For this lab section, refer to Figure 26-6 on page 927 of the book.

Step 1

```
PIX2

static (inside,outside) 130.100.26.8 192.168.1.8 netmask
255.255.255.255 0 0

access-list outside_access_in permit udp any host
130.100.26.8 eq 45000
access-list outside_access_in permit udp any host
130.100.26.8 eq syslog
```

Step 2

```
R6

ip audit notify log
ip audit po max-events 100
ip audit po remote hostid 123 orgid 6666 rmtaddress
130.100.26.8 localaddress 130.100.26.6 port 45000 preference
1 timeout 5 application director
ip audit po local hostid 43 orgid 6666
```

Step 3

```
ip audit notify nr-director
ip audit notify log
logging 130.100.26.8

R6#sho log
Syslog logging: enabled (0 messages dropped, 2 messages
rate-limited, 0 flushes, 0 overruns)
    Console logging: level debugging, 108 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled
    Trap logging: level informational, 113 message lines
logged
        Logging to 130.100.26.8, 8 message lines logged
r6#
```

Step 4

```
ip audit name ids info list 66 action alarm
ip audit name ids attack list 66 action alarm
!
interface Serial0/0
 ip address 140.100.56.6 255.255.255.192
 ip audit ids in
!
access-list 66 permit 140.100.0.0
```

Step 5

```
ip audit po max-events 180
```

Step 6

```
ip audit smtp spam 100
```

Step 7

```
ip audit signature 3100 disable
```

Step 8

```
 ip audit signature 1100 disable
```

Step 9

```
ip audit signature 2154 disable
```

Step 10

```
ip audit name ids info action reset
ip audit name ids attack action reset
```

```
R6#sho ip audit all
Event notification through syslog is enabled
Event notification through Net Director is enabled
Default action(s) for info signatures is alarm
Default action(s) for attack signatures is alarm
Default threshold of recipients for spam signature is 100
Signature 1100 disable
Signature 2154 disable
Signature 3100 disable
PostOffice:HostID:43 OrgID:6666 Msg dropped:0
          :Curr Event Buf Size:180  Configured:180
Host ID:123, Organization ID:6666, SYN pkts sent:881,
ACK pkts sent:0, Heartbeat pkts sent:0, Heartbeat ACK pkts
sent:0,
Duplicate ACK pkts received:0, Retransmission:0, Queued
pkts:0
  ID:1 Dest:130.100.26.8:45000 Loc:130.100.26.6:45000 T:5
S:SYN SENT

Audit Rule Configuration
 Audit name testids
    info actions reset
    attack actions reset
 Audit name ids
    info acl list 66 actions alarm
    attack acl list 66 actions alarm
Interface Configuration
 Interface Serial0/0
  Inbound IDS audit rule is ids
    info acl list 66 actions alarm
    attack acl list 66 actions alarm
  Outgoing IDS audit rule is not set
R6#
```

Cisco IOS IDS Signatures List

Signature	Severity	Complexity	Timeframe	Description
1000 IP Options-Bad Option List	Info	Atomic	Original 59 signatures	Triggers on receipt of an IP datagram where the list of IP options in the IP datagram header is incomplete or malformed. The IP options list contains one or more options that perform various network management or debugging tasks.
1001 IP Options-Record Packet Route	Info	Atomic	Original 59 signatures	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 7 (Record Packet Route).
1002 IP Options-Timestamp			Original 59 signatures	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 4 (Timestamp).
1003 IP Options-Provides,c,h,tcc	Info	Atomic	Original 59 signatures	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 2 (Security options).
1004 IP Options-Loose Source Route	Info	Atomic	Original 59 signatures	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 3 (Loose Source Route).
1005 IP Options-SATNET ID	Info	Atomic	Original 59 signatures	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 8 (SATNET stream identifier).
1006 IP Options-Strict Source Route	Info	Atomic	Original 59 signatures	Triggers on receipt of an IP datagram in which the IP option list for the datagram includes option 2 (Strict Source Routing).
1100 IP Fragment Attack	Attack	Atomic	Original 59 signatures	Triggers when any IP datagram is received with an offset value less than 5 but greater than 0 indicated in the

