2006

Leading hackers down the garden path

Suen Yek
Edith Cowan University

DOI: 10.4225/75/57b267b440cb5
Originally published in the Proceedings of the 4th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 4th 2006.

Leading hackers down the garden path

Suen Yek
Edith Cowan University
syek@student.ecu.edu.au

Abstract

Can a hacker be controlled by predetermined deception? Limiting the decision making capabilities of hackers is one technique of network countermeasure that a honeynet enables. By furnishing a honeynet with a realistic range of services but restricted vulnerabilities, a hacker may be forced to direct their attacks to the only available exploits. This research discusses the deployment of a honeynet configured with a deceptive TELNET and TFTP exploit. Four hackers were invited to attack the honeynet and the analysis of their compromise identified if they engaged in a guided pathway to the intended deception. Hand trace analysis was performed on network log files to determine their primary attack vector. Conceptual analysis and frequency analyses methods were adopted to verify the hacker's compromise and subsequent deception. The results demonstrated how three out of four hackers were lead down a misguided pathway of network deception.

Keywords
honeynet, attack vector, Leximancer conceptual analysis, network deception

INTRODUCTION

In the realms of network security, deceptive techniques may provide an advantage by deterring hackers from genuine systems and the goal may be to monitor the modus operandi of an attack . Honeypots are digital entities that utilise deception as their primary mechanism and may do so by emulating the behaviours of a single device or whole network of devices. Additionally, the honeypot may be constructed to emulate network services utilising the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols. Deceptive techniques can be used to prevent, detect, and gather information on hacker activity . There exist a near infinite number of honeypot-variant architectures to select from when constructing a deceptive network and there are numerous open source and commercial honeypot solutions.

Honeyd is a type of honeynet implementation that creates virtual devices and networks by simulating the operating network stack of configured hosts. Honeyd is able to deceive directed and automated attacks through the purposeful simulation of lower and upper layer network protocols within the Open Systems Interconnect (OSI) reference model. This research utilised a purpose built honeyd honeynet that emulated a wireless bridge as an entry point to a virtual Local Area Network (LAN) of servers, client machines and networking infrastructure. Each of the hosts were configured with a range of services and applications and network routing enabled the discovery of the network's topology. The honeynet emulated chosen vulnerabilities that were designed to direct the hacker's compromise of an emulated TELNET vulnerability on a Cisco 7206 router running IOS 11.7 and a subsequent Trivial File Transfer Protocol (TFTP) vulnerability on the honeynet gateway.

Studies have shown how attack vectors can be predicted and reliably controlled by articulated deception induced by a honeynet . Cohen and Koike investigated how types of network attack were impacted by the deceptive strategy used. The authors designed attack trees to identify pathways of attack. In this research, it was intended that the honeynet configuration would limit a hacker's decision making capabilities and lead them to exploit the only available vulnerabilities that were tailored by the honeynet. The honeynet's log files for each hacker was collected and a combination of analyses was performed to determine the pathway of attack the hackers pursued to reach the intended exploits.

The author performed hand trace analysis on the honeynet log file collected from each hacker. The hand trace analysis involved manual tracing of each network packet to determine the chronological and sequential activities of the hackers. From the hand traces, the primary attack vector of each hacker was determined. The attack

vectors illustrated the pathway of activities each hacker engaged in to reach the intended TELNET and TFTP vulnerabilities in the honeynet. The research showed that three out of four hackers were deceived by the honeynet and their directed deception could be identified.

The results of the hand traced analysis and subsequent attack vectors of each hacker were verified through content and frequency analyses of the network data. The *Statistical Package for the Social Sciences* was used to summarise the frequency distributions of source IP, destination IP and protocol activity involving the honeynet. Content analysis of the honeynet's collected log files for each hacker was performed using the data mining tool Leximancer . The descriptive statistics generated by SPSS and the conceptual maps created by Leximancer were able to validate the hacker's exploit of the intended TELNET and TFTP vulnerabilities that were directed by the honeynet.

Explanation of the honeynet's emulated vulnerabilities

A Cisco router exploit was chosen as the emulated vulnerability for hackers to discover and exploit for two reasons. Firstly, routers are a targeted point because of their potential accessibility to the entire network. Routers may be used as a platform to conduct network scanning and as a launching point for Denial of Service (DoS) attacks internally or externally to the network .

Secondly, there is an overwhelming number of DoS vulnerabilities on routers or the use of routers for network compromise, as indicated by the number of CERT incidents and vulnerabilities reported predominantly involving the Cisco IOS platforms . The Cisco Simple Network Management Protocol (SNMP) exploit for gaining a router's configuration file via TFTP and construction of a Generic Routing Encapsulation (GRE) tunnel is particularly well documented .

For these reasons, a TELNET service was created on one of the honeynet's hosts that emulated a Cisco 7206 router running IOS 11.7. This Cisco router stored a configuration file that could be viewed through brute-forced guessing of the router's TELNET login username and password. The router configuration file could be viewed through the TELNET service which was vulnerable to the TFTP weakness . Through detecting and viewing the Access List Controls (ACLs) in the router's configuration file, a hacker could download and view the file and subsequently resend a modified configuration file back to the honeynet. This stage of the exploit was a proof of concept and if the hacker accomplished a TFTP `GET` and `SET` of a modified configuration file, the conjecture was that the honeynet was able to direct their exploit through deception.

Figure 1 shows a logical configuration of the honeynet's emulated hosts and network topology. The intended exploits were designed as a TELNET service that allowed remote wireless access into the router configuration dialogue. This exploit was emulated on the Cisco 7206 router running IOS 11.1 on the IP address `172.16.3.1`. The router configuration file for the Cisco router could be downloaded using TFTP from the honeynet's gateway IP address of `192.168.1.1`. The hackers were required to spoof their IP address to `192.168.1.2` according to the router configuration's ACL. By viewing the router configuration file, the ACLs permitting TFTP access could be discovered and subsequently exploited.

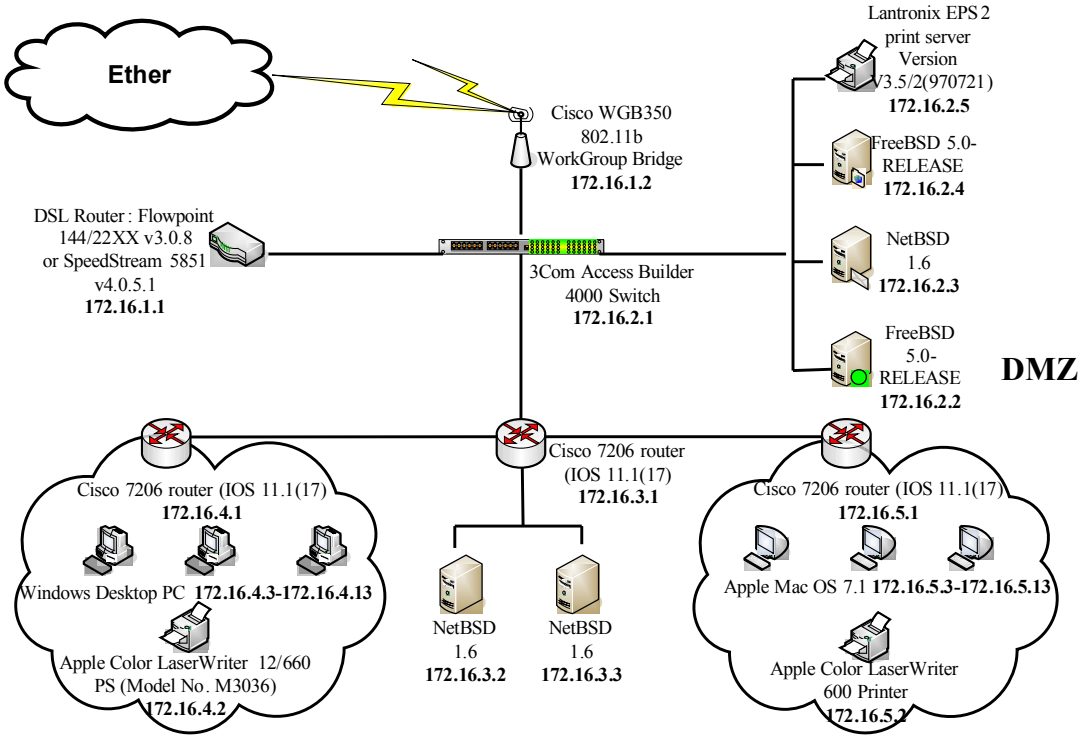

Figure 1 Honeynet logical configuration of hosts and network topology

METHOD

The aim of the hand trace analysis was to establish the attack vector adopted by the hackers and to determine whether they followed the predetermined pathway of deception to the intended TELNET and TFTP vulnerabilities implemented through the honeynet. The hand trace analysis was conducted by the author by manually examining the log files and illustrating the stages of activity the hackers engaged in from their choice of source and destination IP addresses and protocols used. The honeynet's log files were not altered for this analysis and subsequently, the hand traces showed the different pathways each hacker potentially adopted.

