CIW Security Professional Version 4

Version 3.0.0

CIW Security Professional Version 4

Version 3.0.0

Abstract:

The following is a study guide for the CIW Security Professional, Version 4, exam 1D0-470. The pre-requisites to take this course and exam include the Foundations, Server Administrator, and Internetworking courses and exams. The CIW Security courses assume you already have an intimate knowledge of TCP/IP, as well as both NT and Unix Operating Systems. Exam topics include Ports, Protocols, Encryption, Types of Attacks, Firewalls, Risk Assessment, and Operating System Security Fundamentals.

Find even more help here:

Contents:

Network Security and Firewalls

Statistics:

The CIW courseware, *Network Security and Firewalls,* states:

- 1 out of 5 sites on the Internet has had some kind of security breach.
- 50 % increase in intrusions within the last year.
- In the U.S. – 10 Billion is lost yearly due to security breaches.
- Most attacks continue and grow due to lack of resources, untrained staff, (or over burdened staff) and systems going out too fast without proper testing.

Ports:

(You need to know specific ports)

Type	TCP/UDP	Number
FTP - Data	TCP	20
FTP	TCP	21
TFTP	UDP	69
SMTP	TCP	25
POP3	TCP	110
SNMP | Trap	UDP	161 | 162
DNS	UDP	53
TELNET	TCP	23
TIME	UDP	37
TACACS	UDP	49
FINGER	TCP	79
HTTP	TCP	80
NNTP	TCP	119
NTP	TCP	123
NETBIOS	UDP	137-139
BOOTP Server	UDP	67
BOOTP Client	UDP	68
Gopher	TCP	70
LDAP	UDP	389

- You must be familiar with which upper layer protocol works with which lower layer protocol on which port.
- There are 65,536 possible ports; 1023 are well known
- DNS uses UDP/53 when DNS queries need to be resolved. It uses TCP/53 when doing Zone transfers.
- For a listing of all other ports by IANA – Click here

TCP/IP Communications Process:

--SYN→
←SYN / ACK--
--ACK→

- Even though this is standard for TCP communication, there is an added piece. This is called: (Active Open / Close and Passive Open / Close)

Establishing a TCP connection: (Client / Server)

Active Open
Passive Open
ACK
ACK

Terminating a TCP connection:

Active Close
Passive Close
FIN
ACK

- A SYN bit will Synchronize
- A ACK bit will Acknowledge
- A FIN bit will Finish (End)

For more information Click here | Click here for RFC's on this process

Attacking TCP:

- SYN Flood – Starts a TCP session by issuing a SYN request. It never completes and leaves the connection unfinished. If an attacker keeps doing this, nobody will be able to connect to a machine that will not be able to accept valid requests (Denial of Service – DoS)

Address Classes:

A	1-126 (127) | 255.0.0.0
B	128-191 | 255.255.0.0
C	192-223 | 255.255.255.0
D	Multicast
E	*Experimental*

OSI and Security:

Application	***Application layer most difficult to secure*** – SMTP, DNS, SNMP, TELNET, Upper layer protocols.
Presentation	
Session	
Transport	Host to Host
Network	Internet
Data link	Network Access
Physical	

Protocols and Exploits:

FTP:

- FTP (File Transfer Protocol) is not the target of choice of most hackers, but it is exploited frequently.
- As a server admin, you want to keep your FTP server in a DMZ (DeMilitarized Zone) and only allow anonymous access, because a valid user account password can be compromised – FTP sends in cleartext.
- The bad thing about this is that a hacker will look for the FTP server with this type of access - but more importantly, a hacker will look for a directory with WRITE access to either upload Trojans, viruses, or fill the server with so much space that it takes up all hard disk space.
- It is wise to have your operating system on a different hard disk on the server.
- A hacker will also try to fill up a hard disk to kill space available for logging; when that space is taken, the hacker cannot be logged and will crack through the server un-logged.
- Lastly, another attack is if a hacker finds a directory with WRITE access so they can put DATA there and use that area as a staging point, or a download point for other Hackers.

