Chaz Network Security Scanner

THE CRACKERS GROUP INC 2005 (C) **, *Nima Bagheri***

- **website: www.geocities.com/thecrackers_group**

  E-mail : Thecrackers_group <at> yahoo <dot> ca

Introduction to "Chaz" Network Security Scanner

==========

Scan Tool Network Security Scanner (Chaz Edition) is a tool that allows network administrators and Manegements to quickly and easily perform a network security audit.

Chaz combines the functions of 20 scanner.

It also creates reports that can be used to fix security issues on a network.
It also provides hyperlinks to security sites to find out more about these vulnerabilities.

Most employees do not need and should not have access to each other's machines, administrative functions, network devices and so on.
However, because of the amount of flexibility needed for normal operation, internal networks cannot afford maximum security.
On the other hand, with no security at all, internal users can be a major threat to many corporate internal networks.

Poor network security also means that, should an external hacker break into a computer on your network, he can then access the rest of the internal network more easily. This would enable a sophisticated attacker to read and possibly leak confidential emails and documents; trash computers, leading to loss of information; and more.

Not to mention then use your network and network resources to turn around and start attacking other sites, that when discovered will lead back to you and your company, not the hacker.

Most attacks, against known exploits, could be easily fixed and, therefore, be stopped by administrators if they knew about the vulnerability in the first place.
The function of "Chaz" is to assist administrators in the identification of these vulnerabilities and help To find This errors and exploits.

Enumeration of Possible Entry Points
==========

Rogue services and open TCP and UDP ports
SNMP holes
CGI holes
Rogue or backdoor users
Trojan horses or backdoor software
Open shares
Weak network passwords
Enumeration of users, services,Proccess, etc.
IIS Checks
SQL/MSDE Checks

Methods
==========

Information gathering
Operating system identification
Known security issues in software packages
Live host detection

Alerts
==========

Well known security issues are immediately recognized
Intelligent scanning
List of missing Hot fixes and Service Packs on NT/2000/XP machines

Presentable Output
==========

HTML and Text output

Extra Features
==========

Exploitation of NETBIOS (SMB) vulnerability in Windows 95/98/ME
Sniffer TCP/UDP/ICMP
Firewall auditing (Spy Ports)
System Monitoring
SNMP auditing
MS SQL auditing
Boardcast Message
WebSite Scanner
Trace route
Password Cracker (NT BASE)

MD5 Password Cracker
DNS lookup
Mac and Arp auditing
WhoIs client
Remote machine shutdown
Sending E-Mail Address spoofed messages (social engineering techniques used in hacking)
Banner Grabbing
Plug maker
Ping Scanner

Analyzing the Scan Results

==========

Analyzing the results

==========

After a scan, nodes will appear under each machine that Chaz finds.
The left pane will list all the machines and network devices.

Expanding one of these will list a series of nodes with the information found for that machine or network device.

Chaz will find any network device that is currently turned on when doing a network probe.

Depending on the type of device and what type of queries it responds to will determine how well Chaz can identify it and what information it can retrieve.

Once Chaz has finished its scan of the network a screen like the `Analyzing the results' screen shot above will appear.

Depending on the device found different information would be available.
However, for explanation purposes we will assume that the network device found is a Windows machine for most of the information to come.

Network Device IP and Name

- First the IP address of the device we are working on will appear. Next to that the Netbios Name or DNS name depending on the type of device. Finally Chaz will report what OS is running on the device and if it is NT/2000/XP Chaz will report what Service Pack is on the machine.

Netbios Names

- The first node under the device lists Netbios information, such as services, current user logged on, etc. (You can find more information in the section called ***"Additional Results"*** in the next section.)

Trusted Domains

- If the computer is part of a Domain, it will show one or more trusted Domains. Ensure that the trust relationships are setup correctly and this machine actually should trust all Domains listed.

Password Cracker

- The next node is an important one. Check to see that the password is secure, Chaz Can Cracking MD5 Password And NTLM v1,v2.

  You can perform brute force cracking with the option **Use all characters for cracking**. This will of course increase the time for a network audit using Chaz It might also cause various alerts on intrusion detection systems!

