Automating Security Vulnerabilities using Scanning and Exploiting

Ranjana Jadhav, Shubhangi Ovhal, Priyanka Mutyal, Aishwarya Damale, Sriya Nagannawar

Abstract—Cyber security is gaining tremendous importance due to the increased reliance on the internet, computer systems and wireless networks like Wi-Fi and Bluetooth. Explosive growth of internet has invited in new advancements, but these technical advancements have a dark side: Attackers. To sway away the cyber attacks caused by the attackers, it is a vital job to provide a tough security to the arrangement. This research explores the characteristics of our security tool "Autoploit". Autoploit is used for scanning and exploiting. It is applied in checking the security of nodes in LAN and Web application. The process starts with scanning. For scanning of nodes in LAN, IP address is taken as the input and for website, URL of the website is taken as the input. After scanning process is carried out, all the vulnerable open ports are discovered. Banner grabbing gives the services of the vulnerable ports. Later in exploiting, Autoploit has its own exploits. Exploiting is done by version wise attack. It prevents the system from crashing. If the exploiting is successful then it is concluded that the system is not secure enough. Thus Autoploit is used to give the security efficiency report of the tested system.

Keywords— scanning, exploit, reconnaissance, banner grabbing, attack.

I. INTRODUCTION

Hacking is an attempt to expose, disable alter gain or steal unauthorized access to or make unauthorized use of an asset. It targets the computer information system, infrastructure, personal computer devices or computer networks. This leads to loss of sales, reduction in profits loss of data, disruption to trading, loss of business or contract. There is increase in companies investing huge amount of money for preventing an attack even before it happens. The present legal system against the cyber crime has innumerable loop holes. Due to which the corporate as well as the government enterprises have begun to take matters into their own hands.

Their preventive measures initiate by hiring hackers of their own for the purpose of detecting of these loop holes within their networks[1]. Autoploit checks the security of the device. It is used for the system like nodes in LAN and web application. The system exploits the vulnerable ports and if the attack is successful then the system is not secure. Autoploit thus prevents the system from all he further possible cyber attacks.

II. MOTIVATION

Hacking, viruses, malware are some of the real security threats in the virtual world. Wireshark, aircrack, Nessus Professional, OpenVAS are the different tools for scanning[2]. Nmap is used for scanning. But the disadvantage of Nmap is it takes 50-60 min for scanning 65535 ports. The approximate time taken for scanning the 65535 ports is 50 to 60 min. Metasploit is one of the most used tools for exploiting as it is a powerful one. Disadvantage of Metasploit is, it has efficiency only up to 60%. Autoploit is a tool which overcomes the issues of the currently working tools. Autoploit is an improved tool over the current ones. It performs the processes of ethical hacking viz. Reconnaissance, scanning and exploiting in one go[3].

III. LITERATURE SURVEY

At present few tools are present that avoid the external threats to personal networks. Despite of this we are trying to see if it is possible to bypass the tool and attack the personal network. And also check its vulnerabilities and the ports that are open. The tools used for preventing unauthorized access to a computer are as follows:

A. NMAP

Distinctive new servers create map of networks. This eventually audits the security of a network. And then sends packets to the target hosts. Analyzing the responses and identifying hosts on a network is done by this tool. The open ports on target hosts are enumerated in port scanning. To learn application name and version number it interrogates network services on remote devices. Scans proceed in phases and with each phase finishing before the next one begins. Inspecting the device security or firewall by recognizing the network connections which can be made to, or through it is done by this tool. Recognizing the open ports on a target host for inspecting is the next step done by this tool. Mapping, inventory, maintenance and asset management of network are the fields where it is used. It recognizes new servers and hence audits the security of a network. It generates traffic to hosts on a network,

Revised Manuscript Received on May 22, 2019.