				offset field.
1101 Unknown IP Protocol	Info	Atomic	Modified signature of the original	Triggers when an IP datagram is received with the protocol field set to 134 or greater. These protocol types are undefined or reserved and should not be used.
1102 Impossible IP Packet	Attack	Atomic	Original 59 signatures	This triggers when an IP packet arrives with source equal to destination address. This signature will catch the so-called Land Attack.
1104 IP Localhost Source Spoof	Attack	Atomic	41 additional signatures	This signature triggers when an IP packet with a address of 127.0.0.1 is detected.
1105 Broadcast Source Address	Attack	Atomic	41 additional signatures	This signature triggers when an IP packet with a source address of 255.255.255.255 is detected.
1106 Multicast Ip Source Address	Attack	Atomic	41 additional signatures	This signature triggers when an IP packet with a source address of 224.x.x.x is detected.
1107 RFC 1918 Addresses Seen	Info	Atomic	41 additional signatures	This signature fire when RFC 1918 addresses are detected.
1202 IP Fragment Overrun—Datagram Too Long	Attack	Atomic	41 additional signatures	Triggers when a reassembled fragmented datagram would exceed the declared IP data length or the maximum datagram length.
1206 IP Fragment Too Small	Attack	Atomic	41 additional signatures	Triggers when any fragment other than the final fragment is less than 400 bytes, indicating that the fragment is likely intentionally crafted.
2000 ICMP Echo Reply	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type

				field in the ICMP header set to 0 (Echo Reply).
2001 ICMP Host Unreachable	Info	Atomic	Original 59 signatures	Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 3 (Host Unreachable).
2002 ICMP Source Quench	Info	Atomic	Original 59 signatures	Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 4 (Source Quench).
2003 ICMP Redirect	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 5 (Redirect).
2004 ICMP Echo Request	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 8 (Echo Request).
2005 ICMP Time Exceeded for a Datagram	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 11(Time Exceeded for a Datagram).
2006 ICMP Parameter Problem on Datagram	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 12 (Parameter Problem on Datagram).

2007 ICMP Timestamp Request	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 13 (Timestamp Request).
2008 ICMP Timestamp Reply	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 14 (Timestamp Reply).
2009 ICMP Information Request	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 15 (Information Request).
2010 ICMP Information Reply	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 16 (ICMP Information Reply).
2011 ICMP Address Mask Request	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 17 (Address Mask Request).
2012 ICMP Address Mask Reply	Info	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 18 (Address Mask Reply).
2150 Fragmented ICMP Traffic	Attack	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and either the more fragments flag is

				set to 1 (ICMP) or there is an offset indicated in the offset field.
2151 Large ICMP Traffic	Attack	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP) and the IP length > 1024.
2154 Ping of Death Attack	Attack	Atomic	Original 59 signatures	Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP), the Last Fragment bit is set, and (IP offset * 8) + (IP data length) > 65535 that is to say, the IP offset (which represents the starting position of this fragment in the original packet, and which is in 8 byte units) plus the rest of the packet is greater than the maximum size for an IP packet.
3038 Fragmented NULL TCP Packet	Attack	Atomic	41 additional signatures	Triggers when a single fragmented TCP packet with none of the SYN, FIN, ACK, or RST flags set has been sent to a specific host.
3039 Fragmented Orphaned FIN Packet	Attack	Atomic	41 additional signatures	Triggers when a single fragmented orphaned TCP FIN packet is sent to a privileged port (having port number less than 1024) on a specific host.
3040 NULL TCP Packet	Attack	Atomic	Original 59 signatures	Triggers when a single TCP packet with none of the SYN, FIN, ACK, or RST flags set have been sent to a specific host.
3041 SYN/FIN Packet	Attack	Atomic	Original 59 signatures	Triggers when a single TCP packet with the SYN and FIN flags are set and is sent to a specific host.

3042 Orphaned Fin Packet	Attack	Atomic	Original 59 signatures	Triggers when a single orphaned TCP FIN packet is sent to a privileged port (having port number less than 1024) on a specific host.
3043 Fragmented SYN/FIN Packet	Attack	Atomic	41 additional signatures	Triggers when a single fragmented TCP packet with the SYN and FIN flags are set and is sent to a specific host.
3050 Half-open SYN Attack	Attack	Compound	Original 59 signatures	Triggers when multiple TCP sessions have been improperly initiated on any of several well known service ports. Detection of this signature is currently limited to FTP, Telnet, WWW, SSH and E-mail servers (TCP ports 21, 23, 80, 22 and 25 respectively).
3100 Smail Attack	Attack	Compound	Original 59 signatures	Triggers on the very common smail attack against e-mail servers.
3101 Sendmail Invalid Recipient	Attack	Compound	Original 59 signatures	Triggers on any mail message with a pipe (|) symbol in the recipient field.
3102 Sendmail Invalid Sender	Attack	Compound	Original 59 signatures	Triggers on any mail message with a pipe (|) symbol in the From: field.
3103 Sendmail Reconnaissance	Attack	Compound	Original 59 signatures	Triggers when expn or vrfy commands are issued to the SMTP port.
3104 Archaic Sendmail Attacks	Attack	Compound	Original 59 signatures	Triggers when wiz or debug commands are sent to the SMTP port.
3105 Sendmail Decode Alias	Attack	Compound	Original 59 signatures	Triggers on any mail message with : decode@ in the header.
3106 Mail Spam	Attack	Compound	Original 59 signatures	Counts number of Rcpt to: lines in a single mail message and alarms after a user-definable maximum has been