  Password cracker can add a substantial amount of time to a scan, depending on the computer role and number of user accounts on the computer. In addition, attempts to check individual accounts for weak passwords can add Security log entries (Logon/Logoff events) if auditing is enabled on the computer. Note the tool will reset any account lockout policies detected on the computer so as to not lockout any individual user account during the password check. This check is not performed on domain controllers.

  Username used for Cracking

  This is the username that Chaz will use to attempt to break into shares.

  On Microsoft NT/2000/XP machines the administrator account cannot be locked out due to too many incorrect login attempts. That is why the default account name here is Administrator. If the Administrator username has been changed, you can select **This username:** and set it there.

  Chaz can be set to try using the **Currently Logged on user** when it tries to crack the password on a share, but if policies have been setup for account lockout, this will eventually lock the currently logged on users account. Therefore, this is not recommended.

  Note: On a NT/2000/XP box you can do a number of things to thwart an attack such as this. There are many articles and books on this, but two easy things to do are: rename the administrator account and remove it from the administrator group. (Before doing this ensure that other accounts have administrative access.) Also, modifying the Local Security Policy to log Failed Login attempts to the Event Log. (This will not keep the attack from happening, but at least you will be able to see that someone was trying to login to the box and failed.)

  Unpassworded Shares

  If checked, Chaz Network Security Scanner will check machine shares for a password and let you know if any are found without one.

One reason that Unpassworded Shares are dangerous is because of the way some of today's viruses are spreading. Viruses such as Klez spread through open shares; once a machine is infected it will look for shares it has access to and try to infect them. It only takes one person in a company to quickly infect many machines if shares are left open.

Shares

- Open shares, if not secured, are a threat to network integrity. Administrators should make sure that:
  - No user is sharing his/her whole drive with other users.
  - Anonymous/unauthenticated access to shares is not allowed. Chaz now has an option to check for these unpassworded shares and will let you know when it finds them.
  - Startup folders or similar system files are not shared. This could allow less privileged users to execute code on target machines.
- The above is very important for all machines, but especially for machines that are critical to system integrity, such as the Public Domain Controller. Imagine an administrator sharing the startup folder (or a folder containing the startup folder) on the PDC to all users. Given the right permissions, users can then easily copy executables into the startup folder, which will be executed upon the next interactive logon by the administrator.

  Note: If you are running the scan logged in as an administrator, you will also see the administrative shares, for example "C$ - default share". These shares will not be available to normal users.
- With the way Klez and other new viruses are starting to spread, through the use of open shares, all unneeded shares should be turned off, and all needed shares should have a password on them.

Users & Groups

- The next 2 nodes show the local groups and the local users available on the computer. Check this area to ensure that there are no extra user accounts, and verify that the Guest account is disabled. Rogue users and groups can allow users backdoor access!
- Some backdoor programs will reenable the Guest account and grant it Administrative rights, so expand the users node to see the activity of all the accounts and the rights they have.
- Ideally the user should not be using a local account to logon, but should be logging into a Domain or an Active Directory account.
- The last main thing to check is to ensure that the password is not too old.

Services & Processes

- All running services on the machine are listed. Verify that the services running need to be and disable all services that are not required. Be aware that each service can potentially be a security risk and a hole into the system. By closing or switching off services that are not needed, this automatically reduces the security risks on that machine.

General Information

- Network devices, drives and remote time of day shows general information about the computer.
- **Note:** For more information on these see the ***"Additional Results"*** in the next section.

Password Policy

- The next node is an important one. Check to see that the password policy is secure. For example enable a maximum password age and password history. Minimum password length should be something practical, such as 8 characters. If you have Windows 2000, you can enable a secure password policy, network wide, using GPO (Group Policy Objects) in Active Directory.

Registry

- This node gives vital information about the remote registry.
- Click on the Run node to check what programs automatically launch at startup.
- Check that the programs that automatically launch are not Trojans or even valid programs that provide remote access into a machine if such software is not allowed on your network. Any type of Remote Access software can end up being a backdoor that a potential hacker can use to gain entrance.

