View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Research Online @ ECU

Edith Cowan University

Research Online

ECU Publications Pre. 2011

2005

How to build a faraday on the cheap for wireless security testing

Suen Yek
Edith Cowan University

Follow this and additional works at: https://ro.ecu.edu.au/ecuworks

 Part of the Computer Sciences Commons

Yek, S. (2005). How to build a faraday on the cheap for wireless security testing. Proceedings of the 3rd Australian Computer, Network and Information Forensics Conference . (pp. 126-130). Perth, WA: Edith Cowan University.
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/ecuworks/2825

How to build a faraday cage on the cheap for wireless security testing

Suen Yek
School of Computer and Information Science Security
Edith Cowan University
syek@student.ecu.edu.au

Abstract

The commonly known security weaknesses associated with the 802.11b wireless standard have introduced a variety of security measures to countermeasure attacks. Using a wireless honeypot, a fake wireless network may be configured through emulation of devices and the TCP/IP fingerprinting of OS network stacks. TCP/IP fingerprinting is one of the most popular methods employed to determine the type of OS running on a target and this information can then be used to determine the type of vulnerabilities to target on the host. Testing the effectiveness of this technique to ensure that a wireless honeypot using honeyd may deceive an attacker has been an ongoing study due to problems conducting TCP/IP fingerprinting in the wireless environment. Research conducted in a university laboratory showed that the results were ineffective and the time taken to conduct testing could be as long as 60 hours. The subsequent exploration of different testing methods and locations illuminated on an ideal research facility called a faraday cage. The design and construction of the faraday is discussed in this paper as an affordable solution for controlled and reliable testing of TCP/IP fingerprinting against the scanning tool Network Mapper (NMAP). The results are useful when looking to deploy a deceptive honeypot as a defence mechanism against wireless attackers.

Keywords

wired and wireless TCP/IP fingerprinting, wireless NMAP scanning, faraday cage

INTRODUCTION

Research in wireless network security has become a major topic of interest with attacks becoming more apparent as weaknesses in the lower layers of the Open Systems Interconnect (OSI) model reveal the shortcomings of open air transmissions. The 802.11b standard for wireless networking has been vastly adopted and a variety of defence mechanisms has been adopted for countermeasure such as Access Point (AP) firewalls and routing, wireless Intrusion Detection Systems, and the recent experimentation with wireless honeypots. While wireless honeypot research has not been widely explored, ongoing research (Yek, 2003, 2004) has focused on the premise that an emulated wireless network may act as a decoy from genuine systems.

Furthermore, a wireless honeypot may be configured to emulate a wireless network that bridges wired resources to deceive attackers and contain their network compromise while being monitored. The advantages of deploying a wireless honeypot could therefore, detect and capture the attacker before damage is inflicted on genuine resources and assets. One of the challenges found with emulating wireless networks is fine-tuning the data link and networking layers of wireless transmission to appear real to an attacker (*ibid*, 2003; 2004). This paper explains some of the difficulties faced when implementing effective TCP/IP fingerprinting on the network stack of emulated Operating Systems (OS) with a honeypot.

The results of the research into performing TCP/IP fingerprinting over the wireless medium has uncovered a process of discovery into ideal circumstances for testing this technique of OS identification. The goal has been to implement a network of virtual devices called a honeynet as a potential network countermeasure for organisations using wireless networks. The cycle of discovery lead to the construction of a faraday cage, which is a metal encased cage that does not allow the escape of the 12.5 centre length 802.11b wireless electromagnetic frequency radio waves (RF) from the inside. External wireless transmissions are not permitted inside the cage either. The design and physical characteristics of the cage are described in this paper as a financially feasible and easy construction.

TCP/IP FINGERPRINTING IN A WIRELESS ENVIRONMENT

Previous studies into the art of TCP/IP fingerprinting have uncovered it's value in performing OS discovery and subsequent network reconnaissance for attackers, in addition to aiding the administrator in conducting a network audit. The technique may be executed through a port scanning tool such as Network Mapper (NMAP) (Yarochkin, 2005). NMAP is an active scanning tool that sends probing packets to query any unique differences on its target OS. Other active tools include Xprobe2 (Yarochkin & Arkin, 2003) and Queso (Savage, n.d.), which function in a similar manner.

The common feature essential to the tool's success is the ability to reach it's target without disorganising the bit sequences when used over radio waves. This problem is not particularly evident when performing TCP/IP fingerprinting over the wired medium where studies have found that a significant number of emulated OSs could be guessed correctly than over the wireless medium.

