Snort Rules Classification and Interpretation

**Pop2 Rules:**

**Class Type Attempted Admin(SID: 1934, 284,285)**

GEN:SID 1:1934 Message POP2 FOLD overflow attempt Summary This event is generated when an attempt is made to exploit a buffer overflow condition in the Post Office Protocol (POP) command FOLD.

GEN:SID 1:285

Message POP2 x86 Linux overflow

Summary This event generated when an attempt is made to exploit a buffer overflow in the pop2 service.

Impact Remote access. This attack may permit the execution of arbitrary commands on the vulnerable host with the privileges of the user "nobody".

Detailed Information Access to the user "nobody" can be obtained with pop2 or pop3 servers that support "anonymous proxy". "Anonymous proxy" permits the use of a proxy pop server to access mail on another pop server where the user has a valid account. This access to the proxy server as user "nobody". A buffer overflow exists because of improper user input filtering, allowing the attacker to enter an overly long argument to the FOLD command. This may permit the execution of arbitrary commands on the vulnerable server with the privileges of the user "nobody".

Affected Systems Debian Linux 2.1

Redhat Linux 4.2, 5.0, 5.1, and 5.2

University of Washington imap 4.4

University of Washington pop2d 4.4

Attack Scenarios An attacker may attempt to exploit a vulnerable pop2 server, permitting the execution of arbitrary commands with the privilege of user

**Class-Type Misc-Attack(SID: 1935)**

GEN:SID 1:1935 Message POP2 FOLD arbitrary file attempt Summary This event is generated when an attempt is made to exploit a buffer overflow condition in the Post Office Protocol (POP) command FOLD.

Impact Possible remote execution of arbitrary code leading to a remote root compromise.

Detailed Information A vulnerability exists such that an attacker may include files of their choosing when supplying data to a POP server via the FOLD command.

The FOLD command allows the user to specify a mail folder to select. By specifying a very large argument, the user can exploit the buffer overflow condition.
POP3 Rules:

Class-Type Attempted Admin(SID:1866, 1936,1938,2108-2112)
GEN:SID 1:1866 Message POP3 USER overflow attempt Summary This event is generated when an attempt is made to overflow a buffer by supplying a very long username to a POP3 service.
Impact Serious. Several POP3 servers are vulnerable to USER buffer overflows.
Detailed Information A very long string data in place of the username can lead to a buffer overflow situation.

A buffer overflow attack can be used to execute arbitrary code (remote shell). A Denial of Service (DoS) is also possible.

Check your POP3 service for this vulnerability with common vulnerability scanners.
Affected Systems Ipswich IMail 5.0.5, 5.0.6 and 5.0.7 for Windows NT.
Other POP3 mail systems may be affected.
Attack Scenarios An attacker may first check the POP3 daemon version and try a buffer overflow attack using a long username string supplied with the USER command.

This may result in full compromise of the host. A Remote shell can be bound to a port after the attack.

2108…2112 Attempted Admin type
GEN:SID 1:2108 Message POP3 CAPA overflow attempt Summary This event is generated when an attempt is made to exploit a buffer overflow condition in the Post Office Protocol (POP) command CAPA.
Impact Possible remote execution of arbitrary code leading to a remote root compromise.
Detailed Information A vulnerability exists such that an attacker may overflow a buffer by sending multiple line feed characters to a POP server via the CAPA command.

SMTP Rules

Class-Type Attempted Admin(SID: 654,655,657,658,661,663,664)
GEN:SID 1:654 Message SMTP RCPT TO overflow Summary When connecting to port 25 (SMTP) on a computer running a vulnerable SMTP server it is possible to perform a DoS attack. In some cases it might be possible to perform a security breach as well.
Impact Depending on the vulnerable software you may need to restart the SMTP server or perform some level of incident response.
Detailed Information Vulnerable systems:
   Avirt Mail 4.0 (build 4124)
   Avirt Mail 4.2 (build 4807)
   PakMail SMTP/POP3
   Netscape Messaging Server 3.54/3.55/3.6
GEN:SID 1:664 Message SMTP RCPT TO decode attempt Summary This event is generated when maliciously formatted "rcpt to" text is supplied to Sendmail.
Impact Attempted administrator access. A successful attack can allow remote execution of commands with root privileges.
Detailed Information A vulnerability exists in older versions of Sendmail that incorrectly parses message headers. This can allow a malicious user to execute arbitrary commands as root.
Affected Systems Sendmail versions prior to 8.6.10 and any version based on 5.x.
Attack Scenarios An attacker can craft a malicious mail header that executes a command.
Ease of Attack Easy. Use a maliciously formatted header.