SMTP:

- Attacks against an Email server are VERY common. (remember Melissa, I LOVE YOU)
- Social engineering attacks are when you get fraudulent emails.
- Trojans and viruses can also be sent to your email server and spread by users and clients.
- The best ways to protect an email server is to either have it scan each message, or set up a filtering firewall or proxy to scan all messages.
- Lastly, in any case user education is very important. It only takes one user to open an email with a virus and spread it.
- SMTP was not originally made with security in mind – but newer implementations of SMTP servers will offer new security features.
- *Reverse DNS Lookup* is a new feature that will help ensure authentication.
- For securing separate emails – the best way is with encryption (PGP).

HTTP:

- Most of your traffic on your network is generally HTTP or web traffic.
- The server end is fairly simple and secure until you start adding pieces to your server (that introduces holes) like CGI scripts, active server pages, Active X controls and Java applets. There are ways to protect CGI scripts. For an article on this topic, check out: http://www.cgiscripts.net/webapps/articles/security.ppxml
- A notable exploit is a brute force logon when doing an http put, say to FrontPage or any http based web logon. You can change the default port that http uses (80), but this results in needing to notify your clients about the non-default port.
- Again, this is a server you want in your DMZ.

TELNET:

- Part of the TCP/IP stack and used to establish terminal emulation between a client and a server. (Or switch/router)
- Not safe because your passwords are sent in cleartext and can be hacked.
- Use SSH instead – this uses encryption via Public key.
- Do not allow telnet traffic beyond the firewall.
- Telnet is unsecured, so you should use SSH. Secure Shell needs DNS to be functioning or it may not function properly.

SNMP:

- Another unsafe protocol –also allows cleartext passwords.
- Everything is done via community name and if that name is compromised, then all SNMP-enabled devices with that string could also be compromised.
- Filter this at the firewall.

DNS:

- DNS can be attacked and should be kept in the DMZ behind your firewall.
- Hackers will attempt to get a DNS server's Zone files
- There are two ways to do a Zone transfer: either via NSLOOKUP and/ or when a slave (or secondary) name server will query a primary to get its Zone files.
- "Name Poisoning" is when a Hacker is able to insert wrong or false DNS information into a Zone Transfer – usually between a Master and a Slave.
- If this works, the name-to-IP mapping can be manipulated to be wrong – therefore poisoning your DNS solution.
- Here are some other recommendations. To protect DNS servers you need to constantly monitor the server and your firewalls. Look for attacks of all sorts. Make sure you have all current service packs and hot fixes. You can also use transaction signatures and here's an excellent article on this topic: http://www.linux.ie/articles/tutorials/dns-tsig.php

ICMP:

- Internet Control Message Protocol V4
- ICMP performs a number of tasks within an IP Internetwork.
- IP routing specifies that IP Datagrams travel through an Internetwork one-router hop at a time.
- The entire route is not known at the outset of the journey.
- Instead, at each stop, the next router hop is determined by matching the destination address within the datagram with an entry in the current node's routing table.
- Each node's involvement in the routing process consists only of forwarding packets based on internal information.
- IP does not provide for error reporting back to the source when routing anomalies occur.
- This task is left to another Internet protocol: the Internet Control Message Protocol (ICMP.)
- The principal reason for which it was created is reporting routing failures back to the source: ICMP also provides a method for testing node reachability across an internet (the ICMP Echo and Reply messages), a method for increasing routing efficiency (the ICMP Redirect message), a method for

informing sources that a datagram has exceeded its allocated time to exist within an internet (the ICMP Time Exceeded message), and other helpful messages.

- All in all, ICMP is an integral part of any IP implementation, particularly those that run in routers.

- ICMP messages generally contain information about routing difficulties with IP Datagrams or simple exchanges such as timestamp or echo transactions.

Encryption:

Kerberos:

- A method for authenticating a request securely
- Kerberos provides a way for a user to request an encrypted "ticket" or a SESSION key (Session keys are not any one, single security implementation) from an authentication server (AS) that can then be used to request a particular service, like telnet.
- The service could either reject that ticket, or accept it and provide that service.
- Also, a user's password will not have to go through a network.
- Bad thing about Kerberos is that if that server is compromised, (the AS or Ticket Granting Server) then you are vulnerable.
- A version of Kerberos (client and server) can be downloaded from MIT
- Click here for more info and a free download

OTP:

- One time Passwords
- A great method because as its name implies – only uses the authentication once.
- This is a good method to stop password hijacking and snooping.
- If a hacker gets you password – who cares, its now old after a single use.