Auditing

- If the target machine runs Windows NT/2000/XP, Chaz will check if auditing is turned on. It is recommended to turn on auditing on Windows machines. This is an important security feature of Windows that is disabled by default. Turning on auditing will allow you to detect security breaches and check how it occurred.
- Chaz provides a way to turn auditing on, assuming you have administrator rights to the machine, once a machine is scanned.
- To enable auditing on a machine right click, goto **Enabling Auditing on > This Machine**. You can will then see a screen such as the above one. Check the boxes next to the events you want audited on the machine.

Installed Hot Fixes

- The hot fixes node shows what hot fixes are installed. Ensure that your machines have the latest Hot Fixes and Service Packs installed.
- Unfortunately, in the windows world there seems to be no greater security risk than not being up to date on the latest hot fixes and service packs. So make sure you always have the latest patches installed.

Open Ports

- The open ports node lists all open ports found on the machine. (This is called a port scan). Chaz Network Security Scanner does a selective port scan. It does not scan all 65535 TCP and 65535 UDP ports, just the ports it is asked to. To learn more on how to change what ports Chaz is set to scan, look in the manual at ***"Configuring Scan Options, Configuring Ports to Scan"***.
- Each open port represents a service/application; if one of these services can be 'exploited', the hacker could gain access to that machine. Therefore, it's important to close any port that is not needed.

  Note: On Windows Networks, ports 135, 139 & 445 are likely to be open. Hopefully, your Internet firewall is blocking these ports from the outside world.
- Chaz will list all open ports it finds that are setup to be scanned for. If the port is considered a known Trojan port, Chaz will display it in RED, otherwise the port will show up in GREEN. You can see this in the following screen shot:

o **Note:** Even if a port shows up in RED as a possible Trojan port, that does not mean that that a backdoor program is actually installed on the box. Some valid programs will open ports that are the same as some known Trojan ports. One antivirus program uses the same known port as NetBus Backdoor. So always check the banner information provided and run other checks on these machines.

Sniffer TCP/UDP/ICMP

- Sniffer TCP/UDP/ICMP is another technique to use internally. a Sniffer is able to capture any traffic traveling along the network segment to which it is connected. we normally set up sniffers throughout the organization to capture network traffic ,hoping to identify valuable information such as user IDs and Passwords.

Alerts Node (Web Scanner)

The alerts node displays known security issues and informs you how to fix them. These threats can include HTTP issues, NETBIOS alerts, configuration problems and so on.

Alerts are broken down into the following sections: Missing Patches, CGI Abuses, FTP Alerts, DNS Alerts, Mail Alerts, RPC Alerts, Service Alerts, Registry Alerts, Miscellaneous Alerts and Information Alerts.

Missing Patches show up on Windows NT/2000/XP machines if there are any missing Hot Fixes or Service Packs. Chaz will provide a link to the Microsoft page where you can download that individual patch.

CGI Abuses describe issues related to Apache, Netscape, IIS and other web servers.

FTP Alerts, DNS Alerts, Mail Alerts, RPC Alerts, and Miscellaneous Alerts provide links to Bugtraq or other security sites so that you can lookup more information about the problem Chaz found.

Service Alerts can be a number of things. Anything from actual services running on the device in question to accounts listed on a machine that have never been used.

Registry Alerts cover information pulled from a Windows machine when Chaz does its initial scan. It will provide a link to Microsoft's site or other security related sites that explain why these registry settings should be changed.

Information Alerts are alerts added to the database that are issues important enough to be brought to the administrators' attention, but not always damaging to leave open.

IIS Checks

- The IIS 6.0 Common Files are required on the local machine that is remotely scanning an IIS 6.0 server. The IIS 6.0 Common Files can be used to also scan downlevel IIS machines (e.g., IIS 5.0), however the IIS 5.0 Common Files cannot be used to remotely connect to and scan against a machine running IIS 6.0.