Ranjana Jadhav, Dept. Information Technology, Vishwakarma Institute of Technology, Pune, India, ranjana.jadhav@vit.edu
Shubhangi Ovhal, Dept. Information Technology , Vishwakarma Institute of Technology, Pune, India, shubhangi.ovhal16@vit.edu
Priyanka Mutyal, Dept. Information Technology, Vishwakarma Institute of Technology, Pune, India, priyanka.mutyal16@vit.edu
Aishwarya Damale, Dept. Information Technology, Vishwakarma Institute of Technology , Pune, India, aishwarya.damale16@vit.edu
Sriya Nagannawar, Dept. Information Technology Vishwakarma Institute of Technology, Pune, India, sriya.nagannawar16@vit.edu

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

response analysis and response time measurement and then finds and exploits vulnerabilities in a network. At the reconnaissance stage of an arranged attack Network scanning is carried out. A network scanner provides an attacker with data on remote machines. They are alive and the attacker can have communication with it. Scanning consists of Host sweeps/scans, OS scans, port scans and ping sweeps/scans. A host scanning takes place over an entire network followed by reporting machines that are alive on the network. On the other hand, port scan is performed on a single, remote, host system, through its IP Address. It also gives information on services running on the machine. An attacker also looks for open exploitable TCP and UDP ports (services). - A network scanning tool can be used to automatically probe the system for open ports, and generate a report[3].

B. Metasploit

The vulnerabilities are shown using Metasploit and Metasploit also aids in Penetration Testing. It observes malicious activities. Metasploit Framework is not only an open supply but also is the foremost ordinary exploit development framework presently. Breaking into remote systems or test for a computer system vulnerability has become easier due to Metasploit.

C. Metasploit Interfaces:

A free of cost version of Metasploit which provides a command line interface is Metasploit Framework Edition. Metasploit Community Edition has several features to offer such as network discovery, manual exploitation and module browsing. A visual cyber attack management tool that visualizes targets and puts forth exploits built on the vulnerabilities is Armitage and it is a free interface for it. Cobalt Strike is an interface which has all the characteristics of Armitage, generation features, adding post exploitation tool and report[4].

A. Exploiting a system using Metasploit:

It permits the accompaniment of any kind of exploit with any other kind of payload. First of all data regarding the desired target system is gathered before browsing. Port scanning is employed as assistance to check open ports in a network by a host, and OS fingerprinting, by overlooking the information flowing from these systems, tools. The Metasploit imports these vulnerability scanners information and confirms that the planned exploit is acceptable for any existing vulnerabilities. Exploiting a system using Metasploit involves 5 basic steps: Opening move is selecting a particular exploit and configuring it by writing the acceptable code to focus on a system. Second step is to exploit a particular bug in it. Third step checks whether or not the target system is susceptible to the given exploit. In next step we select a payload which is applied on the target system while managing to exploit it. And the last step is choosing the appropriate encoding technique to deceive network trafficking and make it neglect the oncoming payload. Lastly, perform the Exploit[5].

D. Burp Suit

Various tools for performing different testing tasks are all clubbed into Burp Suit and they are as follows:

- Target - This tool contains careful data concerning the applications that are target, and assists to drive the method of testing for vulnerabilities.
- Proxy- This is a web proxy and acts like a middle person between the end browser and the target web application. We can obstruct, modify and inspect the traffic passing in every directions.
- Scanner Professional – Automatically crawling the content and carrying out audit for numerous types of vulnerabilities is done by an advanced web vulnerability scanner.
- Intruder- Automated customized attacks against web applications is carried out by a powerful tool i.e. intruder. It is utilized to execute various tasks for faster and effective testing and is highly configurable.
- Repeater -Exploiting HTTP requests and analyzing the application's responses is the task done by the repeater.
- Sequencer – Sequencer analyzes the quality of randomness in an application's session tokens or other vital data items.
- Decoder- Intelligent decoding and encoding of application info is done by the mentioned powerful tool.
- Comparer – It is used for carrying out differences between two data items.
- Extender- It is used for loading Burp extensions, along with this it extends Burp's functionality using our owns third-party code.
- Clickbandit - It generates Click jacking attacks.
- Collaborator client Professional - Burp Collaborator during manual testing can be used. This is possible with the help of collaborator client professional.
- Mobile Assistant - This tool tests the mobile apps through Burp Suite.

