Network Penetration Testing and Research

Brandon F. Murphy

NASA. John F. Kennedy Space Center

Major: Computer Science

Program USRP Summer

Date: July 30 2013

Network Penetration Testing and Research

Brandon F. Murphy
North Carolina Agricultural and Technical State University
Greensboro, North Carolina, 27411

Nomenclature

IT	= Information Technology
UI	= User Interface
OS	= Operating System
GNOME	= GNU Network Object Model Environment
IP	= Internet Protocol
TCP	= Transmission Control Protocol
UDP	= User Datagram Protocol
FDDI	= Fiber Distributed Data Interface
ISDN	= Integrated Services Digital Network
PPP	= Point-to-Point Protocol
SLIP	= Serial Line Internet Protocol
WLAN	= Wireless Local Area Network
ISN	= Integrated Supply Network
LAN	= Local area network
WEP	= Wired Equivalent Privacy
WPA	= Wi-Fi Protected Access
WPA2/PSK	= Wi-Fi Protected Access II
CPE	= Common Platform Enumeration
PTW	= Pyshkin, Tews, Weinmann
ARP	= Address Resolution Protocol
FMS	= Fluhrer, Mantin, Shamir
EAPOL	= Extensible Authentication Protocol over LAN
AP	= Access Point
IDS	= Intrusion Detection Signatures
Nmap	= Network Mapper
WPS	= Wi-Fi Protected Setup
NASL	= Nessus Attack Scripting Language
S.E.T	= Social Engineering toolkit

I. Introduction

Network security is a growing field of concern for agencies. The IT Security division is tasked with securing an Agency's network. IT Security can protect a network by testing the network for potential threats, and continuous defense against malicious attacks. Network threats in today's age, are forever changing. Hackers with malicious intent are continually attempting to infiltrate networks to steal information. The best way IT Security can defend against these attacks, is to remain current with hacking methods. Remaining up to date on hacking practices is one of the best defenses.

II. Abstract

This paper will focus the on research and testing done on penetrating a network for security purposes. This research will provide the IT security office new methods of attacks across and against a company's network as well as introduce them to new platforms and software that can be used to better assist with protecting against such attacks. Throughout this paper testing and research has been done on two different Linux based operating systems, for attacking and compromising a Windows based host computer. Backtrack 5 and BlackBuntu (Linux based penetration testing operating systems) are two different "attacker" computers that will attempt to plant viruses and or

exploits on a host Windows 7 operating system, as well as try to retrieve information from the host. On each Linux OS (Backtrack 5 and BlackBuntu) there is penetration testing software which provides the necessary tools to create exploits that can compromise a windows system as well as other operating systems. This paper will focus on two main methods of deploying exploits[1] onto a host computer in order to retrieve information from a compromised system. One method of deployment for an exploit that was tested is known as a "social engineering" exploit. This type of method requires interaction from unsuspecting user. With this user interaction, a deployed exploit may allow a malicious user to gain access to the unsuspecting user's computer as well as the network that such computer is connected to. Due to more advance security setting and antivirus protection and detection, this method is easily identified and defended against. The second method of exploit deployment is the method mainly focused upon within this paper. This method required extensive research on the best way to compromise a security enabled protected network. Once a network has been compromised, then any and all devices connected to such network has the potential to be compromised as well. With a compromised network, computers and devices can be penetrated through deployed exploits.

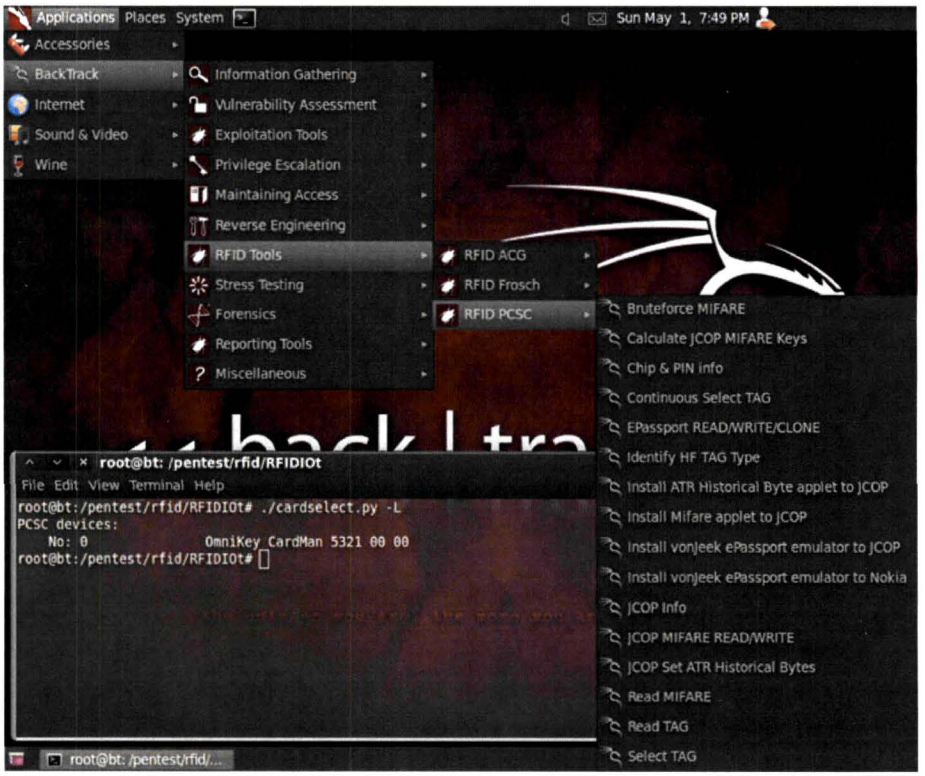
This paper will illustrate the research done to test ability to penetrate a network without user interaction, in order to retrieve personal information from a targeted host.