The deceptive ability of the wireless honeypot is highly dependent on it's ability to emulate OS devices through responding to NMAP's TCP/IP fingerprinting. The honeyd is one such honeypot that creates host OSs that implement a fingerprint containing a sequence of TCP/IP exchanges that are ready to respond when queried. A subsequent database of these fingerprints is maintained by the author of NMAP and is continuously updated and improved by the online security community. While NMAP's use was indented for security purposes, it is also a commonly used tool by attackers of varying sophistication due to the flexibility of the tool and the granularity of which it is able to perform OS discovery (Honeynet Project, 2004; Spitzner, 2002). Attackers would usually progress from the stage of OS discovery to network discovery and consequently begin locating vulnerable targets to execute a tailored attack.

Testing TCP/IP fingerprinting to determine an effective way to countermeasure NMAP and other such scanning tools has proven to be a defiant task because of many variables in the software of the tool, and mostly the nature of the 802.11b wireless environment. Wireless networks face difficulties because of the ease of interference. Interference may be from competing wireless devices including Bluetooth 802.15 transmissions to lights, microwaves or physical objects. Wireless networking in itself requires data to piggyback over RF waves that may travel in omnidirectional pathways that require both the sender and receiver to transmit with a greater overhead and encounter many retransmissions due to lost data or bits.

PROBLEMS ENCOUNTERED WITH WIRELESS TCP/IP FINGERPRINTING

Previous research by Valli (2003) involving the use of honeyd and NMAP employing TCP/IP fingerprinting in the wired environment showed that out of a possible 704 OS fingerprints, NMAP was able to determine 152. Although this only represented approximately 22% of the total possible, the 152 OS fingerprints provided sufficient choices for a deceptive network to employ and deceive unknown attackers (Gupta, 2003). From these successful OS fingerprints, a number were chosen to implement into the first undertaking of wireless testing. It was found that these fingerprints which once were successfully identifying the underling OSs on hosts over the wire could not do so effectively in a wireless environment.

The first wireless TCP/IP fingerprinting conducted (Yek, 2003) was in a university laboratory where there was little interference from competing wireless devices. Furthermore, the proximity of the two interacting devices was within two metres. The tests were performed using NMAP, followed by Nessus (Deraison, 2003) which also employs the NMAP fingerprint engine and performs vulnerability assessments on the target OSs. The unsuccessful results of this testing lead to an inquiry for reasons that may have contributed to the failed fingerprints that were effective on the wire.

The logging facilities afforded by the honeyd honeypot identified only connection attempts to ports and gave IP numbers, which lacked richness in the reporting of network activity. The deductions made from these research outcomes were that packet latency could have been occurring, bits may have been disordered, and TCP/IP packets may not have been performing the three-way handshake effectively.

THE EVOLUTION OF WIRELESS TCP/IP FINGERPRINTING

Subsequent testing was performed using TCPdump (Network Research Group, 2004) to capture raw TCP/IP packets and identify where differences were occurring over the wired and wireless mediums for direct comparison. This testing was also conducted in a university laboratory. The results of the fingerprinting showed that of the then current number of 988 OS fingerprints, 6 could only be fingerprinted on the wire and the wireless concurrently. Additionally, 18 OSs could be fingerprinted on most occasions but not effectively over NMAP's variety of queries, leaving a remainder of 964 fingerprints unanswered. The TCPdump captures were imported into the network protocol analyser Ethereal (Combs, 2004) for view of individual packets.

Ethereal revealed that there were no significant differences between TCP/IP packets aside from usual additional wireless overhead. The most significant indication being that there were few errors in these packets. It was then determined that errors were occurring below the layer three networking level and most likely occurring at the data link and physical layers of the OSI model.

AiroPeek (WildPackets Inc, 2003) was subsequently used to perform a wireless packet capture that included lower level activity. The logs of AiroPeek showed a high number of corrupted packets in addition to detecting extremely high packet levels of the university's newly installed wireless mesh network, also functioning in the 2.4 gigahertz spectrum.

Scan times when conducted in the laboratory could be up to 60 hours when performed over the wireless medium. At that stage of the testing, it was not questioned and assumed that this length of fingerprinting was normal although time consuming. It was then decided that the location of the fingerprinting tests should be changed to prevent interference

from the university's wireless network activity. The proposed solution was a decommissioned cool-room, presumably utilised by students in the hospitality courses. The cool-room appeared ideal as it was encased in metal originally for retaining the low temperatures for food consumables. The metal acted as a barrier from the university's wireless interference in addition to keeping in the wireless transmission of the fingerprinting machine and the honeyd honeypot.

