Design and Develop a Honeypot for Small Scale Organization

Gurleen Singh, Sakshi Sharma, Prabhdeep Singh

Abstract— ***Computer Network and Internet is growing every day. Computer networks allow communicating faster than any other facilities. These networks allow the user to access local and remote databases. It is impossible to protect every system on the network. In industries, the network and its security are important issues, as a breach in the system can cause major problems. Intrusion detection system (IDS) is used for monitoring the processes on a system or a network for examining the threats and alerts the administrator about attack. And IDS provide a solution only for the large scale industries, but there is no solution for the small scale industries so model is proposed for honeypot to solve the problem of small scale industries which is the hybrid structure of Snort, Nmap, Xprobe2, P0f. This model captures the activities of attackers and maintains a log for all these activities. Virtualization is performed with the help of virtual machine. The focus of this paper is primarily on preventing the attacks from external and internal attackers and maintaining the log file using honeypot with virtual machine.***

Index Terms— Intrusion detection system, honeypots, attacker, security.

I. INTRODUCTION

Scale of Internet technology is very large and it is still growing every day. The security of network is required for endurance of the industries which are dependent on the internet to enhance the business and providing services on the network. So security of network is primary concern of the industries for securing the critical information. Giant sums of attacks are noticed in recent years on these kinds of industries. Intrusion detection system (IDS) is used for monitoring the processes on a system or a network for examining the threats and alert the administrator. IDS and firewalls are used for protecting the system and network from attacks, but after so many efforts for security still the network is not fully secured so different types of solutions are proposed by the researchers.

The small scale industries using LAN have to keep high their own security level as the database, server and clients are all handled by themselves. Since threat from internal network is always the big challenge for the administrators, so a solution is required for small scale network to secure their internal network. Our paper provides the solution for the same using honeypot.

Manuscript published on 28 February 2013.
***Correspondence Author(s)**

Sakshi Sharma, Computer Science & Engineering (Networking System), Punjab Technical university,Kapurthala, India.
Gurleen Singh, Computer Science & Engineering (Networking System), Punjab Technical University, Kapurthala, India.
Prabhdeep Singh, Computer Science & Engineering,Punjab Technical University,Kapurthala,India.

II. LITERATURE REVIEW

Honeypot is a non-production system, used for exploiting the attacker and notice the attacking techniques and actions. The objective of honeypots is not only to notice but to tackle the risk and abate it. There are various definitions of honeypots are available as few people take it as a system to lure the attackers and inspect their activities where as other take it as a technology for detecting attacks or real systems formed for getting attacked.

L. Spitzner defines the term honeypot as follows:

A honeypot is a resource whose value is being in attacked or compromised. This means, that a honeypot is expected to get probed, attacked and potentially exploited. Honeypots do not fix anything. They provide us with additional, valuable Information. [1]

In network security, honeypots are used to detect the attackers and learn from their attacks and then modify and develop the system accordingly for security. The loop holes of the network security can be covered with the help of information provided by honeypots.

Honeypot can be figured as a computer system connected with a network for inspecting the vulnerabilities of a computer or a complete network. The loopholes can be examined collectively or individually of any system, as it is a exclusive tool to study about the attackers and their strategies on the network. [2]

Honeypots are normally virtual machines which acts like a real system. Honeypots are classified into two categories on their use:

Research honeypots:

These are the honeypots which are manipulated by researchers and are used to acquire information and knowledge of the hacker society. The knowledge gained by the researchers are used for the early warnings, judgment of attacks, enhance the intrusion detection systems and designing better tools for security.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Production honeypots:
These are the honeypots derived by the industries as a part of network security backbone. These honeypots works as early warning systems. The objectives of these honeypots are to abate the threats in industries. It provides the information to the administrator about the attacks before the actual attack.[1][5]
Honeypots can also be classified on the basis of level of involvement or interaction as:

Low level interaction:

Honeypots that provide only some fake services, these acts as an emulator of the operating system and services. These honeypots are simple to design but also simply detectable. Attacker can just use a simple command to identify it that a low involvement honeypot does not support. An example of this type of honeypot is *Honeyd*.