III. Pentesting Research

Operating Systems

A. BackTrack 5

BackTrack's foundation was built upon Ubuntu. Ubuntu is known for being a very user friendly Linux based operating system. BackTrack uses Ubuntu's UI, but BackTrack is mainly a Linux-based distribution for penetration testing. BackTrack is a great pentesting tool that aids security professionals in the ability to perform vital assessments on computers, and networks within an environment dedicated to hacking. BackTrack as a penetration distribution has been customized down to every package, kernel configuration, script and patch for the sole purpose of the penetration tester.



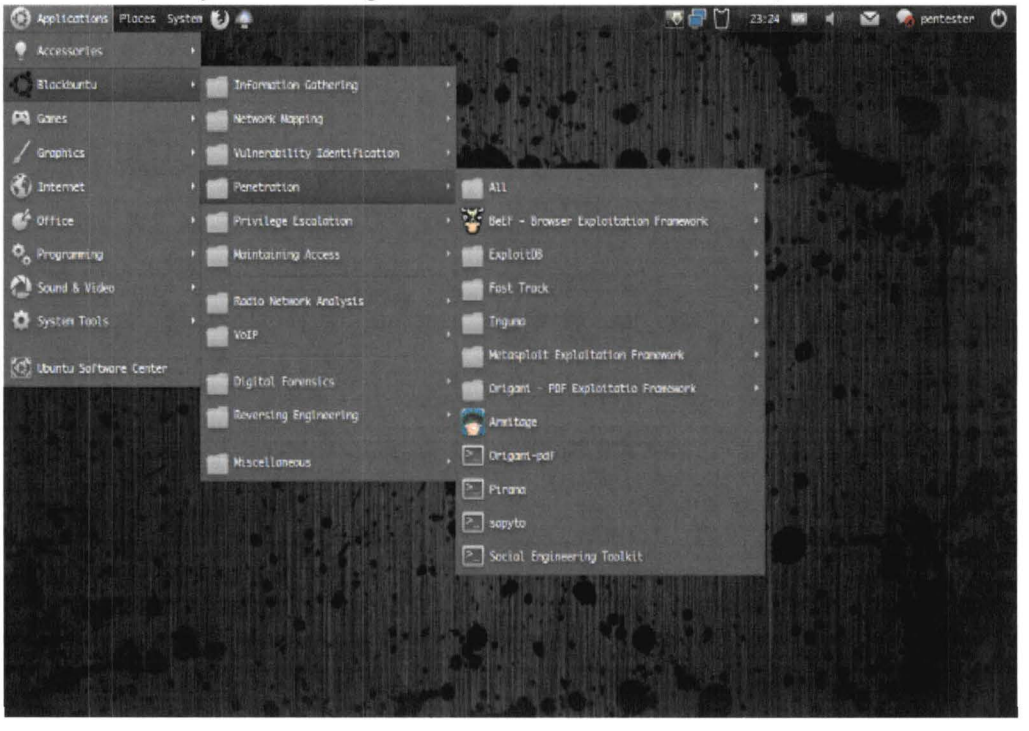
BackTrack was originally designed to be an all in one live CD, used on security audits and was specifically crafted to not leave any fragments of itself on the laptop. BackTrack has expanded to being the most widely adopted penetration testing software frameworks on the market. There are several different features of Backtrack that allows it to be a very useful the tool for security professionals. BackTrack breaks down its pentesting tools into categories. BackTrack pentesting tools are into categories that include Information gathering, Vulnerability assessment, Exploitation tools,

