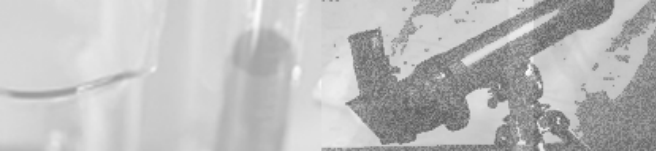
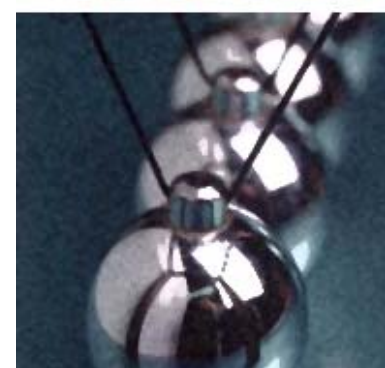


Internet Security

Attack & Penetration

Jack Heyman





Objective of this Presentation

Learning about Attack and Penetration is very encompassing. It requires an extensive amount of time and display in order for one to gain an acute understanding. Thus, the **objective** is to provide a *high-level overview, along with many URL links so that one could leverage those websites for future reference.*

Agenda

1. Types of Network Penetration Tests
2. Terms
3. Methodologies Used
4. Sources for Tools
5. Pre-Testing Tips
6. Phases of The Attack
7. Other Sources
8. Conclusion



Types of Network Penetration Tests

- Network
- Web application
- Remote
- Wireless
- Social engineering
- Physical



Terms

- Threat – something that can cause harm
- Vulnerability – A flaw that can be exploited
- Exploit – A flaw has been compromised
- Active Attack – exploits and manipulates
- Passive Attack – exploits but does not manipulate





Terms

- Ethical Hacking – Identifying and exploiting vulnerabilities with permission
- Penetration Testing – Identifying and exploiting targeted vulnerabilities (specified areas of scope) with permission



Terms

- Vulnerability Assessment – Identifying without exploitation
- Security Audit – Identifying vulnerabilities against audit standards (e.g. NIST)





Methodologies Used

There are 4 primary methodologies used for performing Attack & Penetration Tests:

1. Open Source Security Testing Methodology Manual (OSSTMM)
 - www.isecom.org/osstmm
2. NIST Special Publication 800-42: Guideline to Network Security Testing
 - <http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf>





Methodologies Used

3. Open Web Application Security Project (OWASP)

- www.owasp.org/index.php/OWASP_Testing_Guide_v2_Table_of_Contents

4. Penetration Testing Framework

- www.vulnerabilityassessment.co.uk/Penetration%20Test.html



Sources For Tools

1. Milw0rm

- www.milw0rm.com

2. Packetstorm Security

- <http://packetstormsecurity.org>

3. Hackerstorm

- www.hackerstorm.com

4. Secunia

- <http://secunia.com>



Sources For Tools

5. United States Computer Emergency Readiness Team (US-CERT)
 - www.us-cert.gov/cas/techalerts
6. Mitre
 - <http://cve.mitre.org>





Pre-Testing Tips

- Disable firewall on PC to be used in testing (uninhibited results)
- Remove all personal and sensitive data from testing PC
- Inform Internet Service Provider
- Nondisclosure Agreement (NDA)
- Permission Letter (in case something bad happens)
- Insurance Requirements



Pre-Testing Tips

- Rules of Engagement
 - Defining scope
 - Contacts
 - Testing known or surprise
 - Can data be viewed (e.g. Privacy issues may be different depending on location of data)
 - 3rd Party management
 - Test vs. Production
 - Social Engineering



Phases of The Attack

1. Reconnaissance
2. Scanning
3. Exploitation



Phases of The Attack

Reconnaissance

The objective is to gather information from public sources for the upcoming attack



Phases of The Attack

Reconnaissance

- Use search engines to gain information (e.g. Location of sites, personnel, etc.)
- Use Job boards to identify job openings (e.g. looking for a Security Administrator with experience in CheckPoint – now you know the firewall type)



Phases of The Attack

Reconnaissance

- People Search (e.g. Yahoo)
- Google Maps (to identify location for physical attack)