High level interaction:

High level interaction honeypots provides the real like operating systems and some real services with some real uncertainties. These allow the capturing of information of attacker and record their activities and actions. These are the real machine with one system, with one network interface on network. An example of this type of honeypot is *Honeynet*.[5]

The value of the honeypots is in getting compromised, if the honeypot is not probed then it is of no use. It should be always available for the attackers on the network.

III. NEED OF SMALL SCALE INDUSTRIES

The Small scale industries working on the LAN system have to keep their security level high as no safe security measure or honeypot is designed for small scale industries. The services like database handling, servers and clients handling have to be done by themselves. The model should maintain all log files and the attacker's information that so ever is attacking the networking system. The protection should not be compromised at any cost, i.e. system or the complete network should be secure from an attack which leads to the full security of the data.
The designed system should also be easy to access, the system must not be made like that it will become complex i.e. difficult to understand for a new user. There should not be a problem relating to speed that leads to the slow processing of the data. It should be designed such that whole system should be fully accessible.
Small scale industries need a model for solving these problems. The focus of the model is on the highest security of the system, which means the security should not be vulnerable, and model should solve the above mentioned problems.

IV. HONEYPOT FOR SMALL SCALE INDUSTRIES

Honeypot that is designed for the small scale industry keep information of the complete networking system, keep the records of all log files of the network. The complete attacker's information is gathered and recorded the activities for the security of the system. The protection of complete system is primary objective so that the real system is not going to be compromised at any cost. The honeypot is made easy to access for all users in small scale industries.
The honeypot foe small scale industry is implemented by configuring the 2 or 3 tools together. These tools are used for the information gathering of the attackers. Sniffing is prevented with the help of these tools. Packets can be logged that are coming across our network. It can be used for the port scanning as to know the open and closed ports. Virtual computer can be operated for providing the fake information to the attacker.
A set of services are simulated on the network, so as the honeypot should look like a real machine to the attacker. These services are:-

- HTTP
- SSH
- FTP
- TELNET
- POP3

In the proposed architecture, we have used the various tools for the intrusion detection and noticing the activities of attacker and to make our real system safe. The attacker will attack on the virtual machine and honeypot will capture all activities and behavior of the attacker. This will help us to protect our real system for the future similar kinds of attacks.

V. PROPOSED DESIGN FOR CAMPUS HONEYPOT

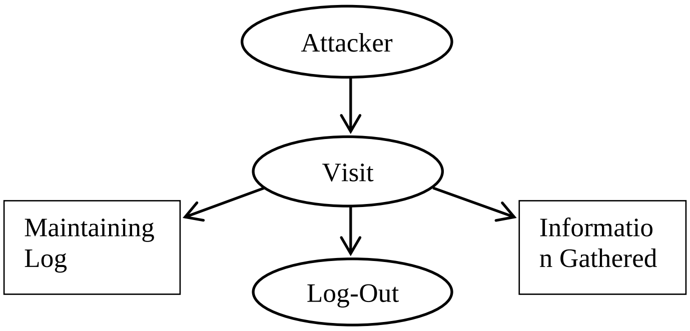


Fig.1.Flowchart

Virtual computer is used as for maintaining the log files and for as much period the attacker is working on virtual machine, his all activities are being noticed, and information is being gathered. It keeps our actual data safe from the attacker.
Various tools are used for the purpose of fingerprinting, foot printing and port scanning.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