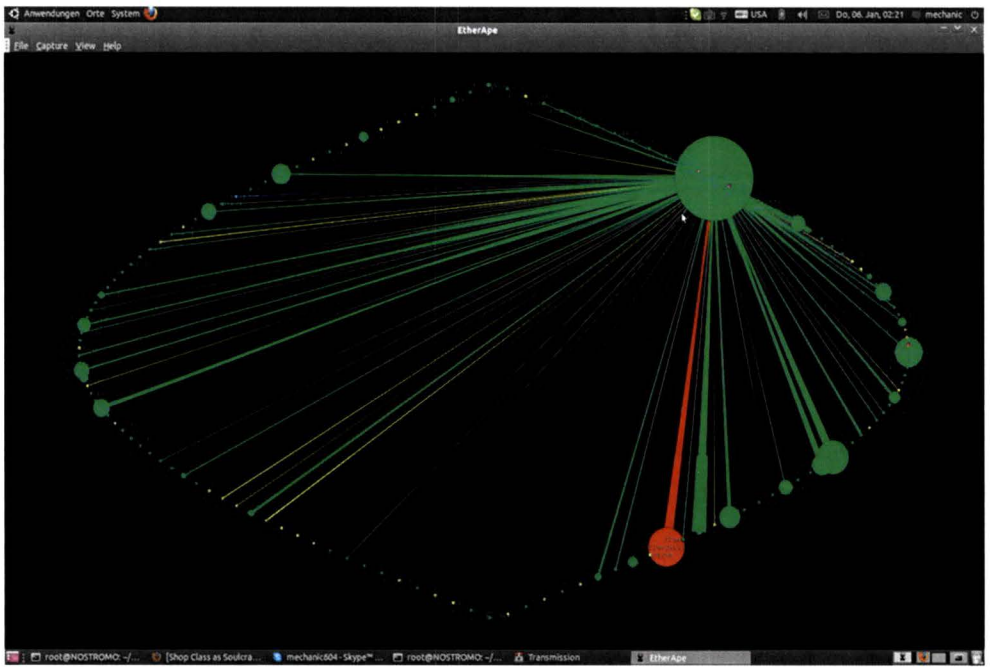
[1] Exploits - is a piece of software, a chunk of data, or sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized).

Privilege escalation, Maintaining access, Reverse engineering, RFID tools, Stress testing, Forensics, Reporting tools, Services, Miscellaneous.
BackTrack includes many well-known security tools including: (To be further explained in other sections)
Metasploit for integration
Wi-Fi drivers supporting monitor mode (raw monitoring mode) and packet injection
Aircrack-ng, Gerix Wi-Fi Cracker, Kismet, Nmap, Ophcrack, Ettercap, Wireshark , BeEF (Browser Exploitation Framework), Hydra, OWASP Mantra Security Framework (a collection of hacking tools, add-ons and scripts based on Firefox), Cisco OCS Mass Scanner (a very reliable and fast scanner for Cisco routers with telnet and enabling of a default password).

B. BlackBuntu

BlackBuntu is a Linux-based distribution for penetration testing. BlackBuntu was specially designed for security training for students and practitioners of IT security. BlackBuntu is penetration testing distribution with a GNOME Desktop Environment. BlackBuntu is currently released using the Ubuntu 10.10 framework build, and reference work from BackTrack. BlackBuntu is currently being built using the Xubuntu 12.04. Xubuntu is a community-developed, GNU/Linux-based, Free/Open Source operating system for personal computers. It is built on a core of the popular Ubuntu operating system and uses the Xfce Desktop Environment. BlackBuntu was designed with Ubuntu users in mind. In retrospect, BlackBuntu is a BackTrack with an Ubuntu look and feel. BlackBuntu comes preinstalled with most of the same tools that BackTrack has to offer, with a few additions of its own. Mostly BlackBuntu gives its users the basic pentesting tools, but if users want other tools then they will have to install them manually. BackTrack would be most preferable to those who are familiar with Ubuntu.





Pentesting software

A. EtherApe

EtherApe is a graphical network monitor for UNIX. EtherApe monitor features link layer, IP and TCP modes, which displays a network's activity graphically. Hosts and links change in size with traffic. Color coded protocols display. EtherApe supports Ethernet, FDDI, Token Ring, ISDN, PPP, SLIP and WLAN devices. EtherApe also uses several other encapsulation[2] formats. EtherApe can filter traffic and can read packets from a file as well as live from the network. Once EtherApe retrieves information, node statistics can be exported into an external file.

B. Aircrack-ng

Aircrack-ng is a network software collection consisting of a network detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11wireless LANs. Aircrack-ng works with many wireless network interface controllers whose driver supports raw monitoring mode. With Aircrack-ng raw monitoring mode, it and can sniff 802.11a, 802.11b and802.11g traffic. Aircrack-ng can run under a Linux and Windows based operating system.

Aircrack-ng can be to used recover a WEP security key once enough WEP packets for a wireless session have been captured using Aircrack-ng's airodump-ng function. The airodump-ng function determines the WEP key (cracking) using two essential methods. The first method is via the PTW approach[3]. PTW is done in two phases. First aircrack-ng only uses ARP packets. If the key is not found, then it uses all the packets that captured to find the key. Users most note that there is an important limitation in using a PTW attack; it currently can only crack 40 and 104 bit WEP keys. The second method uses the FMS/KoreK method[4]. This method incorporates various statistical attacks to discover the WEP key and uses these in combination with brute forcing[5]. Aircrack-ng also comes packaged with a dictionary method for determining the WEP key.

Using Aircrack-ng for cracking WPA/WPA2 pre-shared keys, only a dictionary method is used. A "four-way handshake" is required to retrieve a network security key. For WPA handshakes, a full handshake is composed of four unique packets. Aircrack-ng is capable to work successfully with just 2 packets. EAPOL packets (2 and 3) or packets (3 and 4) are considered a full handshake.