Burp Suite tests the security of the web applications. It is also used in stages right from initial mapping and analysis of application’s attack surface to finding and exploiting security vulnerabilities

E. Angry IP Scanner

This tool is an associate in IP address and port scanner. This is a scanner which is lightweight and cross-platform. This scanner can scan IP addresses having any range and these can be copied and used. Multithreaded approach is used in order to increase the scanning speed. A separate scanning thread is made for every scanned informatics address. This tool pings every IP address to resolve its hostname and if it is alive, after that. After this, the scanner learns the MAC address and scans ports. Any information about scanned IPs is gathered by the Angry IP Scanner with help of plugins. Cain and Abel, Ettercap, EtherPeek, Superscan, QualysGuard are the tools used along with the above 4 tools.

METHODOLOGY

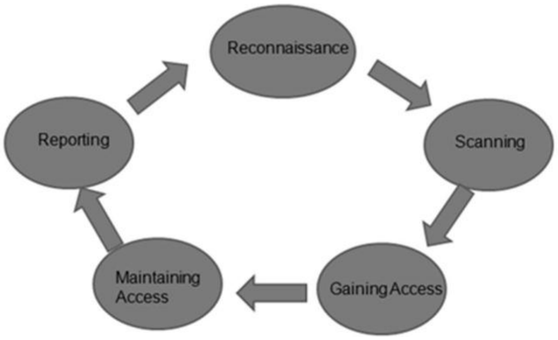


Figure 1: Project Flow Diagram

1. Reconnaissance

The processes and techniques of Foot printing, Scanning & Enumeration are used. Data about a target systemcan be fetched by these techniques. Autoploit gathers information regarding a target system. Autoploit being a versatile tool can be used on both the devices connected in LAN as well as Web application. First of all user has to give target IP or host name (URL) as a input to Autopliot. Then it checks whether the host or target is alive or dead by using ICMP echo method. If host name of target is given then IP of host is extracted by using gethostbyname() function. For Computer system in LAN Autoploit studies the network and finds the alive nodes residing in the network. Autoploit uses the ping utility to check the hosts that are alive. Autoploit sends a ping command to nodes. If node replies to the ping command with a pong response it shows that the node is alive. If there is no reply from the node then the node is dead. The IP's of the nodes which are live will be received by the Autoploit. To establish a connection between client and the target three way handshake is used[6].

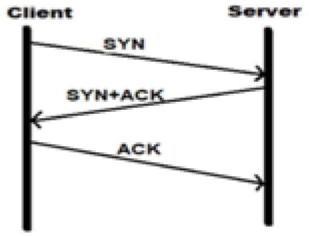


Figure 2: Three way handshake

Following are the steps evolved in reconnaissance

1. *Banner Grabbing-*

Banner grabbing grabs the information about computer system on a network and the services running on its ports. Autoploit uses this technique to check services running on the ports and its versions. In Autoploit it is used to scan particular ports that are 21,22,23,25. A socket is created to connect with this ports. Once the connection is established then Autoploit send data (GET / HTTP /0.1) to target. Then data is received through syn/ack from target like system name and version or kernel version.

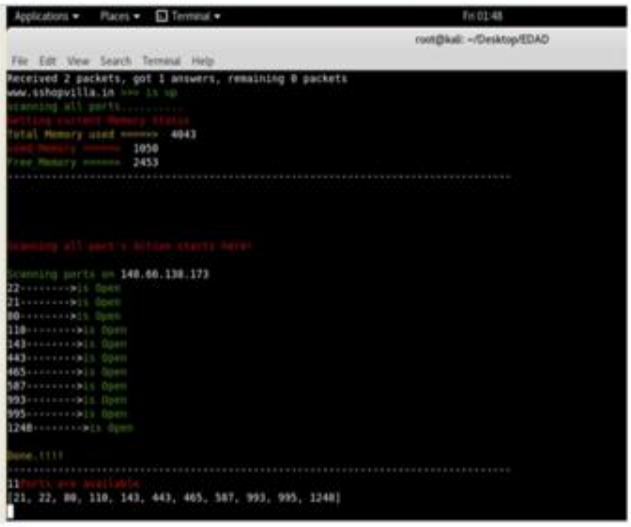
2. *Scanning*

Recognition of live hosts, ports, and services, finding Operating system and architecture of target system, recognizing vulnerabilities and threats in the network are the list of procedures carried out by Scanning process. Creating a profile of the target organization is done by the Network scanning. Fetching more data using complicated and aggressive reconnaissance techniques comes under scanning. The utmost important task of scanning is to check the ports that are vulnerable[7].

