Using XKEYSCORE to Enable TAO

[redacted]
Booz | Allen | Hamilton SDS Analyst
16 July 2009

Purpose of This Briefing

- To show S2 Analysts how to use XKS to enable TAO operations
- The material covers some of the more common searches in XKS, and shows you how to retrieve valuable SIGINT data that S3/TAO finds useful to exploit a target
- It's NOT designed to teach you about TAO (there are many other briefings for that)

Agenda

- What TAO needs from analysts
- TELNET Sessions in XKS
- Identifying Browers
- Web Forum Logins / Passwords
- Webmail Logins / Passwords

Agenda

- What TAO needs from analysts
- TELNET Sessions in XKS
- Identifying Browsers
- Web Forum Logins / Passwords
- Webmail Logins / Passwords

What does TAO need?

- Network Information
  - Logins and Passwords
  - Router configuration information
- Software Information
  - Browser
  - Version Numbers
  - Operating Systems

- NOTE: If target device is under a satellite hop, please consult your TAO Liaison on how to proceed.

How Do We Get That?

- Network Information
  - We target TELNET, FTP, etc for logins and passwords
    - Use a **LOGIN and PASSWORD QUERY** "*TO*" ports of interest (21, 23, 110, 69, etc)
  - WEBMAIL logins and passwords
    - Use **LOGIN and PASSWORD QUERY** "*TO*" ports of interest (80, 3000, 8080) DO NOT use the login/password you find to log in as your target in Airgap. **Ever**. Just record them and pass to TAO.
  - Router configuration information
    - Use "**Full Log DNI query**" FROM port 23 and "From" IP of interest

How Do We Get That?

- Software Information
  - Browsers
    - Use **HTTP Activity** Query and results are in the "browser" field
  - Servers
    - Use **HTTP Activity:** HTTP "Response" traffic contains web server information
- Operating Systems or Version Numbers
  - Using **FULL LOG DNI** we can do "Banner Grabbing" on content FROM port 23 and FROM the target's IP address

Agenda

- What TAO needs from analysts
- TELNET Sessions in XKS
- Identifying Browers
- Web Forum Logins / Passwords
- Webmail Logins / Passwords

Help me Understand Telnet

Administrator attempts to reach remote host using Telnet

From Port 3434 → To Port 23

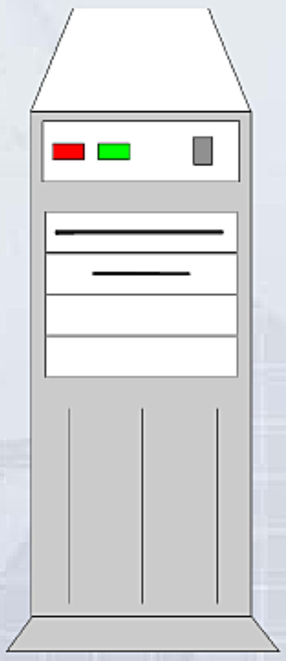
"Telnet 202.[redacted]"

To Port 3434 ← From Port 23

"Welcome to xyz router, Apache 2.0 - Please enter Login & Password"

From Port 3434 → To Port 23

"Username: Admin
Password: Admin"



To Port 3434 ← From Port 23

"Here's your router configuration information

Help me Understand Telnet

Administrator attempts to reach remote host using Telnet

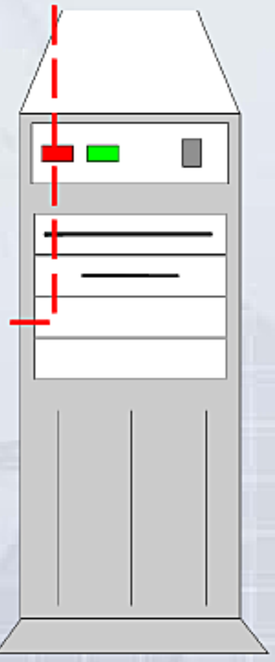
From Port 3434 → To Port 23

"Telnet 202.[redacted]"

Let's make a query and target this traffic!

To Port 3434 ← From Port 23

"Welcome to xyz router, Apache 2.0 - Please enter Login & Password"



From Port 3434 → To Port 23

"Username: Admin
Password: Admin"

To Port 3434 ← From Port 23

"Here's your router configuration information

Banner Grabbing

Search: Full Log

Query Name: [redacted]

Justification: saudi mail server

Additional Justification:

Miranda Number:

Datetime: 1 Week Start: 2009-07-09 00:00 Stop: 2009-0

Client IP:

Username:

Attribute Info: [Populate with Fiel

IP Address: 213.[redacted] From

IP Address: To

Port: 23 From

This is the router's IP address for which you're trying to gain access (mail server maybe?)