SQL/MSDE Checks

- The tool checks for administrative vulnerabilities on each instance of SQL and MSDE found on the computer. All individual SQL checks will be performed on each instance of SQL and MSDE.
- MSDE is a data engine built and based on core SQL Server technology. It is a redistributable database engine that supports single- and dual-processor desktop computers. MSDE is packaged in a self-extracting archive for ease of distribution and embedding. Since it is fully compatible with other editions of SQL Server, users can upgrade from MSDE to SQL Server if an application grows beyond the storage and scalability limits of MSDE.

Banner Grabbing

- The most fundamental of enumeration techniques is Banner grabbing ,Banner grabbing can simply defined as connection to remote application and observing the output ,and it can be surprisingly informative to remote attackers.

Ping Scanner

- Ping scanner is a tool for discoverd IP addresses to see if they are up or live.there are a variety of ways to ping a set ip addresses. the most comonly used is the traditional ICMP ping (with echo requests or echo replies messages),but gaining popularity is a TCP ping.

Plug maker

Plug maker is a tool that allows network administrators , security developer or programer to quickly and easily make security tests for own systems.

with this tool they can test on own system new bugs and vulnerabilities .

they can find new vulnerabilities in security sites like www.securityfocus.com or others security sites.

with plug maker you can send following this security checks:

- Cgi exploites
- Http and ftp exploites
- web exploites
- Buffer overflow
- Cross site scripting
- Denial of Service
- Missing authentication
- Missing encryption
- SQL injection

and with for server's answer .

if you can find your data in exploites the system make a alert for you .

General - Options

==========

Delay & Retries

Scanning Delay is the time Chaz Network Security Scanner waits between packets it sends out. The default is 100 ms.

Depending on your network connection and the type of network you are on (LAN/WAN/MAN) you may need to adjust these settings. If it is set to low you may find your network congested with packets from ChazIf you set it too high a lot of time will be wasted that is not needed.

Wait for Responses is the time Chaz will actually wait for a response from the device. If you are running on a slow or busy network you may need to increase this timeout feature from 500 ms to something higher.

Number of retries is the number of times that Chaz will do each type of scan. During normal circumstances this setting should not need changed. Be aware, however, that if you do change this setting, it will run through each type of scan (NETBIOS, SNMP, and ICMP) that number of times.

SNMP

The option to **Load SNMP enterprise numbers** will allow Chaz to extend support in SNMP scanning. If this is disabled, devices discovered by SNMP that are unknown to Chaz will not report who the vendor is supposed to be. Unless you are running into problems, or trying to increase the load time of Chaz it is recommended to leave this option enabled.

By default most SNMP enabled devices have a read community name of `public', but for security reasons most administrators will change this to something else. If you have changed the default SNMP community name, on your network devices, you will want to add it to the list Chaz uses.

Note: You can add more than one SNMP community name here. For each additional community name you add, the SNMP part of the scan will have to run another time. If you have `public' and `private' set in the community name string, the SNMP scan will run through the whole IP range you give it twice. It will go through it once with the string of `public', and then again with the string of `private'.

Adding Non-Responsive Computers

Because of the possibility of a personal firewall on a machine that blocks NETBIOS, SNMP, and ICMP packets there is now an option to add all non-responsive computers to the list of machines to be port scanned.

Note: This will greatly increase your network scan times, because Chaz Network Security Scanner will need to TCP and UDP port scan each non-responsive host and wait for the timeout to occur on each and every port scanned. Unless you know that there are quite a few machines on your network, setup to be non-responsive to NETBIOS, SNMP, and ICMP packets, it is not recommend using this. Chaz already has a few other checks it does to try to determine if a machine is actually blocking these packets.

Methods for Network Discovery

Here is where you can specify the method(s) used to discover which computers are on. Some devices will not be running NETBIOS or SNMP, but all machines will usually respond to ping.

The **NETBIOS queries** option allows Netbios or SMB queries to be sent out. If the Client for Microsoft Networks is installed on the Windows Machine, or if Samba Services are installed on a Unix machine, then those machines will answer the Netbios type query.

There is the ability to add ScopeID information to the Netbios Query. In most cases this should not be set. However, in special cases some systems might have been set with a ScopeID. If your organization has a ScopeID set on Netbios, input it here.

