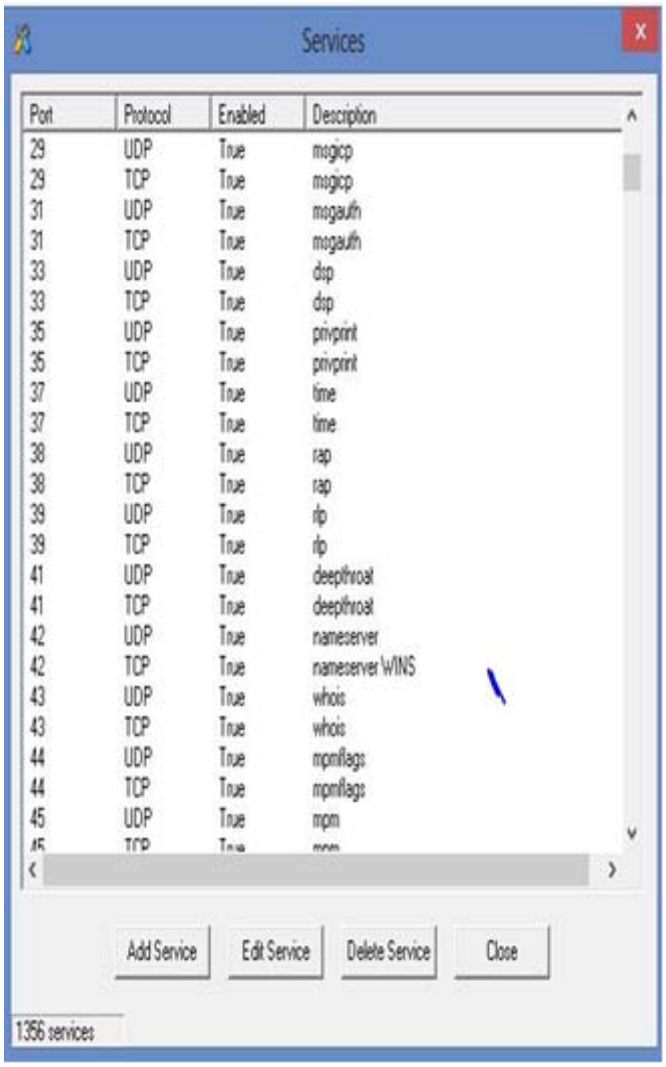


Figure 2: Open ports in network

These are all the ports that seem to be left open. Although it is way too obvious that nobody leaves such a number of port open. It has got SMTP, UDP, FTP all sort of files open. So we need to make a wise and judicious decision to leave a few port open which will make the hacker believe it is not a honeypot but some real ports are open.

Now we will run an Nmap scan of the computer which will have the honeypot running.

