Middle-East Journal of Scientific Research 19 (9): 1146-1149, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.19.9.1265

How Hackers Break in and How They Are Caught

N. Priya

Department of Computer Science,
Bharath University, Chennai, Tamil Nadu, India

Abstract: This thesis explores the relatively new criminal phenomena of computer crime, or as it is more commonly termed, hacking. The foundation for the examination is based on how well traditional psychological theories of crime and deviance explain this new behavior. Dominant theories In each of the categories of psychoanalytic learning and control are discussed.

Key words: Hacking · New Behavior · Deviance Explain

INTRODUCTION

Although Abednego is caught off guard-many ISPs would not have taken such a strong measure so quickly-the setback is minor. The closed account was only one of several he had created after breaking into that ISP. But the termination of the account at that particular moment causes him to be dumped from Internet Relay Chat in the midst of the flames against him. To the others on-line, it looks as if Abednego has been unceremoniously booted or worse, that he has fled for cover.

The thesis concludes that for the most part, traditional psychological theories are deficient with regard to explaining criminal computer behavior. It is argued that differential association and social learning theory may be partially effective in explaining the initial involvement and continuation of criminal computer behavior.

When one computer wishes to talk to another, it must first transmit a short message packet containing a SYN (synchronize) flag.

Thus, a FIN scanner can probe a computer m relative secrecy, without ever having opened any official connections. (Yet, as Abednego will soon learn, there is enough information in even one FIN packet to establish a sender's identity).

Abednego surfs the Internet to search for an advanced stealth port scanner and finds one at an underground Web site. The program, like most other hacker tools, is written in the C computer language. Abednego struggles to compile, or convert, the scanner from C into a form that can be executed on his home PC, which runs on Linux, one of the many variants of Unix.

Abednego's difficulty in converting the software is not unusual because of the many peculiarities of the different flavors of Unix. And Abednego, like many hackers, did not formally study computer science. In fact, also like most hackers, Abednego never learned to program because he never had to: almost any software a computer criminal might ever want is available on the Internet, already written and free for the taking-as long as the hacker knows how to compile it (or has cohorts who do).

The young Dogberry had taken a different path. After befriending a technician at a local ISP, he learned how to administer a network. Before long, Dogberry and the technician were playing computer break-in and defense games. The payoff came when they used the results to help the ISP improve its security. With that success, Dog-berry was hired by the ISP to work part-time while he pursued his computer science degrees. Thus, when Abednego decided to take on Dogberry, he had already made his first mistake. Dogberry is a white-hat (or non-malicious) hacker and a veteran of many cyber battles.

Casing the Joint: Dawn breaks: Abednego has finally finished compiling the code and is ready to deploy it. Within minutes, the FIN scanner has given him a snapshot of the services that refrigerus.com offers to

Corrseponding Author: N. Priya, Department of Computer Science, Bharath University, Chennai, Tamil Nadu, India.

those coming only from an approved IP address. Two that draw his attention are a secure-shell daemon, which is a way to make encrypted Internet connections and a Web server. Then Abednego's heart skips a beat. An unusual port number, 31,659, has also turned up on his FIN scan. Could another intruder have preceded him and left a back door, a secret passage to enter the system undetected?.

Three evenings later Abednego resumes the hunt. But when his computer dials into his account, he finds out his password is no longer good. Upset, he phones the ISP and learns that his account has been shut down because of the FIN scan. Yet this turn of events does little to discourage him. In fact, he is now even more determined [1].

More determined, Abednego now tries to tiptoe around the firewall instead of forcing his way through it. Using yet another of his many hacked accounts, he begins by attempting to catalogue the computers that belong to refrigerus.com. To obtain this information, he tries "nslookup," which initiates a search throughout the Internet for master databases containing directories of IP addresses.

But "nslookup" is unable to retrieve anything useful. Dogberry must have set up the refrigerus.com network so that all packets destined for any of its internal addresses are sent first to a name-server program, which then directs them to the appropriate computers within the network. This process hinders anyone on the outside from learning details about the computers inside the firewall [2].

Abednego's next attempt is through an IP address scanner. First, he converts refrigerus.com to a numerical address, using "nslookup." With that number as a starting place, he scans the IP addresses above and below it. He discovers some 50 Internet host computers. Although there is no guarantee that these belong to refrigerus.com, Abednego knows it is a good bet they do.

Finding a Workaholic: For each of the several dozen Internet hosts at Refigerators R Us, Abednego guesses that there are probably many other desktop computers sitting quietly in employees' cubicles and offices [1]. What are the chances, he muses a few nights later, that somewhere among those hundreds of users are workaholics who circumvent the company firewall by phoning into their computers from their homes to perform late-night tasks? It's simple, really, for someone to buy a modem, connect it to a computer at work and plug a phone line into it before leaving for the day.

Two nights later Abednego dials in and connects with picasso to view his logs. To his dismay he sees that in-formation on the internal network traffic has been encrypted. But the keystroke logger of his sniffer has recorded that someone on picasso had logged on to another computer named fantasia. Abednego now owns a user name and password for fantasia. Open sesame!.

Abednego discovers that the computer is a SPARC workstation used for rendering animated sequences, perhaps for television ads. Because the box is probably a server used by many other computers [3], Abednego begins hunting for a password file, hoping that some of the passwords he finds will also work on other machines inside the company network. He locates the file but discovers only "x" characters where the encrypted passwords should have been. Apparently the information he seeks is hidden elsewhere in a shadowed file. Smiling to himself, Abednego runs the FTP program and tricks it into crashing. Bingo, core dump!.

He perks up as he sees that user names Vangogh and Nancy have recently entered fantasia from the internet through the domain "adagency.com" which lies outside the Refrigerators R Us firewall.