Banner Grabbing

To Port 3434 ← From Port 23

"Welcome to xyz router, Apache 2.0 - Please enter Login & Password"

Session 2 of 431

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protocc
2009-07-11 15:12:30	[redacted]	213.[redacted] (Saudi Arabia)	212.[redacted] (Lebanon)	23	44595	TCP

Session | Header (3) | Meta (6)

Formatter: AUTO | Send to: Download Session | Mode: Full Session | Options | Search Content: Enter text to search

Quick Clicks

- Session
- One-Click Searches
  - Find opposite side of sess
    - 213.[redacted]:23 ->
    - 212.[redacted]:445
  - Find traffic on
    - 212.[redacted]
    - 213.[redacted]
  - Find application
    - terminal/telnet/from_se
  - Find fingerprint
    - misc/network/configura
  - Find email address
    - [redacted]

AUTO FORMATTER: app_id= **terminal/telnet/from_server(port23)** Viewer= **ASCII** formatter. Info=

```
............
--------------------------------------------------------------------------
Cisco Router and Security Device Manager (SDM) is installed on this device.
This feature requires the one-time use of the username "cisco"
with the password "cisco". The default username and password have a privilege level of 15

Please change these publicly known initial credentials using SDM or the IOS CLI.
Here are the Cisco IOS commands.

username <myuser>  privilege 15 secret 0 <mypassword>
no username cisco

Replace <myuser> and <mypassword> with the username and password you want to use.

For more information about SDM please follow the instructions in the QUICK START
GUIDE for your router or go to http://www.cisco.com/go/sdm
--------------------------------------------------------------------------


User Access Verification

Username: ......isp
Password:
```

Banner Grabbing (another example)

To Port 3434

"Welcome to xyz router, Apache 2.0 - Please enter Login & Password"

From Port 23

Datetime	Case Notation	From IP	To IP	From Port	To Port
2009-07-11 04:22:46	[redacted]	125.[redacted] (China)	200.[redacted] (Cuba)	23	2192

Session | Header (3) | Meta (4)

Formatter: AUTO | Send to: Download Session | Mode: Full Session | Options | Search Content: Enter text to se

Quick Clicks

- Session
- One-Click Searches
  - Find opposite side of sess
    - 125.[redacted] ->
      - 200.[redacted]
  - Find traffic on
    - 200.[redacted]
    - 125.[redacted]
  - Find application
    - terminal/telnet/from_se

AUTO FORMATTER: app_id= **terminal/telnet/from_server(port23)** Viewer= **ASCII** format

```
......
      ********************************************
      *                                          *
      *     IAD2000  Integrated Access Device    *
      *                                          *
      ********************************************
    Copyright 2002-2005 Huawei Technology. Co., Ltd.
                  Location Name:
                  Phone  Number:

User name (<=15 chars):
```

Banner Grabbing (another example)

Datetime	Case Notation	From IP	To IP	From Port	To Port
2009-07-12 23:59:33	[redacted]	61.[redacted] (China)	200.[redacted] (Cuba)	23	2541

Session | Header (3) | Meta (3)

Formatter: AUTO | Send to: Download Session | Mode: Full Session | Options | Search Content: Enter text to s

Quick Clicks

- Session
- One-Click Searches
  - Find opposite side of sess
    - 61.[redacted]:23 ->
    - 200.[redacted]:25
  - Find traffic on
    - 200.[redacted]
    - 61.[redacted]
  - Find application
    - terminal/telnet/from_se

```
.........................".
##############################################################################
#                                                                            #
#           Welcome to ZTE Full Service Access Platform                      #
#                                                                            #
#                Press Return to get started                                 #
#                                                                            #
#             Copyright 2005-2009 , ZTE Co.,Ltd.                             #
#                                                                            #
##############################################################################
Login:
```

Banner Grabbing (another example)

Datetime	Case Notation	From IP	To IP	From Port	To Port	Proto
2009-07-13 19:36:52	[redacted]	200[redacted] (Cuba)	210[redacted] (China)	23	44710	TCP

Session | Header (3) | Meta (4)

Formatter: AUTO | Send to: Download Session | Mode: Full Session | Options | Search Content: Enter text to search

AUTO FORMATTER: app_id= **terminal/telnet/from_server(port23)** Viewer= **ASCII** formatter.

Quick Clicks

- Session
- One-Click Searches
  - Find opposite side of sess
    - 200[redacted]:23 ->
      210.[redacted]:44
  - Find fingerprint
    - sigdev/huawei
    - misc/network/configura
  - Find traffic on
    - 210.[redacted]
    - 200.[redacted]
  - Find application
    - terminal/telnet/from_se

```
.....................
*******************************************************************************
*  Copyright(c) 1998-2006 Huawei Technologies Co., Ltd.  All rights reserved.  *
*  Without the owner's prior written consent,                                  *
*  no decompiling or reverse-engineering shall be allowed.                     *
*******************************************************************************
...

Login authentication


Username:...........'.........
Username:
Username:
```

Help me Understand Telnet

Administrator attempts to reach remote host using Telnet

From Port 3434 → To Port 23

"Telnet 202.[redacted]"

From Port 23 → To Port 3434

"Welcome to xyz router, Apache 2.0 - Please enter Login & Password"

Let's make a query and target this traffic!

From Port 3434 → To Port 23

"Username: Admin
Password: Admin"

From Port 23 → To Port 3434

"Here's your router configuration information

Telnet Logins and Passwords

Search: Logins and Passwords

Query Name: [redacted]

Justification: chinese telnet sys admin login password

Additional Justification:

Miranda Number:

Datetime: 1 Day Start: 2009-07-14 00:00 Stop: 2009

User Name:

Password:

Domain:

IP Address: From

IP Address: 202.[redacted] To

Port: From

Port: 23 To

This is the router's IP address for which you're trying to gain access (mail server maybe?)

