SCADA Security

Christian Paulino

Instructor: JanuszZalewski

CEN 4935

Software Project in Computer Networks

Florida Gulf Coast University

10501 FGCU Blvd. S.

Fort Myers, FL 33965-6565

Fall 2012

Draft #9

Submission Date: December 8, 2012

1. Introduction

SCADA stands for Supervisory Control and Data Acquisition. SCADA systems are an important part of most nations' infrastructures. They control a wide variety of operations such as pipelines, chemical plants, power plants, water management systems, etc. Because a SCADA system provides remote monitoring and control, it is perfect for industrial operations that could be hazardous to an operator.

SCADA has come a long way since it was developed in 1960. Low-cost microcomputers made computer control of process and manufacturing operations feasible. Programmable logic controllers also known as PLCs introduced relay ladder logic to the control industrial process. They allowed engineers to program in relay logic instead of using programming languages and operating systems. Initially, control systems were only accessed locally. With the evolution of the microcomputers, PLCs, standard computers, operating systems, and networks, SCADA has expanded into distributed systems. SCADA now allows real-time remote monitoring and control distant operations. The typical SCADA system is networked with a master terminal unit(MTU), one or more controllers for communication, and one or more remote terminal units(RTU).[3] This is illustrated in Figure 1.

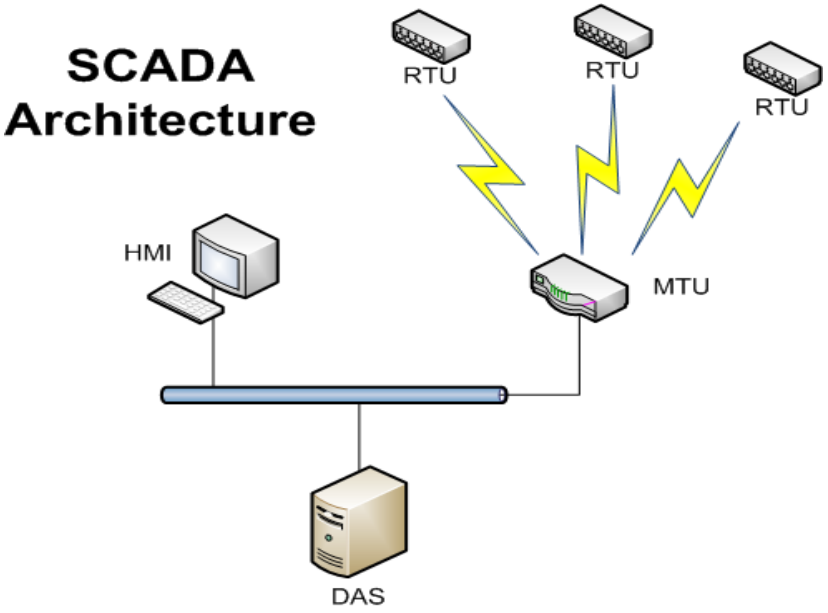

Fig.1. Typical SCADA system setup

(Source: http://isc.sans.edu/diary.html?storyid=13927)

For this project, there is one RTU, one controller, and a workstation connected to the controller. The operator uses a web-based human machine interface(HMI) to control and monitor the system. The RTU and supervisory station are shown in figure 2.

This project focuses on the security aspect of a SCADA system. There are many issues in security when it comes to a SCADA system. Some examples are

- Encryption and Authentication
- Network Traffic Analysis
- Common Security Vulnerabilities

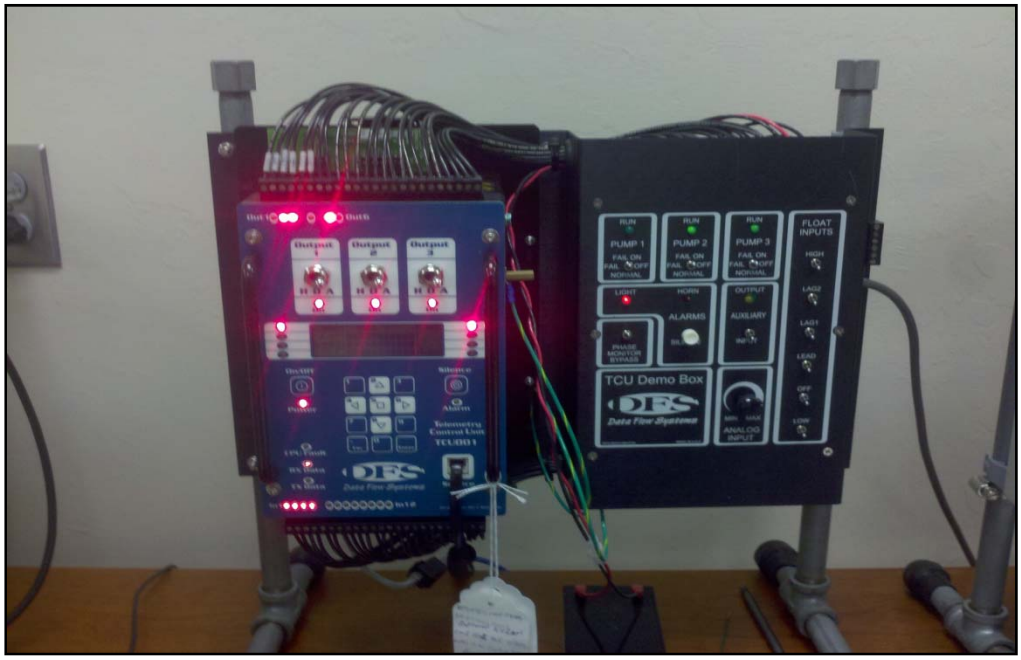

Fig.2.SCADA system RTUin Florida Gulf Coast University CS lab

1.1.Encryption and Authentication

Encryption hides the data and authentication forces the sender of data to prove their identity. SCADA's communication security standards are set in place to protect the system from spoofing, encryption attacks,signature attacks, and protocol attacks, replay of messages, data tampering, and eavesdropping.[6]

Spoofing is when a third party pretends to be one of the communication devices. An encryption attack is an attempt at cracking the encrypted code that protects the data. A signature attack attempts to crack the secret code that proves data hasn't been changed.A protocol attack is an injection of unintended messages such as misleading data or unintended controls. Replaying messages is when a third party captures old data and sends it again. This vulnerability is especially dangerous for controls. Data tampering is when a third party modifies the contents of a message. Eavesdropping is when a third party attempts to get some of the data and use it to their advantage.[6]

The way most of these communication vulnerabilities are prevented, is by dynamically changing the keys used for signatures and encryption. This practice is called key rotation. There are currently two standards for SCADA communication. There is the AGA12 / IEEE 1711 standard and the DNP3 secure authentication standard. AGA12 has a philosophy based on encryption. This philosophy incorporates confidentiality, key technology, cryptographicstandards, and validation. AGA12 protects messages through authenticating the partner device and randomizing the transactions between them. This means that it signs and encrypts all messages.[6]

DNP3 secure authentication has a philosophy that is based on authentication and challenge. This philosophy includes proving identity using challenges and uses key technology.DNP3 protects all actions that are considered critical to the SCADA system. It uses the protocol application layer 'challenge'. Controls and configurations change periodically. A signature is used to prevent tampering. The way authentication challenge works is relatively straightforward. The non-critical messages operate normally. Critical messages are challenged and the operation of a challenged message only goes through if the message passes the challenge. The Master or RTU are able to issue a challenge. Challenges

and responses use session keys. These two standards help protect the communications of a SCADA server using encryption and authentication.[6]

1.2.Network TrafficAnalysis

It is important to analyze patterns of user activity within the network a SCADA system is on. This is done by network traffic traces. Network traffic analysis can be split into four main categories. There is traffic matrix, traffic volume, traffic dynamics, and traffic mixture measurement.[17]

Traffic matrix measurement is done to estimate the volume of traffic between the origin and destination within a network. There are two general approaches to traffic matrix measurement. There is network tomography and direct measurement. Network tomography indirectly infers end-to-end traffic demands based on traffic measurements within the network. Direct measurement holds information of where traffic flows at each point in the network. The points are merged into a central point to find the end point of each flow.[17]

Traffic volume measurements aims to show the total traffic sent or received on a network. This is done by aggregating the total byte or packet count for each source IP address. This can be used to identify heavy users and find possible causes of congestion on the network. This information can be used to determine the source of a possible security risk to a SCADA system.[17]

Traffic dynamics measurement measures the temporal variation in Internet traffic. This is used to test the stability of a network. The tests check for packet delay, packet loss, and detecting possible bottlenecks.

Traffic mixture measurement involves aggregating traffic data over a long period of time. These data are used to detect anomalies, analyze performance, and do security management. The data gathered from network traffic analysis can be of vital importance to the security of a SCADA system.[17]

1.3. Common Security Vulnerabilities

Often times information about a company network is easily obtainable through public routine queries. This public information can be used by attackers to focus their attacks against the network.A website often has data that network intruders will find very useful. Some examples are employee names, e-mail addresses, network system names, and the company's structure. The domain name service (DNS) can provide IP addresses and server information.[19]

A SCADA system may have weak network architecture. The weakness of the architecture increases the risk that an internet based compromise could also compromise the SCADA system. Four common architectural weaknesses include the following.

