples of sites that do this are: WayBack Machine at [archive.org](http://www.archive.org) and Google's cache results.

COUNTERMEASURES for 1-2,3,4,5,17:

A) Much of the information has to be made public and therefore it is difficult to remove it; especially for listed companies. However, it is important to detect and classify the types of information made available to the public. The Site Security HandBook (RFC 2196), ([faqs.org/rfcs/rfcs2196.html](http://www.faqs.org/rfcs/rfcs2196.html)) is an excellent resource for many aspects of security policies. It may be useful to consult them periodically and try to remove confidential data wherever possible.

B) Another possibility is to use aliases that do not allow you to trace directly to your organization, especially when using newsgroups, mailing lists or other public forums.

C) Another possibility is to use the anonymity features offered by the domain provider. For example, Network Solutions and Godaddy offer private registration functions: you pay an additional fee, in addition to the cost of the domain, to ensure that the actual data of physical address, phone number, e-mail and so on are not public.

6 SPIDER SITE:

The use of crawlers is very important because it means downloading the entire content of a website in search of the easiest targets to attack: information on local paths, back-end server names and IP addresses, SQL search queries with passwords, informative comments and other sensitive data in objects:

* static and dynamic pages
* Inclusion, library and support files
* Code sources
* Server Response Header
* Cookies

There are many ways to use a crawler for web applications. o you use wget or HHTRACK or scripts that you can easily find on Github.

HHTRACK= <https://www.httrack.com/>

Wget= <https://www.gnu.org/software/wget/>

Countermeasures 6:

A possible countermeasure about the crawlers is create a sort of trap.

* The first step is to create a trap that can trap crawlers. A web crawler does nothing but connect through an HTTP request to the site to be hit, starting to download everything you find on that page, recursively following each link that is detected within the same page.
* The idea, then, is to make him find an invisible link to a normal visitor, who makes him point to a specific directory, which contains the trap itself. The trap is nothing more than a php script able to ban the crawler's IP, thus preventing any possible access in the future.
* A normal crawler (such as googlebot, bing, etc.) will not be interested in following the hidden link, and will never access the trap because it is denied within the robots.txt file (a file that is normally read and interpreted by any "legal" bot and obviously ignored by those who have malicious intentions).

7 DNS LOOKUP:

Determining where mail is handled is an excellent starting point for locating the target organization's firewall network. Often, within a company, mail is managed on the same firewall system, or at least on the same network so using the Linux host command, you can find out more about it.

Countermeasures:

Look countermeasures 12

8 DETECT HONEYPOT:

There are some Honeypots that can be adopted including:

* Project Honeypot: <https://www.projecthoneypot.org/>
* Maxmind: <https://www.maxmind.com/en/home>
* Spamhaus: <https://www.spamhaus.org/>
* The CINS Army List: <http://www.cinsscore.com/>
* Greensnow: <https://greensnow.co/>
* Akismet: <https://akismet.com/>

Anti-honeypot techniques:

Besides mundane attempts to detect a sandbox or a VM, malware may use additional techniques to detect that it’s being executed within a honeypot.

Check the number of connections: Honeypot systems with multiple environments are used to maximize the detection ratio, so it’s common to run the same sample on several environments simultaneously. Malware can connect back to Command & Conquer (C&C) site. Judging by the number of connections from the same network, C&C can determine that something strange is happening and block all further requests. As a result, the malware won’t go through the entire attack chain.

Check the number of infection attempts: Malware may use so-called run once tactics to identify a honeypot and block further execution if more than one attempt is made to infect a particular host. In that case the loader won’t be provided with the payload and no malware behavior will be triggered.

9 SUB-DOMAINS:

Look 6-Spider site

10 CMS DETECTION:

The determination of the CMS in use allows you to know the source code of the web application: this greatly facilitates the researcher the discovery of vulnerabilities or workarounds to scale the defenses of a system, rather than forcing the application (where possible) to generate errors in order to show small portions of code sometimes unused. Knowing the version of the CMS also allows you to launch attacks through public exploits: an old version of Wordpress could be the springboard for the hacker. There are many ways to extrapolate information about the CMS:

1) *whatweb [domain name]*

2) from scripts already present on github. For the search I used a script present on github that I implemented in my code.

3) Online sites like <https://whatcms.org/>

For every CMS there is a or there are specific attacks. I mean that you can’t use an particular exploit for Wordpress to hack a Joombla CMS.

If, for example, the server in question uses Wordpress as a CMS, you can use WPscan, which is the most famous enumerator for this type of CMS.

It works as a command line:

*wpscan --url [url] --enumerate utp*

This command lists all the resources (users, themes and plugins) of the site in question. This tool also allows you to do bruteforcing attacks using wordlists, output to files or connect to external proxies. Another tool for Wordpress is WPSeku, similar to the first one can be useful to use both to get more concrete information. Maybe the first tool may not be accurate. For each CMS there is a specific attack program. So for Joombal you have JoomScan preinstalled in several Linux distros. For Drupal there would be drupwn, available by downloading the repository from Github.