Telnet Usernames and PWs

From Port 3434 → To Port 23

"Username: Admin
Password: Admin"

Datetime	Case Notation	From IP	To IP	From Port	To Po
2009-07-13 07:37:47	[redacted]	195.[redacted] (Yemen)	202.[redacted] (China)	1047	23

Session | Header (3) | Meta (4)

Formatter: AUTO | Send to: Download Session | Mode: Full Session | Options | Search Content: Enter text to

Quick Clicks

- Session
- One-Click Searches
  - Find opposite side of sess
    - 195.[redacted]:1047
      - 202.[redacted]:2
  - Find traffic on
    - 202.[redacted]
    - 195.[redacted]
  - Find application
    - terminal/telnet/to_serv

AUTO FORMATTER: app_id= **terminal/telnet/to_server(port23)** Viewer= **ASCII** forma

```
USER 123
PASS 321
TYPE I
PORT 195,219,37,199,4,24
RETR 1.exe
QUIT
```

Help me Understand Telnet

Administrator attempts to reach remote host using Telnet

From Port 3434 → To Port 23

"Telnet 202.[redacted]"

To Port 3434 ← From Port 23

"Welcome to xyz router, Apache 2.0 - Please enter Login & Password"

From Port 3434 → To Port 23

"Username: Admin
Password: Admin"

To Port 3434 ← From Port 23

"Here's your router configuration information

Router Configs

KEYSCORE

Search: Full Log

Query Name: [redacted]

Justification: iranian mois telnet traffic configs

Additional Justification:

Miranda Number:

Datetime: Custom Start: 2009-07-12 21:00 Stop: 2009-07-15

Client IP:

Username:

Attribute Info:

IP Address: 78.[redacted] Fr

IP Address: To

Port: 23 From

Data Length: >500

From your target's IP

From Port 23

Greater than 500 bytes

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Router Configs

Datetime	Case Notation	From IP	To IP	From Port
2009-07-15 14:32:13	[redacted]	78.[redacted] (Iran)	85.[redacted] (Iran)	23

Session | Header (3) | Meta (5)

Formatter: ASCII | Send to: Download Session | Mode: Full Session | Options | Search Content: Ente

Quick Clicks

- Session
- One-Click Searches
  - Find opposite side of sess
    - 78.[redacted] ->
    - 85.[redacted]:196
  - Find fingerprint
    - fingerprint/router/cisco/
    - misc/network/configura
    - fingerprint/router/cisco
  - Find traffic on
    - 85[redacted]
    - 78[redacted]
  - Find application
    - terminal/telnet/from_se

```
!
interface Ethernet0
 no ip address
 shutdown
!
interface Serial0
 no ip address
 shutdown
 clock rate 2015232
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
 clock rate 2015232
 no fair-queue
!
 --More-- .........          .........interface Serial2
 no ip address
 shutdown
 clock rate 2015232
 no fair-queue
!
interface Serial3
 no ip address
 shutdown
 clock rate 2015232
 no fair-queue
!
interface Serial1:15
 ip unnumbered FastEthernet0
 encapsulation ppp
 isdn switch-type primary-net5
!
interface Serial2:15
 ip unnumbered FastEthernet0
 encapsulation ppp
```

"Thanks for the router config"

-TAO

Many times will contain Access Control Lists (ACLs) – VERY important pieces of Intel. Copy/Paste out full Config…

Agenda

- What TAO needs from analysts
- TELNET Sessions in XKS
- Identifying Browsers
- Web Forum Logins / Passwords
- Webmail Logins and Passwords

Identifying Web Browsers

- Why?
  - TAO can exploit the browsers that lack strong security

User Agent (Browser) pulls

KEYSCORE

This query targets foreign-based targets visiting known Jihadi web forums to learn about what browsers they use.

Search: HTTP Activity

Query Name: web forum browsers

Justification: targets visiting known jihadi web forums

Additional Justification:

Miranda Number:

Datetime: Custom Start: 2009-07-12 00:00 Stop: 2009-07-15 21:59

HTTP Type:

Host: or *hanein.info or *ansar1.net or *ansarnet.info [Populate with URL Field Builder]

Browser:

Country: !US AND !GB AND !CA AND !NZ AND !AU From

Foreign ☺

Web Forum Visitor profiling

KEYSCORE

HTTP Type	Fm Cou	Fm IP	Host	Browser
get	DJ	196.[redacted]	www.alqimmah.net	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) ; SLCC1; .NET
get	SO	196.[redacted]	alqimmah.net	Nokia2680s-2/1.0 (04.91) Profile/MIDP-2.1 Configuration/CLDC-1.1
get	PK	121.[redacted]	www.alqimmah.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; AskTB5.4)
get	AT	80.[redacted]	www.ashiyane.org	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506;
get	ID	125.[redacted]	www.alqimmah.net	Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.0.11) Gecko/2009060215 Firefox/3.0.11
get	LB	77.[redacted]	hanein.info	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Media Center PC 3.0; .NET CLR 1.0.3705; FDM; Creative AutoUpdat
get			www.alhureya.org	Mozilla/4.0 (compatible; MSIE ◆◆◆◆◆□◆□◆◆◆T◆◆◆□◆◆
			www.al-faloja.info	Mozilla/4.0 (compatible; MSIE 6.0; Windows◆◆◆◆◆◆◆◆□◆□◆◆◆R◆◆◆pE◆◆◆◆◆&□◆◆◆□ NT 5.1; S
get	XX	10.[redacted]	www.ashiyane.org	Opera/9.25 (Windows NT 5.1; U; en)
get	PK	116.[redacted]	www.alqimmah.net	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506;
get	DJ	196.[redacted]	www.alqimmah.net	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
get	PK	203.[redacted]	www.alqimmah.net	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/525.19 (KHTML, like Gecko) Chrome/1.0.154.36 Safari/525.
get	MY	60.[redacted]	www.alqimmah.net	Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_6; en-us) AppleWebKit/525.18.1 (KHTML, like Gecko) Version/3.1.2 Safari/5
get	PK	119.[redacted]	www.hanein.info	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; ImageShack Toolbar 4.5.
			www.hanein.info	Mozilla/4.0 (compatible; MSIE 6.0; Windows ◆◆◆◆◆◆◆◆□◆□◆◆◆R◆◆□fl◆◆◆◆◆9 r◆◆◆□ist=0; vbulle
			www.hanein.info	Mozilla/4.0 (compatible; MSI◆◆◆◆◆◆◆◆□◆◆◆◆◆□◆◆□f(◆◆◆◆◆9
			www.al-faloja.info	Mozilla/4.0 (compatible; MSIE 6.0; Win◆◆◆◆◆◆◆◆□◆□◆◆◆R◆◆□f#◆◆◆◆◆&□Yu◆□□dows NT 5.1; SV
			www.al-faloja.info	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;◆◆◆◆◆◆◆◆□◆□◆◆◆R◆◆□f◆◆◆◆◆&□◆◆VS□ SV
get	MY	60.[redacted]		6-002186B9FB5D}; GTB6; SLCC1; .
get	DJ	196.[redacted]		3.0.8
				□(□USz^K8◆P&◆□□□V□
get	AT	88.[redacted]	www.hanein.info	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; SIMBAR={3EEDE99E-6592-11DE-847E-00158307C8DD}; .NET CLR

This displays the From Country (where target is located), their IP, the website they visited, AND their browser

HTTP Activity to find Browsers

HTTP Type	Fm Cou	Host	Browser
get	CN	mefa.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
get	XX	www.moc.gov.ir	Mozilla/4.0 (compatible; MS
get	IR	www.khcu.gov.ir	Mozilla/4.0 (compatible; MS
get	AE	www.mim.gov.ir	Mozilla/4.0 (compatible; MS
get	PH	edd.behdasht.gov.ir	Mozilla/4.0 (compatible; MS
get	JP	vsa.behdasht.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; FREE; .NET CLR 1.1.4322)
get	IR	www.women.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; GTB6; .NET CLR 3.0.04506.648; .NET
post	MX	it.behdasht.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
get	IR	www.khcu.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705; .NET CLR 1.1
get	PK	cms.mfa.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
get	AE	www.mfa.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0
get	IR	www.khcu.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0
get	CH	www.sabt.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0
get	IR	www.women.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0
get	EU	www2.refah.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0
get	IR	transport.irica.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; InfoPath.2)
get	PK	www.mim.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
get	IR	www.women.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 1
get	IR	www.razavimet.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 1
			/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 1
			/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3
			/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3
get	DE	www.sabt.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3
get	IQ	www.mim.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; FDM)
get	IR	www.iscu.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.2)

Here's another example where we targeted the people visiting *gov.ir websites

POP Quiz:

Which browser are we seeing????

HTTP Activity to find Browsers

HTTP Type	Fm Cou	Host	Browser
get	CN	mefa.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
get	XX	www.moc.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
get	IR	www.khcu.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.507
get	AE	www.mim.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 2.0.50727)
get	PH	edd.behdasht.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; DigExt)
get	JP	vsa.behdasht.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; FREE; .NET CLR 1.1.4322)
get	IR	www.women.gov.ir	Mozilla/4.0 (compatible; MSIE
post	MX	it.behdasht.gov.ir	Mozilla/4.0 (compatible; MSIE
get	IR	www.khcu.gov.ir	Mozilla/4.0 (compatible; MSIE
get	PK	cms.mfa.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
get	AE	www.mfa.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0
get	IR	www.khcu.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0
get	CH	www.sabt.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0
get	IR	www.women.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0
get	EU	www2.refah.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0
get	IR	transport.irica.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; InfoPath.2)
get	PK	www.mim.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
get	IR	www.women.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 1
get	IR	www.razavimet.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 1
get	PK	www.mfa.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 1
get	IQ	www.mim.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3
get	IR	www.shohada.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3
get	DE	www.sabt.gov.ir	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3
get			compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; FDM)
get			compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.2)