Ellipses containing the hacker's activity were drawn to identify the attack pathway taken by the hacker to reach the intended exploits. In the hand traces, several activities appear to be clustered together or stem from a single nexus, which indicated that the hacker attempted several options before discovery of a nexus point from which they could advance further from. The red encircled ellipses identify the primary attack vector for each hacker.

The collected honeynet log files were then filtered for the statistical analysis. The source and destination IP addresses of the hackers and the honeynet, in addition to the protocols associated with those IP addresses were used to perform frequency analysis. The data was statistically analysed using descriptive analysis, which was a method of summarising the log files. Frequency distribution of the hacker's source IPs, the hacker's choice of destination IPs within the honeynet, and the protocols the hackers used was the data utilised for generating the descriptive information. The use of statistical software packages such as SPSS facilitated the analysis process by eliminating human error and speeding up the analytical process in the case of large data sets such as the log files.

Content analysis was performed on the log files using the tool Leximancer. Leximancer creates conceptual maps from data mining and analysing the content of information. The tool is able to visually display identified conceptual themes, their attributes and the interrelationships between concepts. The process of content analysis integrates a systematic approach to identifying content categories from text using explicit coding rules . The combined hand trace, frequency analysis and content analyses methods were used to identify if the hackers followed the predetermined pathway set by the honeynet's deceptive strategies and verified if the exploits occurred.

HACKER ANALYSIS

Hacker 1 Analysis

The hand trace analysis of the honeynet log file for hacker 1 is shown in Figure 3. The red circles highlighted the primary attack vector taken to reach the intended exploits. Only the IP addresses representing hosts within the honeynet, the honeynet IP address of `192.168.1.1` and the hacker's chosen source IP address(es) were identified in the attack vector. The reason for limiting the attack vector to these hosts was because the research intended to demonstrate where the honeynet was able to direct the hackers. Other IP address spaces that were not within the `172.16.0.0/24` network of the honeynet were shown in the hand trace, although not in the attack vector. The honeynet firewall would have blocked responses to network packets that were directed to destination IP addresses not within the honeynet.

The primary attack vector for hacker 1 in Figure 2 indicated the following activities in the honeynet:

- hacker 1 adopted the IP address `192.168.1.2`
- ICMP PING request to `192.168.1.1`
- attempted TELNET on `172.16.1.2`
- NMAP SYN scan on `172.16.1.2`
- ICMP PING request to `172.16.2.1`
- ICMP PING request to `172.16.3.1`
- initiated TELNET on `172.16.3.1`
- attempted TFTP on `172.16.3.1`
- initiated TFTP on `192.168.1.1`

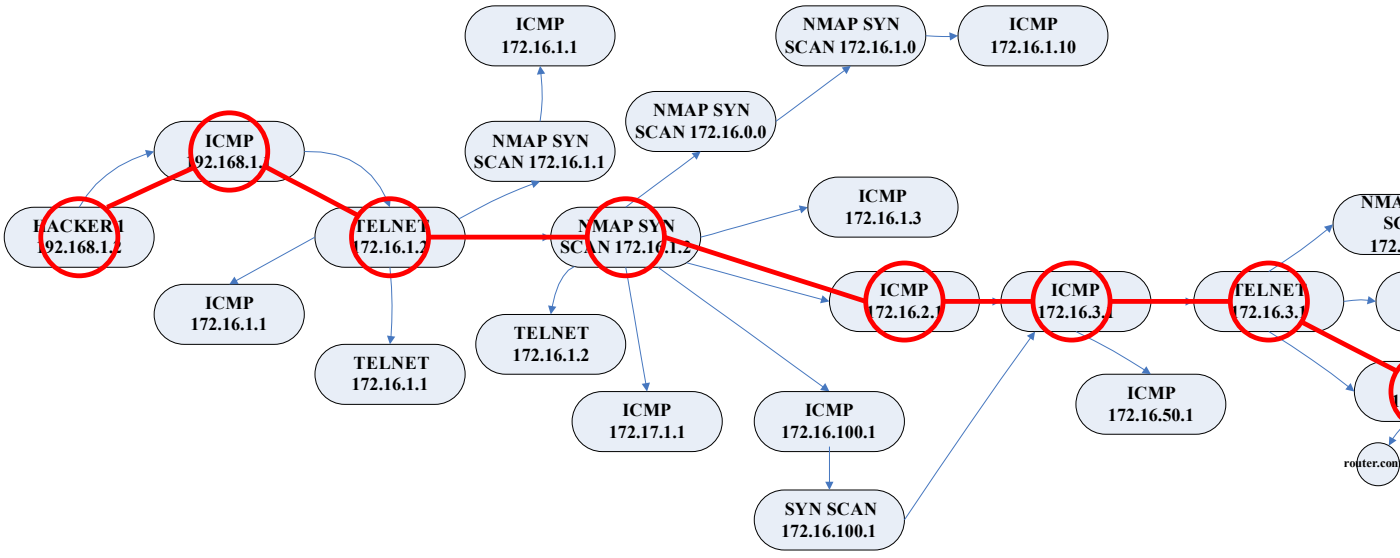

Figure 2 Hand traced attack vector of hacker 1

Frequency statistics generated by SPSS for the destination IP addresses within the honeynet that hacker 1 interacted with showed that host 172.16.3.1 received the most network packets. This host was the *Cisco 7206 router (IOS 11.1(17)* containing the TELNET vulnerability and its frequency was 61,038 occurrences. Hacker 1 interacted with three other hosts within the honeynet, which were 172.16.1.1, 172.16.1.2 and 172.16.2.1 in addition to the honeynet gateway 192.168.1.1. The frequencies of these hosts were significantly less than the 172.16.3.1 host with less than 10,000 occurrences. The 192.168.1.1 host with the TFTP vulnerability received 2,326 network packets from hacker 1.

Table 1 shows the frequency of the protocols for each of the destination IP addresses identified in Figure 1. In Table 1, only one source IP address was detected by SPSS, which was 192.168.1.2 as indicated in the attack vector. For the destination IP address 172.16.3.1, the TELNET and TFTP protocols are highlighted. The protocol frequency for the TELNET service on destination IP address 172.16.3.1 was the highest compared to TELNET attempts made on other destination IP addresses.

The TFTP protocol was also highlighted for the destination IP address 172.16.3.1 as the calculated frequency was highest at 3,060. Even though the TFTP connections could not be achieved on the 172.16.3.1 host, it was identified in the attack vector that hacker 1 originally attempted the TFTP exploit on that host running the remote Cisco router configuration through TELNET. The TFTP protocol was also detected with a frequency of 66, which was the next highest frequency detected, for the destination IP address 192.168.1.1. This IP address was the intended host for the hacker to initiate the TFTP connection and download the router configuration file. Table 1 also indicated that the highest frequency for the protocols used by hacker 1 was TCP.

Table 1 Protocol frequencies per destination IP address for hacker 1

SOURCE IP	DESTINATION IP	PROTOCOL	FREQUENCY
192.168.1.2	172.16.1.1	ICMP	97
		TCP	5,110
		TELNET	53
		HTTP	1
		UDP	21
	172.16.1.2	ICMP	14
		TCP	6,809
		TELNET	37
		UDP	8
	172.16.2.1	ICMP	23
		TCP	1
	172.16.3.1	ICMP	1,149
		TCP	56,638
		TELNET	189
		TFTP	3,060
		UDP	2
	192.168.1.1	ICMP	2,260
		TFTP	66

Figure 3 shows a conceptual map of hacker 1's exploit. The large circles identify major concepts such as the source and destination IP address 192.168.1.2 as Leximancer detected that IP address occurring most frequently in the log file. Other major concepts identified include the protocol TFTP and the attributes that were located in close proximity of that protocol. These attributes are shown in the large red box and include the words Acknowledgement, file router, netascii and octet. The smaller red box highlights the TELNET activity. Attributes that were associated with TELNET on host 172.16.3.1 shown in Figure 3 include the source IP 172.16.3.1, Telnet_Data and login.