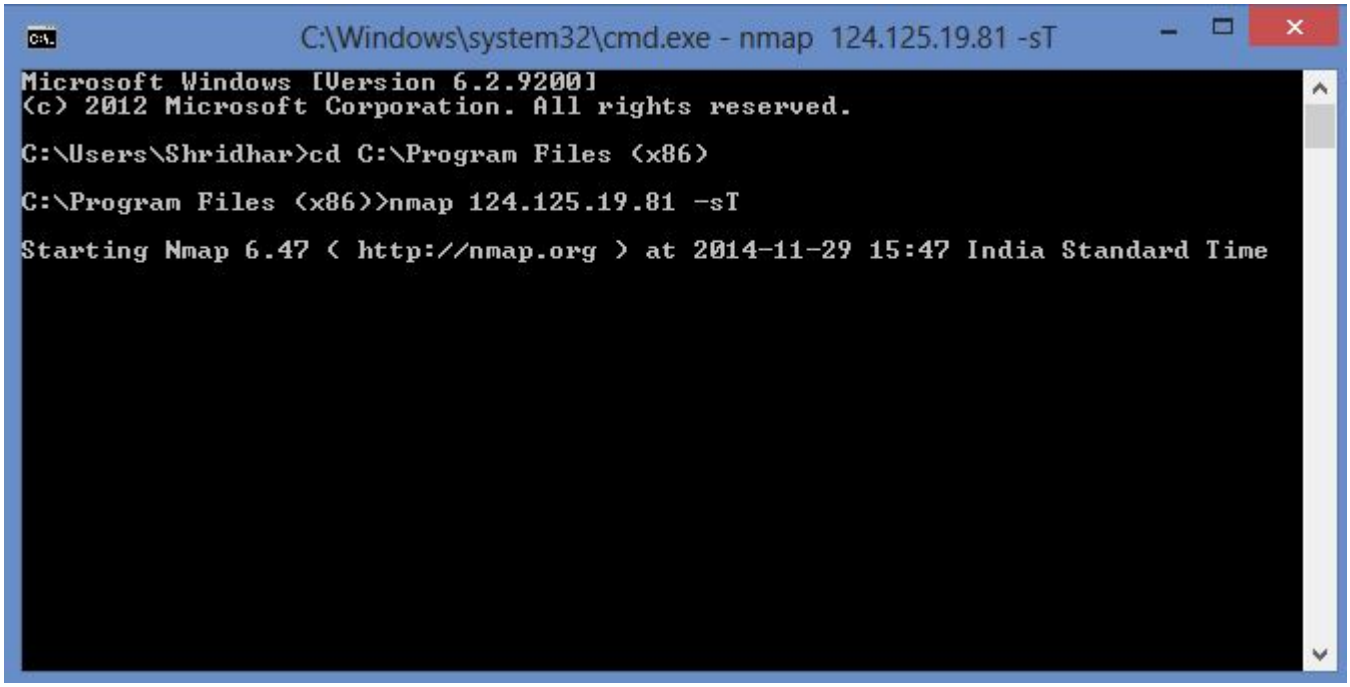
Honeypots can be connected to the production network to check the network vulnerabilities. If the attack is on the honeypot in the production network, then the attacker cam all way to attack the honeypot in the production network and the network is prone to attacks.

Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. [13]

We will use the command on the command line:

nmap IP Address –sT

-sT command is used for a TCP connect scan.



While the attacker would be busy running and attacking the ports we would go back to our machine where the honeypot scanner was running.

Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
11/29/2014	3:47:30 PM	124.125.19.81	54473	0.0.0.0	6101	TCP	0
11/29/2014	3:47:30 PM	124.125.19.81	54478	0.0.0.0	3005	TCP	0
11/29/2014	3:47:30 PM	124.125.19.81	54481	0.0.0.0	83	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54492	0.0.0.0	7007	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54500	0.0.0.0	2022	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54502	0.0.0.0	4045	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54511	0.0.0.0	12174	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54512	0.0.0.0	666	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54524	0.0.0.0	500	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54528	0.0.0.0	2105	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54529	0.0.0.0	33	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54534	0.0.0.0	2605	TCP	0
11/29/2014	3:47:31 PM	124.125.19.81	54535	0.0.0.0	2045	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54546	0.0.0.0	211	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54547	0.0.0.0	7001	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54550	0.0.0.0	1998	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54563	0.0.0.0	79	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54564	0.0.0.0	6004	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54565	0.0.0.0	593	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54566	0.0.0.0	7100	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54573	0.0.0.0	20000	TCP	0
11/29/2014	3:47:32 PM	124.125.19.81	54596	0.0.0.0	212	TCP	0
11/29/2014	3:47:33 PM	124.125.19.81	54617	0.0.0.0	2042	TCP	0
11/29/2014	3:47:33 PM	124.125.19.81	54622	0.0.0.0	617	TCP	0
11/29/2014	3:47:33 PM	124.125.19.81	54627	0.0.0.0	106	TCP	0
11/29/2014	3:47:33 PM	124.125.19.81	54634	0.0.0.0	3269	TCP	0
11/29/2014	3:47:34 PM	124.125.19.81	54659	0.0.0.0	3128	TCP	0
11/29/2014	3:47:34 PM	124.125.19.81	54663	0.0.0.0	70	TCP	0
11/29/2014	3:47:34 PM	124.125.19.81	54667	0.0.0.0	9100	TCP	0
11/29/2014	3:47:34 PM	124.125.19.81	54674	0.0.0.0	4	TCP	0
11/29/2014	3:47:34 PM	124.125.19.81	54685	0.0.0.0	6699	TCP	0
11/29/2014	3:47:34 PM	124.125.19.81	54686	0.0.0.0	2034	TCP	0
11/29/2014	3:47:34 PM	124.125.19.81	54688	0.0.0.0	444	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54708	0.0.0.0	7004	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54709	0.0.0.0	1011	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54711	0.0.0.0	9535	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54722	0.0.0.0	1112	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54742	0.0.0.0	9080	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54744	0.0.0.0	2046	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54745	0.0.0.0	179	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54746	0.0.0.0	42	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54755	0.0.0.0	6007	TCP	0
11/29/2014	3:47:35 PM	124.125.19.81	54760	0.0.0.0	389	TCP	0