---

[2] Encapsulation is a method of designing modular communication protocols in which logically separate functions in the network are abstracted from their underlying structures by inclusion or information hiding within higher level objects.

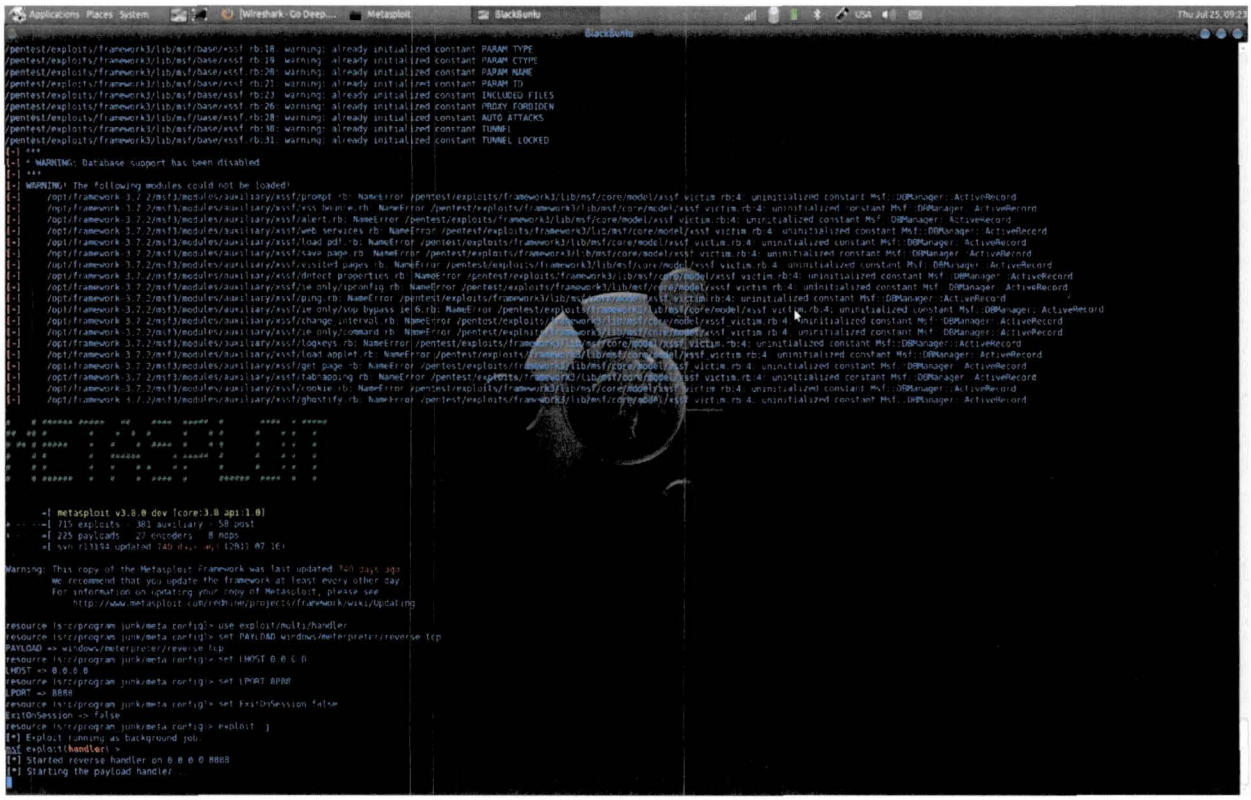
[3] PTW approach decreases the number of initialization vectors or IVs needed to decrypt a WEP key.

[4] The FMS/Korek's WEP Attack is a statistical cracking method for the recovery of a WEP Key. The attack is based on some weakness of the RC4 encryption algorithm well documented in the paper "Weaknesses in the Key Scheduling Algorithm of RC4" from Scott Fluhrer, Itsik Mantin and Adi Shamir.

[5] Brute Forcing is a very general problem-solving technique that consists of systematically enumerating all possible candidates for the solution and checking whether each candidate satisfies the problem's statement.

C. Metasploit

Metasploit is a computer security project that provides information about security vulnerabilities. Metasploit aids in penetration testing and IDS signature development. The Metasploit Framework, can be used as a tool for developing and executing exploit code against a remote target (host) machine or network. Metasploit is also well known for its anti-forensic and evasion tools. Metasploit can be used to reduce the risk of a data breach by downloading our penetration testing solutions. Discovering how vulnerabilities become real risks is a good defense to protecting a network. Metasploit uses the same methods as an outside attacker. Using Metasploit for testing system defenses is more effective if the user uses the same methods that attackers are using in the real world.