GEN:SID 1:657 Message SMTP chameleon overflow Summary This event is generated when an external user sends a HELP command with specific syntax to an internal SMTP server, which may indicate an attempt to exploit a buffer overflow vulnerability in NetManage Chameleon SMTP server.
Impact Severe. Remote execution of arbitrary code, leading to remote root compromise.
Detailed Information NetManage Chameleon SMTP server contains a buffer overflow vulnerability in the HELP command. If the HELP command is used with an argument longer than 514 characters, a buffer overflow condition occurs, allowing the execution of arbitrary code.
Affected Systems Systems running NetManage Chameleon Unix 97 or NetManage Chameleon 4.5.

Class-Type Attempted DOS(SID: 658)
GEN:SID 1:658 Message SMTP exchange mime DOS Summary This event is generated when a denial of service is attempted on a Microsoft Exchange mail server.
Impact Denial of service. This will cause the Exchange server to fail.
Detailed Information A vulnerability exists in Microsoft Exchange 5.5 that causes a denial of service if a MIME header contains the string 'charset = ""'. The Exchange server does not properly handle this MIME header string, causing it to crash.
Affected Systems Microsoft Exchange server 5.5
Attack Scenarios An attacker can supply a malicious string in the MIME header causing the Exchange server to fail.

Class-Type Attempted Recon(SID:659,660,672)
GEN:SID 1:659 Message SMTP expn decode Summary This event is generated when a probe is sent to an SMTP server to determine if the decode alias is supported.
Impact Intelligence gathering activity. This event could be an indication of reconnaissance or an actual attempt to overwrite a sensitive file. If the decode alias is present on the SMTP server, an attacker may use it to overwrite files.
Detailed Information The decode alias was included to allow email to be sent to a username of decode to process the email content through the uudecode program. A malicious user could attempt to email a uuencoded file that would overwrite an existing
sensitive file.
Affected Systems Older UNIX Sendmail versions (~1990-1996)

GEN:SID 1:672 Message SMTP vrfy decode Summary This event is generated when a remote user attempts to scan for a vulnerability in the VRFY command on internal SMTP servers.
Impact Information gathering, possibly leading to a future attack and system compromise.
Detailed Information If the decode alias on the Sendmail server is enabled, an attacker may be able to send messages to the decode alias email address, creating or overwriting files on the server. Vulnerability scanners use the "vrfy decode" command to verify that a decode alias is enabled.
Affected Systems Systems running Sendmail.
Attack Scenarios An attacker scans the server to determine that the decode alias exists. The attacker then sends an email address to the decode alias on the server, with directives to overwrite or create files on the server.

GEN:SID 1:660 Message SMTP expn root Summary This event is generated when an attempt is made to expand the alias of root on a Sendmail server.
Impact Reconnaissance. This is an attempt to discover email addresses associated with the alias of root for a Sendmail server.
Detailed Information An attacker may probe for email addresses associated with the alias of root on a Sendmail server. The "expn" command expands the alias into a list of actual recipients associated with the alias. This command can be used to determine who reads the mail sent to the administrator. It may be used by spammers to get valid email accounts or may be used to discover valid accounts on the Sendmail server.
Affected Systems Versions of Sendmail that do not disable expn.
Attack Scenarios An attacker can telnet to the Sendmail server and issue the command "expn root" to gather email addresses associated with the alias of root.
Ease of Attack Easy. Telnet to the Sendmail server and issue the command "expn root".