Three machines, keyboards and monitors were relocated into the unused cool-room, which acted as a faraday cage. When the machines were powered up to conduct the next round of testing it was found that the temperatures within the once cool-room became excessively hot. The Heating Ventilation Air Conditioning (HVAC) was no longer functioning for that area and air could not be effectively circulated and cooled to allow the machines to operate. While the cool-room acted as a faraday cage effectively to fend off gratuitous wireless traffic, the new problem of temperature regulation had to be dealt with.

It was then proposed to build a faraday cage using a metal cabinet, based on the same premises of the cool-room not allowing the ingress or egress of wireless traffic. A security lecturer at the university had already ordered some metal cabinets for storage and the idea was conceived to utilise and transform one of the cabinets into a faraday cage. The cabinet had previously been purchased at AUD $300 with dimensions of 1.74 metres in height, 0.6 metres in width, and 0.66 metres in depth. These dimensions were not chosen for the purpose of the faraday, they were merely what was available in the university for use. However, these dimensions proved to be ideal to conduct the TCP/IP fingerprinting.

The earlier difficulties regulating the air temperatures in the cool-room were then addressed by drilling a hole at the top of the rear wall of the cage. A small hole was also made in the left, rear corner to allow cabling to pass into the faraday cage and provide outside connection. An earth was also attached to the chassis of the cage to allow any static charge to dissipate into a safe outlet. The fan that was attached was a large sized computer fan, which later proved too small to push air out and retain a cool enough temperature within the faraday to allow three machines to run. Two larger fans were then installed, which costed about AUD $50. One remained at the back wall pushing air out while one was drilled and attached to the bottom back wall to suck air in. The fans were both PAPST-brand Megafans purchased from a local wholesaler. Their diameters were 119 millimetres each, which allowed them 1799 Revolutions Per Minute (RPMs) of rotation. The airflow equated to approximately 27.78 litres of air flow a minute. The noise levels of the fans were as low as 28 decibels.

When the faraday cage was built, the machines were re-entered in. A Keyboard Video Monitor (KVM) switch was utilised to minimise cabling into the faraday. The holes allowing cabling and the fans to operate were large enough to serve their purposes and were not too large to allow the 802.11b RF to seep in or out. This setup allowed just the two PC towers to reside in the cage at 0.44 metres each in height, 0.016metres in width, and 0.45 metres in depth. Their subsequent dimensions did not affect the temperature regulation. The third machine was an IBM laptop, which sat ontop of the two towers.

The resulting total air flow within the faraday, with all the machines inserted, was calculated by the number of litres air flow (27.78) multiplied by 60 seconds, which equalled to 1666.8 litres per minute. This amount is equivalent to 1.6668 cubic metres per minute. When the machines were entered into the cage, the AiroPeek packet capture was run to determine if external 802.11b wireless activity could be detected. AiroPeek did not identify any wireless activity when the cage doors were shut. The machines were then powered up and AiroPeek was able to detect the 802.11b beacons that were being transmitted from the honeypot.

From the beacons, the packet capture identified the Service Set Identified (SSID), which is the name of the network, the Medium Access Address (MAC) and other distinguishing characteristics that aid the identification of the wireless network properties. These properties are beaconed to allow other wireless stations to identify with and connect to, and perform the TCP/IP fingerprinting. Furthermore, ther machines inside the faraday still resembled an open air configuration where they were able to connect via the honeypot's AP.

OUTCOMES OF THE NEW FARADAY CAGE

The subsequent configurations of the new faraday cage proved to be highly beneficial in the outcomes of TCP/IP fingerprinting. The most significant change was the dramatic drop in time to conduct each individual scan. All times fell between a few seconds to no more than two minutes. RF waves were not able to pass through the metal walls and continue their transmission in a directional path. The university's wireless mesh was not able to penetrate through the walls of the faraday and interfere or dilute the wireless transmissions within the cage.

If packet latency was decreased, the machines may not have needed to continuously resend packets reducing packet overloading, which could have previously resulted in a denial of service on the honeypot. The honeypot may not have been able to process packets efficiently when it did not receive sufficient data to send a response. The attack machine may have subsequently kept resending packets attempting to illicit a fingerprint response from the honeypot.

The containment of wireless transmission space most likely allowed both the honeypot and attack machine to exchange packets in a timely manner. However, while the scan times were improved, not all the OSs in honeyd could be

fingerprinted even in the faraday cage. This result was reflective of NMAP's inability to fingerprint all OSs on the wired Local Area Network (LAN) and therefore, would not be likely to fingerprint all OSs via wireless transmission. The goal of the fingerprinting tests however, were to determine a sufficient number of OSs that could then later be configured to emulate fully operational devices in honeyd (Provos, 2004). Additionally, the AiroPeek capture still detected some corrupted packets, which could mean that altered data bits carried on the RF waves may not be avoidable.