D. Zenmap\Nmap

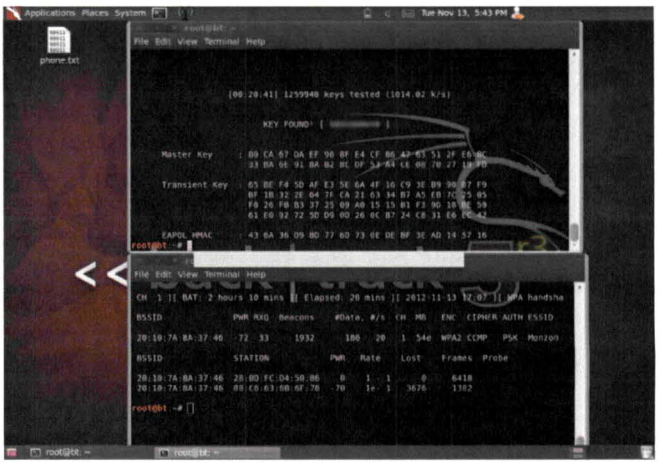
Zenmap is a graphical interface for Nmap the official security scanner. Zenmap is a multi-platform security scanner for Linux, Windows, Mac OS X. Zenmap is a free and open source application which aims to make Nmap easy for novices to use while providing advanced features for veteran Nmap users. Zenmap allows a user to access a command creator, which makes it easy for user to take advantage of Zenmap functions. Zenmap scan results can be saved and viewed later, and later compared with one another to see how they differ. Nmap is a free and open source utility for network discovery and security auditing. Nmap is useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Nmap uses raw IP packets to determine what hosts are available on the network, as well as what services each host are offers, what OS they are running, what type of packet filters/firewalls are being used, and other characteristics. Nmap's has a feature for remote OS detection using TCP/IP stack fingerprinting. Nmap sends a series of TCP and UDP packets to the remote host and inspects nearly every bit in the responses. After performing dozens of tests such as TCP ISN sampling, TCP options support and ordering, IP ID sampling, and the initial window size check, Nmap compares its results to its Nmap OS database of more than 2,600 known OS fingerprints and prints out the OS details if there is a match. Each fingerprint includes a freeform textual description of the OS, and a classification which provides the vendor name, underlying OS, OS generation, and device type. Most fingerprints also have a CPE representation. Nmap was designed to rapidly scan large networks, but works fine against single hosts. Nmap can run on all major computer operating systems.

E. Armitage

Armitage is a scriptable tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework for a user. Armitage organizes the users Metasploit exploit capabilities, into a user friendly hacking process interface. There are features within Armitage for discovery, access, post-exploitation, and maneuver. Armitage's workspaces lets a user define and switch between target criteria quickly and easily. Armitage can also be used to launch scans and imports data from many security scanners. Armitage visualizes the users current targets (located on their network) so they will know what hosts are available for attack. Armitage can recommend to the user exploits and will optionally run active checks to tell them which exploits will work on which host. Once a host system is exploited, Armitage deploys post-exploitation tools built into the Meterpreter agent. With Meterpreter the user can click on a menu where they will escalate their privileges, log keystrokes, dump password hashes, browse the file system, and use command shells of their attacked host.

F. Reaver

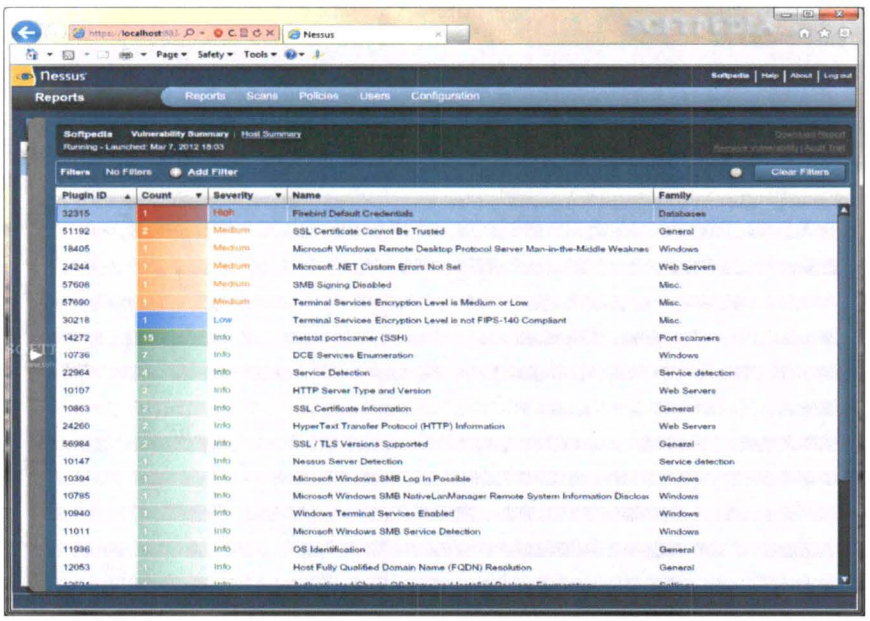


Reaver a Linux based program implements a brute force attack against WPS registrar PINs in order to recover (crack) WPA/WPA2 passphrases. Reaver was designed to be a strong and practical attack agent against WPS. Reaver performs a brute force attack against an AP's WPS pin number. Once the WPS pin is found, the WPA PSK can be recovered and alternately the AP's wireless settings can be reconfigured.