RSA:

- Rivest-Shamir-Adleman
- RSA is an Internet encryption and authentication system

- It uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.
- The RSA algorithm is the most commonly used encryption and authentication algorithm.
- It is included as part of the Netscape and Microsoft web browsers
- RSA Security handles the encryption system. Click here for more info and downloads.
- The company handles the algorithm and also sells development kits for it.

SSL:

- Secure Sockets Layer
- Developed by Netscape, SSL is a protocol for transmitting private documents over the Internet.
- SSL uses a private key to encrypt data that is transferred over the SSL connection.
- Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol for confidential user information, like credit card numbers.
- Most Web pages that require an SSL connection start with https: instead of http.
- S-HTTP, Secure HTTP, is another protocol for transmitting data securely over the World Wide Web.
- Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely, S-HTTP is designed to transmit individual messages securely.
- SSL and S-HTTP are, therefore, complementary rather than competing technologies.
- The Internet Engineering Task Force (IETF) as a standard has approved both protocols.

Denial of Service Attacks: (DoS)

- A denial of service (DoS) attack is an attack where a user or an organization is deprived of the services of a resource they would normally have.
- A loss of service that you get from a DoS may be the unavailability of a particular network service, such as e-mail, or the temporary loss of network connectivity or other services.
- An example may be an Email server that is accessed by thousands of people can occasionally be forced to cease normal operation, thus could cost millions.

- A denial of service attack can also destroy programming applications and files in a computer system.
- DoS attacks are usually intentional and malicious, can sometimes happen accidentally (If you disable specific NEEDED ports on your firewall you therefore deny yourself service to whatever you shut down).
- A DoS attack that does not usually result in theft of information or other security losses.
- DoS attacks can cost the target person or company a great deal of time and money.

See CERT's DoS updates: Click here

Types of Attacks and Problems:

(YOU MUST KNOW ALL ATTACKS)

Buffer Overflow Attack	• The most common kind of DoS attack • Just send **more** traffic to a network address than the buffer can handle. • The attacker may be aware that the target system has a known weakness that can be exploited or an attacker may just randomly try the attack in case it might just work.
SYN Attack	• When a session is initiated between 2 machines on a network, a very small buffer space exists to handle rapidly sent "hand-shake" exchanges that will set up the session. • The session-establishing packet includes a *SYN* field that identifies the sequence in the message exchange. • An attacker can send a number of connection requests quickly and then purposely fail to respond to the replies. • This will leave the first packet in the buffer so that other connection requests will not be accepted. • The packet in the buffer is eventually dropped after a certain period of time without a reply, but the effect of so many of these fake connection requests make it difficult for real requests for a session to become established. • This problem depends on the operating system providing correct settings or allowing the network administrator to tune the size of the buffer and the

	timeout period.
Teardrop Attack	• This attack can exploit vulnerabilities becausethe IP protocol requires a packet that is too large for the next router to handle correctly to be divided into fragments. • The fragment packet identifies an offset to the beginning of the first packet that enables the entire packet to be reassembled by the receiving system. • With teardrop, the attacker's IP puts a confusing offset value in the second fragment. • If the receiving operating system does not have a way to handle this situation, it crashes the system that receives it. • With NT you will receive the all too common BSOD.
Smurf Attack	• An attacker can send an IP PING request to another site. • The ping packet can specify that it be broadcast to a number of hosts within the receiving site's local network. • The packet can also indicate that the request is from another site, the target site that is to receive the DoS. (This is called spoofing.) • The result will be MANY ping replies flooding back to the spoofed host. • If the flood is big enough, the spoofed host will no longer be able to receive real traffic. • They will be DoS and non-functional. • To protect, filter ICMP packets at the firewall.
Viruses and Trojans	• Viruses can replicate across a network in many ways • Can be viewed as DoS attacks where the victim is not targeted, but simply an unlucky host to gets that virus. • Depending on the virus, the DoS can be nothing serious to disastrous. • A Trojan has its payload hidden inside (it's name comes from the story of the Trojan Horse). A user must open it to receive the virus or malicious code.