- The configuration of file transfer protocol (FTP), web, and e-mail servers sometimes unnecessarily provide internal corporate network access.
- Networks connections with corporate partners may not be protected by a firewall.
- Dial-up modem access is unnecessarily granted and dial access policies are often forgone.

Firewalls are not implemented internally leaving little to no separation between network segments.[19]

The lack of real-time monitoring creates a big security risk. If there is a large amount of data coming in from network security devices, it may be overwhelming and cause the attempt at monitoring to fail. Even if there is an intrusion detection system that has been implemented, the network security staff can only recognize individual attacks. This stops organized attack patterns from being recognized. These common vulnerabilities within a SCADA system should be recognized and addressed from the beginning. It is important within a SCADA system to go over every detail of risk and implement measures to prevent potential security breaches.[19]

2. Previous Work

This project is a continuation of previous ones, by T. Bennet[1] and M. Humphries [2]. The following section briefly outlines what was previously accomplished.

2.1 Hardware

The SCADA system for this project has already been setup. The RTU, control unit, and workstation are all able to connect to each other over a network. When switches are flipped on the RTU, the workstation is able to display the status. Besides setting up the SCADA system, some analysis has been done.Florida Gulf Coast University's SCADA system is setup using Red Hat and Apache for the webserver. The computers are on a Computer Science specific network that is controlled by Extreme Networks. The Extreme Networks firewall was determined to provide industrial strength against outside attacks.More analysis was done on the connection between the SCADA server and the workstation. There was a physical layer of risk only. A hacker would have to plug into the Netgear network switch that connects the workstation with the SCADA server. This was the hardware analysis of the previous project.

2.2 Software

The software analysis that was done involved using Netstat, Metasploit and Wireshark.The Netstat tests were done using an SSH connection with Putty on the workstation.

2.2.1 Netstat

The first step of the test displayed all active network connections running through the primary network device. The second step displayed all active connections on the UDP network communication. The third step was to display all the active UNIX domain sockets.

2.2.2 Metasploit

Metasploit was used to perform a penetration test.A penetration test is a test that simulates an attack from an outside malicious source. The first step was to do a brute-force attack. What the brute force did was select all known running processes and try to crack their password. The processes selected were MySQL, HTTP, HTTPS, SSH, Telnet, FTP, LOGIN, SHELL, and SNMP. After 7 minutes the brute-force failed and showed that an attack of that level would not work. The second step was to perform an exploit test. An exploit test involves trying to take advantage of a bug, glitch, vulnerability, etc, in order to gain access to a system. The exploit test ended after three minutes with the attack being unsuccessful.

2.2.3 Wireshark

Wireshark testing was the last part of the analysis done. It was used to analyze packets being sent to and from the SCADA server. After starting a packet capturing session, the workstation was used to logon to the SCADA server. After viewing the current summary of the SCADA system, the packet capturing session was terminated. The packets were filtered down to just the ones related to the SCADA system. These packets were analyzed to show how strong the systems log in security was. The security proved to be strong and thus ended the analysis.

3. Definition of the Problem

A specific SCADA system may have critical importance to the systems infrastructure, which make security extremely important. Because SCADA systems work on a network, they are vulnerable to attack. Important information may be stolen, an operator may be locked out at a critical time, and the control may be disrupted. Many SCADA system operations are delicate. If one is interrupted, it may result in large amounts of damaged equipment, injury to humans, or even death.[3] For this project, the focus is on network intrusions through viruses, worms, and other types of malicious code. A key element for any network to protect against these kinds of risks is the firewall. The firewall needs to be configured appropriately based on the needs of the system.

4. Prospective Solution

Before the security of a system can be enhanced, information on the current level of security must be gathered and analyzed. Following the documentation of the previous project, this project will reproduce the experiment results.[2] These results are the data on the security of FGCU's SCADA system. This data needs to be analyzed to determine the possible security risks in the system.

After the security risks are determined, this project will implement a way to possibly improve the security. The firewall on the SCADA server will be used to do packet-filtering. Packet-filtering examines the packets that are sent to the network. It checks the source IP address, the destination IP address, and the internet protocols carried by the packet.[3] This process is shown in Figure 3. The windows firewall can be configured to either permit or deny incoming packets. Rules will be created that will allow only the necessary connections for operation of the projects SCADA system to enter. This will help ensure connections with malicious intent cannot connect to the system.

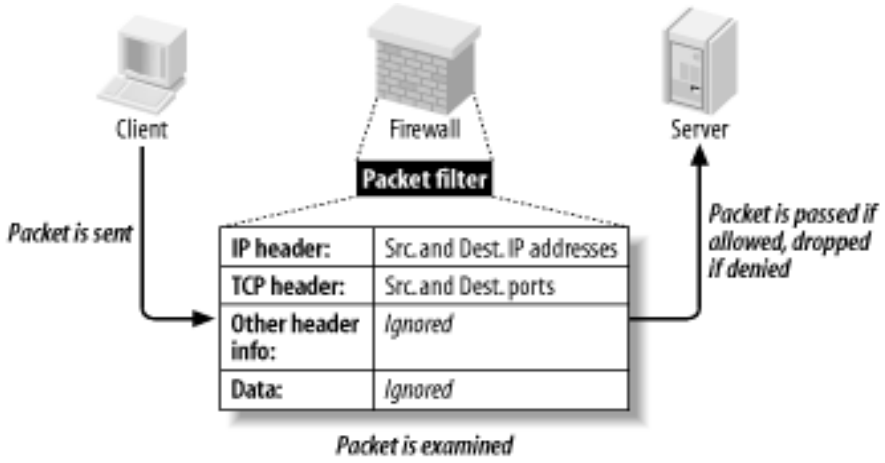

Fig.3. Packet filtering process

(Source: http://fengnet.com/book/Building.Secure.Servers.with.Linux/bssrvrlnx-CHP-2-SECT-5.html

5. Implementation

The first step is to see what connections are running on the SCADA server. The tests were conducted via Putty on the workstation through an SSH connection.The command “netstat –at” was entered and all active networks going through the network device were displayed. The results are shown in Figure 4.

```
[mgr@HyperTACII mgr]$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0    268 HYPERTACII:ssh          69.88.163.28:57279      ESTABLISHED
tcp        0      0 *:dfsinfo               *:*                     LISTEN
tcp        0      0 *:mysql                 *:*                     LISTEN
tcp        0      0 *:www                   *:*                     LISTEN
tcp        0      0 *:https                 *:*                     LISTEN
tcp        0      0 *:printer               *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 *:ftp                   *:*                     LISTEN
tcp        0      0 *:time                  *:*                     LISTEN
tcp        0      0 *:telnet                *:*                     LISTEN
tcp        0      0 *:shell                 *:*                     LISTEN
tcp        0      0 *:login                 *:*                     LISTEN
tcp        0      0 *:finger                *:*                     LISTEN
tcp        0      0 *:auth                  *:*                     LISTEN
tcp        0      0 *:1024                  *:*                     LISTEN
tcp        0      0 *:sunrpc                *:*                     LISTEN
[mgr@HyperTACII mgr]$
```

Fig.4. Active TCP Internet Connections

Next, the command “netstat –l” was entered to display the active connections on UDP network communication.The results are shown in Figure 5.

```
[mgr@HyperTACII mgr]$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:dfsinfo               *:*                     LISTEN
tcp        0      0 *:mysql                 *:*                     LISTEN
tcp        0      0 *:www                   *:*                     LISTEN
tcp        0      0 *:https                 *:*                     LISTEN
tcp        0      0 *:printer               *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 *:ftp                   *:*                     LISTEN
tcp        0      0 *:time                  *:*                     LISTEN
tcp        0      0 *:telnet                *:*                     LISTEN
tcp        0      0 *:shell                 *:*                     LISTEN
tcp        0      0 *:login                 *:*                     LISTEN
tcp        0      0 *:finger                *:*                     LISTEN
tcp        0      0 *:auth                  *:*                     LISTEN
tcp        0      0 *:1024                  *:*                     LISTEN
tcp        0      0 *:sunrpc                *:*                     LISTEN
udp        0      0 *:dfsvoice              *:*
udp        0      0 *:1044                  *:*
udp        0      0 *:1043                  *:*
udp        0      0 *:1042                  *:*
udp        0      0 *:dfspatch              *:*
udp        0      0 *:dfshsuport            *:*
udp        0      0 *:1041                  *:*
udp        0      0 *:1040                  *:*
udp        0      0 *:1039                  *:*
udp        0      0 *:driver5               *:*
udp        0      0 *:driver6               *:*
udp        0      0 *:driver0               *:*
udp        0      0 *:1038                  *:*
udp        0      0 *:1037                  *:*
udp        0      0 *:1036                  *:*
```

Fig.5. Active Network UDP Connections

The last netstat command that was run was “netstat –xl”. This displayed the active UNIX domain sockets. The results are shown in Figure 6.

```
[mgr@HyperTACII mgr]$ netstat -xl
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node Path
unix  0      [ ACC ]     STREAM     LISTENING     796    /tmp/.font-unix/fs7100
unix  0      [ ACC ]     STREAM     LISTENING     791    /var/lib/mysql/mysql.sock
[mgr@HyperTACII mgr]$
```

Fig.6. Active UNIX Domain Socket

The next step is to see how the workstation and the SCADA server interact. A software package called Wireshark was used to this purpose. Wireshark is a packet capturing program than can be used to analyzepackets that are sent over a network.[30]Figure 7 shows how Wireshark was used to capture the packets in the CS lab where the workstation and SCADA server are located.