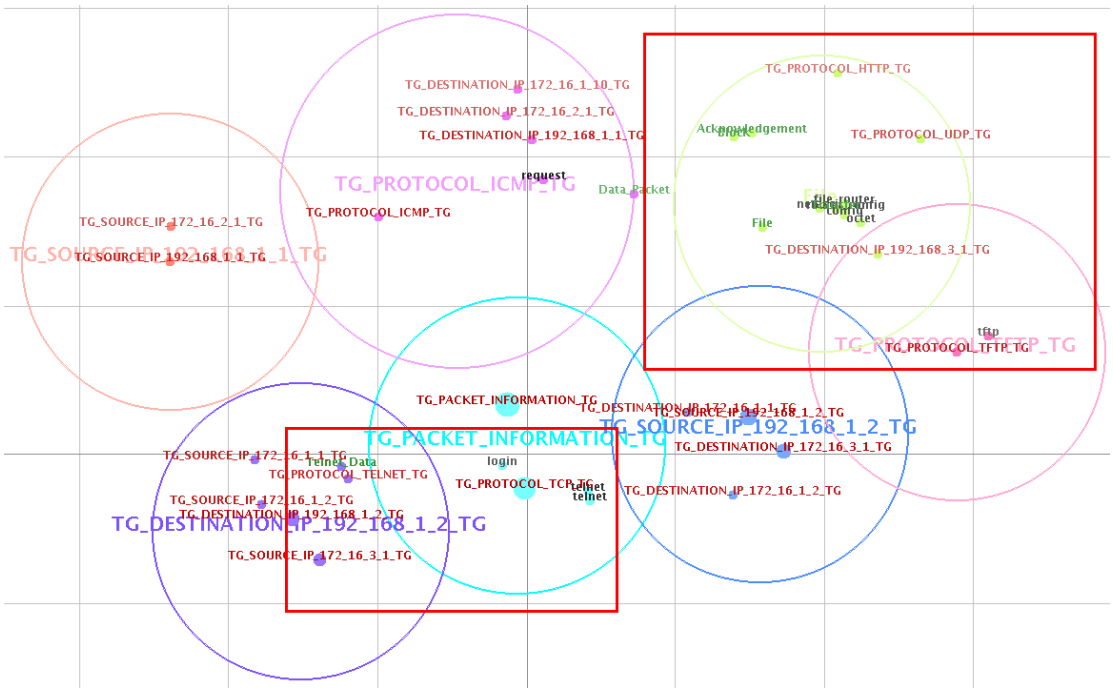

Figure 3 Conceptual map of hacker 1's exploit

Hacker 2 Analysis

Hackers 2 and 3 chose to perform their attacks together. Four identities were used to name four different IP addresses in this round of attack. Shadowed ellipses indicated that both hackers engaged in the same activity at approximately the same time. Figure 4 illustrates the attack vector for hacker 2; however, the hand trace for both the hackers was combined in the same analysis. Figure 4 indicated a source IP address of `192.168.1.10` for hacker 2 and `192.168.1.100` for hacker 3. Hacker X and hacker Y were labelled independently as the log file indicated multiple source addresses not originating from the honeynet. The positioning of hacker X at source IP address `172.16.1.2` indicates the approximate time when this IP address appeared in the log file. There were less then five packets generated from this source IP address, excluding the honeynet; therefore, they did not impact on the results or analysis.

The location of hacker Y at source IP address `192.168.1.11` was also positioned in the hand trace analysis at the approximate time when the IP address appeared in the log file. From the sequence of activities, it was determined that hacker X and Y were most likely hacker 2. This deduction meant that hacker 2 adopted two or more simultaneous IP addresses during their attack. The author's observation on hacker 2's conversation to hacker 3 also supported this inference.

The hand trace analysis of hackers 2 and 3 commenced with a range of ICMP v6, Simple Service Delivery Protocol (SSDP), Domain Name Service (DNS), Multicast DNS (MDNS) and the Internet Group Management Protocol (IGMP) packets that did not identify a source IP address. It could be determined that they originated from hacker 2 because this hacker initially utilised an Apple Mactintosh laptop device, which the MDNS is specific to. Hacker 2 then changed their laptop to an IBM during their attack alleging problems with the former device. This change of device most likely coincided with the adoption of the `192.168.1.11` source IP address indicated as hacker X.

The activities involved in hacker 2's primary attack vector was as follows:

- hacker 2 adopted the IP address `192.168.1.10`
- NMAP TCP on `192.168.1.1`
- SYN on `192.168.1.1` in parallel with ICMP PING `192.168.1.1`