	• 2 popular Trojans are Netbus and Back Orifice.
Physical Attacks	• A maliciously cut cable.
Brute Force	• Brute Force is performing an attack until it is cracked. This is the most time consuming attack, but it eventually pays off as long as the hacker does not run out of time, or nothing is changed.
Dictionary attacks	• Either systematically entering every character you can to guess a password, or using a "dictionary" like program to try every character to crack a password.
Root Kits	• A back door for many UNIX systems. • The control stage is when it is introduced • It is comprised of many programs that will replace legitimate programs with Trojans. • Hackers can get back door entry and additional tools to use (like protocol analyzers), which they can use to look at the network • Even worse- these new tools can hide themselves and the activities they are performing. • They are very hard to detect but may be found with checksum analysis and port scanning.
Social Engineering (Non-Direct attacks)	• A way for hackers to trick users into giving up their credentials or accidentally giving hackers access to resources through trickery or mistake. • Hackers might imitate others and trick a Help Desk agent into changing a password. (As an example)
Spoofing	• Ipv4 is prone to spoofing because it does not have the security enhancements that Ipv6 has. • Spoofing is the act of generating false information in a packet header. • It is very hard to trace. • It is a means to gain unauthorized access or to act as a trusted port for the purpose of either gaining access or gaining information by acting as someone else (Deceiving) • Because of the trusting nature of TCP/IP – Ipv4,

	the receiving system does not question the address in the packet of whom sent it – it just trusts it.
Man in the middle	• A hacker intercepts a TCP/IP conversation between two hosts or servers, and poses as one of the legitimate parties during communication. • The hacker does not take over any one connection - just intercepts data in the middle and re-transmits it to the one party while they communicate. • , • This attack is used to sniff passwords or information from a legitimate transaction to be used for their advantage. • The best defense is to use very strong encryption.
Hijacking	• This is similar to the man-in-the-middle attack, except the hacker intercepts the data and ACTS as or IMPERSINATES the other person you think you are in contact with. • The other party may still be there, but the hacker has taken over the connection completely (not hanging out in the middle of it) and assumed that person's identity. • Instead of being the man in the middle – the hacker is now the man at the other end!
Illicit Server	• When you have an unauthorized daemon or service running on your system that can cause harm. • An Illicit server can secretly open a port and provide service that IS NOT AUTHORIZED. • Examples: Netbus and BackOrifice 2000.
Front Door	• The hacker has all the correct information to get into a system and does not have to perform any additional work to get that information. • They essentially walk through the front door of your systems. • They will imitate a user that is legitimate to gain access to the systems or network.

Back door (Bugs)	• Some way of entry that you may not have known about, that you left intentionally or that a programmer left in the program to get into the system past any security set up for keeping the system secure. • OR a bug in the system that gives an attacker a back door into a system.
Ping Of Death	• A Hacker will crash a system when sending an ICMP-based packet that is more than 65,536 bytes. • It causes a buffer overflow.
Land Attack	• A Hacker can send an IP packet (Spoofed) to another computer and have the identical Source / Destination address. • This DoS based attack causes a system slowdown or a system crash.

Note: Another common attack that should be noted is ***Windows Spoofing***. I have seen actual occurrences of Windows Spoofing, and it can be very effective. This is when someone poses as a website in hopes that you will reveal information – like your social security number, bank account, passwords, etc. It is a mock of the actual web site you visit. Most commonly, hackers poses as AOL and offer deals if you "log in" but if you look at the URL in you browser, you will quickly realize- it is not AOL. The only prevention or help for this is *user education*.

Security Implementation Steps:

- Needs and resources categorization
- Defining a Security Policy
- Securing each and every resource and service
- Perform logging, testing and evaluation
- Repeat this process and KEEP CURRENT.

Means of Protection:

- Disable or remove unnecessary resources and services
- Change default settings
- Protect against profiling (the hacker's ability to determine of whatever network host the hacker is dealing with) You can profile with a Packet Sniffer
- Define system policies and security policies

- ***SEGMENT*** information: place the operating system and files on a separate partition or hard drive all together.