The browser is “MSIE 6.0” = Internet Explorer 6.0

Mozilla 4.0 is NOT a browser

HTTP Activity to find Browsers

Fm IP	Fm Cou	HTTP T	Host	Browser
114.[redacted]	KR	get	mine.mim.gov.ir	Mozilla/4.0 (compatible; NaverBot/1.0; http://help.naver.com/customer_webtxt_02.jsp)
114.[redacted]	KR	get	www.mim.gov.ir	Mozilla/4.0 (compatible; NaverBot/1.0; http://help.naver.com/delete_main.asp)
217.[redacted]	AT	get	www.mfa.gov.ir	Mozilla/4.0 (compatible;)
202.[redacted]	CN	get	women.mim.gov.ir	Mozilla/5.0
66.[redacted]	DE	get	www.qazvin.gov.ir	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
193.[redacted]	FR	get	www2.refah.gov.ir	Mozilla/5.0 (compatible; Konqueror/3.5; Linux) KHTML/3.5.5 (like Gecko) (Exabot-Thumbnails)
94.[redacted]	FR	get	www.icm.gov.ir	Mozilla/5.0 (compatible; MJ12bot/v1.2.5; http://www.majestic12.co.uk/bot.php?+)
81.[redacted]	AT	get	www.mim.gov.ir	Mozilla/5.0 (compatible; monitis.com - free monitoring service; http://monitis.com)
61.[redacted]	CN	get	www.moc.gov.ir	Mozilla/5.0 (compatible; YodaoBot/1.0; http://www.youdao.com/help/webmaster/spider/;)
72.[redacted]	NL	get	www.sabt.gov.ir	Mozilla/5.0 (en-us) AppleWebKit/525.13 (KHTML, like Gecko; Google Wireless Transcoder) Version/3.1 Safari/525.13
80.[redacted]	AE	get	intl.mim.gov.ir	Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_4_11; en) AppleWebKit/525.18 (KHTML, like Gecko) Version/3.1.2 Safari/525.2
77.[redacted]	FR	get	www.behdasht.gov.ir	Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_5; fr-fr) AppleWebKit/525.18.1 (KHTML, like Gecko) Version/3.1.2 Safari/525
87.[redacted]	IT	get	www.mefa.gov.ir	Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_7; it-it) AppleWebKit/530.18 (KHTML, like Gecko) Version/4.0.1 Safari/530.1
115.[redacted]	CN	get	www.mefa.gov.ir	Mozilla/5.0 (Macintosh; U; Intel Mac OS X; zh-cn) AppleWebKit/523.15.1 (KHTML, like Gecko) Version/3.0.4 Safari/523.15
88.[redacted]	DE	get	www.sabt.gov.ir	Mozilla/5.0 (Macintosh; U; PPC Mac OS X 1 [redacted] 530
41.[redacted]	EG	get	miningstrategy.mim.gov.ir	Mozilla/5.0 (SymbianOS/9.2; U; Series60/3. [redacted] Kit
85.[redacted]	IR	get	www.irica.gov.ir	Mozilla/5.0 (SymbianOS/9.2; U; Series60/3.1 NokiaN95_8GB/31.0.015; Profile/MIDP-2.0 Configuration/CLDC-1.1) AppleWebK
85.[redacted]	RU	get	www.mefa.gov.ir	Mozilla/5.0 (Windows; U; Windows NT 5.1; ar; rv:1.9.0.11) Gecko/2009060215 Firefox/3.0.11
80.[redacted]	AT	get	www.mfa.gov.ir	Mozilla/5.0 (Windows; U; Windows NT 5.1; ar; rv:1.9.0.9) Gecko/2009040821 Firefox/3.0.9
193.[redacted]	DE	get	www.moc.gov.ir	Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1.13) Gecko/20080311 Firefox/2.0.0.13 (.NET CLR 3.5.30729)
217.[redacted]	IR	get	mpo-kj.gov.ir	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.11) Gecko/2009060215 Firefox/3.0.11
80.[redacted]	IR	get	www.tabrizcommerce.gov.ir	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/525.19 (KHTML, like Gecko) Chrome/1.0.154.53 Safari/525.
85.[redacted]	DE	get	selection.behdasht.gov.ir	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/528.8 (KHTML, like Gecko) Chrome/2.0.156.1 Safari/528.8
193.[redacted]	FR	get	lawoffice.mohme.gov.ir	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/530.17 (KHTML, like Gecko) Version/4.0 Safari/530.17
78.[redacted]	IR	get	www.bim.gov.ir	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/530.5 (KHTML, like Gecko) Chrome/2.0.172.31 Safari/530.5

Firefox, Chrome and Safari

Mobile Browsers

Browser

iRAPP/1.5.0 NokiaN96-1/1.20; Series60/3.2 Profile/MIDP-2.1 Configuration/CLDC-1.1

Mozilla/4.0 (compatible; MSIE 5.0; Series60/2.6 Nokia6630/5.03.21 Profile/MIDP-2.0 Configuration/CLDC-1.1)

Mozilla/4.0 (compatible; MSIE 5.0; Series80/2.0 Nokia9300/4.53 Profile/MIDP-2.0 Configuration/CLDC-1.1)

Mozilla/4.0 (compatible; MSIE 5.0; Series90/1.1 Nokia7710/4.10.0 Profile/MIDP-2.0 Configuration/CLDC-1.0)

Mozilla/4.0 (compatible; MSIE 6.0; Symbian OS; Nokia N70/5.063 8.3.0.1

Mozilla/4.0 (compatible; MSIE 6.0; Symbian OS; Nokia N70/5.070 5.3.0.1

Mozilla/4.0 (compatible; MSIE 6.0; Symbian OS; Nokia N70/5.070 6.4.0.1

Mozilla/4.0 (compatible; MSIE 6.0; Symbian OS; Nokia N70/5.073 7.3.0.1

Mozilla/4.0 (compatible; MSIE 6.0; Symbian OS; Nokia N70/5.074 1.4.0.1

Mozilla/5.0 (SymbianOS/9.2; U; Series60/3.1 Nokia5700/3.27; Profile/MIDP-2.0 Configuration/CLDC-1.1) AppleWebKit/413 (KHTML,

Mozilla/5.0 (SymbianOS/9.2; U; Series60/3.1 Nokia5700/3.83.1; Profile/MIDP-2.0 Configuration/CLDC-1.1) AppleWebKit/413 (KHTML

Mozilla/5.0 (SymbianOS/9.2; U; Series60/3.1 Nokia5700/4.21; Profile/MIDP-2.0 Configuration/CLDC-1.1) AppleWebKit/413 (KHTML,