•TCP SYN on `172.16.1.1`

•TCP SYN on `172.16.1.2`

•hacker 2 adopted the IP address `192.168.1.11`

•TCP SYN on `172.16.3.1`

•TCP SYN on `172.16.5.1`

•TCP SYN on `172.16.4.1` & `172.16.4.254`

•TCP SYN on `172.16.3.2`

•initiated TELNET on `172.16.3.1`

•hacker 2 adopted the IP address `192.168.1.2`

•attempted TFTP on `172.16.3.1`

•initiated TELNET on `172.16.3.1`

•initiated TFTP on `192.168.1.1`

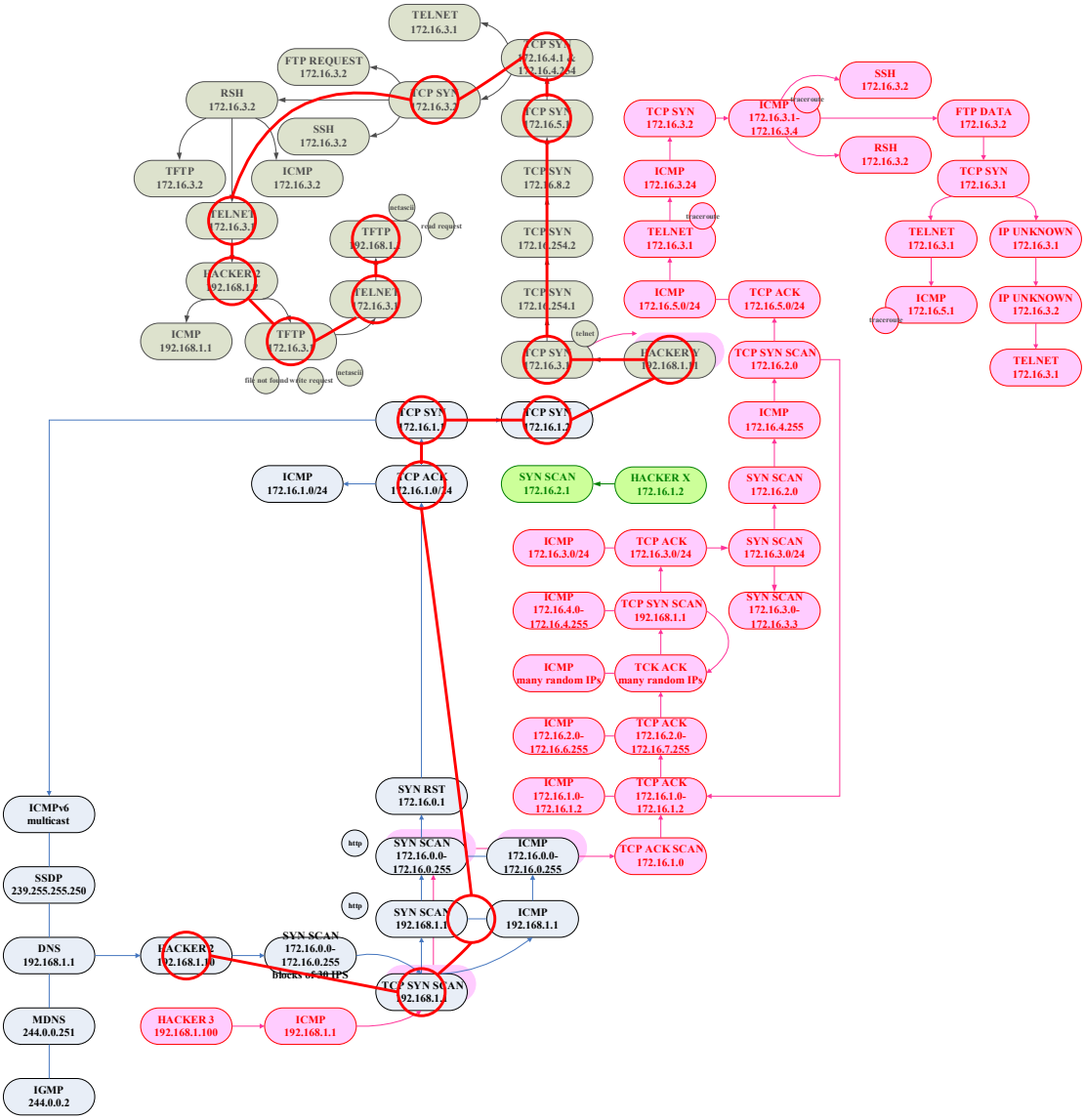

Figure 4 Hand traced attack vector of hacker 2

The SPSS statistical analysis performed on the honeynet's log file of hacker 2's attack showed the three source IP addresses identified in hacker 2's hand traced analysis. The destination IP address with the highest frequency was the `172.16.3.1` host with 12,533 occurrences. The host `172.16.3.2` received the second highest frequency with 7,706 occurrences followed by the `192.168.1.1` host with 6,884 occurrences.

In Table 2, the three destination IP addresses that hacker 2 interacted with using the source IP address `192.168.1.10` is shown. These destination IP addresses corroborate with the destination IP addresses within the honeynet of the hand traced attack vector. From the source IP address `192.168.1.2`, the protocol frequencies for the destination IP address `172.16.3.1` show TELNET with 1,068 occurrences, which was the highest occurrence of TELNET activity for any destination IP address. The TFTP protocol frequency for destination IP addresses `172.16.3.1` and `192.168.1.1` show 15 and 24 occurrences respectively. Table 2 also shows a TELNET frequency of 943 for the destination IP address `172.16.3.1` when using the source IP address `192.168.1.11`, which was before hacker 2 spoofed their IP address to `192.168.1.2`. All the protocol frequencies for each destination IP address could not be shown as the table was too large. However, the table provided the protocol frequencies for the destination IP addresses which SPSS detected as the most frequently visited across all source IP addresses for hacker 2.

SOURCE IP	DESTINATION IP	PROTOCOL	FREQUENCY
192.168.1.10	172.16.1.1	ICMP	4
		TCP	3,362
		TELNET	1
	172.16.1.2	ICMP	1
		TCP	1,675
	192.168.1.1	ICMP	5
		TCP	6,658
192.168.1.2	172.16.3.1	ICMP	2
		TCP	5,364
		TELNET	1,086
		UDP	2
		TFTP	15
	192.168.1.1	ICMP	10
		TCP	6
		TFTP	24
192.168.1.11	172.16.3.1	ICMP	3
		TCP	5,112
		TELNET	943

Table 2 Protocol frequencies per destination IP address for hacker 2

Figures 5 and 6 show conceptual maps that Leximancer generated from the honeynet's log file of hacker 2's attack. In Figure 5, the red box highlights the main concept which was the TFTP protocol. The attributes detected by Leximancer that were associated with the TFTP protocol included `router_config`, `Read_Request`, `Data_Packet`, and `Transfer` in close proximity to one another. In Figure 6, the red box highlighted concepts and attributes that were associated with TELNET protocol. The identified attributes included `Telnet_Data` and the destination IP address `172.16.3.1`.

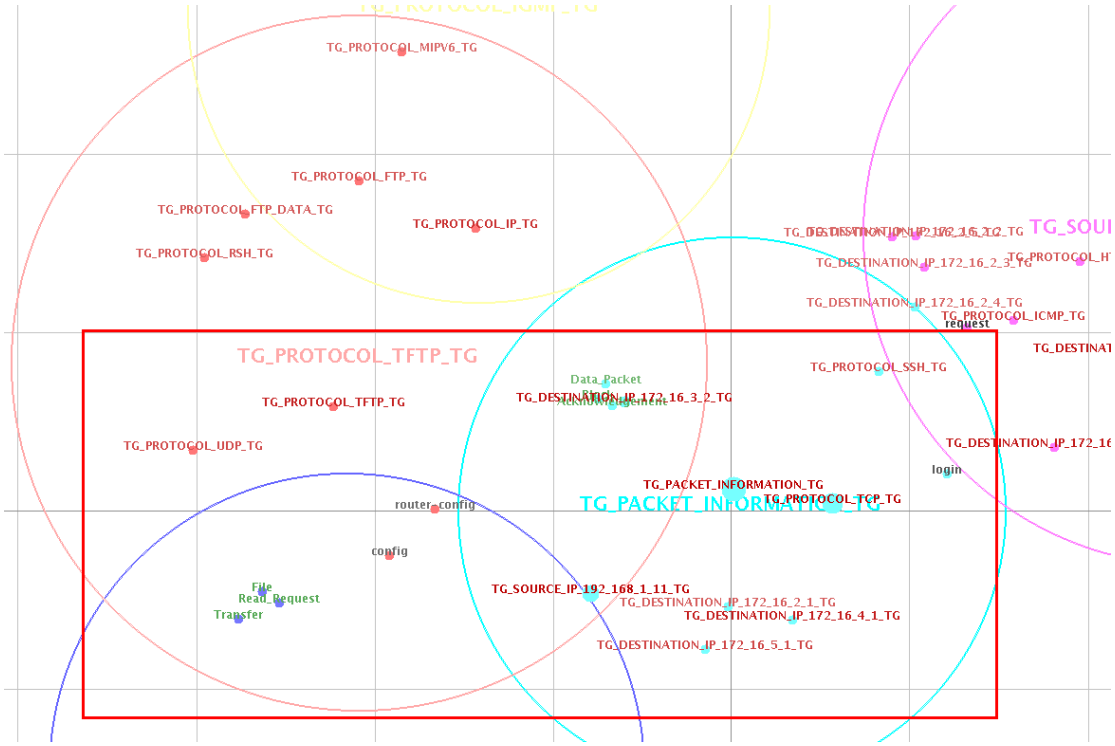

Figure 5 *Conceptual map of hacker 2's exploit of the TFTP vulnerability on host* `192.168.1.1`