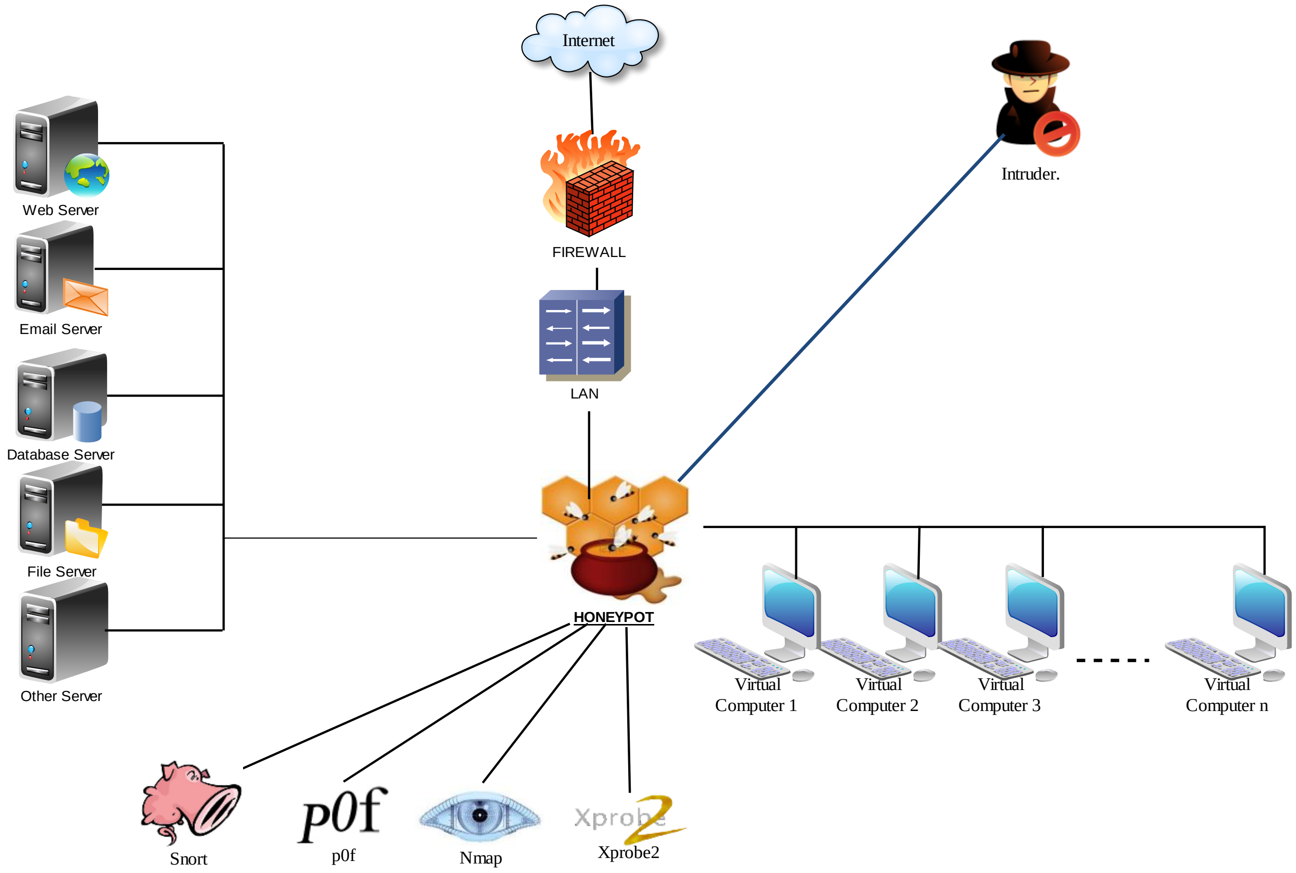
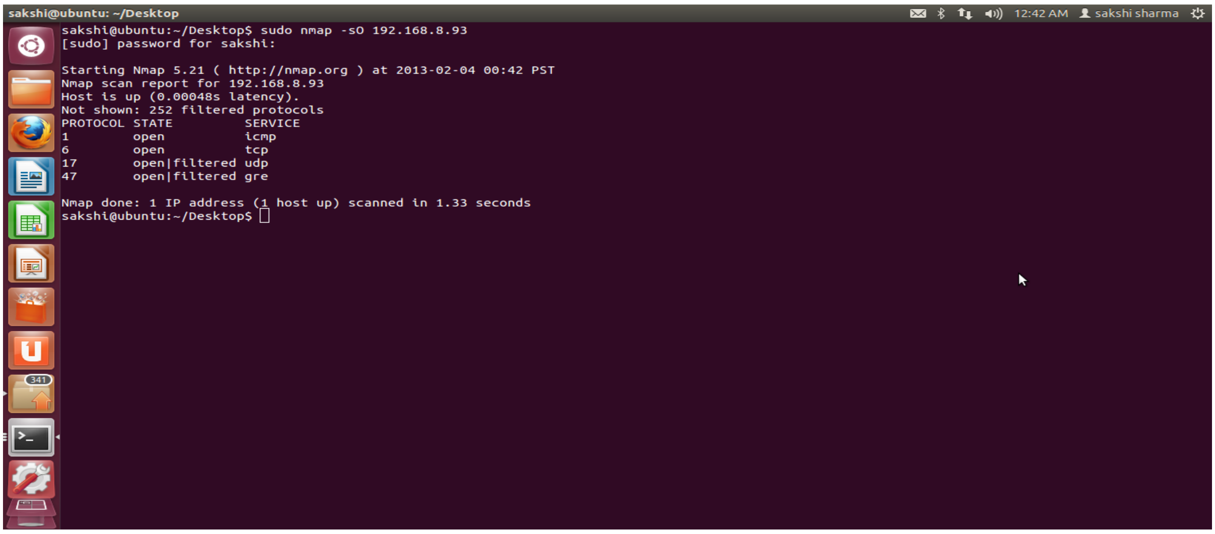