Phases of The Attack

Reconnaissance

- Whois
 - Provides address ranges
 - DNS information
- Regional Internet Registries (RIR)
 - Points of contact
 - Network address space



Phases of The Attack

Reconnaissance

- DNS Lookups (Queries)
 - Maps names into IP addresses
 - Zone transfers



Phases of The Attack

Scanning

The objective is to learn more about the target's technologies deployed



Phases of The Attack

Scanning

Types:

- Network Sweeps
 - Identifies IP addresses
- Network Traces
 - Maps network topology
- Port Scanning
 - Identifies ports that are open



Phases of The Attack

Scanning

Types:

- OS Fingerprinting
 - Identifies operating system types
- Versions
 - Identifies versions deployed
- Vulnerability Scans
 - Generates listing of known vulnerabilities



Phases of The Attack

Scanning

Scanners to utilize:

- TCPdump
 - www.tcpdump.org
- Windump
 - www.winpcap.org/windump/default.htm
- Hping
 - www.hping.org



Phases of The Attack

Scanning

Scanners to utilize:

- Layer Four Traceroute (LFT)
 - <http://pwhois.org/lft/>
- Nmap
 - www.insecure.org
- AMAP
 - <http://freeworld.thc.org/thc-amap>



Phases of The Attack

Scanning

Scanners to utilize:

- Nessus
 - www.nessus.org
- Retina
 - www.eeye.com



Phases of The Attack

Scanning

Scanners to utilize:

- Superscan
 - www.foundstone.com
- Saint
 - www.saintcorporation.com



Phases of The Attack

Exploitation

Exploitation is gaining access to a target machine with the goal being: gain control and do what you want.

There are many tools that can be utilized and most of them can be extremely dangerous. Extreme caution should be employed if any of these tools are deployed.



Phases of The Attack

Exploitation

Tools to utilize:

- Microsoft baseline Security Analyzer (MBSA)
- Metasploit
- Netcat
- Netstumbler
- PWDump



Phases of The Attack

Exploitation

Questions: What should you do once you have exploited the system?

Answer: Obtain the password file for a complete takeover (you will be able to do what you want).



Phases of The Attack

Exploitation

Tools to utilize in cracking the password file:

- Keyloggers
 - www.spectorsoft.com
- John the Ripper
 - www.openwall.com/john



Phases of The Attack

Exploitation

Tools to utilize in cracking the password file:

- Cain
 - www.oxid.it
- Rainbow Tables
 - www.antsight.com/zsl/rainbowcrack



Other Sources

- www.sans.org
- www.pauldotcom.com
- www.samspade.org
- www.geektools.com
- www.whois.net
- www.DNSstuff.com





Other Sources

Regional Internet Registries

- North America
 - www.arin.net
- Europe, Middle-East, and Central Asia
 - www.ripe.net
- Asia and Pacific Region
 - www.apnic.net



Other Sources

Regional Internet Registries

- Latin America and Caribbean
 - www.lacnic.net
- Africa
 - www.afrinic.net





Conclusion

Performing an Attack & Penetration is a very detailed and arduous engagement. My goal was to provide a very high level overview of the process for performing such an engagement, along with supporting links.

Performing such a review requires extensive skill and experience because the risks of destruction are too high. As such; I hope this presentation sheds some light on how extensive and detailed such an engagement can be. Should you be faced with a tester performing such a review; this presentation shall be a starting point to ensure the test team is acting with care and due diligence. This presentation shall also serve as a starting point for those wishing to learn more about the testing process.



What are the critical security vulnerabilities and can they be mitigated to an acceptable level of risk; or will people constantly be held hostage by hackers?

Jack L. Heyman

What are the critical security vulnerabilities?

Prior to describing the critical security vulnerabilities; it is necessary to define vulnerability. Vulnerability is a weakness that can be exploited if not appropriately safeguarded. For the confines of this paper, a *security* vulnerability is a weakness within Information Technology (e.g. firewall, PC, etc.) that must have adequate controls in place in order for the level of risk to be acceptable. A simple example is whether or not a person should lock their car door in a neighborhood that has recently experienced high car theft. The crime rates will impact the risk level of that vulnerability. The controls put in place (e.g. locking the door or installing an alarm) will reduce the risk of the vulnerability being exploited.