Scanning methods used in Autoploit are as follows:

- TCP scan
- Window scan
- FIN scan
- X-mas scan

Autoploit scans the ports starting from 0 to 65535.The specialty of the Autoploit scanning is the usage of the threading. It uses 512 threads for scanning, hence it reduces the processing time. It requires only 20-30 seconds to scan all the ports. It uses thread pool executer module to execute port scan on the target. It pings the host and port number. If there is any result from host i.e. in syn/ack packet then port is considered as closed else it is open. All the open ports are stored in a array for future reference. The output of the scanning shows all the vulnerable ports



```
Received 2 packets, got 1 answers, remaining 0 packets
www.sshopvilla.in ==> is up
Scanning all ports..........
Getting current Memory Status
Total Memory used ======> 4043
Used Memory ======> 1050
Free Memory ======> 2453
-----------------------------------------------------------------------------


Scanning all port's Action starts here!

Scanning ports on 148.66.138.173
22--------->is Open
21--------->is Open
80--------->is Open
110--------->is Open
143--------->is Open
443--------->is Open
465--------->is Open
587--------->is Open
993--------->is Open
995--------->is Open
1248--------->is Open

Done.!!!!
-----------------------------------------------------------------------------
11Ports are available
[21, 22, 80, 110, 143, 443, 465, 587, 993, 995, 1248]
```

Figure 3: Open ports

```
1) Import required libraries(time, socket, termcolor, getpass, scapy, os, queue, threading, subprocess, random, concurrent, urllib,re)
2) Take input from user (host name or target IP)
3) Check host is up or down by using ICMP echo method
4) If ip is given then go to step 7) else continue
5) Check for protocol of URL (http/https) by getting content of website using url along with browser module
6) Extract IP of URL using socket gethostbyname(url)
7) Define thread variable having value 512, an array for storing open ports and connection_timeout=1
8) Use thread pool executer module to execute port scan on target.
9) For port range from 1 to
      65535 Ping host and
```

Algorithm for scanning

2. *Exploiting*

Letting clients to grab power of a system, exploiting its vulnerabilities is the part of exploiting.

Autoploit has its own created new exploits. Each exploit is created in different files having

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

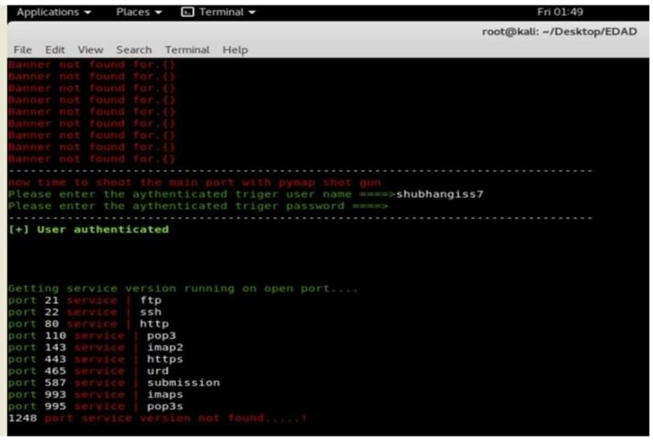
extension .py. These exploits are used for attacking the victim. Threading is used for exploiting which gives excellent performance time.

The ports which are open are attacked version wise by the exploits. For e.g. If port 22 is open, then FTP attack is performed.

To get service and version of open ports Autoploit uses TCP socket. Then it is connects to target IP and its port. Then data (i.e. services and versions of ports) is received from target to Autoplot. This data is stored by Autoploit. After getting service and version of open port, Autoploit finds particular exploit for service and version of open ports from stored exploits file. Then it uses auxiliary scanner to predict whether the version is exploitable or not. If version is exploitable then Autoploit sends payloads through exploits. Then payload is injected to the target. With the help of this injected payload in the target system Autoploit receives data from target.If payload is injected in system successfully then attack is said to be successful means version is vulnerable. If payload is not injected in target system then attack is said to be unsuccessful then version is not vulnerable.

