УДК 621.51:314/316

# THE IMPORTANCE OF CYBERSECURITY IN THE MODERN WORLD

Babiy V.P., the first year IT student
Scientific supervisor: Deryabina N.V., Ph.D., Associate Professor
Kemerovo State University

Information technology encompasses a wide range of fields and applications. They contain a variety of technologies, technological processes, as well as information systems that are used for the purpose of processing, storing, transmitting, and analyzing data. Information technology plays a significant role in all spheres of today's world, including cybersecurity.

The purpose of the article - highlighting the methods of testing for penetration into a system or network using the examples of the practical part.

Cybersecurity is a field of knowledge and practices or advanced technologies that help protect critical systems, computers, servers, and networks from digital attacks. As the number of users working and connecting to the World Wide Web from different parts of the world increases every day, attackers are trying to develop different methods or different types of attacks to gain access to resources in order to steal valuable data, intentionally fail to perform business, or even extort money.

The main job of a cybersecurity specialist is to test a computer, server, network, application or website for penetration, that is, to analyze a system for security and the presence of vulnerabilities (pentest), as well as to protect a system for an active attack (such as a DDoS attack, brute-force attack, phishing, SQL injection, etc.). It may sound strange, but the fact is the set of tools of a cybersecurity specialist can be compared with the hackers' ones. It should be noted that a security specialist (ethical hacker) knows how to hack. The only thing that distinguishes them is the purpose of the hack.

Basically, the white hat hackers work in an operating system (unusual for ordinary users) differs from Windows – Linux. The reason is the fact that Kali Linux contains features like security analysis, security auditing, and penetration testing. Also, with the Linux OS, tools for pentesting, hacking and information analysis are already pre-installed, such as:

1. **Aircrack-ng**. A set of utilities for detecting wireless networks, intercepting transmitted information and traffic of various WEP/WPA/WPA2 audits, as well as for pentesting, wireless network penetration testing;

2. **Metasploit**. The program that provides information about vulnerabilities, penetration testing of systems and networks, and the launch of a malicious code, as well as it helps to gain the access to the information necessary for a hacker;

3. **Nmap.** A program for scanning networks, their IP addresses, as well as the ability to configure the number of objects to be scanned. An IP address is one of the most important pieces of information about a computer, server, or network. Know-

ing the IP, a hacker can find out any information about the network/computer, and then the ability to penetrate this network/computer;

4. **Wireshark**. A program that analyzes traffic for Ethernet computer networks and "knows" the structure of a wide variety of network protocols.

Let's use the “nmap utility” as an example to try to find open ports through an IP address that belonged to the author's computer. In this example, there was no attempt to penetrate into other nodes or ports, but the main task of a white hat hacker is to find out the IP of the system, then penetrate and identify vulnerable and open ports.

To find out your personal IP, just open a command prompt and write the ipconfig command in Windows. The rest of this project was done on the Kali Linux command line. This project can be considered very easy, since a personal IP address was taken and checked for the vulnerability of open ports and hosts in the author's system. Kali Linux already has the nmap program installed out of the box, so just write the following command:

~$ nmap -O <ip-address>,

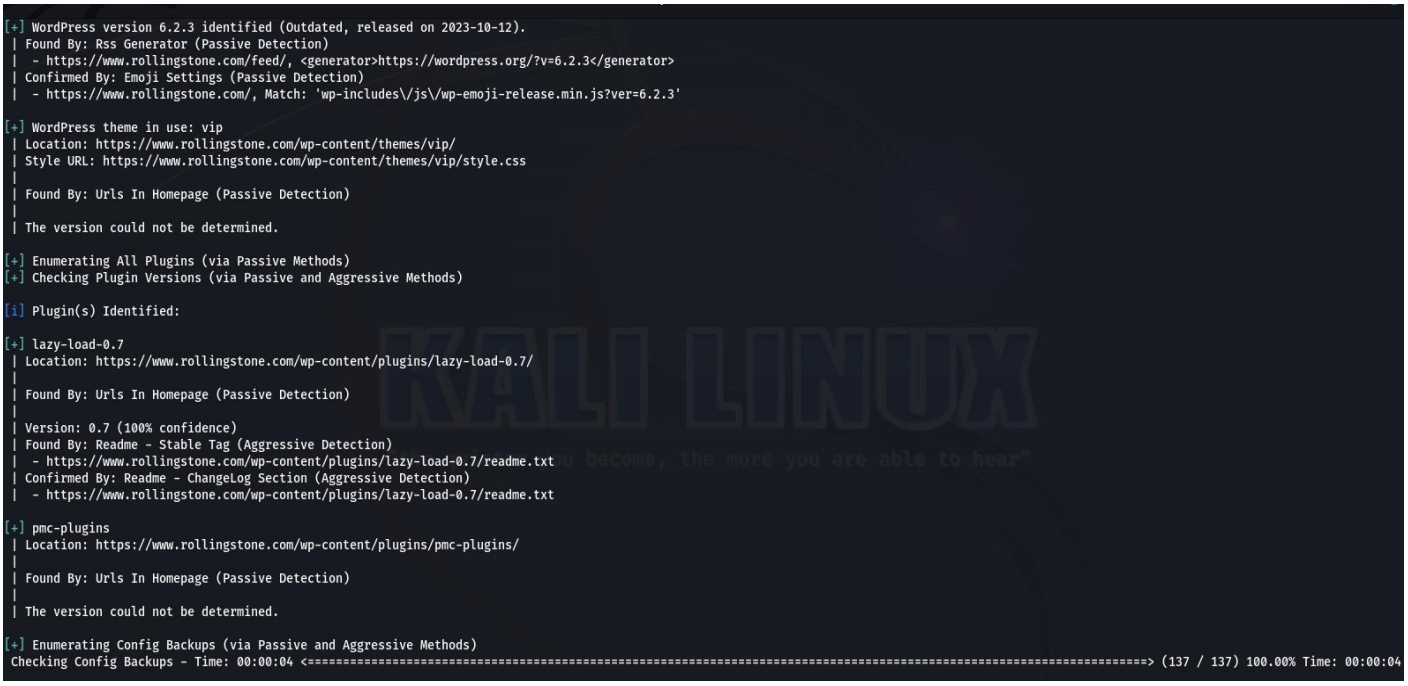
where instead of <ip-address> you must specify the IP address. For example:

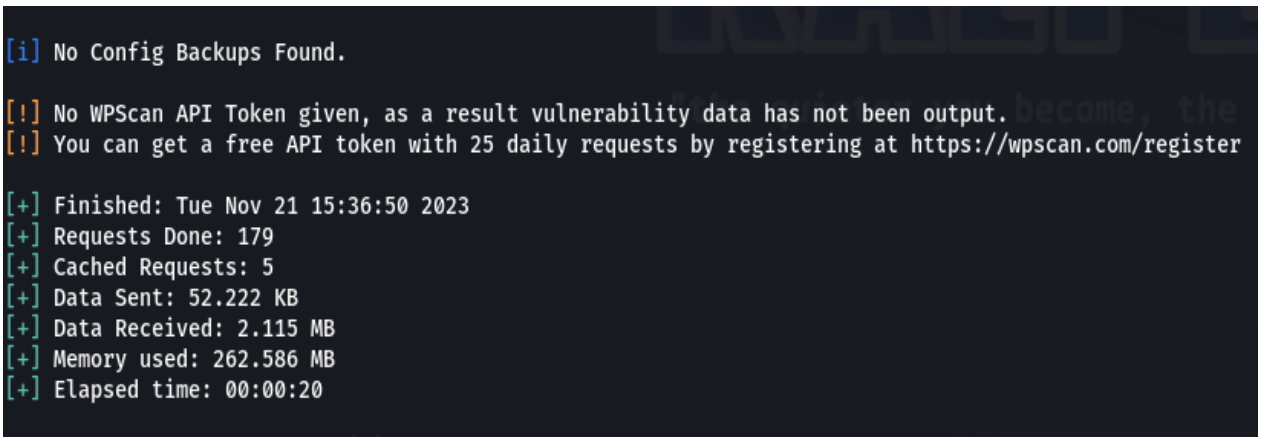
```
┌──(root㉿kali-anon)-[/home/babiyvictor]
└─# nmap -O 192.[redacted]
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-14 20:50 +07
Nmap scan report for 192.168.177.175
Host is up (0.0012s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1042/tcp open  afrog
1043/tcp open  boinc
5357/tcp open  wsdapi
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (95%), QEMU (90%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (95%), QEMU user mode network gateway (90%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.53 seconds
```

This command displayed all the ports open in the system in a column with the names of all available ports under the PORT name. If there is further deepening, then there is an opportunity to penetrate these ports and access some information (depending on the type and protocol of the port).