This section of the paper will describe the critical security vulnerabilities by type. For each of the security vulnerability types, an explanation of the critical vulnerability will be explained, along with mitigating controls to be placed in operation for the risk to be acceptable. The following table lists the critical security vulnerability types:

Table 1: Critical Security Vulnerability Types

Critical Security Vulnerability Types	
1	Personal Computer (PC) Security
2	Wireless Networks
3	Firewalls
4	Server Security

Throughout this paper, the critical security vulnerability types will be displayed in tables along with their appropriate sub-types. PC security is the first of the security types; as this is usually the first access point used for gaining entry to a network.

Personal Computer Security

Table 2: PC Security Vulnerabilities

Critical Security Vulnerability	
1	Improper hardening of the PC

The PC is usually the first entry point onto a network and as such, it is critical to ensure that PCs are hardened (secured) appropriately. If a PC is not appropriately secured; a user runs the risk of their authentication credentials being compromised and subsequently utilized as an exploit such as identity theft. It is unfortunate, but there are very basic and fundamental security parameters that should be deployed on all PCs, and yet in many large organizations it is relatively easy to compromise a PC. The following are a list of the fundamental vulnerabilities and their explanations for securing a PC:

Table 3: PC Vulnerabilities – Improper Hardening of the PC

#	PC Vulnerability	Description
1	Guest accounts should be disabled.	If a user has authenticated to their user account successfully, their id can still be compromised. To compromise the PC, simply reboot the computer and hit the Escape (Esc) key so that the PC defaults to the Guest account. For further details on how to compromise the data; refer to PC

		Vulnerability number 5.
2	Screen savers should be enabled.	Without the use screen savers, a user that has authenticated to a PC can be compromised while the PC is unattended (e.g. when the user is out to lunch).
3	The order of boot should be modified.	Typically, PCs boot to the Compact Disk Read-Only-Memory (CD-ROM) prior to the C drive. When the PC boots, a Windows boot disk can be placed in the CD-ROM tray so that authentication can bypass the user authentication screen.
4	Run should be disabled.	Having Run enabled allows a user to run programs that may cause adverse harm to the user or network.
5	Adding and removing programs should be disabled.	This vulnerability is where the exploit may occur, which ultimately impacts the user and the network. There are many software applications that can be utilized to gain authentication credentials or privacy related data. For example, Cain software is a sniffer as well as a password cracker. This can be installed on a PC and used to crack the passwords. Another example is keylogger software. This can be used to record all keystrokes, chats, websites visited, emails and more. By disabling this feature, the user will be prohibited from adding or removing dangerous software applications.
6	Authentication must be required when logging onto a PC.	PCs can be setup so that authentication is not required. If this occurs the PC is wide open for exploits.

As noted above, it is critical to properly harden the PC. For these reasons, the use of public PCs (e.g. cruise ships, kinkos, etc.) are very dangerous. There may be keylogger software installed that can easily capture the user id and password to be exploited at a subsequent date. If

the appropriate controls are not utilized above, it is relatively easy to steal an identity. Let's assume that a publicly traded company has not deployed the controls noted above. A user (such as an employee) could install software such as Cain (password cracker) or SpectorSoft (keylogger software) to obtain the user id and password of an employee. Once this is obtained, the sky is the limit. If that password is the same or similar to other related passwords (e.g. banking sites visited); then identity theft can now occur. Another example is the installation of malware or viruses onto the network via downloading of bad software and data from the Internet. If a user is not prohibited from downloading and installing programs; then control will be decentralized away from the IT department and the organization runs the risk of introducing viruses, worms, and malware to the network via poor PC controls.

Wireless Networks

Many people today are thrilled about the prospects that wireless networks have to offer. Although they provide ease of use as well as availability; there is a high price that must be accounted for. This is a relatively new technology deployed, even though it has become ubiquitous. The following table lists the primary wireless security vulnerabilities:

Table 4: Wireless Network Security Vulnerabilities

Critical Security Vulnerabilities	
1	Improper Service Set identifier (SSID) setting.
2	Modifying the administrative (admin) password for the wireless router.
3	Mapping the wireless router to the PC Media Access Control (MAC) address.