When we look at the honeypot scanner we would see the attack date, time, remote id and port of the attacker as well as the local IP and local port at which the attack was directed.

Although a many times attacker may know that a honeypot is used in system to lure him. So further refinement can be done in such a way that attacker does not feels he is being trapped.

7. Conclusion and Future Scope

Network security concerns are increasing day by day as the mode and style of attackers are evolving each day. This paper deals with countering such attacks measures by possibly tracing the attacker and its mode of attack. Honeypot approach is used which not only makes the attacker to go for an attack but also alert the network administrators of a possible intrusion by trailing the attacker. Honeypots can be used together with some other form of security such as an IDS to increase its efficiency.

References

[1] Miss.Swapnali Sundar Sadamate.," Honeypot Mechanism – the Autonomous Hybrid Solution for Enhancing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014 p.p 854-858
[2] "Know Your Enemy: Honeynets.", available at http://www.honeynet.org/papers/kye.html.
[3] Karthik, S., Samudrala, B. and Yang, A.T., "Design of Network Security Projects Using Honeypots." , Journal of Computing Sciences in Colleges, 20 (4)

[4] A. Chandra, K. Lalitha, "Honeypots: A New Mechanism for Network Security", Department of Computer Science and Systems Engineering, Sree Vidyanikethan Engineering College A. Rangampet , Tirupati. Vol 04, Special Issue01; 2013. http://ijpaper.com/
[5] Karthik Sadasivam, Banuprasad Samudrala, T. Andrew Yang. "Design of Network Security Projects using Honeypots", University of Houston
[6] "Honeypots: Catching the Insider Threat", available at Lance Spitzner Honeypot Technologies Inc. lance@honeypots.com
[7] "Honeypots" available at : http://en.wikipedia.org/wiki/Honeypot_%28computing%29
[8] Iyatiti Mokube, Michele Adams, "Honeypots: Concepts, Approaches, and Challenges", Department of Computer Science, Armstrong Atlantic State University
[9] L. Spitzner, "Honeypots: Tracking Hackers," Boston, USA: Addison Wesley, Parson Education, ISBN 0 321108957, 2003
[10] Navneet Kambow, Lavleen Kaur Passi, "Honeypots: The Need of Network Security", International Journal of Computer Science and Information Technologies, Vol. 5 (5), 2014
[11] Matthew L. Bringer, Christopher A. Chelmecki, and Hiroshi Fujinoki, "A Survey: Recent Advances and Future Trends in Honeypot Research", "I. J. Computer Network and Information Security", September 2012 in MECS
[12] "Honeypot Definition" - PC Magazine available at: http://www.pcmag.com/encyclopedia_term/0,2542,t=honeypot&i=44335,00.asp, 24 March 2009
[13] Kumar Shridhar, Nikhil Gautam, "A Prevention of DDos Attacks in Cloud Using Honeypot ", International Journal of Science and Research, Volume 3 Issue 11, November 2014, p.p 2378-2383
[14] Network Mapper" available at : http://nmap.org/

Author Profile

Kumar Shridhar is currently enrolled in final year of his B.Tech programme (2011-2015) from Bhagwan Parshuram Institute of Technology. He is a certified objective C programmer and a certified ethical hacker. He is currently working on improving the network security issues. Beside these, he loves watching football and listening music

Mayank Jain is currently pursuing his B.Tech(2011-2015) from Bhagwan Parshuram Institute of Technology. He is an oracle certified java programmer and a certified .Net developer. He is currently working on improving his database and data mining skills. Besides these, he loves watching football and movies.