Common Targets:

- DATABASES – the database is the jackpot
- Routers / Switches that are unprotected
- DNS and WINS servers or servers using SMB
- WEB and FTP servers

Why SMB (or SAMBA)? SMB is susceptible to man-in-the-middle attacks. This is thwarted with SMB signing but can put a load on your network – and many Administrators may not even know about the possible attacks hackers attempt on SMB.

Routers can be targeted for attack because, if they are being managed (which they usually are), they may be using SNMPv1, which uses cleartext and has a common community string generally used in all the managed routers and switches.

Routers and switches are also targeted for Administrators who use TELNET – again sending authentication information in cleartext. Remember to filter Telnet and SNMP ports at the firewall.

Firewalls:

- A firewall is used to create a somewhat protective barrier that tries to prevent unauthorized access to your information or computer systems.
- A firewall is a combination of hardware and software, and protects your internal systems or hosts from outside access. (Do not forget though that some attacks come from WITHIN your organization.)
- A Firewall should be an entry point to your network.
- Typical Firewall setups would use ONE Firewall as a choke point, but these days that is simply not the case. There is generally an external firewall, A DMZ (Where your Bastion Hosts exist: Web server, DNS server, FTP server, Mail relay, etc) and then the internal firewall.
- In a simple setup, your firewall would advertise one address out to the Internet; your servers would reside behind the firewall and use a private addressing scheme. (Or use a server or router performing NAT translation)
- A firewall can be a PC (personal firewall software), server (Multi-homed with firewall software installed on it), or a router (with Access-lists and filters, etc.)
- You can implement more than one firewall on your network and many networks include combinations of different kinds of firewalls at certain access points. (Defense in depth)

- A firewall can help to regulate the type of traffic that can access the private network. (Protects the internal network from the Internet or an un-trusted network)

Roles of Firewalls:

Implement Company's Security Policy	• Your firewall is an important and critical piece of your design. • It should be a means to enforces the security policy.
Create a Choke point	• A single point in your network through which **all** traffic will be funneled. • This would hopefully disable any other way into you network if there were only one way in or out. • Beware of users with modems dialing out avoiding your choke point. A modem bank can get hacked with a War Dialer • This allows you to monitor a single area rather than having to worry about many different entry points to your internal network.
Log Internet Activity	• The firewall should log **all** activity • Most advanced firewall products will also allow you to create alarming and filtering rules. • Make sure to protect your logs from being removed, deleted or even worse – changed.
Limit Network Exposure	• The firewall should hide your internal network and its addressing. • Your Web, DNS, and FTP and Mail relay servers should be the only things accessible and seen.

Firewall Types:

(YOU MUST KNOW ALL TYPES)

Packet-filtering Firewall "A router can do this" *"Network layer"*	• Packet filters will look at a packet's source and destination name and let it pass or drop based on the rule set that has been programmed. • A benefit to packet filters is that they work quickly. • A disadvantage is that they do not have a chance to analyze the packet in great detail.
Circuit-level Gateway *"Main feature is NAT* *"Session layer"*	• Its primary advantage is NAT. • It can severely limit productivity, which is a big disadvantage due to its complex nature. Users need training. • A circuit-level gateway will monitor TCP handshaking between packets from trusted to un-trusted hosts • A circuit-level gateway relies on data contained in packet headers • Circuit-level gateway filters packets at the Session layer of the OSI model. • It operates two layers higher than a packet-filtering firewall. (Session – Network) • If you need to filter upper layer traffic (Telnet, etc) you need an application-level gateway.
Application-level Gateway *"Said to work at all layers of the OSI"*	• Runs at the Application and Presentation layer of the OSI model • Uses a specialized program for each type of application or service that needs to pass through the firewall. • A benefit of an application gateway is that it can perform a somewhat detailed analysis of data. • A disadvantage is the possible need for a custom program made for each application that uses the firewall. • Application gateways are slower than other firewall types and might not perform well to