Fig. Proposed architecture.

Any system on the internet network is not safe and the attacking activities are growing, so it can be foreseen that no system on the network is safe. All the set of tools together working as an intrusion detection system and are being used for the early warnings to the administrator. The services simulated on the virtual machines are a simple telnet server, SSH server, POP3 server. These services are composed to execute on any port.

VI. IMPLEMENTATION AND RESULTS

The Flow chart shows that the attacker is attacking our honeypot as it is a real system. When the attacker Visit our system, the log files are made of the attacker, his activities are recorded and the actions are noticed for the future security of the real system. All this information is stored in information gathered.

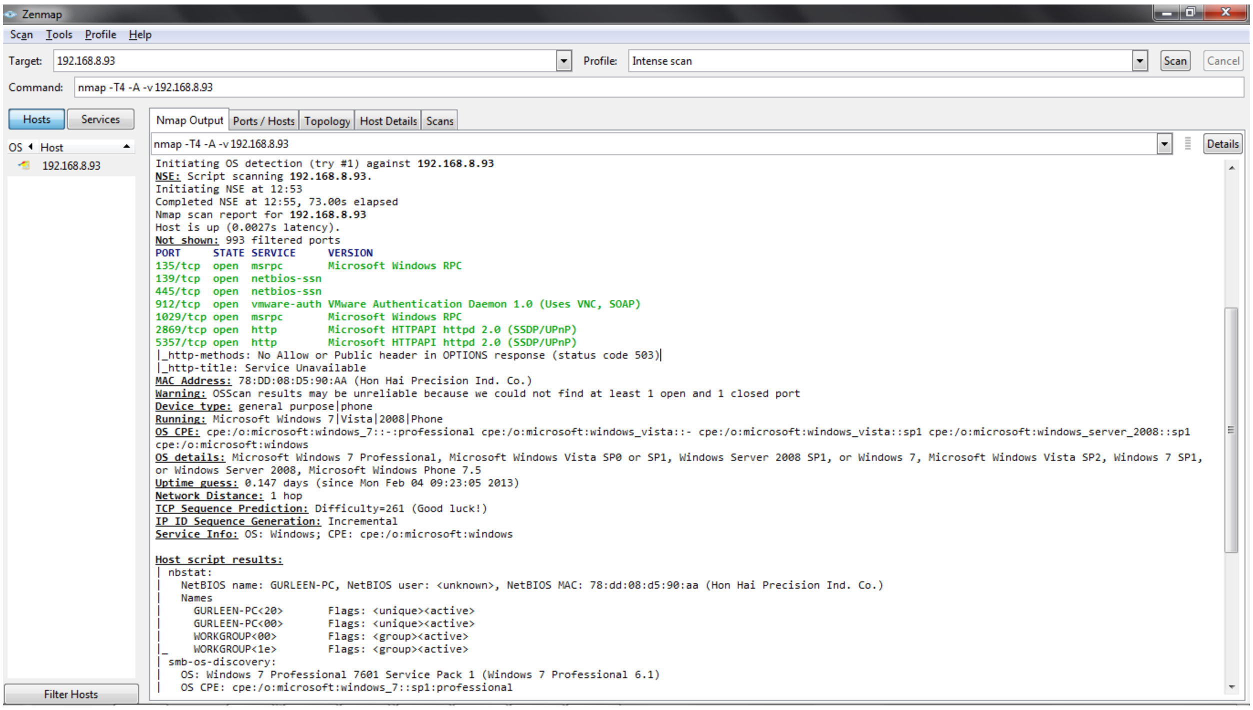


```
sakshi@ubuntu:~/Desktop$ sudo nmap -sO 192.168.8.93
[sudo] password for sakshi:

Starting Nmap 5.21 ( http://nmap.org ) at 2013-02-04 00:42 PST
Nmap scan report for 192.168.8.93
Host is up (0.00048s latency).
Not shown: 252 filtered protocols
PROTOCOL STATE         SERVICE
1        open          icmp
6        open          tcp
17       open|filtered udp
47       open|filtered gre

Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds
sakshi@ubuntu:~/Desktop$ 
```