Improper SSID setting

The SSID is the name that is provided when a computer searches for a wireless network. The first action to be taken is to disable the SSID broadcast. This prevents other computers (or users) from seeing your wireless network. That doesn't mean the wireless network is not there; it just means that the computer doesn't present this as one of the wireless networks. The second action to be taken is to change the SSID name. All wireless routers come with a standard name such as Linksys or Netgear. If a user has disabled the SSID broadcast, but hasn't changed the name, then it will be fairly easy to authentication since one of the two means of authentication would be known (the id piece).

Modifying the admin password for the wireless router

All wireless routers come with a standard id and password. The configuration settings are important because one can modify the type of encryption (or disable encryption completely), as well as other key parameters such as the encryption key. If the wireless router is not locked and hardened appropriately; any user who hacks into the wireless router can modify the encryption key and lock out the primary user from their wireless network.

Mapping the wireless router to the PC MAC address:

If one wants to ensure that only intended users are on the wireless network; the wireless router must be locked to a MAC address so that only those PCs with the assigned MAC addresses (identified on the wireless router) can access the wireless router. Even if a user knows the SSID and the user credentials; they will be restricted from gaining access to the wireless network. The only way to circumvent this control is to gain control of the admin privileges over

the wireless router (or sniff the encrypted wireless traffic); thus the reason for deploying all of the controls described above.

What can a user do if they gain access to a wireless network? The dangers of being exposed on a wireless network are identity theft. Using simple hacking software such as Cain, Kismet, or Netstumbler, a user can pull wireless network traffic and decrypt the authentication credentials to be exploited at a subsequent date. These hacking tools are all free and can be downloaded from the Internet with a simple Google search. Furthermore, an individual can even purchase laptop antennas, which increases the range of wireless networks on a laptop. Cain software will also inform the user of all wireless networks within the network vicinity. If a user without IT knowledge is utilizing a wireless network; there is a high probability that they have kept the SSID name the same. A hacker can merely intercept the traffic and decrypt the password via the Cain and Kismet software. It is a bit more complicated because the data will need to be converted from zeros and ones to human readable language; however it is not impossible.

Firewalls

The next vulnerability category concerns firewalls. Once a user has penetrated a user's credentials, the next motive will likely be to breach the firewall. A firewall is a line of defense and can be deployed in a variety of ways. The firewall acts in a similar fashion as the Immigration and Naturalization Service (INS). The firewall is the officer at the front gate. It is there to determine if the traffic is suspicious as well as possessing the appropriate credentials. Similarly, a person trying to enter the United States must have a visa if they are from a country where the United States requires one. If the person has the unexpired visa; they will be permitted to enter. Conversely, if the person doesn't have the visa, they will not be permitted into the

United States. If a person attempting to enter the United States is acting very nervous and out of the ordinary; the INS officer may be alerted to provide more questioning. These are all similar in nature to a firewall. Data traverses via ports, protocols, and services. This is similar to airports and ports. Planes cannot land in the port of Miami, just like boats cannot dock in Miami International Airport. There are 65,565 ports that can be used for how data traverses from one network to another. The means by which the data traverses is by an appropriate protocol. The firewall inspects the data in terms of the IP header, destination port, protocol, as well as payload (depending on the type of firewall). Below is a listing of the critical firewall vulnerabilities.

Table 5: Firewall Vulnerabilities

Critical Security Vulnerabilities	
1	Use of a single firewall
2	Firewall settings are not appropriate

Use of a Single firewall

The first mistake that organizations make is the use of a single firewall. There are three primary categories of firewalls. They are static filter, stateful, and stateful inspection (SI). The following are advantages and disadvantages of the respective firewall types:

Table 6: Firewall Types and Descriptions

Firewall Type	Description
Static	Each packet is examined individually. Examines IP or transport header for source and destination ports and flags. This type of firewall doesn't maintain memory.