Mozilla/5.0 (SymbianOS/9.2; U; Series60/3.1 Nokia5700/5.11; Profile/MIDP-2.0 Configuration/CLDC-1.1) AppleWebKit/413 (KHTML,

Mozilla/5.0 (SymbianOS/9.2; U; Series60/3.1 Nokia6110Navigator/3.58; Profile/MIDP-2.0 Configuration/CLDC-1.1) AppleWebKit/413 (KHTML, like Gecko) Safari/413

Mozilla/5.0 (SymbianOS/9.2; U; Series60/3.1 Nokia6120c/3.83; Profile/MIDP-2.0 Configuration/CLDC-1.1) AppleWebKit/413 (KHTML, like Gecko) Safari/413

Mozilla/5.0 (SymbianOS/9.2; U; Series60/3.1 Nokia6120c/4.21; Profile/MIDP-2.0 Configuration/CLDC-1.1) AppleWebKit/413 (KHTML, like Gecko) Safari/413

Mozilla/5.0 (SymbianOS/9.2; U; Series60/3.1 Nokia6120c/5.11; Profile/MIDP-2.0 Configuration/CLDC-1.1) AppleWebKit/413 (KHTML, like Gecko) Safari/413

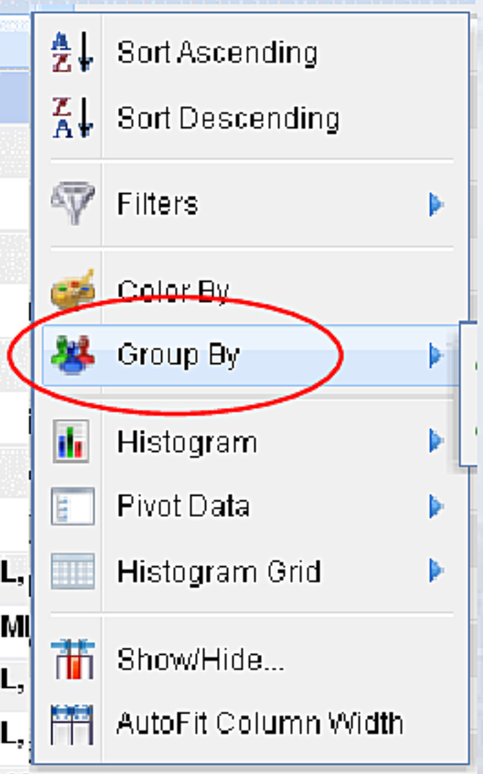
Mozilla/5.0 (SymbianOS/9.2; U; Series60/3.1 Nokia6120c/6.01; Profile/MIDP-2.0 Configuration/CLDC-1.1) AppleWebKit/413 (KHTML, like Gecko) Safari/413

Mozilla/5.0 (SymbianOS/9.2; U; Series60/3.1 Nokia6120c/6.51; Profile/MIDP-2.0 Configuration/CLDC-1.1) AppleWebKit/413 (KHTML, like Gecko) Safari/413

Mozilla/5.0 (SymbianOS/9.2; U; Series60/3.1 NokiaE51-1/100.34.20; Profile/MIDP-2.0 Configuration/CLDC-1.1) AppleWebKit/413 (KHTML, like Gecko) Safari/413

Mozilla/5.0 (SymbianOS/9.2; U; Series60/3.1 NokiaE51-1/200.34.36; Profile/MIDP-2.0 Configuration/CLDC-1.1) AppleWebKit/413 (KHTML, like Gecko) Safari/413

Mozilla/5.0 (SymbianOS/9.2; U; Series60/3.1 NokiaE51-1/300.34.56; Profile/MIDP-2.0 Configuration/CLDC-1.1) AppleWebKit/413 (KHTML, like Gecko) Safari/413



If you have thousands of results, try to “Group By” to “dedupe” results

Watch for Mobile browsers!

Agenda

- What TAO needs from analysts
- TELNET Sessions in XKS
- Identifying Browers
- Web Forum Logins / Passwords
- Webmail Logins / Passwords

Web Forum Logins/PW

KEYSCORE

Search: Logins and Passwords

Query Name: [redacted]

Justification: foreign jihadi web forum users' logins passwords

Additional Justification:

Miranda Number:

Datetime: 2 Days Start: 2009-07-13 00:00 Stop: 2009-07-15 23:5

User Name:

Password:

Domain: *moqawmh.com or *al-shouraa.com or *alhur

IP Address: From

IP Address: To

Port: From

Port: To

Country: !US AND !GB AND !CA AND !NZ AND !AU From

Foreign ☺

Datetime	Case Notation	From IP	To IP	From Port	To Por
2009-07-15 11:27:11	IRS1021A	92[redacted] (Iran)	207.[redacted] (United States)	9253	80

Session | Header (3) | Meta (11) | Attachments (19)

Formatter: AUTO | Send to: Download Session | Mode: Full Session | Options | Search Content: Enter text to search

AUTO FORMATTER: app_id= **mail/webmail/vbulletin** Viewer= **DNI_PRESENTER** formatter. Info=

Quick Clicks

- Session
- Attachments
  - unknown
    - text
      - embedded_base6
      - embedded_base6
      - embedded_base6
      - embedded_base6
      - unknown_500.x-w
      - embedded_base6
      - embedded_base6
      - embedded_base6
      - embedded_base6
      - embedded_base6
      - embedded_base6
      - embedded_base6
      - embedded_base6
      - embedded_base6
      - embedded_base6
      - embedded_base6
      - embedded_base6
      - embedded_base6
- One-Click Searches
  - Find opposite side of se
    - 92.[redacted]:925
    - 207.[redacted]