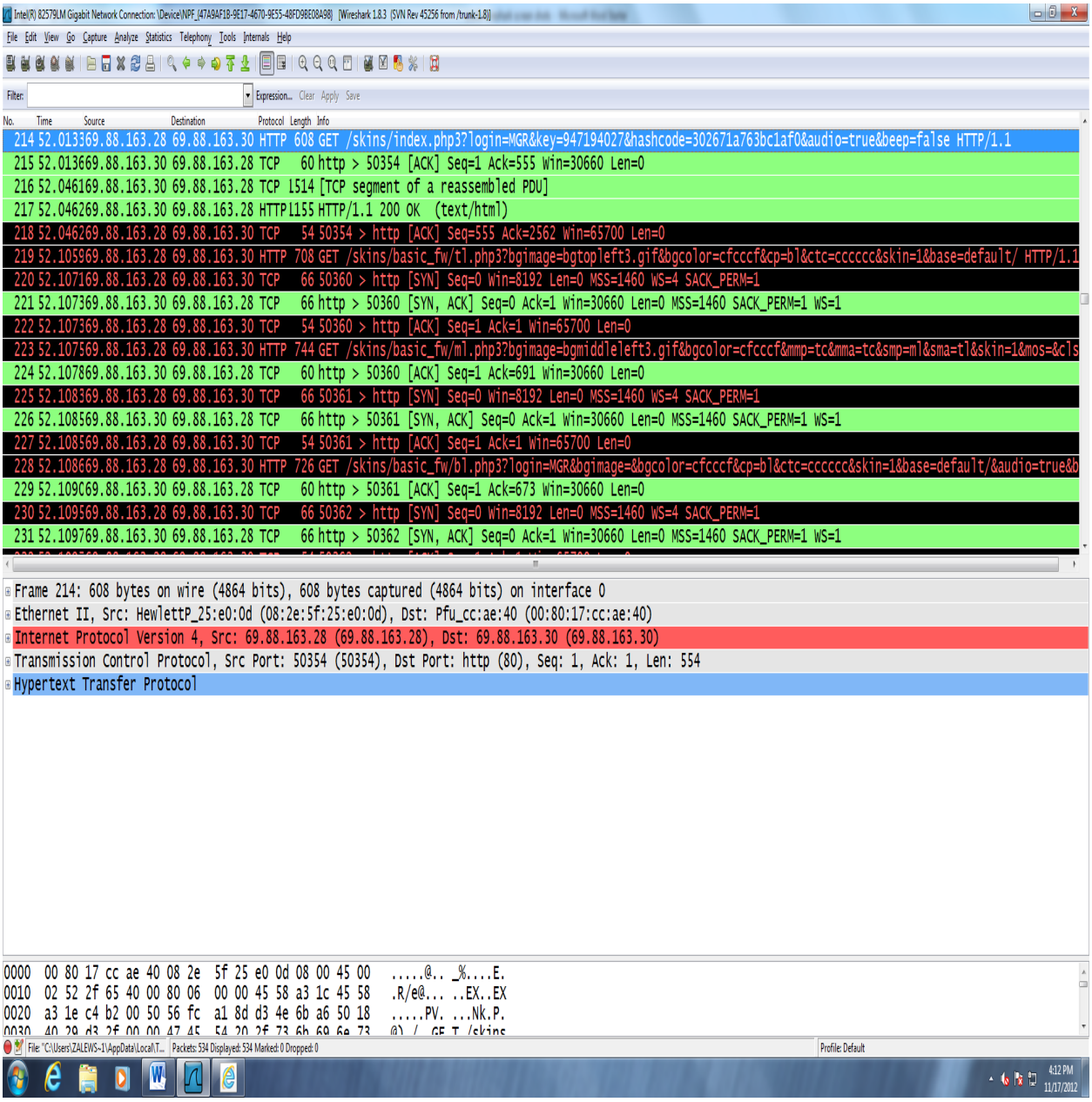

Fig.7. Whireshark all packets

The Wireshark results were filtered to include only packets sent from the workstation to the SCADA server as shown in Figure 8. The filtering is done by entering a command into the filter text box. The filter text box is highlighted green in Figure 8. To filter by IP address, both source and destination addresses are required. The command used to filter between the workstation and the SCADA server is

`“ip.src==69.88.163.28 and ip.dst==69.88.163.30”.`

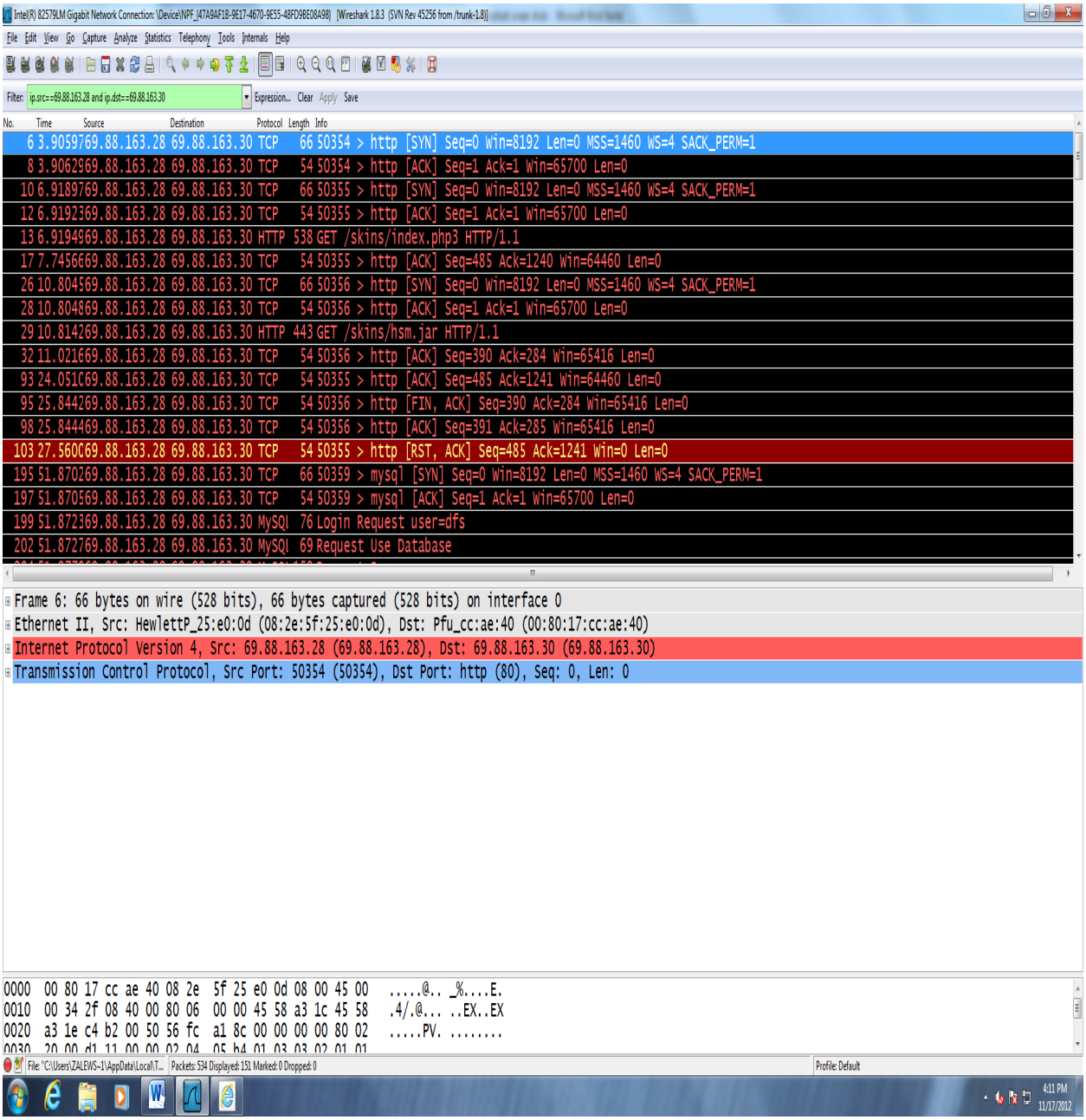

Fig.8. Wireshark workstation to SCADA server packets

Next Wireshark was filtered even further to highlight the login packet. This is shown in Figure 9. This was found by using the ctrl + f function. After hitting ctrl + f, String needs to be selected and then any String that resides in the list of packets can be found. In this case it was mgr, which is the username. The username was searched for until the packet that displayed both the username and the key. That packet is the one that was used to login.