Stateful	This firewall is very similar to a static firewall; however it has memory; thus this can be a more efficient firewall.
SI	This firewall type has the features of a stateful firewall; however the firewall examines the payload as well (e.g. understanding the network protocols and making decisions based on the payload).

There are many benefits to using multiple firewalls. A mistake that is commonly made is the use of a single firewall with the notion that the best product can be purchased. This is not necessarily true and the benefits of each firewall type can be deployed effectively. The following represents the advantages and disadvantages of the different firewall types:

Table 7: Firewall Advantages and Disadvantages

Advantages	Disadvantages
Static Firewalls	
<u>Ingress filtering and Spoof Prevention</u> – Blocking specific Internet Protocol (IP) addresses (e.g. source IP of the internal network) is more efficient with the Central Processing Unit (CPU) and system resources than other firewall types. Other firewall types may review the payload and allow the traffic based on that review.	<u>No memory</u> – Because this type of firewall has no memory, it may process the same request multiple times in the same manner; thus utilizing system resources unnecessarily.
<u>No Payload Review</u> – Because the payload is not reviewed, this ensures that the firewall processes requests quickly and ensures movement of data.	<u>No Payload Review</u> – The firewall has no ability to review the payload; thus it may block traffic which shouldn't be blocked.
Stateful Firewalls	
<u>Memory</u> – This type of firewall retains memory in the state table; thus saving time on	<u>No Payload Review</u> – The firewall has no ability to review the payload; thus it may block

future repetitive tasks.	traffic which shouldn't be blocked.
SI Firewalls	
<u>Payload Review</u> – Because the payload is reviewed; this firewall can strategically be placed behind the Demilitarized Zone (DMZ), where a static firewall can be placed at the network border. This enables effective examination of traffic from within the perimeter.	<u>Slow the network</u> – If this type of firewall is positioned incorrectly, it could bring the network to a halt from the overworked examination of the payload (e.g. placed on the border of the perimeter).

As described above, each firewall type offers advantages and disadvantages. Thus the deployment of only one of the firewalls would be a mistake. For example, a good network topology would be to place a static firewall at the border to allow traffic that is explicitly permitted in the firewall rulebase. To increase defense-in-depth principles; a SI firewall could be placed behind the DMZ to effectively examine payloads that have first been scrutinized and permitted by the static firewall.

Firewall Settings are not appropriate

There are several key measures that must be deployed on all firewalls:

- Filter (by prohibiting) any inbound traffic that has a source IP of the internal network. Inbound traffic with an internal IP address can only be a spoof, with exploitation as the motive.
- Block all inbound traffic with loopback as the source IP address. This can also be used for exploitation purposes.
- Block all inbound traffic that originates from a source that is not appropriate:

- A country to which the organization should not be communicating with (e.g. Department of Defense may block all traffic from Iran).
- Source IP addresses that have not been allocated by the Internet Assigned Numbers Authority (IANA).
- Consider modifying 'inspect scripts' within the firewall. A popular Checkpoint Firewall (FireWall-1) is estimated to inspect the payload for approximately ten protocols; where the remaining protocols are handled via stateful packet filtering. In order for the firewall to inspect on all the protocols; the inspect scripts must be modified; however most firewall vendors void the warranty if the inspect scripts are modified.
- Deploy an 'Implicit Deny' rule so that anything not specifically allowed from the firewall rulebase will be denied. This prevents bad traffic from entering the perimeter.
- Disable vulnerable services such as echo, discard, chargen, finger, and daytime services. These services provide information to would-be attackers that can provide reconnaissance data for a future attack.
- Limit Internet Control Message Protocol (ICMP) messages. These messages provide information about the network that can be used for exploitation purposes.
- The firewall should be set to disallow transmissions such as Post Office Protocol -3 (POP) unless it is over a secure means such as Secure Shell (SSH). Sending data via POP-3 is in clear-text. This is very dangerous, because users typically have the same passwords for their personal email (e.g. banking, investments, etc.) as they do for their work emails (or some derivation of the same password). If someone is able to sniff the wire, they could easily

capture a user id and password via the clear-text protocol, which could later be used in an adverse manner.