	meet the needs of a large network base.
Demilitarized Zone (screened subnet)	• A DMZ refers to a separate network that sits between the Internet and your internal network. • This zone contains your e-commerce systems. (Mail relays, FTP server, Web server, etc) • On one side of the DMZ is a firewall that protects the DMZ from the Internet. • On the other side of the DMZ is a firewall that protects the internal network from the DMZ.
Proxies (Or Proxy Server) Note: Windows Proxy Server uses specific NAT terminology: *Trusted*- the network or the host that will be permitted to access the Proxy Server *Trusting*- allows traffic from internal interface to come into the Proxy Server Note: Usually add-on applications, like Surf Control, are used with proxy to add more granularity to filtering..	• Proxies give centralized control of traffic, a more efficient use of bandwidth and will hide the real IP addresses of machines located behind the proxy. • Proxies make great sense from a security standpoint. They contain network access to a single machine, and this will make firewall rule sets a lot easier to program and set up. • They can also hide the actual IP address of the internal machine from the outside machine, which has a very large security benefit as well. • Proxies allow you to have private addressing (10.x.x.x) and you can perform NAT, Network Address Translation. (From private to public) • All the outside machines ever see is the IP address of the proxy server. • Proxies can also store or cacheinformation that is requested repeatedly by inside machines. (Internet, Browser-based requests) • Proxy server 2.0 by default does not listen to inbound service ports, so it is deemed an example of a secure implementation. • Proxies' cache drive must be on NTFS partition!

Screened Hosts	• Offers added security by using Internet access to deny or permit certain traffic from the Bastion Host. • This is the first stop for traffic, which can continue only if the Screening Router lets it through. (Filtering)
Dual-Homed Hosts	• Based on a server with two (dual-homed) or more (Multi-Homed) network interfaces • Host acts as a router between the network and the interfaces to which it is attached (If you configure it – the Host can enable IP forwarding and build up a RIT.) Routing Information Table • Host blocks direct traffic between the private network and the Internet, when configured to do so. • In screened Subnetting, the Bastion Host is placed on its own Subnetwork. Two screening routers are used to do this. One sits between the subnet and the private network, and the other between the subnet and the Internet.
Tri-Homed Hosts	• Combines elements of a Screening Router and a Screened Host. • Security is centered on the screening routers by using interfaces for the Internet, the private network, and the subnets that contain the Bastion Hosts and application servers.
Bastion Hosts	• Allows external network clients access to internal services. • These servers sit in a DMZ, or a separate segment that is not connected to the internal network without going through a firewall. • They generally sit outside the internal network's firewall – but sit inside the external network's firewall. (In a three part

	firewall system) • Runs few services – email, FTP, DNS, Web • Should not require authentication or store any sensitive data • You want them to be hardened. • Disable unneeded services and make sure you have the LATEST security fixes and patches installed! • Unbind unnecessary protocols from the NIC card.
Screening Routers	• Basic type of firewall that uses only the packet-filtering capability to control and monitor network traffic passing through the border. Can block traffic between networks or to and from specific hosts on an IP-port level. • A CHOKE router is the only point in.

Stateful Inspection:

- Stateful Inspection firewalls perform a more detailed analysis than other firewall types like packet filters.
- They can look at a packet's relationship with other packets that have been passed through and they also look at the traffic passing over time.
- This will allow for a better analysis of traffic and make a more accurate firewall solution.

NAT - Network Address Translation

- Mechanism for reducing the need for globally unique IP addresses.
- NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.
- Also known as Network Address Translator.
- NAT allows private Internetworks by using non-registered IP addresses to connect to the public network, such as the Internet or backbone that uses registered IP addresses (public).
- NAT can use a router to connect two networks together (Or a multihomed server capable of translation).

- NAT acts like a firewall by keeping individual IP addresses hidden; it can be configured to advertise only one address for the entire network to the outside world.

Private Addresses:

Class A	10.0.0.0	10.255.255.255
Class B	172.16.0.0	172.31.255.255
Class C	192.168.0.0	192.168.255.255

- Steps for Conducting a Risk Assessment: Check for a Written Security Policy.
  - The best way to perhaps understand what you are dealing with is to **first** check the security policy.
  - This is your road map.
- Analyze, Prioritize, and Categorize Resources
  - This is where you need to look at and discover the most critical pieces of the network.
  - Ask key questions to determine risk
- Consider Business Concerns
  - This is where you can look at your customers needs and perhaps aim you solution to meet those needs.
- Evaluate Existing Perimeter and Internal Security
  - This is where your network can differentiate itself from perhaps other networks.
  - This is where you would see what kind of security is already there in place.
- Use Existing Management and Control Architecture
  - If you already have elements in place - use them.