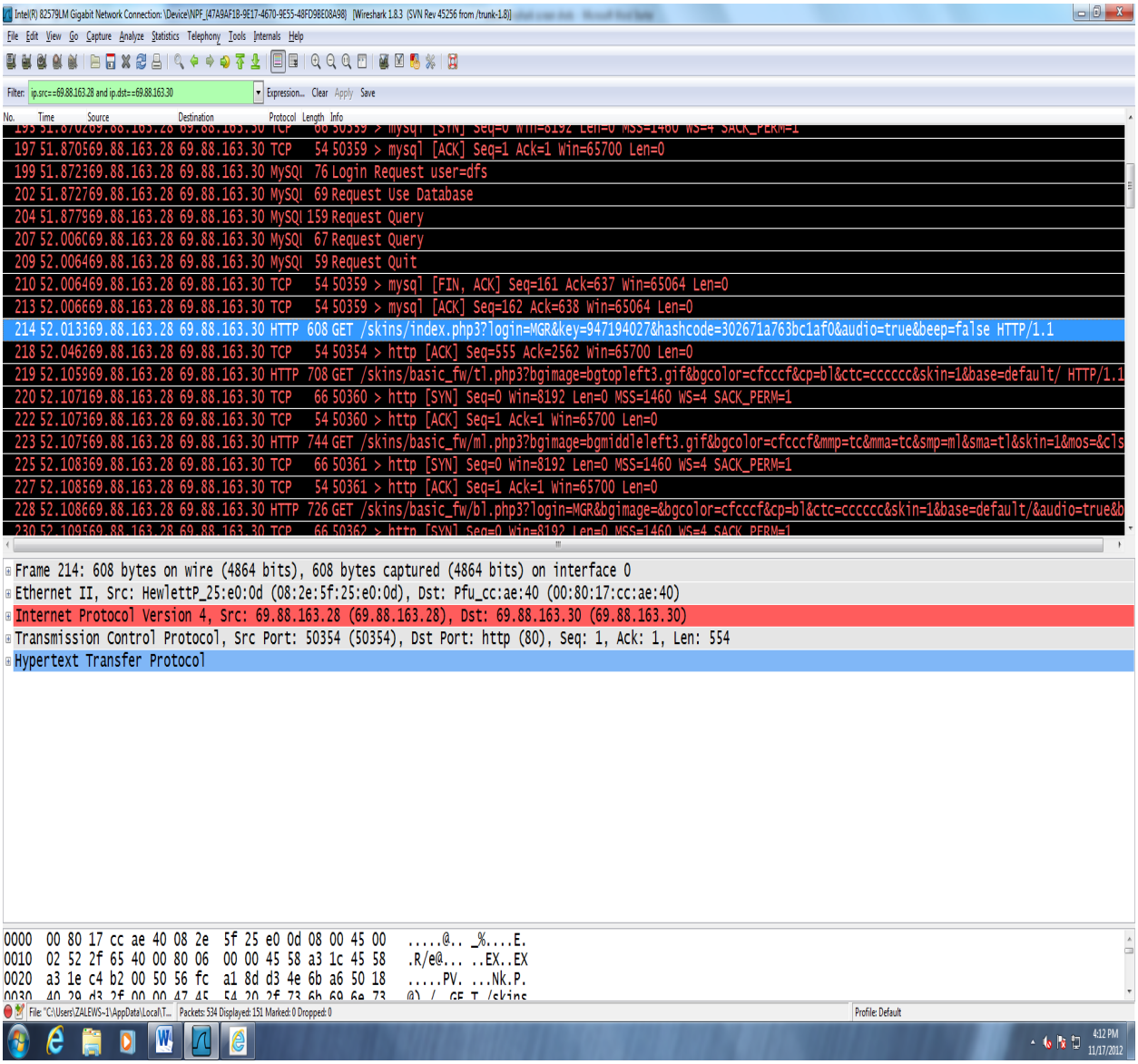

Fig.9 Wireshark login packet

The last step is to see how the SCADA server fairs against attacks. This is done with a penetration testing tool called Meatasploit.Metasploit is a software that has various penetration tests built into it.[31]Before running any tests, the SCADA server needs to be detected. This is done by running a scan with metasploit looking for the SCADA server's IP address which is 69.88.163.30. The results of the scan are shown in figure 10 and the detected IP addresses are shown in figure 11.