				exceeded (default is 250).
3107 Majordomo Execute Attack	Attack	Compound	Original 59 signatures	A bug in the Majordomo program will allow remote users to execute arbitrary commands at the privilege level of the server.
3150 FTP Remote Command Execution	Attack	Compound	Original 59 signatures	Triggers when someone tries to execute the FTP SITE command.
3151 FTP SYST Command Attempt	Info	Compound	Original 59 signatures	Triggers when someone tries to execute the FTP SYST command.
3152 FTP CWD ~root	Info	Compound	Original 59 signatures	Triggers when someone tries to execute the CWD ~root command.
3153 FTP Improper Address Specified	Attack	Atomic	Original 59 signatures	Triggers if a port command is issued with an address that is not the same as the requesting host.
3154 FTP Improper Port Specified	Attack	Atomic	Original 59 signatures	Triggers if a port command is issued with a data port specified that is <1024 or >65535.
3215 IIS DOT DOT EXECUTE Attack	Attack	Compound	41 additional signatures	Triggers on any attempt to cause Microsoft's Internet Information Server to execute commands.
3229 Website Win-C-Sample Buffer Overflow	Attack	Compound	41 additional signatures	This signature triggers when an attempt is made to access the win-c-sample program distributed with WebSite servers.
3233 WWW count-cgi Overflow	Attack	Compound	41 additional signatures	This signature triggers when an attempt is made to overflow a buffer in the cgi Count program.
4050 UDP Bomb	Attack	Atomic	Original 59 signatures	Triggers when the UDP length specified is less than the IP length specified. This malformed packet type is associated with a denial of service

				attempt.
4051 Snork	Attack	Atomic	41 additional signatures	This signature triggers when a UDP packet with a source port of either 135, 7, or 19 and a destination port of 135 is detected.
4052 Chargen DoS	Attack	Atomic	41 additional signatures	This signature triggers when a UDP packet is detected with a source port of 7 and a destination port of 19.
4100 Tftp Passwd File	Attack	Compound	Original 59 signatures	Triggers on an attempt to access the passwd file via TFTP. Indicative of an attempt to gain unauthorized access to system resources.
4600 IOS UDP Bomb	Attack	Atomic	41 additional signatures	This signature triggers on receipt of improperly formed SYSLOG transmissions bound for UDP port 514.
5034 WWW IIS newdsn Attack	Attack	Compound	41 additional signatures	This signature triggers when an attempt is made to run the newdsn.exe command via the http server.
5035 HTTP cgi HylaFAX Faxsurvey	Attack	Compound	41 additional signatures	Triggers when an attempt is made to pass commands to the CGI program faxsurvey. A problem in the CGI program faxsurvey, included with the HylaFAX package from SGI, allows an attacker to execute commands on the host machine. These commands will execute at the privilege level of the HTTP server. There are no legitimate reasons to pass commands to the faxsurvey command.
5041 WWW Anyform Attack	Attack	Compound	41 additional signatures	This alarm triggers when an attacker attempts to execute arbitrary commands through the anyform

				cgi-bin script.
5043 WWW Cold Fusion Attack	Attack	Compound	41 additional signatures	This alarm triggers when an attempt is made to access example scripts shipped with Cold Fusion Servers.
5044 WWW Webcom.se Guestbook Attack	Attack	Compound	41 additional signatures	This alarm triggers when an attacker attempts to execute arbitrary commands through Webcom.se's rguest.exe or wguest.exe cgi-bin script.
5045 WWW xterm Display Attack	Attack	Compound	41 additional signatures	Triggers when any cgi-bin script attempts to execute the command xterm -display.
5050 WWW IIS .htr Overflow Attack	Attack	Compound	41 additional signatures	This signature triggers when an .htr buffer overrun attack is detected, indicating a possible attempt to execute remote commands, or cause a denial of service against the targeted Windows NT IIS server.
5055 HTTP Basic Authentication Overflow	Attack	Compound	41 additional signatures	A buffer overflow can occur on vulnerable web servers if a very large username and password combination is used with Basic Authentication.
5071 WWW msacds.dll Attack	Attack	Compound	41 additional signatures	An attempt has been made to execute commands or view secured filed, with privileged access.
5081 WWW WinNT cmd.exe Access	Attack	Atomic	41 additional signatures	Triggers when the use of the Windows NT cmd.exe is detected in a URL.
5090 WWW FrontPage htimage.exe Access	Attack	Atomic	41 additional signatures	Triggers when the FrontPage CGI program is accessed with a filename argument ending with "0,0".