Risk Assessment Stages:

- Discovery
  - Where you as the auditor test your network for security effectiveness.
  - Most time consuming

  - During this stage you map out the network and attempt to discover every resource
- Penetration
  - In this stage, you bypassed all access control. (Passwords / logins)
  - Here is where you inspect systems for possible weakness and try to break into that weakness.
- Control
  - Remember – you never actually go through with the control of the resources, but show your business client *that you can control it*.
  - Show how to ensure prevention.

Tools and Services:

(YOU MUST KNOW ALL TOOLS)

NSLOOKUP and WHOIS	• A DNS troubleshooting tool that, when combined with a WHOIS query, can be used to learn much about a network. • With WHOIS you can find a primary and secondary name server and other valuable information. • If you can successfully imitate a secondary name server with NSLOOKUP you can initiate a Zone transfer with a Master. • If you can pull this off, you will have the names and IP addresses of all systems that use that server for resolving names to IP's, the subnets used, and perhaps the role of the server based on the server name.
HOST command	• A Unix-based command that is used to help retrieve information about your hosts on the network. • It will also covert IP's to hostnames and hostnames to IP's. • It is capable of Conduction Zone Transfers.

	• You can get name-server-based information. • You can also learn about the domains mail servers.
TRACEROUTE or TRACERT	• This utility is used to discover the number of hops (or the number of routers) that a packet has to travel to get to its destination. • You can use it to get a general layout of someone's network and maybe some bottlenecks or trouble areas in the network.
Ping Scanner	• If you ping a server you can gain its address • Once you have that address, you can begin to ping all other addresses on that network and when you get a reply back, you start building a map based on those replying addresses. • This is a also called Network mapping • A Ping Scanner will automatically ping a specific range you put into it.
Port Scanner	• This is very similar to a Ping scanner but instead of just replying back the validity of IP's – it will also report active UDP and TCP ports that are available on the scanned system.
Share Scanner	• A Windows network will obviously have some kind of file sharing going on, and, if that is the case, then NETBIOS on port 139 will be active. • A scan of the networks shares will report back the share names – IT WILL NOT break into these shares, just report that they are in fact shared.

Unix File Names and Locations:

/	Root
/sbin	Commands- administrative
/bin	Commands – User
/usr	O/S bulk
/usr/bin	Commands – System

/usr/local	Software packages locally installed
/usr/include	Include files
/usr/src	Source code
/usr/local/src	Locally installed packages source code
/usr/sbin	Commands – administrative
/var	Spool files- log files
/var/log	Log files
/export	Shared file systems
/home	Home directories for users
/opt	Software that is optional
/tmp	Temporary files
/proc	Used to access kernel variables

NT File Names and Locations:

\%Systemroot%	Directory that contains the O/S's system files includingthe registry log and regedit.exe
\%Systemroot%\profiles	Contains the administrative profile as well as all other user profiles. (personal folder, browser temporary cache, desktop data)
\%Systemroot%\system32	Contains many other important subdirectories.
\%Systemroot%\system32\ config	Contains SAM, SAM.LOG, Security.log, application.log, and event.log
\inetpub	Contains IIS 4.0 system files, including \wwwroot and \ftproot.
\Program files	Will contain the folders for most of the applications installed on the system.

CERT's Steps for Recovering from a UNIX or NT System Compromise

Operating System Security Fundamentals

NT Security

- Level **C1** security will require that users log on, and it will require the allowance of group ID's.
- Level **C2** security will require the user log on WITH A PASSORD, and has some kind of auditing mechanism.
- **DAC** – or Discretionary Access Control – in general that means the specific owner of a particular resource MUST be allowed to have control over the access to that resource
- **DAS** –Discretionary Access Security - (C2), this is the level at which the system can differentiate between the specific users (but will treat them as unique) and a system level of protection will exist for the data, files, resources, and system processes.
- A security mechanism called *Traffic Padding* is a mechanism that will allow additions to your Network-layer packets so you can basically hide them from monitors or scanners or make them all look alike so they are not singled out.
- A good rule of thumb is to only allow users access to what they need to do their work. Do not over-assign rights and privileges and take away what is not needed. Remember – NT by default is WIDE open.
- To implement strong security in NT passwords you must use passfilt.dll with passprop.exe.