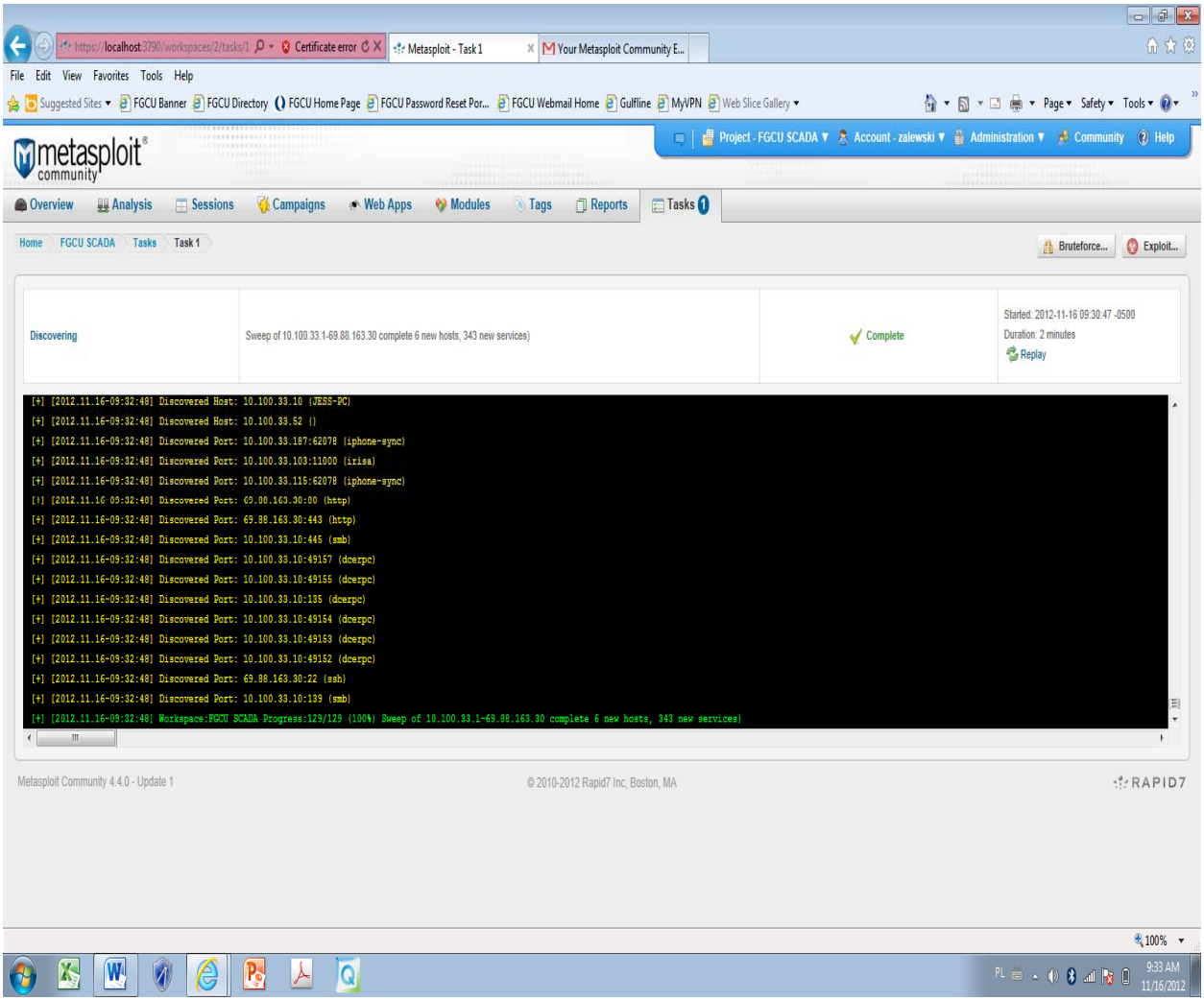

Fig.10 Metasploit scan results

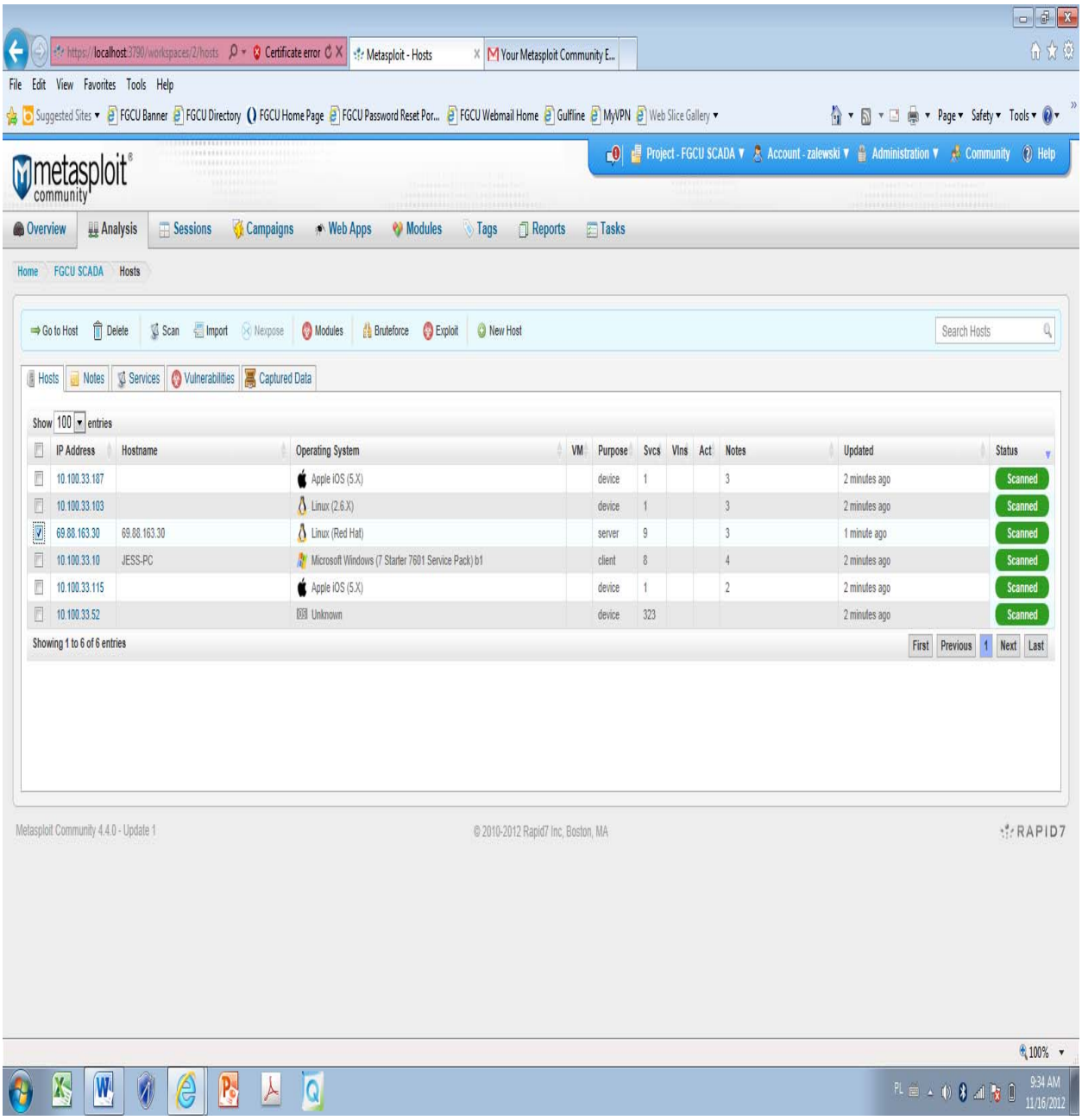

Fig.11 Metasploit detected IP addresses

After the SCADA server is detected, the penetration tests can start.The first test is the bruteforce test. A brute force tests to see how secure the SCADA server's keys are. Metasploit generates a bunch of different keys and attempts to enter the SCADA server with each one. In this experiment, the test failed. That means that the SCADA server is secure against a brute force attack. Figure 12 shows the results of the test.

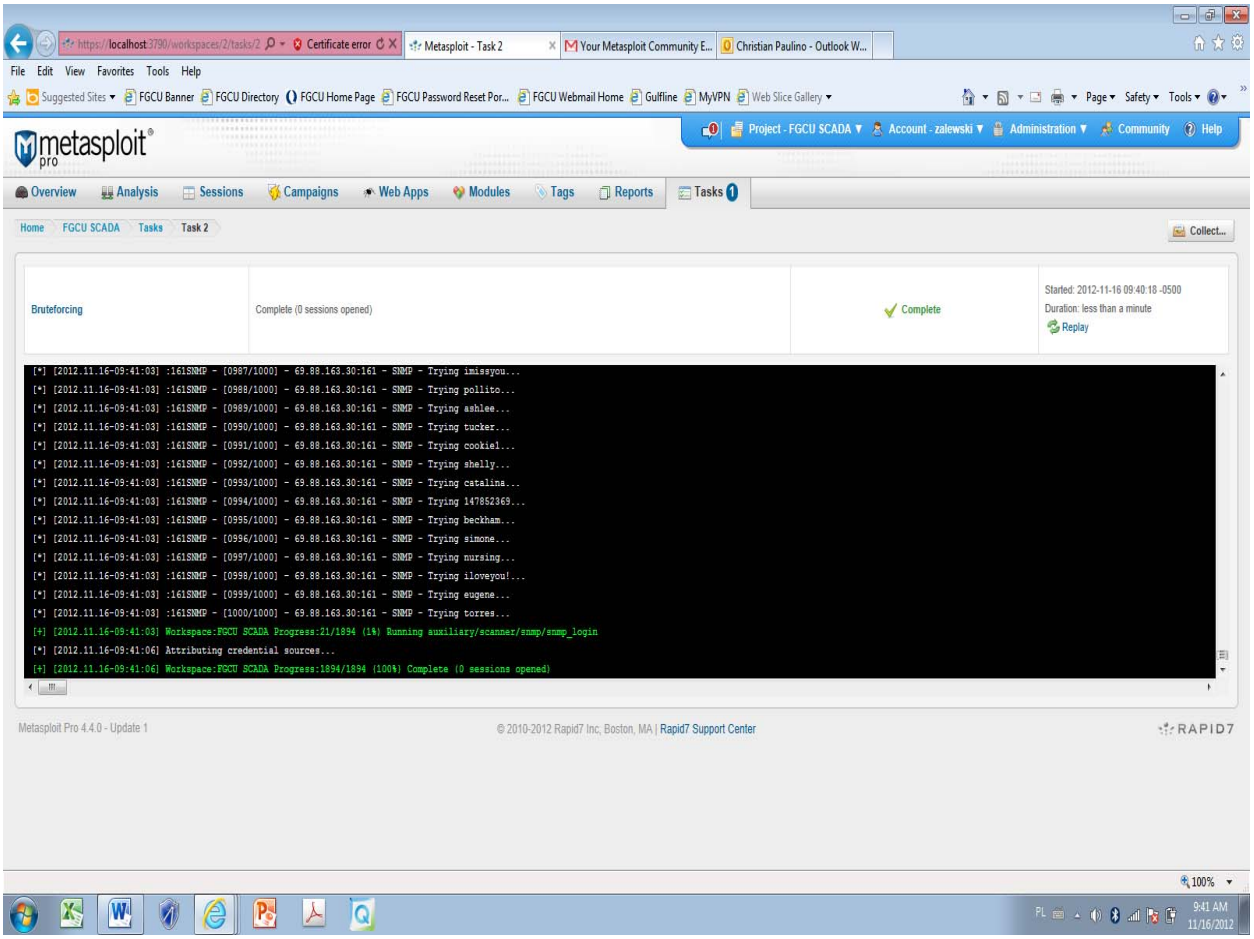

Fig.12 Metasploitbruteforcetest results

The last test is an exploit test. An exploit test checks for any faults in the SCADA server and attempts to use them to get into the server. The exploit tests against the SCADA server failed, which means there weren't any faults detected by Metasploit that could be abused. The results of this test are shown in figure 13. The overall results page of all the tests is displayed in figure 14.