Let's move on to the next practical part, here we use the WPScan utility. The WPScan tool allows you to check WordPress (on the basis of which a wide variety of sites are made - business card sites, blogs and even online stores) for vulnerabilities. In addition, it also provides detailed information about the active plugins. A well-protected blog does not provide much information, but it's still worth trying. Using this tool on the Linux command line looks like this:


(babiyvictor㉿kali-anon)-[~]
$ wpscan --url https://www.rollingstone.com/
WordPress Security Scanner by the WPScan Team
Version 3.8.24
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[+] URL: https://www.rollingstone.com/ [192.0.66.114]
[+] Started: Tue Nov 21 15:36:30 2023
Interesting Finding(s):
[+] Headers
| Interesting Entries:
| - server: nginx
| - x-hacker: If you're reading this, you should visit wpvip.com/careers and apply to join the fun, mention this header.
| - x-powered-by: WordPress VIP <https://wpvip.com>
| - host-header: a9130478a60e5f9135f765b23f26593b
| - x-ua-compatible: IE=Edge
| - content-security-policy: upgrade-insecure-requests, frame-ancestors 'none'
| - content-security-policy-report-only: default-src data: 'unsafe-inline' 'unsafe-eval' https: blob: http://*.files.wordpress.com wss://www.rollingstone.com; report-uri https://pmcuri.report-uri.com/r/d/csp/reportOnly
| - x-rq: arn1 96 185 443
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] This site has 'Must Use Plugins': https://www.rollingstone.com/wp-content/mu-plugins/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 80%
| Reference: http://codex.wordpress.org/Must_Use_Plugins


[+] WordPress version 6.2.3 identified (Outdated, released on 2023-10-12).
| Found By: Rss Generator (Passive Detection)
| - https://www.rollingstone.com/feed/, <generator>https://wordpress.org/?v=6.2.3</generator>
| Confirmed By: Emoji Settings (Passive Detection)
| - https://www.rollingstone.com/, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=6.2.3'
[+] WordPress theme in use: vip
| Location: https://www.rollingstone.com/wp-content/themes/vip/
| Style URL: https://www.rollingstone.com/wp-content/themes/vip/style.css
| Found By: Urls In Homepage (Passive Detection)
| The version could not be determined.
[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
[i] Plugin(s) Identified:
[+] lazy-load-0.7
| Location: https://www.rollingstone.com/wp-content/plugins/lazy-load-0.7/
| Found By: Urls In Homepage (Passive Detection)
| Version: 0.7 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - https://www.rollingstone.com/wp-content/plugins/lazy-load-0.7/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - https://www.rollingstone.com/wp-content/plugins/lazy-load-0.7/readme.txt
[+] pmc-plugins
| Location: https://www.rollingstone.com/wp-content/plugins/pmc-plugins/
| Found By: Urls In Homepage (Passive Detection)
| The version could not be determined.
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:04 <==========> (137 / 137) 100.00% Time: 00:00:04


[i] No Config Backups Found.
[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[+] Finished: Tue Nov 21 15:36:50 2023
[+] Requests Done: 179
[+] Cached Requests: 5
[+] Data Sent: 52.222 KB
[+] Data Received: 2.115 MB
[+] Memory used: 262.586 MB
[+] Elapsed time: 00:00:20

The blog cannot be hacked right away, but you will get information about its vulnerabilities. All sorts of system information, such as the PHP version, are also available. And in this example, the rollingstones.com site was checked for vulnerabilities. From the screenshots above, you can understand that the following information is known about this site: the utility determined the version of currently installed WordPress, found the name of the site's server, as well as plugins and their versions that the site uses, and confidential files such as readme.

So, in the modern world where digital information plays a tremendous role in all spheres of life, the importance of cybersecurity is becoming critical. Cybersecurity encompasses the methods and measures that are taken to protect computer systems, networks, and data from threats, attacks, and unauthorized access. Cybersecurity is becoming increasingly important as digital information becomes more valuable and technology-dependent. Increased threat awareness, regular updating and improvement of systems, and the use of modern methods and technologies allow us to effectively combat cyber threats and protect our digital information.

**References:**

1. https://www.microsoft.com/ru-ru/security/business/security-101/what-is-cybersecurity
2. https://ru.m.wikipedia.org/wiki/Kali_Linux