Security Components of NT:

- SIDs (or Security Identifiers) are assigned to all computers, users and groups.
- A SID is generated by a combination of:
    - Computer name
    - Current time
    - The amount of time that current user mode thread has been using the CPU or CPU time.
- After a user has been validated they receive an access token, which is a kind of validated pass to access their resources. The access token is made up of the users SID and any other group SIDs they are in. This is only issued at login. If any changes are made the user must re-login to gain new privileges.
- All objects within the NT system have security descriptors, which hold the settings for security. This is what is contained in a descriptor:

  - Owner's SID
  - Group SID
  - *DACL*
  - *SACL*
- A DACL (Discretionary Access Control list) will possess a list of both users and groups and whatever permissions they have. (Allowed or Denied)
- The SACL (System Access Control List) will have contained a list of any events that are set to audit for that particular object.
- An ACE (Access Control Entry) will exist for each and every permission entry assigned to any object. – *Either AccessAllowed or AccessDenied*.

More Security Concerns and Suggestions:

- Always weigh the benefits of added security against the increased level of difficulty to the end users.
- The administrator's account is not affected by account lockout
- A word of advice: keep the administrator's account available as a dummy account and monitor and audit it carefully.
- PARTITION the drive! Put O/S on one, files on another, etc.
- Know the difference between share points and share permissions. Permissions are only assigned to the points- if you give "read" to the top level of the share point – all folders / directories and files will assume that "read" permission.
- To remove some risk, remove or disable services not in use.

UNIX Security:

- A hacker's primary goal is to gain Root level access and privileges.
- Unix is very susceptible to buffer overflow attacks
- Do not use telnet – it is unsecured. Use SSH instead.
- User accounts must have an entry in the /etc/passwd file.
- Password aging information is handled by the **chage** command in Linux and by the **passwd** command in Solaris.

UNIX Commands:
(Must know)

chage

-m Minimum number of days between password changes	**-d** Number of days since January 1, 1970 (Unix Epoch) the password was last changed
-M Maximum number of days between password changes	**-I** Specifies the period of inactivity after password expires
-W # of warning days before user gets a message	**-l** Lists the current settings
-E Expiration date for the account	

umask

7 –Read Write Execute	**3** –Write Execute
6 –Read Write	**2** –Write
5 –Read Execute	**1** –Execute
4 -Read	**0** – Access absent

- Usually the permission by default would be –666 (plain files)
- Or perhaps for a directory or an executable – 777

chmod

- Used to manipulate the file permissions
- Absolute mode – chmod 777 /filename
- Symbolic mode – chmod a+rw /filename (- subtract + add)

UIDS – GIDS – SUIDS – SGIDS

- UIDS are identified Uniquely in: /etc/passwd
- GIDS are identified Uniquely in: /etc/group
- Used by the Unix kernel to grant security-based access

- When a program changes its UID, it will have a SUID (Setuid)
- Similarly, a GID would be called a SGID (Setgid)
- A SUID or SGID will grant a user more permission than was initially entitled.
- This needs to be monitored closely

rlogin

- rlogin is so easily violated, most admins won't use it.
- It can be used to bypass a normal password prompt.
- rlogin can be used if the file is checked at login (hosts.equiv - .rhost).
- If the permissions are compromised, however, then just about anyone can attack your system.
- The primary, well-known weakness of many "old" protocols is that most data is sent in clear text. As far as admin privileges, in Unix we call it "ROOT" which gives you full access. Never use the rlogin/rsh/rexec suite of tools (called the r-utilities) as root. They are subject to many sorts of attacks, and are dangerous to run as root. Also, never create a .rhosts file for root. For more information on why to avoid rlogin and telnet, please see: http://www.securityportal.com/research/ssh-part1.html

Check out our CIW Security Professional, Version 3 Cramsession (Exam 1D0-370)

Special Thanks to Robert J. Shimonski (Rshimonski@Hotmail.com) for contributing this Cramsession. Make sure to visit his site at: http://www.rsnetworks.net