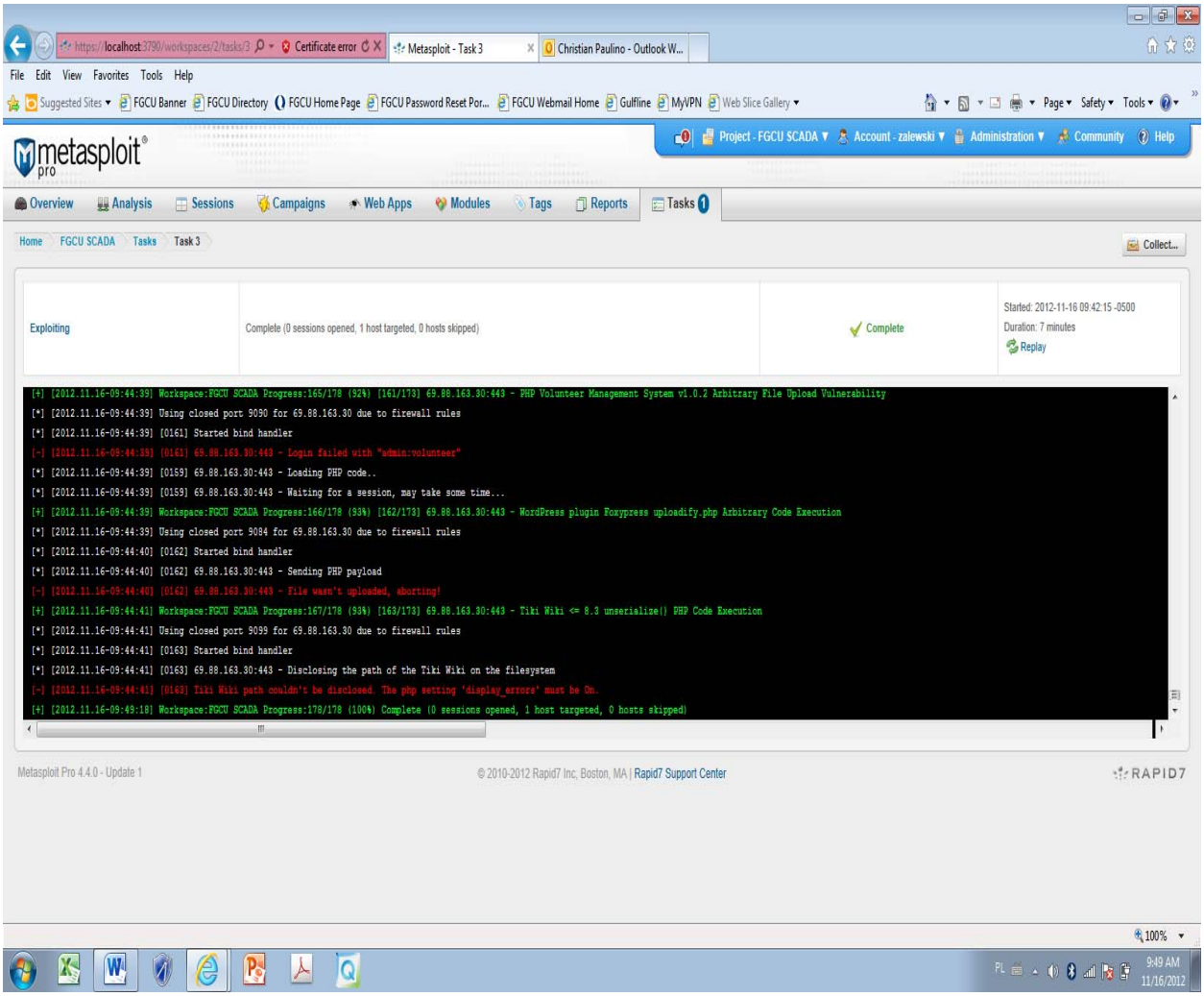

Fig.13 Metasploit exploit test results

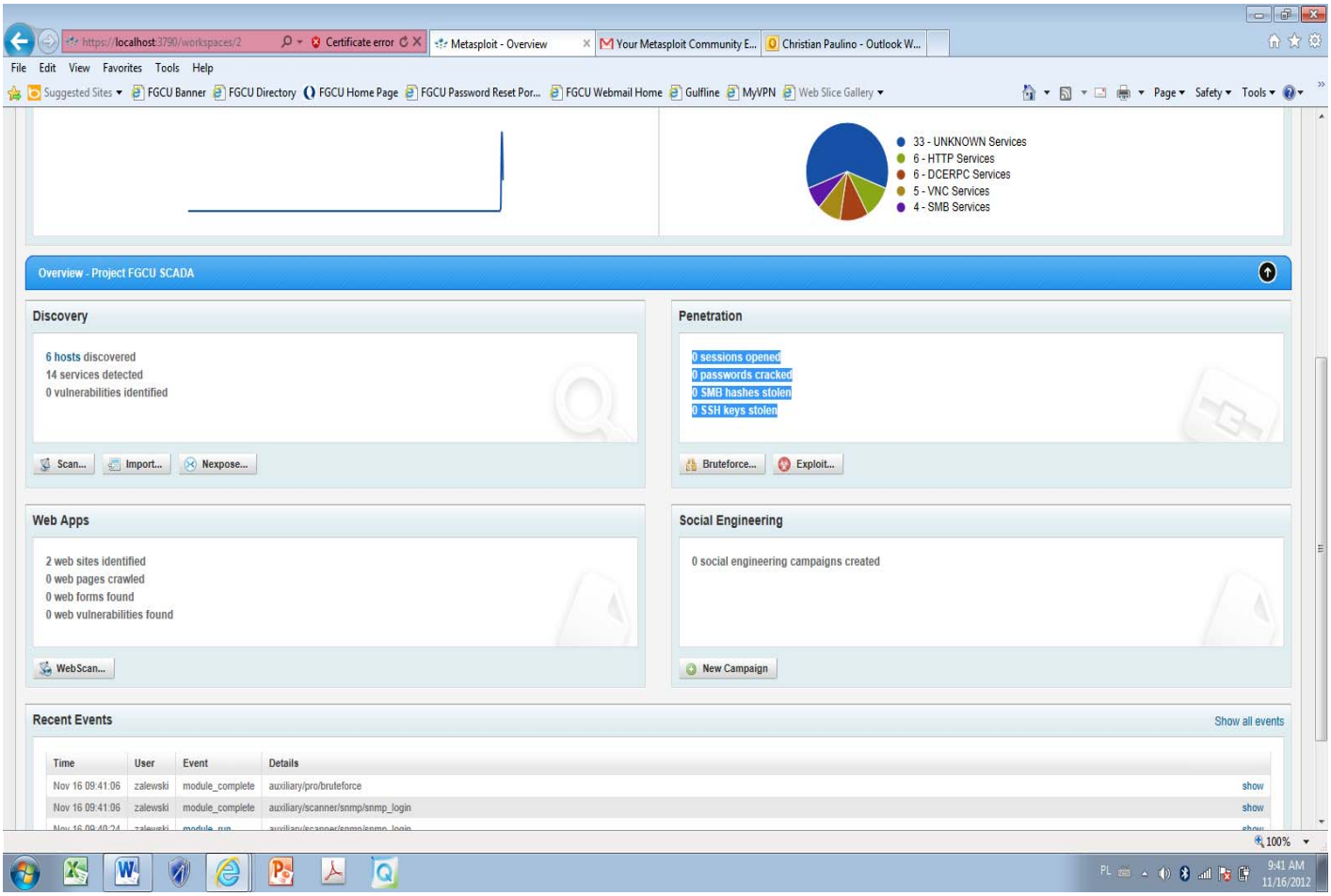

Fig.14 Metasploit results overview

Appendix A.

User Manual

Wireshark

1. Turn on the SCADA workstation and log in under the username Zaleski with the passwordikselaz

2. Start Wireshark from theWindows start menu(Figure 15)

3. Once inside Wiresharkfrom the Capture dropdown menu choose the Interface. This will bring up the window with Ethernet card information in which the MAC card has to be selected.(Figure 16 and Figure 17)

4. Start the packet capturing process by going the Capture dropdown menu and clicking start(Figure 18)This will result in a packet capturing screen (Figure 18A)

5. Open SCADA FrontEnd from the desktop icon(Figure 19)

6. Log in under the user name mgr. The password is htiimgr(Figure 20)

7. Open up the customized view for the SCADA server. First click the view button and then click the custom button (Figure21, Figure 22 and Figure 23)

8. Stop the packet capturing process (Figure 24)

9. The results can now be viewed. The implementation section shows the experimentation results from the packets captured.