The **SNMP queries** option will allow SNMP packets to be sent out with the Community String that was set in the General tab. If the device responds to this query, Chaz will request the Object Identifier from the device and compare that to a local database while determining what that device is.

Ping Sweep does an ICMP ping of each network device. (See **Note:** below)

Each of the above query types can be turned off, but Chaz uses all 3 types of queries to help it determine the type of device and the OS running on it. If you choose to turn any one of these off, Chaz will still attempt to identify the device and the OS on it. (Chaz may not be as reliable if it is not doing a full scan.)

Note: Some personal firewalls will block a machine from even sending out an ICMP echo, but in most cases you will probably not see this on your corporate network.

Additional Tools and Features

- DNS Lookup
- WhoIs Client
- Trace Route
- SNMP Walk
- SNMP Audit
- Send Message
- Enumerated Computers

DNS lookup

This tool resolves the Domain Name to a corresponding IP address and in addition provides information about the domain name, such as whether it has an MX record etc..

To obtain information about a domain name:

- Specify the hostname to resolve
- Specify the information to retrieve:
- **Basic Information -** I.e. host name and to what ip this resolves
- **Host Information -** Known technically as the HINFO, and usually includes information such as hardware and what OS runs on the specified domain (most DNS entries do not contain this information for security reasons.)
- **Aliases -** returns information on what A Records the Domain might have.
- **MX Records** known also as Mail exchangers records, shows which mail server(s) and in what order are responsible for this domain.
- **NS Records** indicate which name servers are responsible for this domain.

In addition it is possible to specify an alternative DNS server

Whois Client

This tool will lookup information on a domain or IP address. You can select a specific Whois Server from the options area, or you can use the 'Default' option which will select a server for you

Trace Route

This tool shows the network path that Chaz followed to reach the target machine.

SNMP Walk

This feature is enabled when a host has SNMP running on it. It enables Chaz to "walk through" a SNMP service, which will reveal a lot of information, such as enumeration of open ports, services running, and so on.

It is described in more detail in the ***"Additional Tools"*** section of the manual.

SNMP Audit

The SNMP Audit tool, allows you to perform an SNMP audit on a device and audit for weak community strings.

Some network devices will have alternative or non-default community strings. The dictionary file contains a list of popular community strings to check for. The default file it uses for the dictionary attack is called snmp-pass.txt. You can either add new community names to this file, or direct the SNMP audit to use another file altogether.

To use the utility, input the IP address of a machine running SNMP and click Retrieve.

Send Message

This option allows Chaz to send NETBIOS Messenger messages with a spoofed source IP address. This option could allow social engineering attacks.

Sending a spoofed message

Note: In some cases the sending of messages to workstations will fail. The Microsoft Client not being installed on the machine could cause this, or other utilities used to block messaging. If the message was sent successfully it will tell you that the message was sent.

Enumerate Computers

This utility will search your network for Domains and/or Workgroups on it. Once it has found that, you will have the ability to scan those Domains for a list of computers in them. Once it has performed its scan it will list whatever OS is installed on that machine, and any comments that might be listed through NETBIOS.

Computers can be enumerated using one of the following methods

- From Active Directory - This method is much faster and will also enumerate computers that are currently switched off
- Using the Windows Explorer interface - This method is slower and will not enumerate computers that are switched off.

You can specify which method to use from the `Information Source' tab. Note that you will need to perform the scan using an account that has access rights to Active Directory.

Installation
==========

Simple: Run it in VB 6 or Install Program

System Requirements
==========

This utility works properly on all 32-bit versions of Windows, including
Windows 98/ME, Windows NT, Windows 2000, and Windows XP. If you want to
use it on Windows NT, you should add psapi.dll into your system32 folder.

Bug Reporting
==========
If you find bugs in the program please either post them to the Web Forum listed above

or email them to: Thecrackers_group <at> yahoo <dot> ca

2005 THE CRACKERS GROUP INC (C) , Nima Bagheri

website: www.geocities.com/thecrackers_group

E-mail : Thecrackers_group <at> yahoo <dot> ca