Fig. NMap tool in Linux.

Nmap giving us the details of the open and filtered ports, states, services it providing and protocols of target system.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.



Target: 192.168.8.93

Profile: Intense scan

Command: nmap -T4 -A -v 192.168.8.93

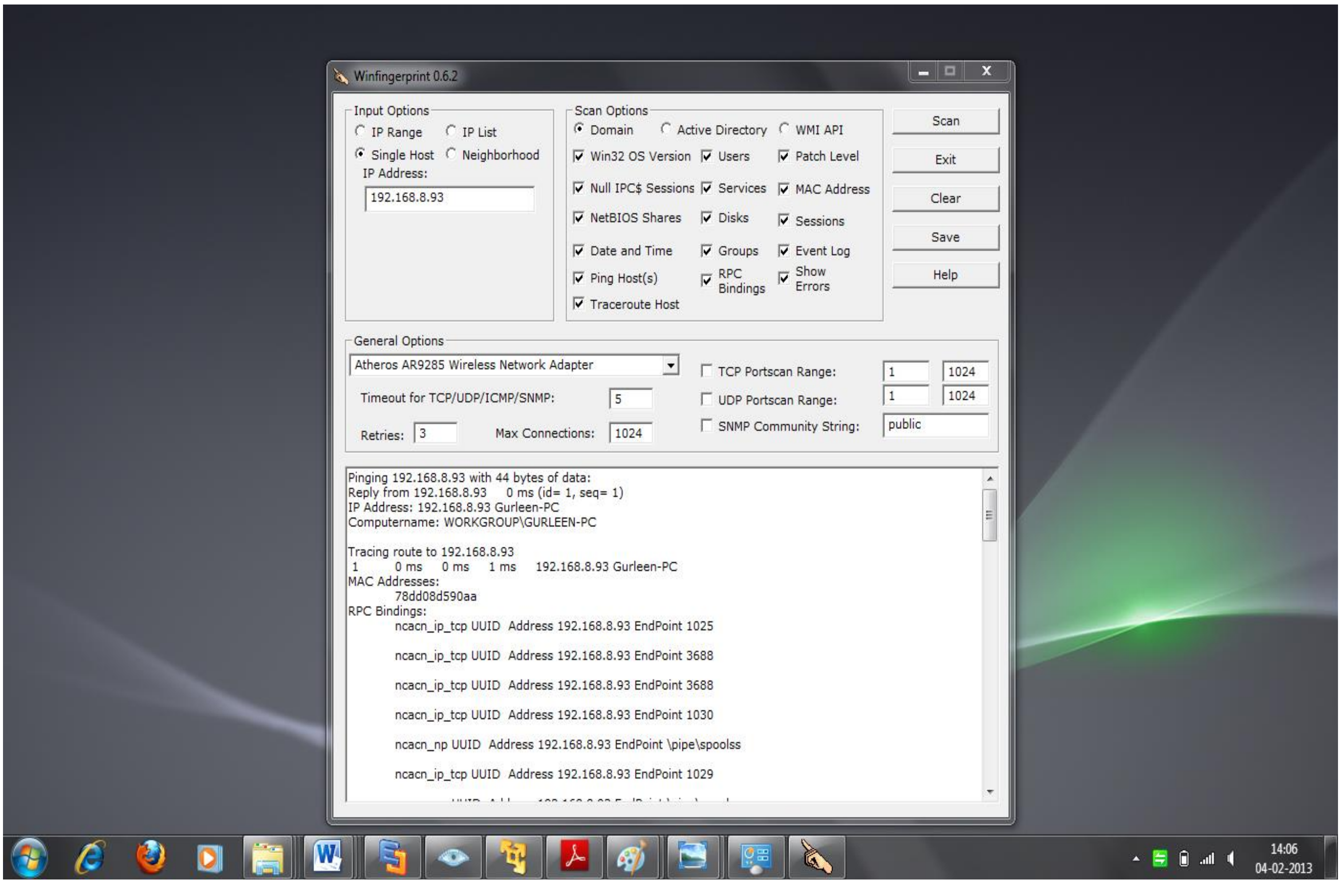
192.168.8.93

nmap -T4 -A -v 192.168.8.93

```
Initiating OS detection (try #1) against 192.168.8.93
NSE: Script scanning 192.168.8.93.
Initiating NSE at 12:53
Completed NSE at 12:55, 73.00s elapsed
Nmap scan report for 192.168.8.93
Host is up (0.0027s latency).
Not shown: 993 filtered ports
PORT     STATE SERVICE     VERSION
135/tcp  open  msrpc       Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  netbios-ssn
912/tcp  open  vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1029/tcp open  msrpc       Microsoft Windows RPC
2869/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
|_http-title: Service Unavailable
MAC Address: 78:DD:08:D5:90:AA (Hon Hai Precision Ind. Co.)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running: Microsoft Windows 7|Vista|2008|Phone
OS CPE: cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1