Figures forwireshark user manual

Fig.15 Opening Wireshark

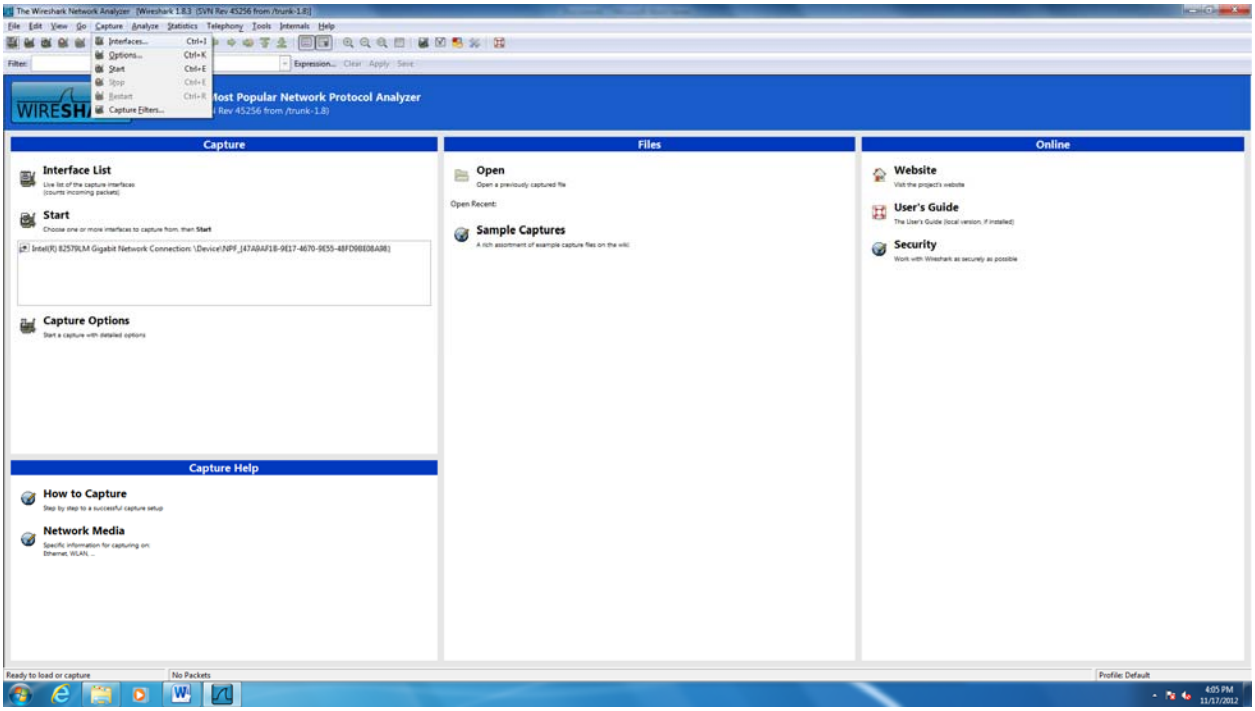

Fig.16 Select Interfaces Wireshark

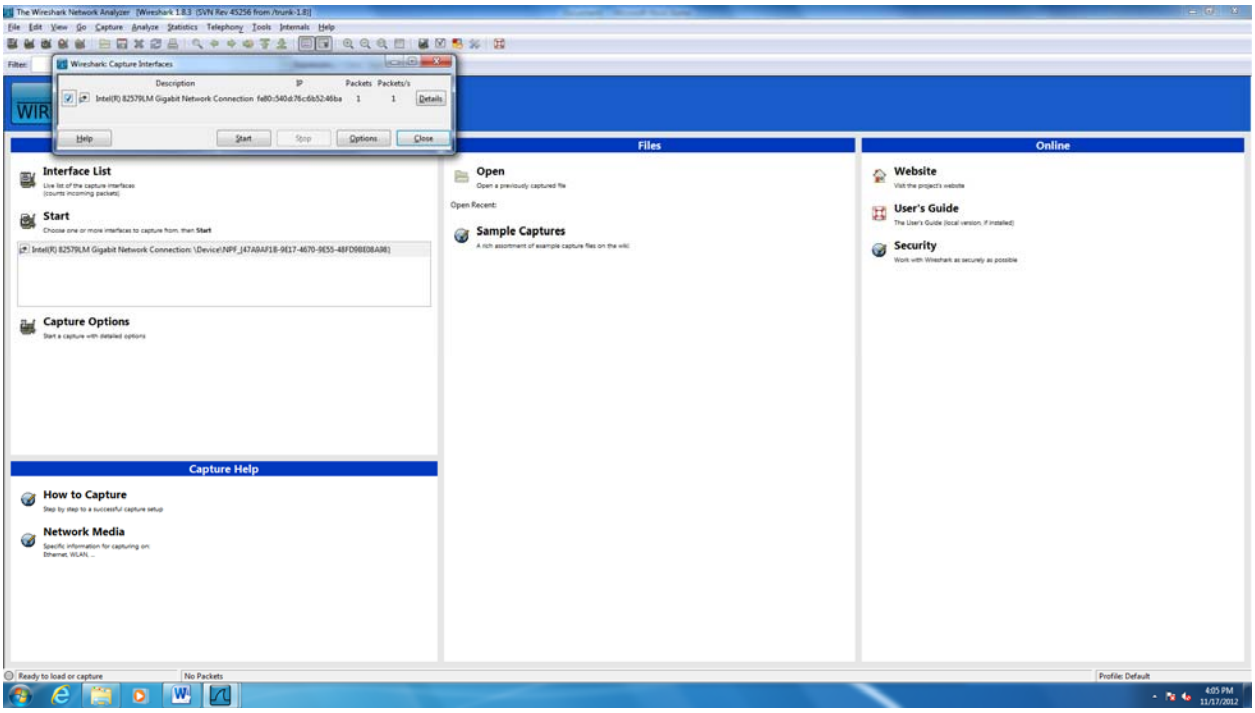

Fig.17 Select SCADA server interface

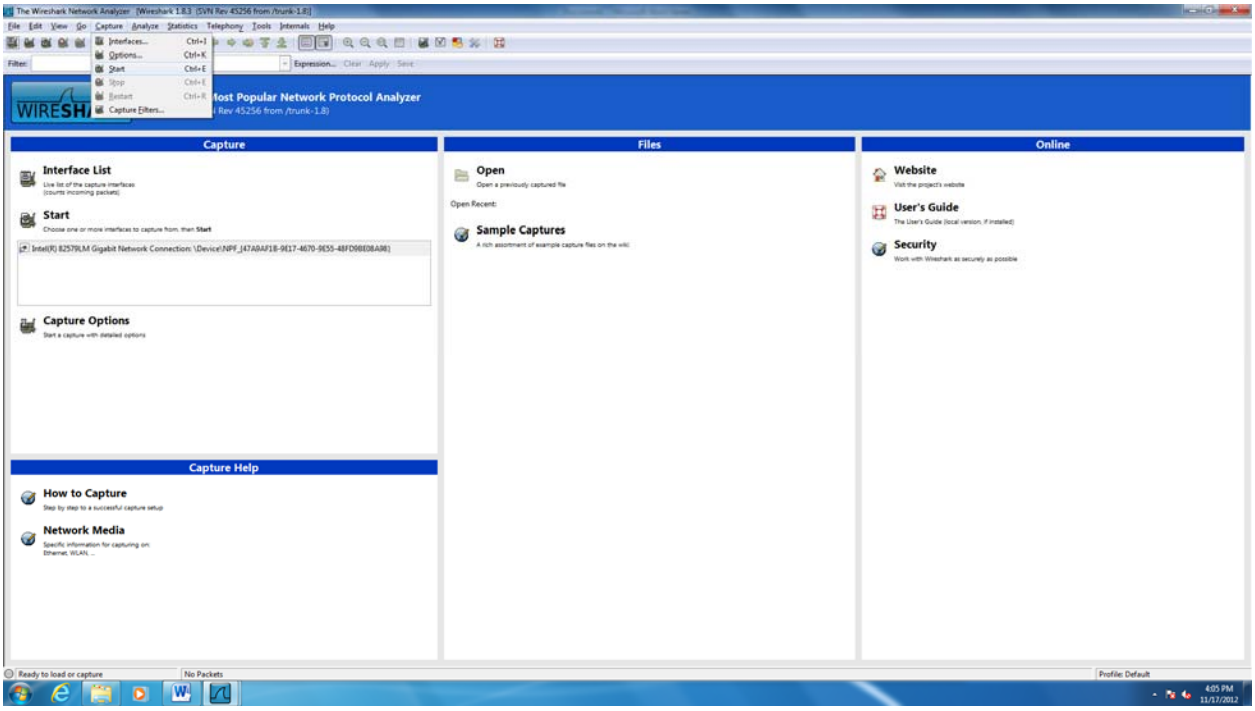

Fig.18 Start Wireshark packet capturing

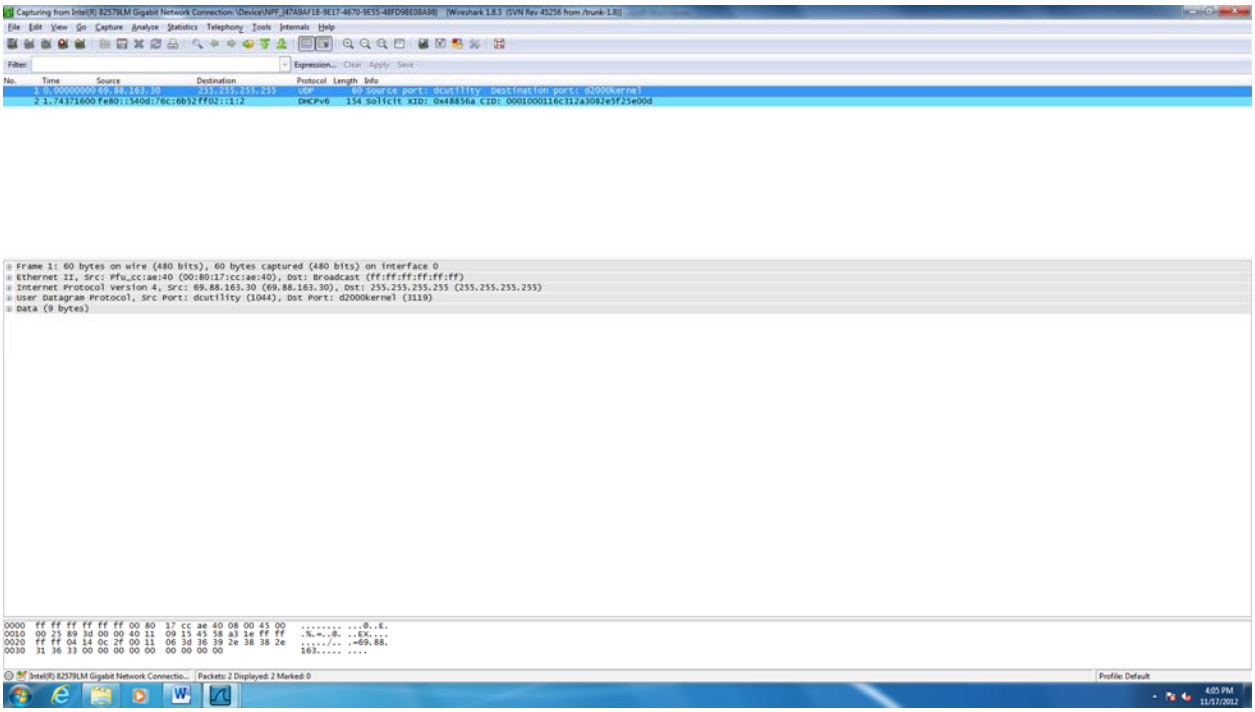

Fig.18A Wireshark packet capturing screen

Fig.19 Open SCADA FrontEnd

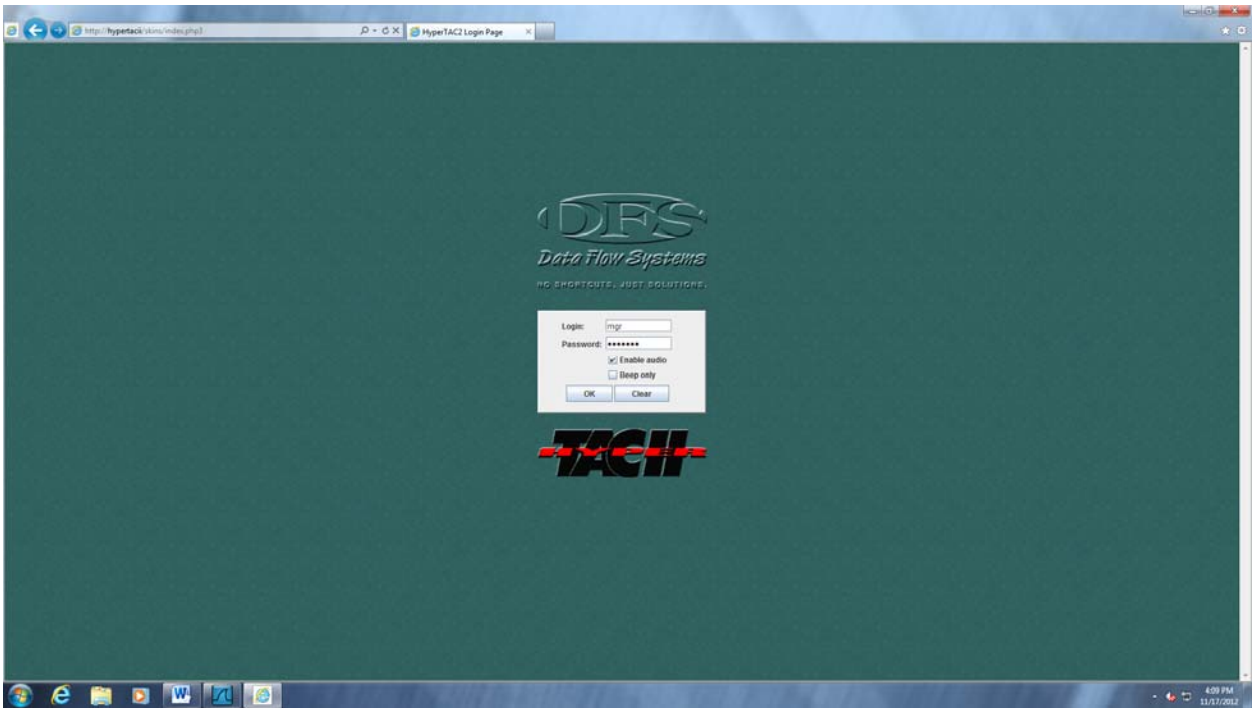

Fig.20 Log into SCADA FrontEnd