5114 WWW IIS Unicode Attack	Attack	Atomic	41 additional signatures	Triggers when an attempt to exploit the Unicode ../ directory traversal vulnerability is detected.
5116 Endymion MailMan Remote Command Execution	Attack	Atomic	41 additional signatures	Endymion MailMan insecurely uses the perl function open(), which allows user-supplied input containing shell metacharacters to be executed as shell commands with the privilege level of the CGI script.
5117 phpGroupWare Remote Command Exec	Attack	Atomic	41 additional signatures	phpGroupWare is a multi-user groupware suite that is freely distributed. There exists a problem in the software could allow users to remotely execute malicious code by exploiting a vulnerable include() command.
5118 eWave ServletExec 3.0C File Upload	Attack	Atomic	41 additional signatures	UploadServlet is a servlet that ServletExec contains in its server side classes.
5123 WWW Host: Field Overflow	Attack	Atomic	41 additional signatures	This alarm will fire if web traffic is detected sending an abnormally large GET request with a large 'Host' field.
6050 DNS HINFO Request	Info	Atomic	41 additional signatures	Triggers on an attempt to access HINFO records from a DNS server.
6051 DNS Zone Transfer	Info	Atomic	41 additional signatures	Triggers on normal DNS zone transfers, in which the source port is 53.
6052 DNS Zone Transfer from High Port	Attack	Atomic	41 additional signatures	Triggers on an illegitimate DNS zone transfer, in which the source port is not equal to 53.
6053 DNS Request for	Attack	Atomic	41 additional	Triggers on a DNS request for all

All Records			signatures	records.
6054 DNS Version Request	Attack	Atomic	41 additional signatures	Triggers when a request for the version of a DNS server is detected.
6055 DNS Inverse Query Buffer Overflow	Attack	Atomic	41 additional signatures	This alarm triggers when an IQUERY request arrives with a data section that is larger than 255 characters.
6056 DNS NXT Buffer Overflow	Attack	Compound	41 additional signatures	This alarm triggers when a DNS server response arrives that has a long NXT resource where the length of the resource data is > 2069 bytes OR the length of the TCP stream containing the NXT resource is > 3000 bytes.
6057 DNS SIG Buffer Overflow	Attack	Compound	41 additional signatures	This alarm triggers when a DNS server response arrives that has a long SIG resource where the length of the resource data is > 2069 bytes OR the length of the TCP stream containing the SIG resource is > 3000 bytes.
6062 DNS Authors Request	Info	Atomic	41 additional signatures	Alarms when a DNS query type TXT class CHAOS is detected with string "Authors.Bind" (case insensitive).
6063 DNS Incremental Zone Transfer	Info	Atomic	41 additional signatures	Alarms when a DNS query type of 251 is detected.
6100 RPC Port Registration	Info	Atomic	Original 59 signatures	Triggers when attempts are made to register new RPC services on a target host.
6101 RPC Port Unregistration	Info	Atomic	Original 59 signatures	Triggers when attempts are made to unregister existing RPC services on a target host.
6102 RPC Dump	Info	Atomic	Original 59	Triggers when an RPC dump request is issued

			signatures	to a target host.
6103 Proxied RPC Request	Attack	Atomic	Original 59 signatures	Triggers when a proxied RPC request is sent to the portmapper of a target host.
6150 ypserv Portmap Request	Info	Atomic	Original 59 signatures	Triggers when a request is made to the portmapper for the YP server daemon (ypserv) port.
6151 ypbind Portmap Request	Info	Atomic	Original 59 signatures	Triggers when a request is made to the portmapper for the YP bind daemon (ypbind) port.
6152 yppasswdd Portmap Request	Info	Atomic	Original 59 signatures	Triggers when a request is made to the portmapper for the YP password daemon (yppasswdd) port.
6153 ypupdated Portmap Request	Info	Atomic	Original 59 signatures	Triggers when a request is made to the portmapper for the YP update daemon (ypupdated) port.
6154 ypxfrd Portmap Request	Info	Atomic	Original 59 signatures	Triggers when a request is made to the portmapper for the YP transfer daemon (ypxfrd) port.
6155 Mountd Portmap Request	Info	Atomic	Original 59 signatures	Triggers when a request is made to the portmapper for the mount daemon (mountd) port.
6175 rexd Portmap Request	Info	Atomic	Original 59 signatures	Triggers when a request is made to the portmapper for the remote execution daemon (rexd) port.
6180 rexd Attempt	Info	Atomic	Original 59 signatures	Triggers when a call to the rexd program is made. The remote execution daemon is the server responsible for remote program execution. This may be indicative of an attempt to gain unauthorized access to

				system resources.
6190 statd Buffer Overflow	Attack	Atomic	Original 59 signatures	Triggers when a large statd request is sent. This could be an attempt to overflow a buffer and gain access to system resources.
8000 FTP Retrieve Password File	Attack	Atomic	Original 59 signatures	Triggers on string passwd issued during an FTP session. May indicate someone attempting to retrieve the password file from a machine in order to crack it and gain unauthorized access to system resources.