Class-Type Attempted User(SID: 665,668-671)
GEN:SID 1:665 Message SMTP sendmail 5.6.5 exploit Summary This event is generated when a remote user attempts to exploit a Sendmail vulnerability where a remote user can execute arbitrary code on an server running older versions of Sendmail.
Impact Severe. Remote execution of arbitrary code, leading to remote root compromise.
Detailed Information Earlier versions of Sendmail contain a vulnerability in message header parsing. This vulnerability can be exploited by a remote user who sends an email message with a malformed MAIL FROM value to a vulnerable Sendmail implementation. The server then executes any arbitrary shell code included in the text of the email.
Affected Systems Systems running Sendmail versions lower than 8.6.10.
Attack Scenarios An attacker sends an email using |usr/bin/tail|usr/bin/sh as the MAIL FROM value. Arbitrary shell code placed in the text of the email message is executed by the mail server with the security context of Sendmail.
GEN:SID 1:671 Message SMTP sendmail 8.6.9c exploit Summary This event is generated when an external attacker attempts to exploit a vulnerability in Sendmail, where unexpected characters in ident messages are not properly parsed. Impact Severe. Remote execution of arbitrary code, leading to remote root compromise. Detailed Information Sendmail 8.6.10 and earlier versions contain a vulnerability related to the parsing of unexpected characters (in this case, newline characters and a carriage return) in commands passed from ident to Sendmail. An attacker can use a specially crafted command with unexpected characters in an ident response to Sendmail. The message is not properly parsed and Sendmail forwards the response, with included commands, to its queue. The commands are then executed while the message awaits delivery in the Sendmail queue, causing the included arbitrary code to be executed on the server in the security context of Sendmail. Affected Systems Systems running unpatched versions of Sendmail 8.6.10 or earlier.

Class-Type Suspicious Login(SID:2275)

GEN:SID 1:2275 Message SMTP AUTH LOGON brute force attempt Summary This event is generated when an attempt is made to gain access to an SMTP server using brute force methods. Impact Attempted remote access. This event may indicate that an attacker is attempting to guess username and password combinations. Alternately, it may indicate that an authorized user has entered an incorrect username and password combination a number of times. Detailed Information An SMTP server will issue an error message after a failed login attempt. This may be an indication of an attacker attempting brute force guessing of username and password combinations. It is also possible that an authorized user has incorrectly entered a legitimate username and password combination. This event will be generated after a number of failed attempts. Affected Systems SMTP servers.

SNMP RULES:

Class-Type Attempted Recon(SID: 1411,1413,1414,1415,1419)

GEN:SID 1:1415 Message SNMP Broadcast request Summary This event is generated when an SNMP-Trap connection over UDP to a broadcast address is made. Impact Information gathering Detailed Information The SNMP (Simple Network Management Protocol) Trap daemon usually listens on port 161, tcp or udp.
An attacker may attempt to send this request to determine if any devices are using SNMP.

Affected Systems Devices running SNMP Trap daemons on well known ports.

Attack Scenarios An attacker sends a packet directed to udp port 161, if successful a reply is generated and the attacker may then launch further attacks against the SNMP daemon on the responding IP addresses.

GEN:SID 1:1413 Message SNMP private access udp Summary This event is generated when an SNMP connection over UDP using the default 'private' community is made.
Impact Information gathering
Detailed Information SNMP (Simple Network Management Protocol) v1 uses communities and IP addresses to authenticate communication between the SNMP client and SNMP daemon. Many SNMP implementations come pre-configured with 'public' and 'private' communities. If these are not disabled, the attacker can gather a great deal of information about the device running the SNMP daemon.

Affected Systems Devices running SNMP daemons with 'public' community enabled.

Attack Scenarios An attacker scans a range of IPs for SNMP servers having the 'public' community set and gathers information about the hosts.

Class-Type Misc-Attack(SID: 1442,1426,1427,1409,1892)

GEN:SID 1:1427 Message SNMP PROTOS test-suite-trap-app attempt Summary This event is generated when an attempt is made to attack a device using SNMP v1.
Impact Varies depending on the implementation. Ranges from Denial of Service (DoS) to code execution.
Detailed Information SNMP is a widely adopted protocol for managing IP networks, including individual network devices, and devices in aggregate.

Several network devices come pre-installed with this protocol for management and monitoring.

A number of vulnerabilities exist in SNMP v1, including a community string buffer overflow, that will allow an attacker to execute arbitrary code or shutdown the service.