On average Reaver will recover the host AP's plain text version of their WPA/WPA2 passphrase in 4-10 hours. The time it would take Reaver to recover the passphrase, depends on how complex the user set their passphrase.

G. Nessus

Nessus is a comprehensive security and compliance auditing tool with automatic monitoring auditing of configurations, patches, and web applications. Nessus is free of charge for personal use in a non-enterprise environment, but is available for purchase for companies who which to utilize its capabilities. Nessus's goal is to detect potential vulnerabilities on the tested systems. Nessus allows the user to scan for the following types of vulnerabilities:



Vulnerabilities that allow a remote hacker to control or access sensitive data on a system.

Misconfiguration (e.g. open mail relay, missing patches, etc.).

Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack.

Denials of service against the TCP/IP stack by using mangled packets

Nessus operations begin by, doing a port scan with one of its four internal port-scanners to determine which ports are open on the target system and then tries various exploits on the open ports. Nessus has vulnerability tests, available for subscriptions, optimized for custom network interaction. Nessus has vulnerability tests which are written in NASL a scripting language, specific to Nessus.

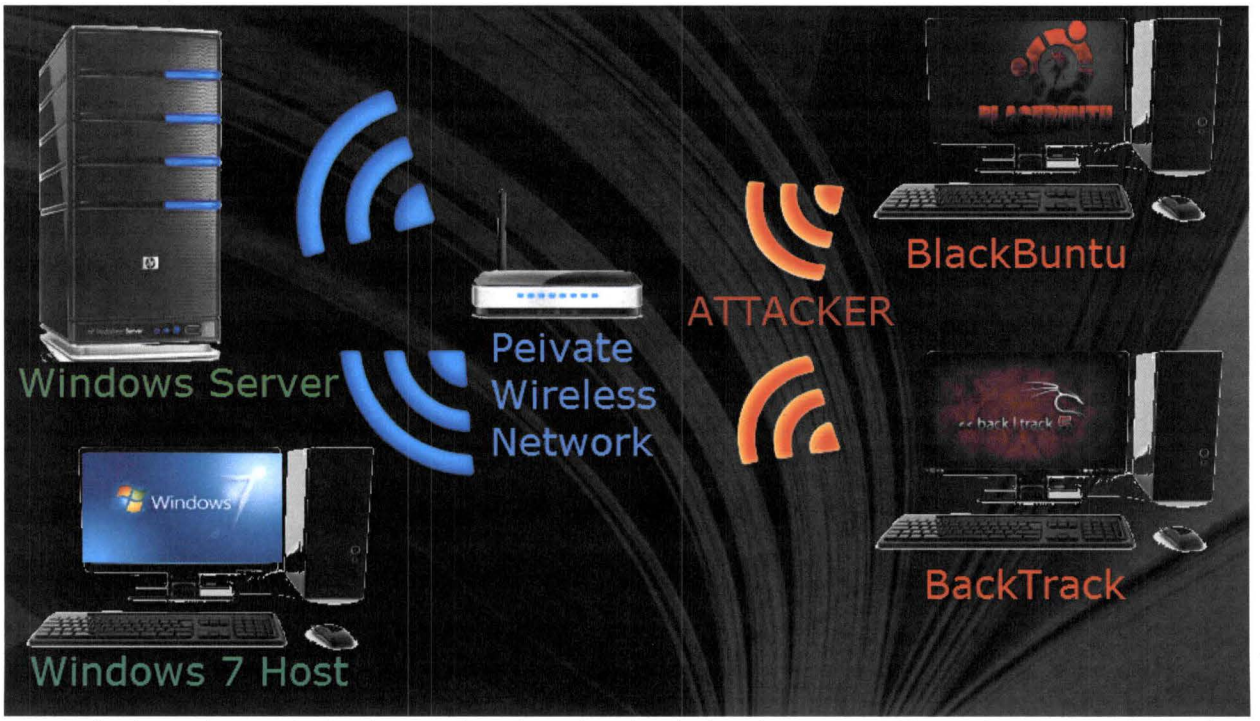
IV. Project Plan

The research project plans were to find a way to infiltrate a user's or agencies Network, and retrieve information. Research had to be done to find numerous ways of infiltration that are used in today's hacking practices. With this knowledge testers are to set up their own private network (ideally mimicking the current agencies network), and then scan and test for system and network vulnerabilities.

In addition to this project plan researchers where to look into ways of infiltrating a network without user interaction. Upon completion of this research, a compiled a list of recommended software, tools and pentesting methods will be given to the IT security department for review for future testing purposes.

V. Testing

A. System Set Up



To begin testing, an isolated network and workstation had to be set up. This workstation consisted of one Windows 2008 server, one BackTrack 5 Linux system (Attacker), one BlackBuntu Linux system (attacker), and two Windows 7 PCs (Hosts). The Windows 2008 server and the two Windows 7 PCs we're connected to their own private network, as to simulate or represent NASA's current private network. BackTrack and BlackBuntu were not connected to this private network or any other network as to simulate outside attackers. Their addresses were set statically.