- Firewalls must be augmented by both a Network Intrusion Detection System (NIDS) and a Host Intrusion Detection System (HIDS). A NIDS is network based, thus the review is more broad-based. The primary advantage is that if an attack occurs; utilizing a NIDS could help identify the cause of the attack. A HIDS is specific in nature and doesn't offer the broad-based review of the packets. The advantage of a HIDS is that because the review is much less; resources are more conserved. Regarding the NIDS, not only the payload is reviewed, but also the packet header; whereas this is not reviewed in a HIDS. Another advantage of the HIDS is that it is behind the DMZ, so data that has entered the network perimeter will likely be decrypted. For this reason, the HIDS can analyze the payload better (in some respects) than a NIDS. For these reasons, it is essential to deploy a NIDS as well as a HIDS at key hardware points on the network.
- Firewalls should also be set so that sensitive or adverse services running on an unnatural port are detected and corrected. For example, Telnet is a service used for gaining access to systems remotely while authentication occurs in clear-text. Telnet usually runs on port 23. If the firewall setting prevents listening on port 23, one may be inclined to think that Telnet is not possible. It is possible to deploy Telnet on a port other than port 23, which in this case would bypass the firewall setting.

Can the security vulnerabilities be mitigated to an acceptable level of risk?

After describing the critical vulnerabilities above; it appears that network administrators and security officers have their work cut out for them. There are many vulnerabilities and they represent an array of different technologies such as servers (e.g. Windows, Unix, etc.), wireless networks, firewalls, and more. The IT profession has become similar to the medical profession. For example, if one has an issue with their foot; they will likely see their general physician, who will then refer them to the podiatrist. The general doctor will likely not be able to answer the concerns of the patient with regards to the foot. This is very similar to the IT profession. The network administrator ensures network connectivity and availability, whereas the security officer is concerned about security violations. The primary way that organizations can attempt to mitigate security vulnerabilities is to have external reviews or audits concerning the most critical software and hardware. This will allow the organizations to ensure specialists and independent parties are testing for vulnerabilities, which in turn will identify remediation efforts to be deployed.

Another way that organizations can ensure vulnerabilities are properly mitigated is for their IT personnel to have adequate training. It is a full-time job identifying new security vulnerabilities and this should be left to the professionals who work on this all year. There are many conferences and workshops where hacking and vulnerability prevention techniques are taught such as by the SANS Institute or Black Hat conferences. These types of venues are ideal for employees to stay abreast of the latest vulnerabilities, where they can then deploy the latest techniques in order for there to be mitigating controls in place.

Regarding the question of whether security vulnerabilities can be mitigated to an acceptable level of risk; the answer is yes. However, the answer is predicated on the time

sensitivity of vulnerabilities. Organizations can deploy the proper techniques to mitigate security vulnerabilities to an acceptable level of risk; however this is only as of a point in time. If there is a new vulnerability to which the organization hasn't yet mitigated; then this can be exploited, which brings up another question to be addressed in the next section.

Will people be held hostage to hackers or can there be a sufficient degree of controls in place to safeguard critical data?

Unfortunately, the answer to the question above is that there will be a constant battle between those trying to protect data, and those trying to access the data in an unauthorized manner. Being held hostage by hackers implies that organizations will not have the wherewithal to combat the current or future threats. Organizations will not be held hostage to hackers; however they *must* deploy the proper preventive, detective, and corrective controls and stay abreast of the latest threats and vulnerabilities, or else they will fall victim to hackers.

As most organizations' servers are connected to the Internet in some fashion (e.g. DMZ, firewall, proxy server, etc.); they can become exposed to attackers fairly quickly. Hackers don't need to be at a terminal attempting to attack one by one. If an organization has a port with known vulnerabilities attached to the Internet there is a good chance it will be attacked within one hour. For these reasons, as well as the vulnerabilities listed above; it is essential and imperative that organizations ensure their systems are hardened. Although organizations and people are not necessarily held hostage to hackers; this is a very thin line. Without proper and appropriate security measures in place, vulnerabilities can and will be exploited very quickly.