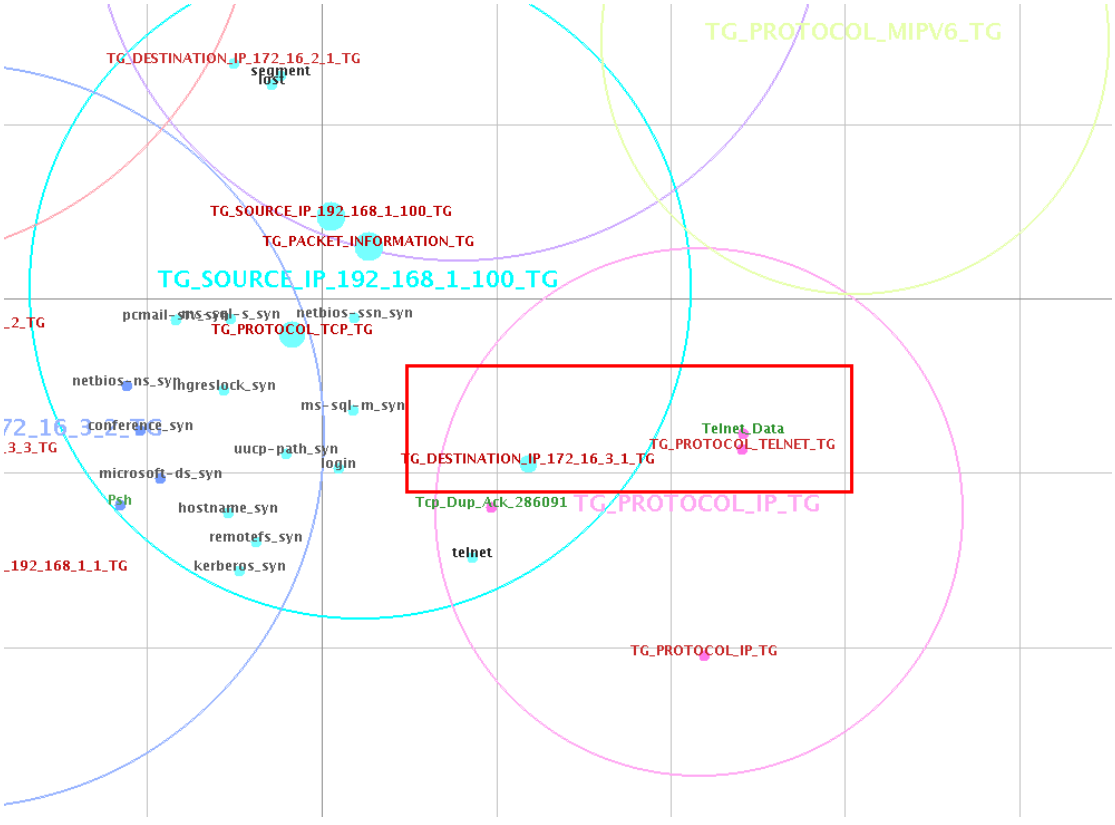

Figure 6 *Conceptual map of hacker 2's exploit of the TELNET vulnerability on host* `172.16.3.1`

Hacker 3 Analysis

Figure 7 illustrates the hand traced attack vector for hacker 3, which after the ICMP PING requests and TCP SYN scans on network `172.16.0.0/16` was a succession of scan activity on a diverse range of IP addresses.

It was found in the analysis that hacker 3 did scan numerous host and network IP addresses that were not within the specified range of the honeynet; however each non host IP address was dropped by the honeynet's firewall.

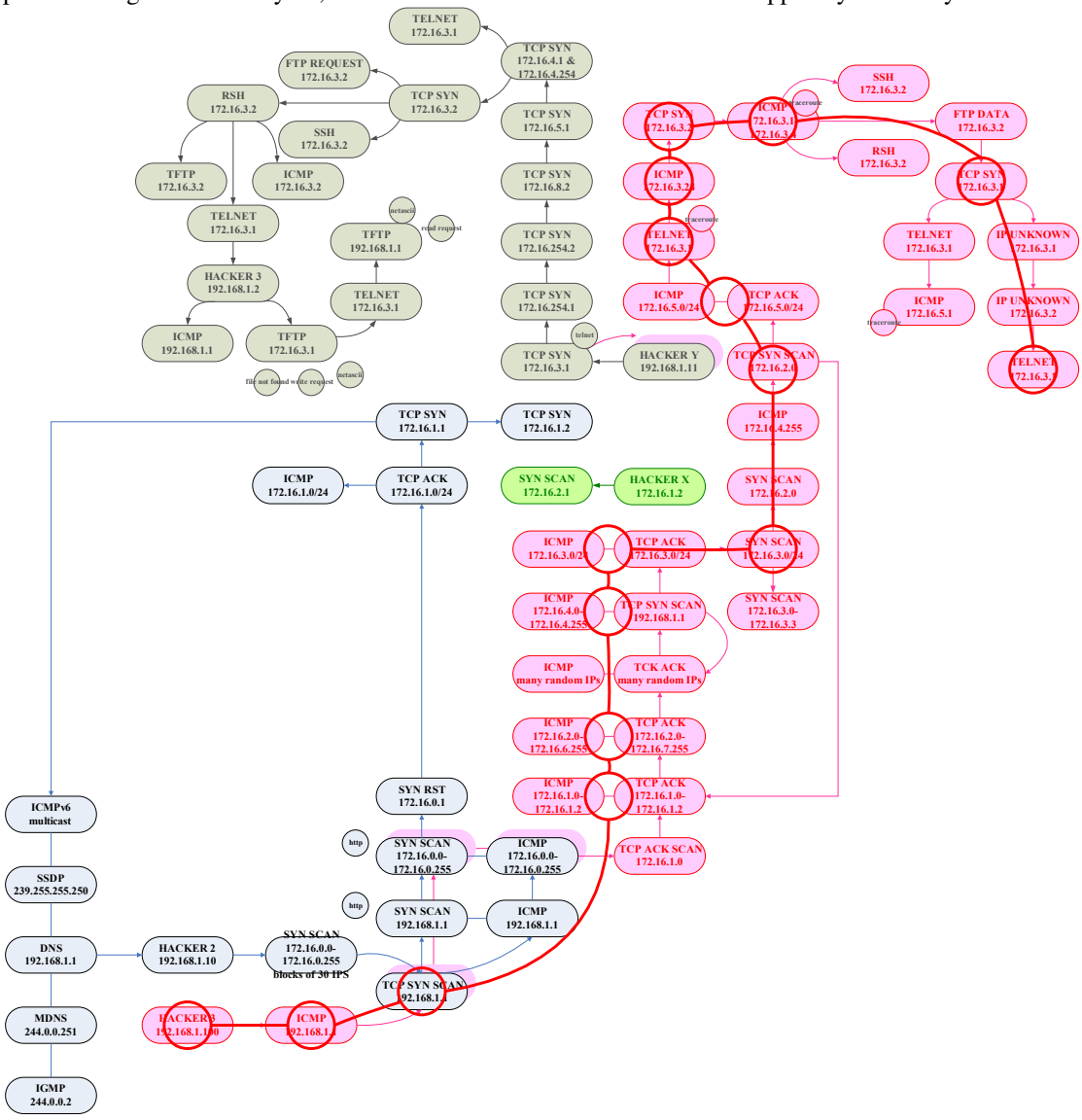

Figure 7 Hand traced attack vector of hacker 3

Hacker 3 performed a series of TCP ACK and ICMP PING requests on the `172.16.1.0/24`, `172.16.2.0/24`, `172.16.3.0/24`, `172.16.4.0/24` and `172.16.7.0/24` networks. Additionally, hundreds of random IPs were scanned in blocks of approximately 30 IP addresses. The nature of the logged packets indicated that hacker 3 utilised a tool to select and scan arbitrary IP addresses. This technique would have been ineffective host and network reconnaissance as the honeynet would not have responded to any of the IPs outside of the designated `172.16.0.0/24` network of the honeynet. This technique seemed unusual and hacker 3's attack vector did not appear to follow a meaningful pathway of activity.

Hacker 3's proposed attack vector included the following activities involving the honeynet:

- hacker 3 adopted the IP address `192.168.1.100`
- ICMP PING on `192.168.1.1`
- TCP SYN on `192.168.1.1`
- TCP ACK and ICMP PING on `172.168.1.1 - 172.16.1.2`
- TCP ACK and ICMP PING on `172.16.2.1-172.16.2.5`

- •TCP SYN on 192.168.1.1 and ICMP PING on 172.16.3.1-172.16.3.3
- •SYN scan on 172.16.3.1-172.16.3.3
- •TCP ACK on 172.16.5.1-172.16.5.13
- •attempted TELNET on 172.16.3.1
- •TCP SYN on 172.16.3.2
- •ICMP PING 172.16.3.1-172.16.3.3
- •TCP SYN 172.16.3.1
- •initiated TELNET on 172.16.3.1

The frequency analysis performed on the honeynet log files for hacker 3 detected 27 unique destination IP addresses. In the analysis, hacker 3 sent most network packets to host 172.16.3.1, which had a frequency of 20,579; host 172.16.3.2 had a frequency of 8,715 and host 192.168.1.1 had the third highest frequency of 7,008. Given that the protocol frequencies for each of the 27 unique destination IP addresses could not be shown in single table, the protocol frequencies of the three main destination IP addresses were shown instead in Table 3.