Affected Systems Any implementation of SNMP v1 protocol

Attack Scenarios An attacker needs to send a specially crafted packet to UDP port 161 of a vulnerable device, causing a Denial of Service or possible execution of arbitrary code.
SQL Rules

Class type Attempted User

GEN:SID 1:676 Message MS-SQL/SMB sp_start_job - program execution Summary
This event is generated when a command is issued to an SQL database server that may result in a serious compromise of the data stored on that system.
Impact Serious. An attacker may have gained administrator access to the system.
Detailed Information This event is generated when an attacker issues a special command to an SQL database that may result in a serious compromise of all data stored on that system.

Such commands may be used to gain access to a system with the privileges of an administrator, delete data, add data, add users, delete users, return sensitive information or gain intelligence on the server software for further system compromise.

This connection can either be a legitimate telnet connection or the result of spawning a remote shell as a consequence of a successful network exploit.

GEN:SID 1:702 Message MS-SQL/SMB xp_displayparamstmt possible buffer overflow Summary
This event is generated when an attempt is made to exploit a known vulnerability in Microsoft SQL.
Impact Information gathering and data integrity compromise. Possible unauthorized administrative access to the server or application.
Detailed Information This event is generated when an attempt is made to gain unauthorized access to an implementation of Microsoft SQL server or client. This can lead to unauthorized access and possibly escalated privileges to that of the administrator. Data stored on the machine can be compromised and trust relationships between the victim server and other hosts can be exploited by the attacker.

Class Type Shellcode Detect(SID: 691,692,693)

GEN:SID 1:692 Message MS-SQL/SMB shellcode attempt Summary
This event is generated when a command is issued to an SQL database server that may result in a serious compromise of the data stored on that system.
Impact Serious. An attacker may have gained administrator access to the system.
Detailed Information This event is generated when an attacker issues a special command to an SQL database that may result in a serious compromise of all data stored on that system.
Such commands may be used to gain access to a system with the privileges of an administrator, delete data, add data, add users, delete users, return sensitive information or gain intelligence on the server software for further system compromise.

This connection can either be a legitimate telnet connection or the result of spawning a remote shell as a consequence of a successful network exploit.

**ClassType Misc Activity(SID: 2050)**

GEN:SID 1:2050 Message MS-SQL version overflow attempt Summary of MS-SQL server running on a host.
Impact Denial of Service, possible code execution and control of the server.

**Class Type Misc Attack(SID: 2004)**

GEN:SID 1:2004 Message MS-SQL Worm propagation attempt OUTBOUND Summary
This event is generated when an attempt is made by the "Slammer" worm to compromise a Microsoft SQL Server. Specifically, this rule generates an event when the worm activity eminates from the protected network.
Impact A worm targeting a vulnerability in the MS SQL Server 2000 Resolution Service was released on January 25th, 2003. The worm attempts to exploit a buffer overflow in the Resolution Service. Because of the nature of the vulnerability, the worm is able to attempt to compromise other machines very rapidly.

**Telnet Rules**

**Class-Type Attempted DOS(SID: 713)**

GEN:SID 1:713 Message TELNET livingston DOS Summary This event is generated when an attempt is made to exploit a known vulnerability in a Lucent/Livingston Portmaster router.
Impact Denial of Service (DoS).
Detailed Information This event is generated when an attempt is made to issue a Denial of Service (DoS) attack against a Livingston/Lucent router. In some situations malformed data sent to the Telnet service on the router can cause the DoS to occur.

**Class-Type Attempted Admin(SID: 714,715,1252)**

GEN:SID 1:715 Message TELNET Attempted SU from wrong group Summary This event is generated when a telnet server sends an error message regarding a failed user attempt to issue the 'su' command to get root privileges.
Impact Failed root access. This attack occurs when a user attempts to get root privileges using the su command.
Detailed Information An attacker may attempt to gain root privileges by issuing the su command. This implies that the attacker has successfully connected to the telnet server with an account other than root. A failed attempt will cause an error message to be generated indicating that the user is not a member of an authorized group to obtain root privileges.
Affected Systems All telnet servers.
Attack Scenarios An attacker may attempt to gain root privileges on a telnet server.
Ease of Attack Simple
False Positives It is remotely possible that a legitimate user with multiple user accounts may attempt to issue su command from the wrong account.