Backtrack is a fairly simple operating system to maneuver. Its layout is well organized and comes fitted with many useful tools for pentesting. Most software provided by BackTrack required research to implement, but otherwise was pretty straight forward. BlackBuntu was easy to adapt to for it is closely related to the Ubuntu operating system. With prior experience of Ubuntu, BlackBuntu is the easy tool for beginning learners of pentesting. Though it doesn't come preinstalled with as much software as BackTrack, BlackBuntu allows the user to manually install the software at no additional cost. One can utilize BlackBuntu just as they would BackTrack.

B. Initial testing

1. S.E.T

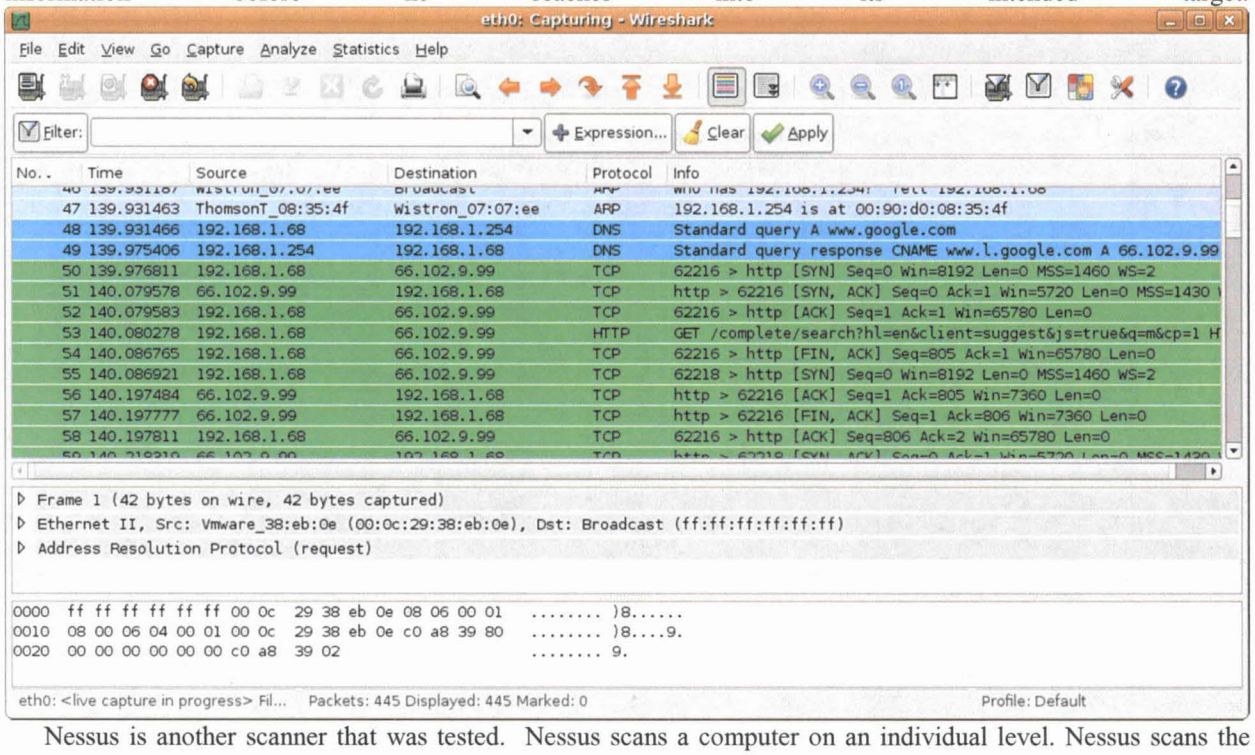
In the beginning stages of testing research is done on how to socially exploit a user's system. The choice to socially exploit user system is because user interaction is easily applied. For instance it would be easier for a user to click on a program and let a hacker into a system rather than a hacker manually infiltrate the system without the user interaction. The way this exploit works is a hacker makes or downloads an exploit and deploys it in a common area where a user will unknowingly click on such exploit. Hackers usually disguised to exploit common programs and or sites that users commonly use. Depending on the exploit hacker can gain access to the user's computer and network in which it is connected. Once a hacker has access to both the system and network the hacker then has the ability to retrieve information from the system and network to use for their purposes. Such exploits can be created through Metasploit using its S.E.T function. With Metasploit's S.E.T function a user can create an exploit with certain properties that allow them to take over a user's computer without their knowledge. On our dedicated system we were able to specifically deploy an exploit onto one of our native Windows 7 host computers virtually undetected. With this exploit successfully deployed on both Linux systems research results show that we were able to access and retrieve files from our target. Note at this point our host computers do not have any antivirus and or firewall activated. Upon the completion of these tests, antivirus and firewall were installed and turned on both windows system to simulate security of NASA known systems. Upon applying these security measures, and running the antivirus program this system quickly picks up on the exploit that was deployed on both systems. With a more advanced exploit that is designed to cloak its activities, a hacker will then be able to get around such security measures.