Clearly these are the most famous so for the smaller one such as Plone you have to search the internet for some scripts that can enumerate all the resources.

*According with a report about CMS Wordpress represent a vector for hacker. In fact is more vulnerable, because it uses plug-in with bug of security. The last example is that of EasyWP SMTP, a plug-in to configure and handle the send of the email with over 300.000 installation. In version 1.3.9 a bug in the import system allows you to modify the wp options table, thus allowing pirates to create a new user with administrator powers. The flaw has been repaired quickly, but those who use the plugin must update it to version 1.3.9.1.*

11 SERVER WEB VERSION DETECTION:

For this research I used a technique called Banner grabbing, which is a process to collect details regarding any remote PC on a network and the services running on its open ports. An attacker can make use of banner grabbing in order to discover network hosts and running services with their versions on their open ports and moreover operating systems so that he can exploit it.

I can get info about web server using nmap, nc,telnet, curl. In my program I used netcat(nc), but there is another program more interesting called Dmitry. Dmitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU)Linux Command Line Application coded in C. Dmitry has the ability to gather as much information as possible about a host. Base functionality is able to gather possible subdomains, email addresses, uptime information, tcp port scan, whois lookups, and more.

Dmitry –b is used for banner grabbing for all open ports; Type following command to grab SSH banner of remote PC.

*dmitry -b ip of victim*

Dmitry= <https://tools.kali.org/information-gathering/dmitry>

Countermeasures 11:

Look Countermeasures 18

12 ZONE TRANSFER DNS:

Once all domains associated with the target have been identified, the DNS can be interrogated. The DNS is a distributed database used to associate IPs to host names and vice versa. If the DNS is configured with a low level of security, it may be possible to obtain important information about the target.

One of the serious configuration problems that a system administrator can commit is to allow unreliable Internet users to perform a DNS zone transfer. It allows a secondary master server to update its zone database from the primary master. This provides redundancy in DNS management, for cases where the primary server is not available.

The problem with this technique arises when an organization does not use a public/private DNS mechanism to separate external DNS data (which are public) from internal, private data. In this case, the hacker could access host names and internal IP addresses. Providing internal IPs to an untrusted user on the Internet is like providing a complete and detailed map of an organization's internal network.

Another technique is to use the nslookup client generally provided on UNIX and WIndows. You can use nslookup in interactive mode:

*$nslookup*

*> set type=any*

*> ls -d example.com. >> /tmp/zone\_out*

with type=any we set each record type, so you can work on any available DNS record (man nslookup) to get a complete list.

With the ls option it is used to list all records associated with the domain example.com. The -d option is used to list all records in the domain. Everything is redirected to a file /tmp/zone\_out. At the end of the process it is possible to open the file to analyze it.

Countermeasures 12:

DNS provides a wealth of information for hackers, so reducing the amount of data available on the Internet is important. From the perspective of the host configurator, the ability to perform zone transfers should be restricted to authorized servers only.

A good solution would be to implement encrypted Transaction SIGnature (TSIG) systems to allow only trusted users to transfer zone data. Restricting zone transfers extends the time it takes for hackers to search for IPs and host names. However, as name searches remain accessible, hackers may manually perform reverse lookups on all IP addresses for a given network block. Therefore, external nameservers must be configured to provide information only on systems directly connected to the Internet. They should never be configured to disclose internal network information. Finally, it is preferable not to use the HINFO record.

13 SUBNET LOOKUP:

Improved network security

With logical divisions between subnets, you have greater control over who has access to what. For example, in our departmental example, you could easily restrict those in engineering from accessing file server containing sensitive sales information, and prevent sales from accessing a share that houses classified engineering blueprints.

When you divide your network into subnets, you can also better contain security incidents. Because there are clear separations between subnets, you can set rules to limit traffic between each distinct subnet, and you can reduce exposure to security incidents. For example, you can better contain a virus outbreak to one department, limit the information a hacker is able to obtain, or restrict which devices are open to attack once a portion of a network is compromised.

However, the subnet request of a particular company may be concealed or rejected by the use of firewalls or proxies.

14 TRACEROUTE:

Traceroute is a useful tool for determining the response delays and routing loops present in a network pathway across packet switched nodes. It also helps to locate any points of failure encountered while en route to a certain destination.

Countermeasures 14:

A) However, in the Internet, Traceroute messages are often blocked by routers in various Autonomous Systems (AS), making Traceroute highly inaccurate in many cases.

B) Many of the commercial systems for network intrusion detection (NIDS) and intrusion prevention (IPS) allow network recognition activities to be identified. In addition, one of the best NIDS, freeware, and Snort(snort.org) programs can detect these activities. Or depending on how your website's security system is set up, you can configure your border routers to limit ICMP and UDP traffic to specific systems only, in order to minimize public exposure.

15 PORT DETECTION:

The open port checker is a tool you can use to check your external IP address and detect open ports on your connection. This tool is useful for finding out if your port forwarding is setup correctly or if your server applications are being blocked by a firewall. This tool may also be used as a port scanner to scan your network for ports that are commonly forwarded. It is important to note that some ports, such as port 25, are often blocked at the ISP level in an attempt to prevent malicious activity.