Class-Type Suspicious Login(SID: 719,710,2406)

GEN:SID 1:719 Message TELNET root login Summary This event is generated after an attempted login to a telnet server using the username root.
Impact Remote root access. This may or may not indicate a successful root login to a telnet server.
Detailed Information This event is generated after a telnet server observes an attempted login with the username root. It is not possible to tell from this event alone whether or not the attempt was successful. If this is followed by a login failure event, the root login did not succeed. However, if no failure message is observed and the rule with SID 718 is enabled, this may indicate that the root login succeeded.
Affected Systems Telnet servers.

Class-Type Successful Admin(SID:1253)

GEN:SID 1:1253 Message TELNET bsd exploit client finishing Summary This event is generated after a successful exploit of the BSD derived Telnet daemon.
Impact Remote root access. This may or may not indicate a successful root
compromise of a telnet server.
Detailed Information This event is generated after a possible successful attempt to compromise
a server running a BSD derived version of Telnet. A buffer overflow condition exists that may present an attacker with the opportunity to execute code of their choosing.

The attacker does not need to login to the server to exploit this vulnerability, only a connection to the server is needed.
Affected Systems Multiple Vendor Telnet servers running versions of telnetd derived from the BSD telnet daemon.

Class-Type Bad Unknown(SID:717,718)
GEN:SID 1:717 Message TELNET not on console Summary This event is generated when a failed remote telnet connection occurs using the root account.
Impact Failed root access. This event indicates that an attacker tried an failed to connect to a telnet server using the root account.

Detailed Information Telnet servers can be configured to disallow connections using the root account. If root privileges are required, the root user must log on to the telnet server's console directly. A failed telnet connection using the root account will generate an error message.
Affected Systems Telnet servers.

Class-Type Not Suspicious
GEN:SID 1:716 Message INFO TELNET access Summary This event is generated when a remote user successfully connects to a telnet server.
Impact Remote access. This event may be an indication of a successful telnet connection by an authorized or unauthorized user.
Detailed Information A message is generated by a telnet server after a successful connection. This particular event occurs when a remote user who does not belong to the internal network successfully connects to a telnet server. This may be a legitimate connection by an authorized user or a undesired connection by an unauthorized user. Since telnet connections are not encrypted, it is possible that user accounts and passwords may be sniffed and used by attackers. Telnet connections are not considered to be secure especially over the Internet. Secure shell is the recommended service for remote connectivity since it uses encrypted sessions.
Affected Systems Telnet servers.
Attack Scenarios An attacker may attempt to connect to a telnet server after sniffing a username and password.
TFTP Rules

Class-Type Attempted Admin (SID: 1941,2337)

GEN:SID 1:1941 Message TFTP GET filename overflow attempt Summary This event is generated by an attempt to exploit a buffer overflow in TFTP file handling routines. Impact Implementation Dependent. Several implementations of TFTP are vulnerable to a buffer overflow when processing long TFTP get requests. This could allow arbitrary code execution or result in a Denial of Service condition. Detailed Information Insufficient bounds checking on requested filenames results in a simple to exploit buffer overflow condition. This condition can be exploited by making a request for an overly long file name.

Class-Type Successful Admin (SID: 1441-1443)

GEN:SID 1:1442 Message TFTP GET shadow Summary This event is generated when a TFTP GET request is made for the "shadow" file. This could be an indication that a remote attacker has compromised a system on the network and is transferring sensitive files back to the attacking system. Impact The "shadow" file normally stores encrypted password hashes and users names for Unix based systems. If this file is being transferred over the network using TFTP it is normally an indication of a system compromise.

In some situations this rule may only indicate a generic TFTP scan attempt, as the attacker may be scanning a large range of IP addresses for TFTP improperly configured TFTP servers.

Class-Type Bad Unknown(SID: 518-520)

GEN:SID 1:518 Message TFTP Put Summary This event is generated when a TFTP PUT request is made. This is an indication that someone is attempting to create or place a file on the server. Impact A TFTP PUT requests allows a remote attacker to create, modify, or replace files on the server running TFTP. If the TFTP server allows anonymous TFTP PUT requests it could be possible to upload malicious files and payloads to the server. Detailed Information This rule will generate an event on in-bound TFTP PUT requests. Attackers may use TFTP to upload and download files from a server that is properly or improperly configured. This could result in malicious payload being uploaded to the server or sensitive files being downloaded.