cpe:/o:microsoft:windows
OS details: Microsoft Windows 7 Professional, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1,
or Windows Server 2008, Microsoft Windows Phone 7.5
Uptime guess: 0.147 days (since Mon Feb 04 09:23:05 2013)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat:
|   NetBIOS name: GURLEEN-PC, NetBIOS user: <unknown>, NetBIOS MAC: 78:dd:08:d5:90:aa (Hon Hai Precision Ind. Co.)
|   Names
|     GURLEEN-PC<20>       Flags: <unique><active>
|     GURLEEN-PC<00>       Flags: <unique><active>
|     WORKGROUP<00>        Flags: <group><active>
|_    WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
```

FIG. NMAP ON WINDOWS

In windows operating system NMap is providing the name, MAC address, open port, state, services and version of the target operating system



○ IP Range ○ IP List
● Single Host ○ Neighborhood

IP Address: 192.168.8.93

● Domain ○ Active Directory ○ WMI API
☑ Win32 OS Version ☑ Users ☑ Patch Level
☑ Null IPC$ Sessions ☑ Services ☑ MAC Address
☑ NetBIOS Shares ☑ Disks ☑ Sessions
☑ Date and Time ☑ Groups ☑ Event Log
☑ Ping Host(s) ☑ RPC Bindings ☑ Show Errors
☑ Traceroute Host