CONCLUSION

TCP/IP fingerprinting is one effective method for an attacker to discover OS devices for possible target. It's usage over wired mediums have shown it to be a strategic method of exploit and the subsequent development of honeypots adopting countermeasures. The transition of TCP/IP fingerprinting to the wireless environment however, has revealed difficulties in the handling of packets over the RF waves.

Testing TCP/IP fingerprinting over the wireless medium has proven to be a cycle of discovery where once a university laboratory was perceived to be an appropriate testing location. Results quickly indicated that numerous interfering variables such as other wireless traffic and physical obstacles prevented the efficient transmission of packets. The confines of a metal cage were then conceived as an ideal testing environment. The subsequent utilisation of the faraday cage allowed wireless testing of TCP/IP fingerprinting between the honeyd honeypot and an attack machine utilising NMAP.

Results of testing inside the faraday cage included vastly improved scan times, which were reduced from 60 hours down to two minutes in some cases. This phenomenon was attributed to the cage peripheral being confined in space to disallow wireless packet transmissions to dissipate and scatter beyond the reception of the honeypot's antenna. Additionally, it appeared that the outside wireless network transmissions were eliminated from the cages as they could not penetrate through the metal construct. The implications of such a result highlights the value of using a faraday cage, in which it's construction was very simple and inexpensive, for wireless TCP/IP fingerprinting.

The importance of effective TCP/IP fingerprinting over a wireless environment is imperative to constructing a honeypot that can deceive an attacker seeking a wireless entry point into an organisation's network. Wireless honeypots that are deployed may alert an organisation to the unsolicited connection of wireless stations or devices. Attackers that intentionally attempt connections to a wireless network may perform reconnaissance techniques to determine the nature and topology of the network in addition to locating individual hosts that may be compromised. The first stage to this endeavour is often a TCP/IP scan to identify host OSs. Therefore, a wireless honeypot that can effectively countermeasure this technique may contain the attacker's attempts and later also provide forensic evidence of the compromise.

Building a faraday cage that is both economical and easy to construct is part of the development towards network countermeasures against wireless attacks. A testing environment that is able to eliminate confounding variables allows researchers to experiment and explore varying defence mechanisms for countermeasures that can be singled out at the physical layer, data link layer, and network layer as has been the process of discovery in this research. It is intended that when upper layer protocols and applications are added to the honeyd honeypot, the faraday will act as a great assistance towards identifying and distinguishing where errors are occurring and where deceptive mechanisms are failing. The faraday allows for more apparent insight into the complex and intricate workings of wireless attack and subsequent defence.

REFERENCES

Combs, G. (2004). Ethereal (Version 0.9.14) [Network packet analyser].

Deraison, R. (2003). Nessus (Version 2.0) [Network vulnerability scanner].

Gupta, N. (2003). *Is honeyd effective or not?* Paper presented at the 1st Australian Computer, Information and Network Forensics Conference, Scarborough, Western Australia.

Honeynet Project. (2004). *Know your enemy: Learning about security threats* (2nd ed.). Boston: Addison-Wesley.

Network Research Group. (2004). TCPdump (Version 3.8.3) [Network traffic viewer].

Provos, N. (2004). *Honeyd - network rhapsody for you*. Retrieved 12 February, 2004, from http://www.citi.umich.edu/u/provos/honeyd/

Savage. (n.d.). Queso (Version no version) [Fingerprinting tool].

Spitzner, L. (2002). *Know your enemy*. Indianapolis: Addison-Wesley.

Valli, C. (2003). *Honeyd - a fingerprinting artifice.* Paper presented at the 1st Australian Computer, Information and Network Forensics Conference, Scarborough, Western Australia.

WildPackets Inc. (2003). AiroPeek (Version 2.0) [Wireless packet capture]. Walnut Creek, California.

Yarochkin, F. (2005). NMAP: network mapper (Version 3.75) [Network exploration tool and security scanner].

Yarochkin, F., & Arkin, O. (2003). Xprobe2 (Version 2.02) [Fingerprinting tool].

Yek, S. (2003, 25 November). *Measuring the effectiveness of deception in a wireless honeypot.* Paper presented at the 1st Australian Computer Network & Information Forensics Conference, Scarborough.

Yek, S. (2004, 26 November). *Implementing network defence using deception in a wireless honeypot.* Paper presented at the 2nd Australian Computer Network, Information and Forensics Conference, Fremantle.

COPYRIGHT

Suen Yek ©2005. The author/s assign the School of Computer and Information Science (SCIS) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCIS & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.