SOURCE IP	DESTINATION IP	PROTOCOL	FREQUENCY
192.168.1.100	172.16.3.1	ICMP	92
		TCP	18,846
		TELNET	659
		IP	888
		UDP	8
	172.16.3.2	ICMP	43
		TCP	8,595
	192.168.1.1	ICMP	66
		TCP	6,942

Table 3 Protocol frequencies per destination IP address for hacker 3

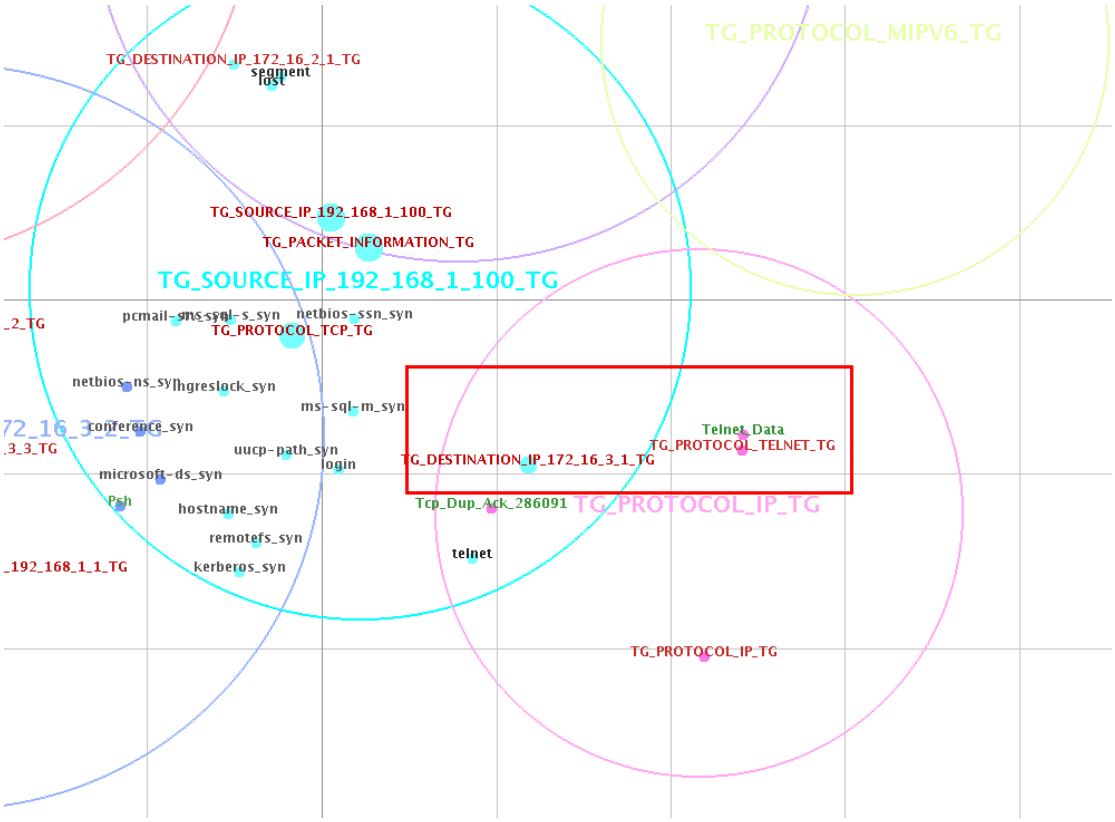

Figure 8 Conceptual map of hacker 3's attempted exploit

Table 3 identified the protocol frequencies for the three main destination IP addresses hacker 3 interacted with. According to the hand traced analysis of hacker 3, TELNET was attempted on the `172.16.3.1` host with a frequency of 659. The TCP and ICMP protocols had the highest frequencies for most hosts. Protocols such as FTP, RSH and SSH were also detected by SPSS on the `172.16.3.2` host but are not shown in the table. No TFTP protocols were detected for the `192.168.1.1` host or the `172.16.3.1` host. Figure 8 shows the conceptual mapping of hacker 3's attack. In the red box, the attributes `Telnet_Data` and destination IP `172.16.3.1` which were in close proximity to one another. No TFTP attributes were shown around the `172.16.3.1` or `192.168.1.1` destination IP addresses.

Hacker 4 Analysis

The hand trace analysis and proposed attack vector of hacker 4 is shown in Figure 9. The initial packet logs showed ICMP v6 multicast, router solicitation and neighbour solicitation packets without a source IP address. The hacker initially adopted the IP address `192.168.1.100` and subsequently changed their IP address to `192.168.1.20`. The activities involved in hacker 4's attack vector with the honeynet was as follows:

- hacker 4 adopted the IP address `192.168.1.100`
- hacker 4 adopted the IP address `192.168.1.20`
- TCP SYN on `172.16.1.1-172.16.1.2`
- TCP SYN on `172.16.4.1-172.16.4.13`
- ICMP PING on `172.16.4.1-172.16.4.13`
- ICMP PING on `172.16.5.1-172.16.5.13`
- ICMP PING on `172.16.1.1-172.16.1.2`
- TCP SYN on `192.168.1.1`

- TCP SYN on 172.16.3.1
- initiated TELNET on 172.16.3.1
- hacker 4 adopted the IP address 192.168.1.2
- initiated TFTP on 172.16.3.1

The SPSS frequency analysis of the honeynet's log file from hacker 4 showed that all the hosts within the honeynet received network packets from hacker 4. The hosts detected with the highest frequency was 172.16.1.2 with 88,777 occurrences, 172.16.5.3 with 63,590 occurrences, followed by 172.16.3.1 with 52,789 occurrences. Host 172.16.3.1 was the third most frequent destination IP address and the destination IP address 192.168.1.1 was the fourth most frequent with 13,736 occurrences. As all the protocol frequencies for each destination IP addresses could not be shown in a single table, the reduced information is shown in Table 4.

SOURCE IP	DESTINATION IP	PROTOCOL	FREQUENCY
192.168.1.100	192.168.1.1	ICMP	1
192.168.1.2	192.168.1.1	TFTP	7
192.168.1.20	172.16.3.1	ICMP	43
		TCP	51,953
		TELNET	742

Table 4 Protocol frequencies for the destination IP addresses detected for hacker 4

Table 4 shows the three source IP addresses that hacker 4 adopted and the protocol frequencies for the destination IP addresses associated with TELNET and TFTP. Hacker 4 did not conduct much network activity when using the source IP address 192.168.1.1 as indicated by their hand trace analysis and attack vector. However, the TFTP protocol was detected when hacker 4 spoofed to the 192.168.1.2 IP address and only 7 packets were identified with this destination IP address. The conceptual maps generated for hacker 4's attack is shown in Figure 10 and Figure 11. The red highlighted box in Figure 9 shows the attributes Read_Request, File and Block and source IP 192.168.1.2 associated with the TFTP protocol concept. Figure 10 shows the Telnet attribute associated with the destination IP 172.16.3.1 concept.