Algorithm for exploiting

```
1) Check open port stored in array
2) Create an array to store service and version of open
   ports
3) Then get service version of open ports using socket.
      • create TCP socket
      • connect to IP and port
      • store received data (i.e. services and versions
        of ports) to service_version array
4) After getting service and version of open port then
   find particular exploit for service and version of open
   ports from stored exploits
5) Create auxiliary scanner to check whether the
   version is exploitable or not
6) If version is exploitable then send payload through
   exploit. 7)Then inject payload to the target to send and
   receive data from target to attacker
8) If payload injected in system successfully then attack
```



```
Banner not found for.()
Banner not found for.()
Banner not found for.()
Banner not found for.()
Banner not found for.()
Banner not found for.()
Banner not found for.()
Banner not found for.()
Banner not found for.()
--------------------------------------------------------------------------------
now time to shoot the main port with pymap shot gun
Please enter the aythenticated triger user name ====>shubhangiss7
Please enter the aythenticated triger password ====>
--------------------------------------------------------------------------------
[+] User authenticated



Getting service version running on open port....
port 21 service | ftp
port 22 service | ssh
port 80 service | http
port 110 service | pop3
port 143 service | imap2
port 443 service | https
port 465 service | urd
port 587 service | submission
port 993 service | imaps
port 995 service | pop3s
1248 port service version not found.....!
```

Figure 4: Getting service version

4. Maintaining Access:

Maintaining the access to the target until the person finishes the tasks he has planned to accomplish in that target is the aim of Autoploit.

5. Reporting:

Autoploit creates a report where information like the open ports, the attacks performed on the open ports are all maintained. Along with this Autoploit automatically screenshot the output and store it. The advantage of the automated screen shot technique is the report cannot be manipulated.[8]

CONCLUSION

Autoploit is a tool which has overcome the issues of the currently working tools. It is an improved tool over the current ones. Autoploit performs the processes of ethical hacking viz. Reconnaissance, scanning and exploiting in one go. Additional technique which adds up to the efficient performance of Autoploit is the use of Threading.

In the similar manner Autoploit scans the system and checks for the vulnerable ports. The use of threading increases the performance of Autoploit. After scanning, vulnerable ports are attacked version wise. Thus prevents the system from crashing. If the inflicted attack gives the successful status, the security strength is weak. Autoploit generates a report which displays the open ports and clicks snap shots of the output. These snap shots are hard to be manipulated. Hence Autoploit can prove to be an ideal tool for checking the security of the system and thus making it aware of the further cyber attacks.

	Autoploit	Nmap	Metasploit
Scanning Time	10-20 sec (To scan 65535 port)	50-60 min	-
Exploit accuracy	80%	-	60%
Version wise attacking	Yes	-	No

Table 1: Comparison between Nmap, Metasploit and Autoploit

REFERENCES

1. Regner Sabillon, Victor Cavaller, Jeimy Cano, Jordi Serra- Ruiz.(2016) “Cybercriminals, Cyberattacks and Cybercrime Privacy, security and control” IEEE International Conference on Cybercrime and Computer Forensic (ICCCF).
2. Brijesh Kumar Pandey,Alok Singh,Lovely lakhmani balani.(2015)”ETHICALHACKING TOOLS(Tools,Techniques and Approaches)” Conference
3. Brad Arkin, Scott Stender, Gary McGraw: “Software Penetration Testing”[J]. IEEE Security & Privacy, 2005, 3(1): 84-87.
4. Gordon “Fyodor” Lyon,” Nmap Network Scanning,”2009.
5. Xia Yi-min, etc. “Security Vulnerability Detection Study Based on Static Analysis”. Computer Science, 2006.33(10).
6. Gurpreet K. Juneja1,(2013)” ETHICAL HACKING: A TECHNIQUE TO ENHANCE INFORMATION SECURITY’ International Journal of Innovative Research in Science, Engineering and Technology
7. Ashiqur Rahman,Kantibhusan Roy,Atik Ahmed Sourav,Al- Amin Gaji.(2016)”Advanced Network Scanning”American Jornal of Engineering Research(AJER)(for scanning)
8. Hannes Holm,Teodor Sommestad. (2016) ”SWED:Scanning,vulnerabilities,exploits and Detection” IEEE