Abednego can hardly fall asleep that morning. His adrenaline flowing, he buzzes with the knowledge that he will soon "own" Refrigerators R Us.

Closing in for the Kill: The next evening Abednego makes short work of breaking into adagency.com. At first he uses IP spoofing to trick that computer into recording a false IP address for his location. By probing adagency.com with SYN packets to elicit ACK/ SYN responses with an assortment of sequence numbers, Abednego's program is able to tease out a pattern from which he can then guess the next sequence numbers and use that knowledge to fake his origin. Abednego quickly installs a sniffer on adagency.com and uses a secure-shell program to create an encrypted connection for logging on to fantasia.

Tomorrow he will ask those folks exactly what is going on. He will also call the system administrator at adagency.com, a colleague whom he once helped to install some new system software.

Just as Dogberry is about to head home for the night, the phone in his office rings. An angry customer complains that Refrigerators R Us's Web site features a pornographic movie with a refrigerator as a prop[3]. After bringing up and viewing the defaced Web page, Dogberry moves quickly to sever the umbilical Ethernet cable that connects the company network to the Internet.

Abednego is enraged when his obscene masterpiece is taken down so quickly But he is also worried that he has left too much evidence behind, so he returns using the dial-up line to picasso-an entryway that is still unknown to Dogberry. He buys time by reformatting completely the administrative computer's hard disk, which shuts down the company network, temporarily thwarting Dogberry's efforts to gather details of the attack [2].

Abednego, still peeved about the Web site, has one final act that night: he unleashes a flood of data packets against refrigerus.com. Soon Dogberry gets a frantic call from a company salesperson who, using her laptop PC and a phone line in her hotel room, wants to retrieve her important e-mail but has been unable to connect to the mail server at Refrigerators R Us.

Dogberry then reloads a clean version of his main administrative computer. Next, on a Windows NT server that Dogberry knows has not been tampered with, he deploys T-sight, an advanced antihacker program that can monitor every machine on the company network.

Pride Goeth Before: Just two nights later Dogberry is standing watch at 8:17 PM. when he discovers someone once again entering admin.refrigerus.com. It is Abednego. Why has he returned so soon? Abednego was exhilarated when he learned that his pornographic Web site had become the talk of the hacker underground. He had even rated a brief mention on CNN. The publicity and his hubris were a potent combination, making Abednego feel invincible [4].

In fact, tonight he has brazenly reentered Refrigerators R Us without his customary caution. After dialing into a guest account on an ISP, he telnetted directly to adagency.com to gain faster access to fantasia's back door [5-10].

CONCLUSION

Soon after, FBI agents raid Abednego's apartment and confiscate his PC. The hard disk of the computer will reveal all. Abednego had taken the precaution of erasing incriminating files from his PC after each night's escapade. He is chagrined to learn that the FBI can extract that information from his hard drive even after it had been erased and overwritten several times. Soon a laboratory has recovered details of his past trespasses, including the time he romped through the computer system at a major banking institution in the Northeast [11-15].

REFERENCE

1. Additional information can be obtained at http:/ /www.geek-girl.com/bugtraq, http://ntbugtraq. ntadvice.com, http://rootshell.com, http://www. infowar.com, http://www.antionline.comand http://www.happyhacker.org
2. Internet Firewalls and Network Security. Second edition. Chris Hare and Karanjit Siyan. New Riders Publishing, Indianapolis, 1996.
3. The Giant Black Book of Computer Viruses. Second edition. Mark Ludwig. American Eagle Publications, Show Low, Ariz., 1998.
4. Essential System Administration. Second edition. Eileen Frisch. O'Reilly and Associates, Sebastopol, Calif., 1995.
5. Maximum Security: a Hacker's Guide to protecting your in. Ternet site and network anonymous. Sams Publishing, Indianapolis, 1997.
6. Kumaravel, A., 2013. An application of non-uniform cellular automata for efficient Cryptography, Xplore, pp: 1200-1205.
7. Kumaravel, A., 2013. Routing algorithm over semi-regular tessellations, Xplore, pp: 1180-1184.
8. Kumaravel, A., 2013. Algorithm for automaton specification for exploring dynamic labyrinths, Indian Journal of Science and Technology, 6(5).
9. Kumaravel, A., 2013. Application of non-uniform cellular efficient cryptography automata, Indian Journal of Science Technology, 6(5S): 4561-4566.
10. Kumaravel, A., 2013. Introducing an efficient programming paradigm for object-oriented distributed systems, Indian Journal of Science and Technology, 6(5S): 4597-4603.
11. Shafaq Sherazi and Habib Ahmad, 2014. Volatility of Stock Market and Capital Flow Middle-East Journal of Scientific Research, 19(5): 688-692.
12. Kishwar Sultana, Najm ul Hassan Khan and Khadija Shahid, 2013. Efficient Solvent Free Synthesis and X Ray Crystal Structure of Some Cyclic Moieties Containing N-Aryl Imide and Amide, Middle-East Journal of Scientific Research, 18(4): 438-443.
13. Pattanayak, Monalisa and P.L. Nayak, 2013. Green Synthesis of Gold Nanoparticles Using Elettaria cardamomum (ELAICHI) Aqueous Extract World Journal of Nano Science and Technology, 2(1): 01-05.

14. Chahataray, Rajashree. and P.L. Nayak, 2013. Synthesis and Characterization of Conducting Polymers Multi Walled Carbon Nanotube-Chitosan Composites Coupled with Poly (P-Aminophenol) World Journal of Nano Science and Technology, 2(1): 18-25.
15. Parida, Umesh Kumar, S.K. Biswal, P.L. Nayak and B.K. Bindhani, 2013. Gold Nano Particles for Biomedical Applications World Journal of Nano Science and Technology, 2(1): 47-57.