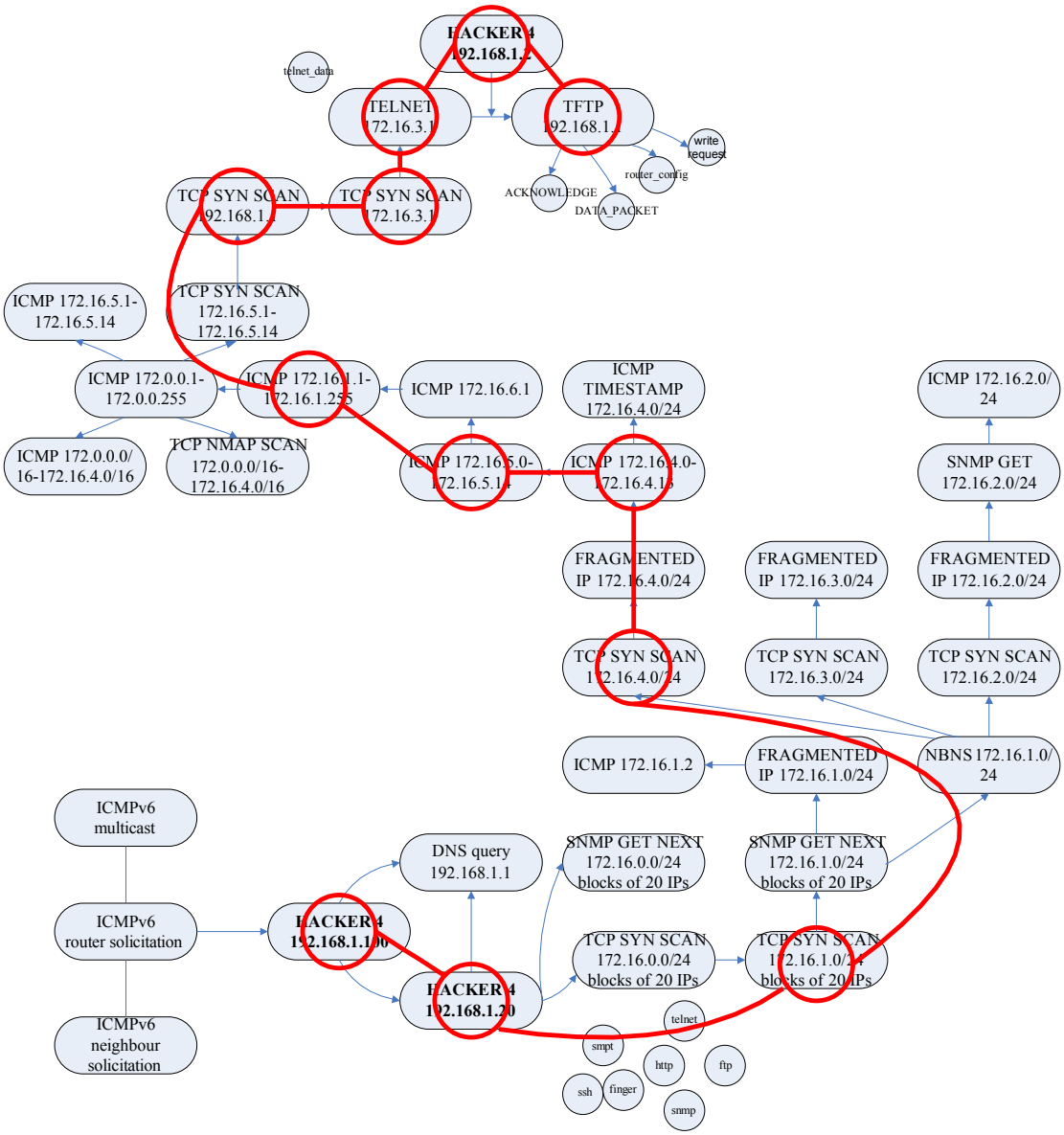

Figure 9 Hand traced attack vector of hacker 4

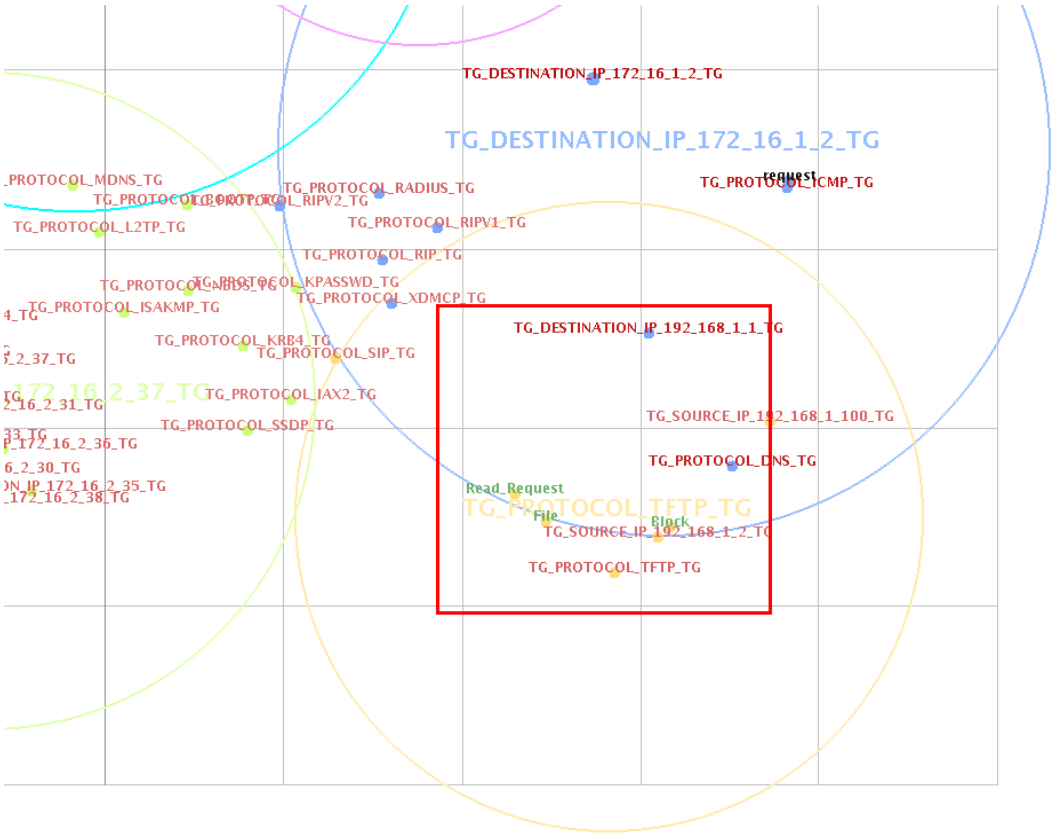

Figure 10 *Conceptual map of hacker 4's exploit of the TFTP vulnerability on host* `192.168.1.1`

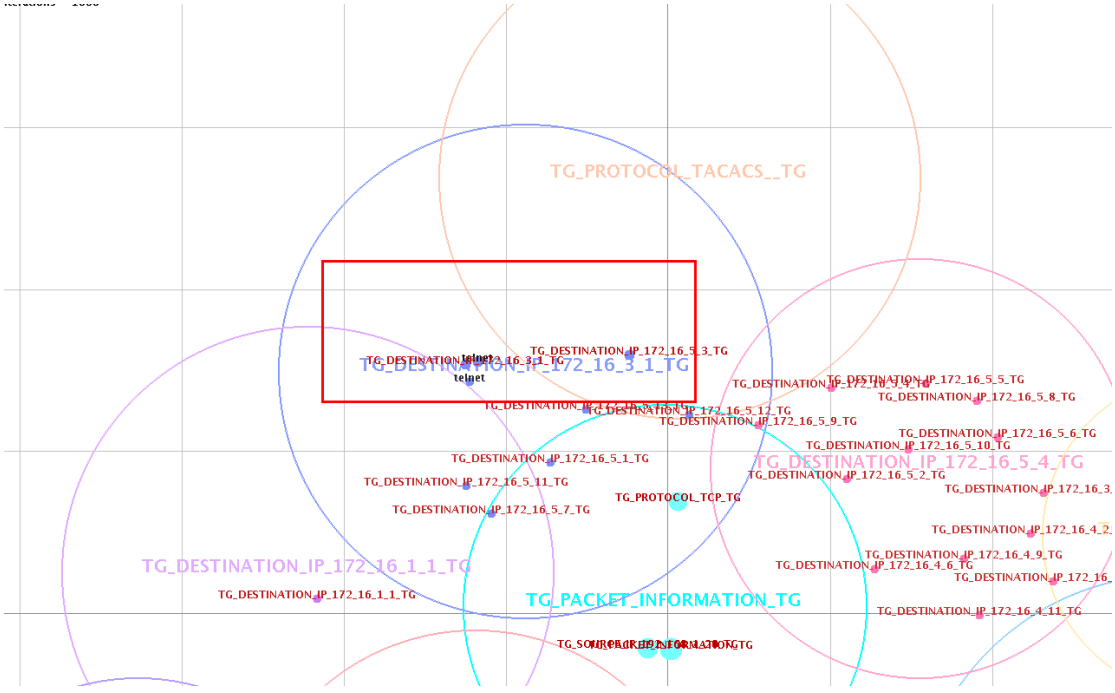

Figure 11 *Conceptual map of hacker 4's exploit of the TELNET vulnerability on host* `172.16.3.1`

DISCUSSION OF RESULTS

From the identified attack vector of hacker 1, it may be inferred that this hacker predominantly focused on hosts in the honeynet that were networking infrastructure. These hosts included the *Cisco WGB350 802.11b WorkGroup Bridge* on IP address 172.16.1.2, the *DSL Router: Flowpoint 144/22XX v.3.0.0 or SpeedStream 5851 v4.0.5.1* on IP address 172.16.1.1 and the *Cisco 7206 router (IOS 11.1(17)* on IP address 172.16.3.1. From the hand trace analysis, it could be determined that hacker 1 focused on identifying TELNET services typically running on infrastructure type operating systems (OSs). Hacker 1 did perform some NMAP TCP/IP port scanning, which is often used to determine host OS names, version numbers, and services or applications running on ports. However, hacker 1 did not appear to exploit services other then TELNET on other hosts. From hacker 1's hand trace analysis and attack vector, it may be inferred that they were aiming to discover and exploit Cisco routers running TELNET.