Atheros AR9285 Wireless Network Adapter

Timeout for TCP/UDP/ICMP/SNMP: 5

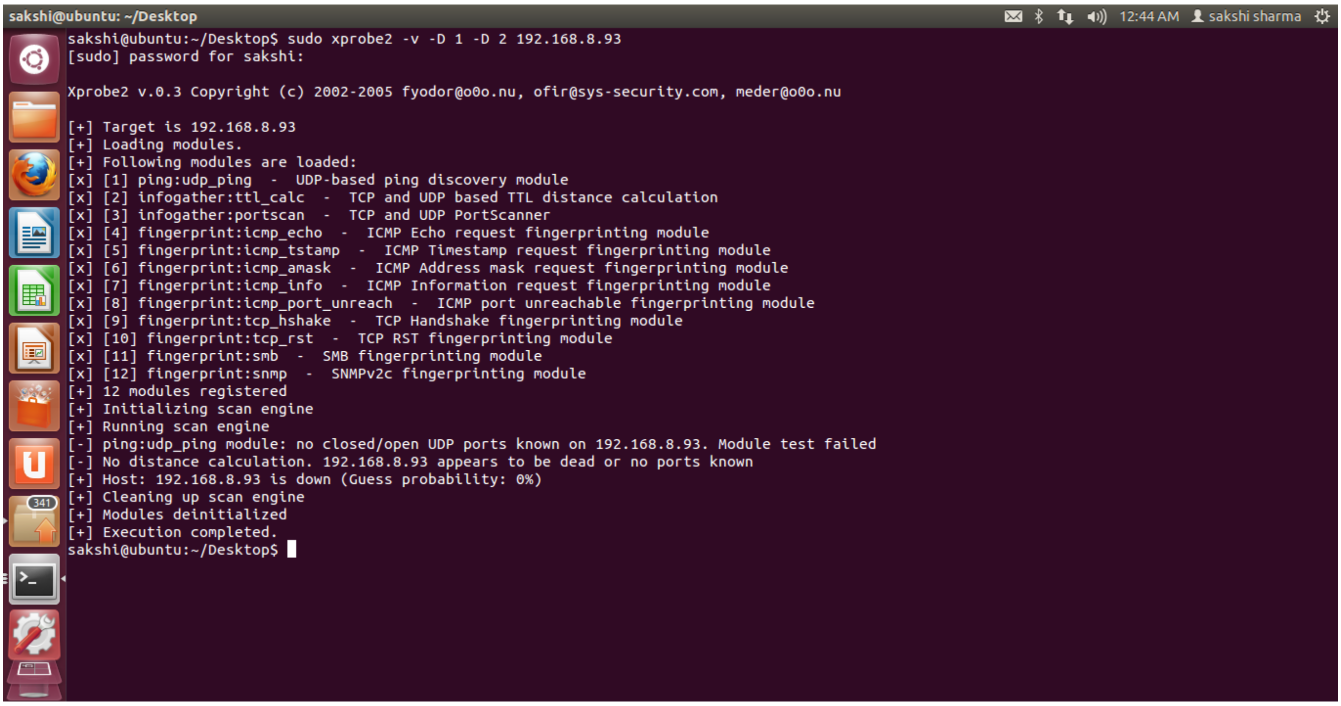
Retries: 3 Max Connections: 1024

☐ TCP Portscan Range: 1 1024
☐ UDP Portscan Range: 1 1024
☐ SNMP Community String: public

```
Pinging 192.168.8.93 with 44 bytes of data:
Reply from 192.168.8.93     0 ms (id= 1, seq= 1)
IP Address: 192.168.8.93 Gurleen-PC
Computername: WORKGROUP\GURLEEN-PC

Tracing route to 192.168.8.93
 1        0 ms    0 ms    1 ms    192.168.8.93 Gurleen-PC
MAC Addresses:
        78dd08d590aa
RPC Bindings:
        ncacn_ip_tcp UUID  Address 192.168.8.93 EndPoint 1025

        ncacn_ip_tcp UUID  Address 192.168.8.93 EndPoint 3688

        ncacn_ip_tcp UUID  Address 192.168.8.93 EndPoint 3688

        ncacn_ip_tcp UUID  Address 192.168.8.93 EndPoint 1030

        ncacn_np UUID  Address 192.168.8.93 EndPoint \pipe\spoolss

        ncacn_ip_tcp UUID  Address 192.168.8.93 EndPoint 1029
```