Display Information: HTTP-POST/Form-Data

UIS Web Form Display

Form Fields	
s	
securitytoken	e3eebef2d93b3b578369032964ae9edac62a442b
do	addmember
url	http://www.ashiyane.org/forums/register.php?do=register
agree	1
password_md5	
passwordconfirm_md5	
day	0
month	0
year	0
username	[redacted]
password	[redacted]
passwordconfirm	[redacted]
email	[redacted]@yahoo.com
emailconfirm	[redacted]@yahoo.com
imagestamp	d382qy
imagehash	b976e8497b5a4aec43a49ad2969958e1

Agenda

- What TAO needs from analysts
- TELNET Sessions in XKS
- FTP Sessions in XKS
- Identifying Browers
- Web Forum Logins / Passwords
- Webmail Logins / Passwords

Webmail Logins – Why?

- Masquerade as user and read mail
  - Useful, but secondary to….
- Potentially use Login/PW to get full access to web server itself
  - Port 80 is useful, but….
  - Port 3000 has XDaemon traffic (woo hoo! Let's take a look)

Web Mail Logins XKEYSCORE

Search: Logins and Passwords

Query Name: [redacted]

Justification: Iranian based webmail servers in iran.

Targeting foreign-based (non-5EYES) Iranian government webmail users

ion:

ber:

me: 1 Week Start: 2009-07-08 00:0

Webmail Ports

User Name:

Password:

Domain: *gov.ir

IP Address: From

IP Address: To

Port: From

Port: 80 or 3000 or 8080 To

Users in and out of Iran

Country: IR or BR or VE or CO or SA or KW or ZA From

Country: To

KEYSCORE

X-KEYSCORE C2C Session Viewer

Session 38 of 134

Datetime	Case Notation	From IP	To IP	From Port	To Port	Protocol
2009-07-13 11:54:00	[redacted]	193.[redacted] (Guinea)	217.[redacted] (Iran)	50423	80	TCP

Session | Header (3) | Meta (6)

formatter: AUTO | Send to: Download Session | Mode: Full Session | Options | Search Content: Enter text to search

Quick Clicks

- Session
- One-Click Searches
  - Find opposite side of sess
    - 193.[redacted] 50423
    - 217.[redacted] 80
  - Find traffic on
    - 217.[redacted]
    - 193.[redacted]
  - Find application
    - http/proxy_to_server/s
  - Find proxy hash
    - c03a567a
  - Find x-forwarded-for IP
    - 193.[redacted]

AUTO FORMATTER: app_id= **http/proxy_to_server/squid_proxy** Viewer= **DNI_PRESENTER** formatter. Info=

Display Information: HTTP-GET

Send to Agility Rea

GET /load_users.php HTTP/1.0

Accept:	image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*
Referer:	http://wvisa.mfa.gov.ir/logo_top_user.php
Accept-Language:	fa
Accept-Encoding:	gzip, deflate
User-Agent:	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host:	wvisa.mfa.gov.ir
Cookie:	azhans_name=---
	azhans_user=[redacted]
	azhans_pass=[redacted]
	azhans_semat=user
	user=THR
	username=---
	place=deleted
	famil=deleted
	__utma=238135644.2300981863224871400.1239874722.1243255420.1107685748.4
	__utmz=238135644.1107685748.4.4.utmcsr=fardanews.com|utmccn=(referral)|utmcmd=referral|utmcct=/fa/pages/links.php
Via:	1.1 centremounainternet-cache.com:3128 (squid/2.6.STABLE16)
X-Forwarded-For:	193.[redacted]

Webmail Logins

- More webmail examples…

Chinese webmail users

KEYSCORE

Search: Logins and Passwords

Query Name: [redacted]

Justification: chinese webmail logins

Additional Justification:

Miranda Number:

Datetime: Custom Start: 2009-07-12 21:00 Stop: 2009-07-15

User Name:

Password:

Domain:

IP Address: From

IP Address: 200.[redacted] To

Port: From

Port: 80 or 3000 To

Country: CN From

XDaemon Logins (webmail)

KEYSCORE

Session 15 of 114

Datetime	Case Notation	From IP	To IP	From Port	To Port
2009-07-11 10:08:42	[redacted]	61.[redacted] (China)	200[redacted] (Cuba)	18445	3000

Session | Header (3) | Meta (6) | Attachments (1)

Formatter: AUTO | Send to: Download Session | Mode: Full Session | Options | Search Content: Enter text to search

AUTO FORMATTER: app_id= **http/post/x-www-form-urlencoded** Viewer= **DNI_PRESENTER** formatter. Info

Quick Clicks

- Session
- Attachments
  - unknown
    - text
      - unknown_621.x-ww
- One-Click Searches
  - Find opposite side of sess
    - 61.[redacted] 18445 ->
    - 200.[redacted]
  - Find traffic on
    - 200.[redacted]
    - 61.[redacted]
  - Find application
    - http/post/x-www-form-

TOP SECRET//COMINT//20320108

ID: sess_orig_proc | **Document type:** HTTP-POST/Form-Data

Display | Raw Data | CCDF

Document Information: File — Expand all

Contents (1) — Expand all

File name	File size	Attachments
html	9	0

Display Information: HTTP — Send to A

UIS Web Form

Form Fields	
User	[redacted]
Password	[redacted]
Logon	Autofirma

Form Fields	
User	[redacted]
Password	[redacted]
Logon	Autofirma

KEYSCORE

Search: Logins and Passwords

Query Name: [redacted]