The frequency analysis indicated that hacker 1 had reached the intended TELNET vulnerability on the 172.16.3.1 host and made continuous attempts to guess the login and password. The generated concept map provided an alternate visual representation of the intended exploits occurring. The primary concepts identified by Leximancer's content analysis included hacker 1's IP address and network packet data associated with the TELNET and TFTP exploits. When combined with the hand trace analysis and frequency statistics, it was deduced that hacker 1 was deceived by the honeynet and was directed to exploit the intended TELNET and TFTP vulnerabilities.

From hacker 2's hand trace analysis, it could be inferred that their attack involved mostly scanning and identification of hosts. Hacker 2 attempted to exploit many services that were discovered to run on the hosts they scanned using NMAP SYN and RST set network packets. The attack vector for hacker 2 indicated that the TELNET service on destination IP address 172.16.3.1 was discovered after some scanning was conducted on the 192.168.1.1 host, and hosts in the 172.16.1.0/24, 172.16.3.0/24, 172.16.4.0/24 and 172.16.5.0/24 networks.

When hacker 2 discovered the TELNET service on destination IP address 172.16.3.1, they were able to guess the login and password and accessed the router configuration file. Hacker 2 then spoofed their IP address from 192.168.1.11 to 192.168.1.2 to match the ACL and attempted a TFTP of the router configuration file on the 172.16.3.1 host as hacker 1 had done. This attempt was unsuccessful and hacker 2 resumed the TELNET session on host 172.16.3.1, most likely to re-read the router configuration file and ACLs. This hacker subsequently initiated a TFTP connection to the correct 192.168.1.1 destination IP address and downloaded the router configuration file. A modified router configuration file was sent back to 192.168.1.1 and the exploit was complete.

According to hacker 3's attack vector, they did not exploit the intended TELNET and TFTP vulnerabilities. Their attack vector indicated that they used various types of NMAP scanning techniques and sent ICMP PING requests to hosts. Around the time hacker 2 (shown as hacker Y) discovered the TELNET service was accessible on the host 172.16.3.1, hacker 3 changed their network activity. In hacker 3's hand trace analysis, there was an apparent shift from randomly scanning and PINGing the 172.16.5.0/24 network to attempting TELNET on the 172.16.3.1 host. This behaviour was most likely explained by hacker 2 informing hacker 3 of their discovery.

It was highly likely that both hackers were colluding when SSH, RSH, and FTP data transfers were attempted on the 172.16.3.2 host by hacker 3. A near mirror image of these particular activities was reflected in hacker 2's hand trace analysis. Subsequent to the failed attempts on services running on the 172.16.3.2 host, hacker 3 sent packets which the log file recorded as IP UNKNOWN payloads to both the 172.16.3.1 and 172.16.3.2 hosts. They may have been deliberately malformed packets sent to the target hosts to illicit information from them. Hacker 3 then re-tried TELNET attempts on host 172.16.3.1. At this stage, hacker 2 had completed the exploit and hacker 3 ceased their attack as well. It was not apparent if hacker 3 was following

a distinct pathway, the hand trace analysis and attack vector indicated they used random techniques indicative of confusion.

The conceptual mapping of hacker 3's attempted exploit indicated that hacker 3 made an attempt on the intended TELNET vulnerability in the honeynet. The honeynet did not direct the deception of hacker 3 and from the proposed attack vector, hacker 3 may have adopted random scanning techniques indicative of a naïve attacker. This inference may be supported by the amount of scanning that hacker 3 conducted on IP addresses that were well outside the honeynet's `172.16.0.0/24` network.

Hacker 4 focused primarily on reconnaissance of hosts and the network, which was indicative from the amount of scanning that was performed. The hand trace analysis and proposed attack vector for hacker 4 indicated that this hacker conducted large amounts of scanning using multiple tools to verify their results. This technique resulted in protocol frequencies higher than the previous three hackers. Hacker 4 was able to detect the TELNET service on destination IP `172.16.3.1` and guess the login and password. Hacker 4 appeared to have comprehended the router configuration file and ACLs on their first attempt because they did not attempt to initiate a TFTP connection to the same `172.16.3.1` host as hacker 1 and 2 had done. This hacker spoofed their IP address to match the ACL of the router configuration file immediately after their discovery and was able to successfully use TFTP to acquire and modify the router configuration file before sending it back to the honeynet.

It could not be determined why hacker 4 focussed on the hosts `172.16.1.2` and `172.16.5.3`; although, from the attack vector, it was visible that hacker 3 did reach the `172.16.3.1` host. The TFTP protocol was detected when hacker 4 spoofed to the `192.168.1.2` IP address and only 7 packets were identified with this destination IP address. This supported the deduction that hacker 4 did not require multiple attempts to exploit the TFTP vulnerability. The `172.16.3.1` host received mostly TCP network packets; however, the TELNET protocol was detected also. The conceptual maps indicated that the intended TELNET and TFTP exploits were achieved by hacker 4.

CONCLUSION

Cohen and Koike's study showed that network attack was impacted by the deceptive strategy used. In this research, the deceptive strategies of the honeynet were based on the purposeful emulation of the TCP/IP suite of protocols for network deception. The honeynet utilised the honeyd program to create virtual hosts and a network, which was able to respond to the hacker's TCP/IP scanning. Honeyd changes network packet headers so that they appear to be generated from genuine OS hosts. The result was that the hacker's interaction with the honeynet was controlled and directed from the TCP/IP level of the OSI model.

The types of activities detected in each hacker's attack vector identified NMAP scan techniques, which utilised manipulated TCP/IP network packets and ICMP PING requests. From this network level interaction, the hacker's were able to discover hosts, and the services and applications that were running on the hosts. This stage of reconnaissance was controlled by the honeynet by allowing host OS platforms and versions to be discovered through TCP/IP network scanning, which is also called TCP/IP fingerprinting . Honeyd incorporates the Address Resolution Protocol (ARP) to allow created hosts to be bound to an IP address and the honeynet's firewall blocked ICMP requests to all other destination IP addresses not within the honeynet's IP network. This technique allowed the honeynet to control responses to the ICMP PING requests sent by the hackers. By controlling the responses to TCP/IP scanning and ICMP PING requests, the honeynet was able to limit the hacker's ability to scan and identify potential hosts for exploit.

The TELNET vulnerability was also emulated through a PERL script that manipulated the TCP/IP network packets to show that the service was real. Honeyd manipulated the packet headers so that they appeared to be generated from a host running the TELNET service and the TELNET emulation was achieved by the TELNET PERL script extracting packet data such as the login and the commands used. The PERL code instructed the honeynet to respond to the correct commands and issue error messages to router commands that the honeynet did not intend the hacker's to gain access to. Even though TELNET runs at the Application layer of the OSI model, the emulation was performed at the Networking layer of the OSI. Therefore, the hacker's could be deceived

about the TELNET service because the tools and techniques they relied on utilised TCP/IP connections. The honeynet was thus able to limit the hacker's to the TELNET commands leading only to the TFTP exploit.

The TFTP service was enabled on the honeynet's gateway IP address of `192.168.1.1`. The service was listening for connections using the TFTP `SET` and `GET` commands. Therefore, the honeynet was preconfigured for the exploit. The hacker's were directed to this exploit because the remote TELNET service only allowed the commands to login and view the router configuration file. From this capability, the hacker's were alerted to the potential weakness of the router in that TFTP connections were permitted from a single IP address. Subsequently, three out of the four hackers were directed and deceived by the honeynet into pursuing the TFTP exploit.

It could be inferred that when a honeynet provides a baited vulnerability, such as the TELNET and TFTP vulnerabilities, hackers are drawn to the opportunity. By limiting the network attack opportunities through the deceptive capabilities of the honeynet, hackers may be deceived in two ways. Firstly, if the honeynet is able to emulate its host and network capabilities at the TCP/IP network packet level, the tools and techniques utilised by hackers deceive the hackers through the authenticity of network responses. Secondly, by directing the hacker's ability to exploit vulnerabilities, the honeynet could guide the hacker to the intended deception without the hacker's knowledge that they were being controlled. The outcome of the research indicated that hacker's may be directed and deceived by a honeynet through predetermined network deception at the TCP/IP level.

REFERENCES

COPYRIGHT