Fig. Winfingerprint on Windows

It is a port scanning tool for the windows. It gives us the details of the version of OS, system name, MAC address, tracing route, RPC binding and event logging.



```
sakshi@ubuntu:~/Desktop$ sudo xprobe2 -v -D 1 -D 2 192.168.8.93
[sudo] password for sakshi:

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is 192.168.8.93
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:udp_ping  -  UDP-based ping discovery module
[x] [2] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [3] infogather:portscan  -  TCP and UDP PortScanner
[x] [4] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [5] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x] [6] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting module
[x] [7] fingerprint:icmp_info  -  ICMP Information request fingerprinting module
[x] [8] fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinting module
[x] [9] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [10] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [11] fingerprint:smb  -  SMB fingerprinting module
[x] [12] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 12 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:udp_ping module: no closed/open UDP ports known on 192.168.8.93. Module test failed
[-] No distance calculation. 192.168.8.93 appears to be dead or no ports known
[+] Host: 192.168.8.93 is down (Guess probability: 0%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
sakshi@ubuntu:~/Desktop$
```

Fig. Xprobe2 on Linux OS

Xprobe2 is Linux based Fingerprinting tools. It has given the details of the loaded modules using packets of the target system.Xprobe2 is used for identification of remote operating system.

Hence the result shows that the data is secured on the system as the attacker is operating on virtual machine. The honeypot is recording the activities and behavior of the attacker and make the real system safe for the future attacks. The log files are maintained and information is gathered for analyzing the attacker.

We have used many tools to provide fake services in the virtual system so that it looks like a real system. So when the attacker attacks on these types of systems, it is found that the system is running with the real services and applications, so attacker cannot judge that it is a fake system. The services like http, SSH, telnet are operated on the fake system.

VII. CONCLUSION

In this work, we have analyzed the results of honeypot to capture the activities of hacker in a small scale industry. The configured tools are being used as information tool for the analysis the behavior of the hacker . the configured tools are also maintaining the log and gathering the information on its own which are very helpful for the administrator..

REFERENCES

1. Y.K.Jain, S. Singh "Honeypot based Secure Network System" in IJCSE. Vol 3. No.2 Feb 2011.
2. H.Artail, H.Safa, M.Sraj,I.Kuwalty , Z.Masri "A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks " Science Direct, 2006.
3. U.A.Sandhu, S.Haider, S.Naseer, O.U.Ateeb "A Survey of Intrusion Detection & Prevention Techniques" in IPCSIT vol.16, 2011.
4. V.M.Boncheva "A Short Survey of Intrusion Detection Systems" 2007.
5. R.Baumann, C.Plattner "honeypots" Diploma Thesis in Computer Science, 2002
6. C.Doring "Improving network security with honeypots", 2005
7. R.K.Singh, T.Ramanujam "Intrusion Detection System Using Advanced Honeypots" IJCSIS vol. 2, no. 1, 2009.
8. L.Spitzner "Honeypot:Definitions and Values" 2002.
9. F.Zhang, S.Zhou, Z.Qin, J.Liu "Honeypot: a Supplemented Active Defense System for Network Security" IEEE 2003.
10. D.Schnackenberg, K.Djahandari, D.Strene "Infrastructure for Intrusion Detection and Response " DISCEX, 2000.
11. S. Mrdovic, E. Zajko "Secured Intrusion Detection System Infrastructure", ICAT 2005.
12. Y.Bai, H.Kobayashi "Intrusion Detection Systems: Technology and Development" AINA, 2003.
13. G.Bhatti, R.Singh, P.Singh "A look back at issues in the layers of TCP/IP model" IJERMC, vol.1, Issue.2, 2012.

AUTHOR PROFILE

Gurleen Singh presently pursuing M.Tech in the Department of Computer Science & Engineering (Networking System) at Punjab Institute of Technology (PIT), Kapurthala, Punjab, India. The degree B.Tech from DAVIET, Jalandhar, Punjab.

Sakshi Sharm presently pursuing M.Tech in department of Computer Science & engineering (Networking system) at Punjab institute of technology (PIT) kapurthala, Punjab, India. And Completed B.Tech in computer science from lovely professional University, Phagwara.

Prabhdeep Singh working with Punjab Technical University, as an Assistant Professor in the department of Computer science and engineering. Has completed M.E from Thapar University and his research areas are algorithm design, Cloud Computing, Network Security, Software Process Re-engineering,Software Testing and Debugging.