Countermeasures 15:

Protection from port scanning is often achieved through the use of a firewall.

A firewall monitors incoming and outgoing connections through one's personal computer. One technique used by firewall technology is the opening of all the ports at one time. This action stops port scans from returning any ports. This has worked in many situations in the past, however, most experts agree it is best to have all open ports investigated individually.

Another approach is to filter all port scans going to one's computer. An individual can also choose to port scan his or her own system, which enables one to see the personal computer through the eyes of a hacker.

Firewalls are the best protection one can invest in with regard to port scanning. Firewalls deny outside access to an individual's personal computer. With this type of protection, a personal computer is essentially hidden from unwelcome visitors and is also protected from a variety of other hacking techniques. With firewall software, an individual is assured that his or her sensitive and personal information remains protected.

In today's age of cyber-crimes, identity theft, and the myriad of other criminal activities which can be executed through electronic technology, one should never assume that he or she can be too careful. Most people who have become the victim of cyber theft, or other similar crimes, state they wish they would have paid closer attention to the tools available through which their personal computers could have been made safer, and less vulnerable to attack.

16 OPERATING SYSTEM OF TARGET MACHINE:

There are different types of analyses that are carried out to distinguish one operating system from another:

1) Test FIN = A FIN packet is sent to an open door. RFC 793 states that the correct behaviour is not to respond. However, many stack implementations (such as Windows 7/200x/Vista) respond with FIN/ACK.

2) Proof counterfeit flag= An undefined TCP flag is set in the TCP header of a SYN packet. Some OS such as Linux, respond with the flag set in their response packet.

3) ISN sampling (Initial Seuqence Number) = The premise is to find a pattern in the initial sequence chosen by the TCP implementation in response to a connection request.

4) Monitoring of the "nonfragmentation bit" = Some OS set the nonfragmentation bit to improve performance. It would be possible to monitor these bits to determine which types of operating systems exhibit this behavior.

5) CWND TCP= keeps track of the initial CWND on returned packets. For some stack implementations, this size is unique and this information is useful for the accuracy of the fingerprinting mechanism.

6) Limitation of error messages ICMP= SO can execute RFC 1812 and limit the sequence in which error messages are sent. By sending UDP packets to some randomly selected high number ports, you can count the number of "unreachable host" messages received within a given time interval. This type of survey is also useful for determining whether there are open UDP ports.

7) Integrity of returned error message= Some stack implementations may alter IP headers when returning ICMP error messages. By examining the types of header alterations, you can make assumptions about the target operating system

Countermeasures 16:

For the search of the operating system on the web server the only solutions that can be adopted to have some protection are:

1) FreeBSD that supports the TCP\_DROP\_SYNFIN kernel option, used to ignore a SYN+FIN packet sent by Nmap in a stack fingerprinting operation.

However, the support of RFC 1644 "Tcp Extension for Transactions" is violated.

2) Adopt reliable and secure proxies or firewalls that should be left exposed to Internet scanning activities. In fact, hiding is not the best line of defense.

3) Some sysadmin try to block the User Agents considered malicious. The User Agent summarizes some information about the client that makes the request: in the case of a Browser, it can communicate the type of browser, the model and the type of OS in use; other times it can use poor or "standardized" information according to the programming framework/language that was used to design a program.

On the net you can find some self-configuring scripts including long lists of "bad bots" to block: a good starting point is the Ultimate Bad Bot Blocker available both on Apache and for nginx.

17 EXTRACT EMAIL FROM WEB-SITE:

Look 4-Whois

18 DBMS DETECTION:

IG implements a mechanism thanks to the Metasploit framework, to identify the DBMS of web servers that have port 3306 open. Thanks to the implemented procedure, the version of the DBMS in use is possible.

Possible attacks there are thanks to SQL injection. The documentation about attack are in this links.

<https://www.owasp.org/index.php/Testing_for_MySQL>

Countermeasures 11-18:

Mitigating a scan on several fronts can be a difficult task if you do not have the necessary skills. The different possible scenarios do not allow you to determine precisely the possible solutions to the many problems, so you can rely on Managed Server solutions as well as using a Reverse Proxy. Or use a historical application like Snort or Suricata that is able to detect intrusion attempts in a network.

In general database vulnerabilities are:

* Network Attacks
* Database engine bugs
* Integrated vulnerable objects
* Weak or default passwords
* Wrong configurations
* Indirect attacks

Finally , when it comes to IT security at the operating system level, the reference point is certainly OpenBSD. This is confirmed by the fact that it is the operating system widely used by both ISPs (Internet Service Providers) and embedded systems, and was the first to implement the IPsec (IP security) protocol, widely used in VPN (Virtual Private Network).

OpenBSD represents one of the best choices in the realization of high security systems, such as firewalls, thanks to its PF (Packet Filter), as well as in IDS (Intrusion Detection System) intrusion control systems, as well as in server solutions or as a router.

OpenBSD: <https://www.openbsd.org/>