Justification: chinese webmail logins

Additional Justification:

Miranda Number:

Datetime: Custom Start: 2009-07-12 21:00 Stop: 200

User Name:

Password:

Domain: *126.com

IP Address: From

IP Address: To

Port: From

Port: To

Country: CN From

Webmail Logins PWs

Datetime	Case Notation	From IP	To IP	From Port	To Port
2009-07-15 07:53:19	[redacted]	10.34.35.45 (Private Address)	61.[redacted] (China)	2745	80

Session | Header (3) | Meta (9) | Attachments (1)

Formatter: AUTO | Send to: Download Session | Mode: Full Session | Options | Search Content: Enter text to search

AUTO FORMATTER: app_id= **mail/webmail/coremail** Viewer= **DNI_PRESENTER** formatter. Info=

Quick Clicks

- Session
- Attachments
  - unknown
    - text
      - unknown_395.x-ww
- One-Click Searches
  - Find opposite side of sess
    - 10.34.35.45:2745 ->
      - 61.[redacted]:80
  - Find traffic on
    - 61.[redacted]
    - 10.34.35.45
  - Find application
    - mail/webmail/coremail
  - Find email address
    - [redacted]

Document Information: File

Contents (1)

File name	File type	File size	Attachment
html	HTTP-POST/Form-Data	138	0

Display Information: HTTP-POST/Form-Data

UIS Web Form Display

Form Fields	
domain	126.com
language	0
bCookie	
username	[redacted]@126.com
savelogin	
user	[redacted]
password	[redacted]
style	-1
enter.x	µÇ¡¡Â¼

KEYSCORE

Datetime	Case Notation	From IP	To IP	From Port	To Port
2009-07-13 07:27:18	[redacted]	82[redacted] (United Arab Emirates)	79[redacted] (Iran)	32227	80

Session | Header (3) | Meta (7) | Attachments (1)

Formatter: AUTO | Send to: Download Session | Mode: Full Session | Options | Search Content: Enter text to search

AUTO FORMATTER: app_id= **mail/webmail/vbulletin** Viewer= **DNI_PRESENTER** formatter. Info=

Quick Clicks

- Session
- Attachments
  - unknown
    - text
      - unknown_402.x-ww
- One-Click Searches
  - Find opposite side of sess
    - 82[redacted]32227
    - 79[redacted]:80
  - Find traffic on
    - 79[redacted]
    - 82[redacted]
  - Find application
    - mail/webmail/vbulletin

ID: sess_orig_proc | **Document type:** HTTP-POST/Form-Data

Display | Raw Data | CCDF

Document Information: File — Expand

Contents (1) — Expand

File name	File type	File size	Attachments
html	HTTP-POST/Form-Data	158	0

Display Information: HTTP-POST/Form-Data — Send

UIS Web Form Display

Form Fields	
username	[redacted]
passwd	[redacted]
Submit	ورود
option	com_user
task	login
return	L2hvbWUuaHRtbA==
1dfabb339f736fbfa32843e9ebf36b52	1

Identifying Servers

- Web Servers run particular software
  - E.g. Apache, Microsoft IIS, Unix, et…
  - TAO has exploits for particular ones

XKS query to find server info

- This targets Jihadi web forums for their Server information

Search: HTTP Activity

Query Name: [redacted]

Justification: jihad web forums

Additional Justification:

Miranda Number:

Datetime: 3 Days Start: 2009-07-12 00:00 Stop: 2009-07-

HTTP Type: response

Host: *moqawmh.com or *al-shouraa.com or *alhur [Populate with URL]

Country: !US AND !GB AND !CA AND !NZ AND !AU To

Foreign ☺

XKS query to find server info

KEYSCORE

Search: HTTP Activity

Query Name: [redacted]

Justification: ir mois web servers

Additional Justification:

Miranda Number:

Datetime: Custom Start: 2009-07-12 21:00

HTTP Type: response

IP Address: regex:87\.247\.16[0-3]\.[0-255] From

Country: !US AND !GB AND !CA AND !NZ AND !AU To

This is the network to which I'm trying to gain access (IR MOIS).

Foreign ☺

Results for Server query

- In the HTTP Activity results, you see the servers listed

Server Type	G
Apache/2.2.11 (Unix) PHP/4.4.7 with Suhosin-Patch mod_ssl/2.2.11 OpenSSL/0.9	
Apache/2.2.11 (Unix) PHP/5.2.6 with Suhosin-Patch mod_ssl/2.2.11 OpenSSL/0.9	
Apache/2.2.11 (Unix) PHP/5.2.8	
Apache/2.2.11 (Unix) PHP/5.2.8 with Suhosin-Patch mod_ssl/2.2.11 OpenSSL/0.9	
Apache/2.2.11 (Unix) PHP/5.2.9	
Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i mod_autoindex_cc	
Apache/2.2.2 (Unix)	
Apache/2.2.3 (CentOS)	
Apache/2.2.3 (Debian) DAV/2 mod_perl/2.0.2 Perl/v5.8.8	

Summary

- Many times when we task TAO we have back/forth conversations about how to exploit the target. These slides should help you find the things that TAO needs from S2 Analysts. It's difficult to cover all of the examples of how XKS can help, but this is a good start..

- Good luck.