2. Network mapping

In order to identify devices that were on our private network we use certain mapping tools that allowed us to see what devices were connected to our networks as well as they're open ports, operating system and vulnerabilities that they had. EtherApe has a specific mapping tool that allows researchers to view the traffic in an out of network. EtherApe displayed in visual map of the requested data going across the network. This map displays all devices connected to the network and their communications back and forth to each other. With this information BackTrack and BlackBuntu could then identify (through manual implementation) each computer or device and see their potential vulnerabilities on each operating system.

Another mapping tool tested was Wireshark. Wireshark allows researchers to do intensive mapping across the network. Information gathered from Wireshark illustrates all packages and data being transferred across the

network. Information as to who is requesting information from whom, was each requested answered by the receiver, was each requested responded to, etc. With this information hackers could use this as a mode to intercept information before he reaches into its intended target.



Nessus is another scanner that was tested. Nessus scans a computer on an individual level. Nessus scans the device that it is installed on, and searches for vulnerabilities and rates them for their level of threat potential. Nessus can be used on a system to see where it's vulnerable, and help individuals see where they would have to focus more on security.

3. Brute Force Attack

After continuous research on how to socially exploit a user's system, it was decided that a brute force attack would be most effective in infiltrating a user system without their knowledge. The project plan was to find a way to gain access to the private network by stealing the networks Wi-Fi security key. With the private network security key, the simulated hacking computers will be able to map the entire network all devices connected to the network and potentially exploit all devices on the network. After much research it was found that network systems secured with WEP were easily hackable. Using basic functions within both backtrack and BlackBuntu our Wi-Fi key was determined. It was also understood that WPA and WPA2 were the most secure network encryption types. After compiling all research on this subject, Reaver was the best possible option for retrieving a WPA and WPA2 security key. Documentation on Reaver shows that it uses a modified version of Aircrack-ng. Reaver takes advantage of Aircrack-ng's functionality, but takes time. After proper installation, and run a few procedural commands Reaver takes hours but has the potential to crack a WPA or WPA2 security key.

VI. Issues

We were faced with a number of issues throughout the research process. The initial setups for some systems stalled and were unresponsive. The most notable issue that was faced, were system updates. System updates were imperative for most applications to work. These applications required that the OS, required plugins, or outdated features be updated. Unfortunately, NASA's security measures prevented such updates from being possible. This means that NASA's security infrastructure is very reliable.

VII. Conclusion/Results

To conclude there are many tools that can be useful to the IT security department. EtherApe is a good tool to visualize the network. A user can see the entire network as a web, as well as show them the amounts of traffic that is being requested. Armitage could be a useful tool, for testers to see if they can deploy in house exploits across the

network without detection. If this is possible then testers will be able to reverse engineer their exploit in order to patch their systems vulnerabilities. With a fully up to date system Reaver would be a very effective tool. When Reaver meets its requirements it can retrieve a WPA or WPA2 security key. If so, then IT Security may want to look into mode advanced firewalls and or brute force attack recognizers.

Acknowledgments

I would like to thank the NASA KSC Education office for giving me this opportunity to attend this summer's internship program. I would also like to thank Software Systems Assistant Tamiko Fletcher, IT Project Manager David Campbell, Chief Information Security Officer and IT Security Office Chief Henry Yu, for giving me the opportunity to work in their division. Their help and guidance help me to learn and accomplish all that has been reported in this paper. I would also like to thank the department's staff. The staff members were very helpful with answering any questions that I had, and they offered their support.

References

[1] BlackBuntu
URL: http://www.blackbuntu.com
URL: http://www.blackbuntu.com/about
URL: http://www.linux.com/directory/Distributions/security-enhanced/blackbuntu

[2] Xubuntu
URL: http://xubuntu.org/
URL: http://xubuntu.org/about/
URL: https://en.wikipedia.org/wiki/Xubuntu

[3] Backtrack 5
URL: http://www.backtrack-linux.org/
URL: http://www.backtrack-linux.org/about/

[4] Etherape
URL: http://etherape.sourceforge.net/
URL: http://etherape.sourceforge.net/introduction.html

[5] Metasploit
URL: http://www.metasploit.com/
URL: http://en.wikipedia.org/wiki/Metasploit_Project
URL: http://www.rapid7.com/products/metasploit/
URL: http://www.rapid7.com/products/metasploit/editions-and-features.jsp?p=features_list

[5] Zenmap
URL: http://nmap.org/zenmap/
URL: http://nmap.org/

[6] Aircrack-ng
URL: http://www.aircrack-ng.org/
URL: http://en.wikipedia.org/wiki/Aircrack-ng
URL: http://www.aircrack-ng.org/documentation.html

[7] Nessus
URL: http://www.tenable.com/products/nessus
URL: http://www.tenable.com/products/nessus/features#tabs-1
URL: http://www.tenable.com/products/nessus/features#tabs-2

[8] Reaver
URL: https://code.google.com/p/reaver-wps/
URL: https://code.google.com/p/reaver-wps/wiki/README

[9] Armitage
URL: http://www.fastandeasyhacking.com/