References

Internet Assigned Numbers Authority (n.d.). Retrieved April 1, 2008, from www.iana.org

Internet Storm Center (n.d.). Retrieved April 1, 2008, from www.incidents.org

2600 The Hackers Choice (n.d.) Retrieved April 1, 2008 from <http://www.2600.com/>

Spector Soft (n.d.) Retrieved April 1, 2008 from <http://www.spector.com/>

KeyKatcher (n.d.) Retrieved April 1, 2008 from

<http://www.electronickits.com/spy/finish/computer/key.htm>

Drivers License Search (n.d.) Retrieved April 1, 2008 from <http://www.license.shorturl.com/>

Intelius (n.d.) Retrieved April 1, 2008 from <http://www.intelius.com/>

Interpol (n.d.) Retrieved April 3, 2008 from <http://www.interpol.int/>

Spy Gadgets (n.d.) Retrieved April 3, 2008 from <http://www.spygadgets.com/>

Spysite (n.d.) Retrieved April 3, 2008 from

http://www.spysite.com/home.php?show_all_categories=1

Nannycam (n.d.) Retrieved April 3, 2008 from <http://www.knowyournanny.com/>

Ligovosoftware (n.d.) retrieved April 3, 2008 from

http://www.lingvosoft.com/main.jsp?do=products-view_item&item=11141&refid=248&vTransferId=9DCIKTLLARG6VV5QMJ9QFQSM

[A](#)

Whois.net (n.d.) Retrieved April 3, 2008 from <http://www.whois.net/>

Ironkey (n.d.) Retrieved April 3, 2008 from <https://www.ironkey.com/>

National Sex Offender (n.d.) Retrieved April 3, 2008 from <http://www.familywatchdog.us/>

Hping (n.d.) Retrieved April 3, 2008 from <http://www.hping.org/>

IP Small Services (n.d.) Retrieved April 3, 2008 from http://www.rhyshaden.com/ip_small.htm

IBM Internet Security Systems (n.d.) Retrieved April 4, 2008 from <http://www.iss.net/>

Nessus (n.d.) Retrieved April 4, 2008 from <http://www.nessus.org/nessus/>

Netstumbler (n.d.) Retrieved April 4, 2008 from <http://www.netstumbler.com/>

Nmap (n.d.) Retrieved April 4, 2008 from <http://insecure.org/>

Shields Up (n.d.) Retrieved April 4, 2008 from <http://www.grc.com/intro.htm>

Retina (n.d.) Retrieved April 5, 2008 from <http://www.eeye.com/html/index.html>

Spam Mimic (n.d.) Retrieved April 6, 2008 from <http://www.spammimic.com/index.shtml>

TCP/IP Guide (n.d.) Retrieved April 7, 2008 from

http://www.tcpipguide.com/free/t_IPAddressClassABandCNetworkandHostCapacities.htm

Erasure (n.d.) Retrieved April 7, 2008 from <http://www.heidi.ie/eraser/>

Infoworld (n.d.) Retrieved April 8, 2008 from <http://www.infoworld.com/>

Hackerstorm (n.d.) Retrieved April 9, 2008 from www.hackerstorm.com

Cain (n.d.) Retrieved April 10, 2008 from www.oxid.com

Rainbow Tables (n.d.) Retrieved April 10, 2008 from

<http://www.antsight.com/zsl/rainbowcrack/>

Kismet (n.d.) Retrieved April 11, 2008 from <http://www.kismetwireless.net/download.shtml>

Microsoft Baseline Security Analyzer (n.d.) Retrieved April 12, 2008 from

<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>

Appendix A - Acronyms

BIOS	Basic Input/Output System
CD-ROM	Compact Disk Read-Only-Memory
CPU	Central Processing Unit
DMZ	Demilitarized Zone
DNS	Domain Name Service
DoS	Denial of Service
Esc	Escape
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
HIDS	Host Intrusion Detection System
INS	Immigration and Naturalization Service
IP	Internet Protocol
MBSA	Microsoft Baseline Security Analyzer
NIDS	Network Intrusion Detection System
PC	Personal Computer
POP	Post Office Protocol

SI	Stateful Inspection
SSH	Secure Shell
SSID	Service Set Identifier