Fig.21 Select view tab in SCADA FrontEnd

Fig.22 Select custom view tab in SCADA FrontEnd

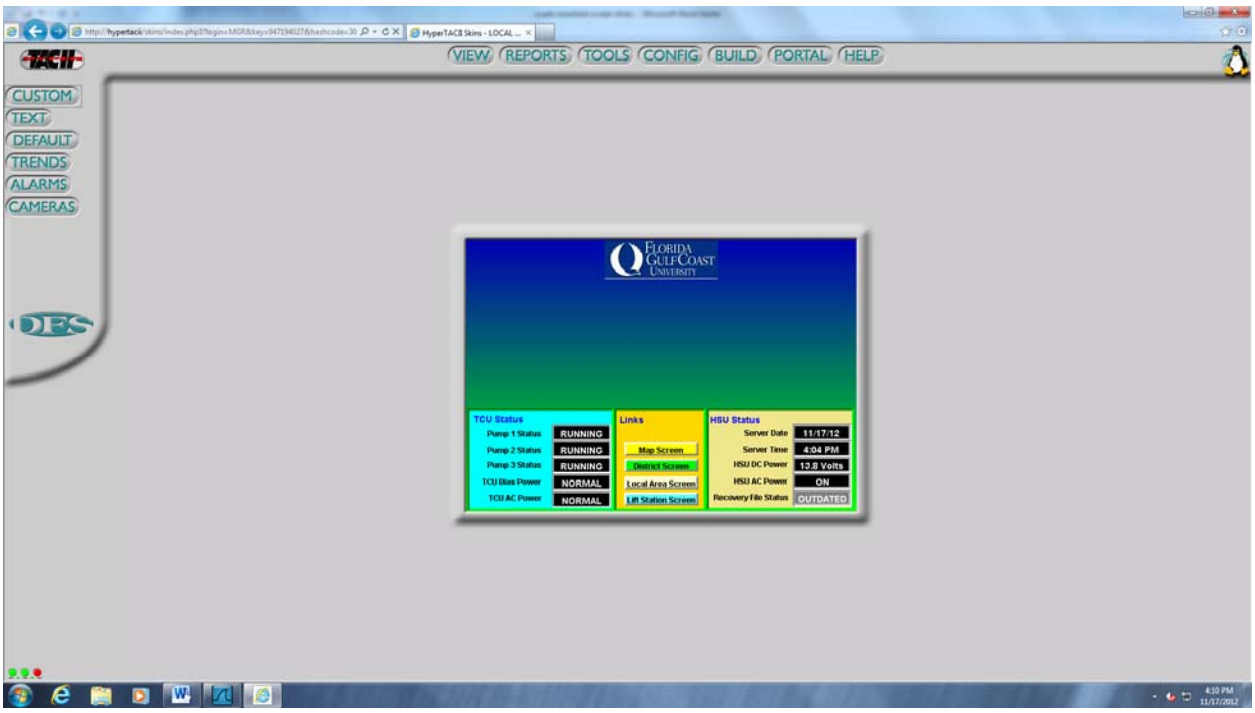

Fig.23 SCADA server statistics

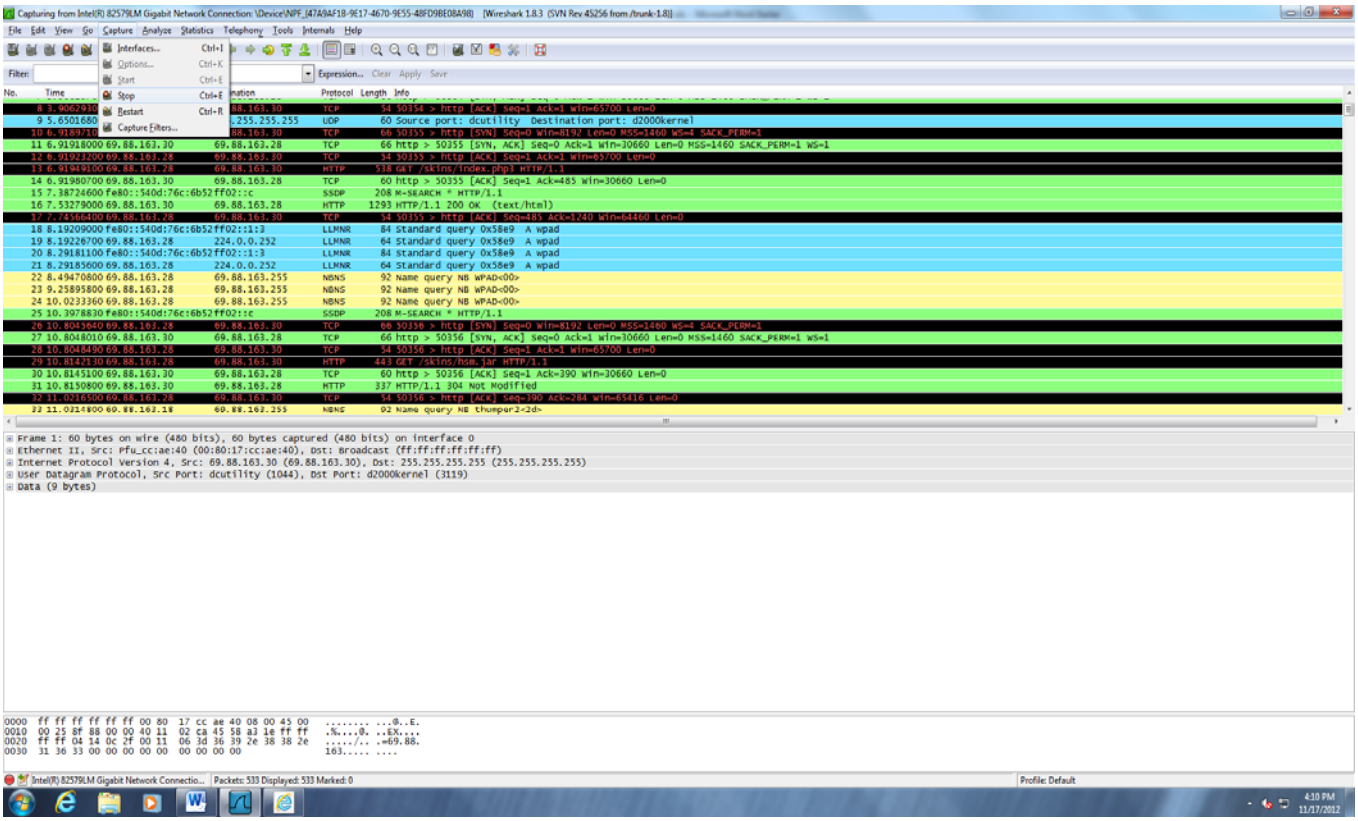

Fig.24 Stop Wireshark packet capturing

Metasploit

1. Open Metasploit from the Windows start menu. Navigate to the Metasploit folder and then click Access Metasploit Web UI.(Figure 25)

2. Log into the Metasploit Web UI under the username zalewski. The password is "ikswelaz1!" (Figure 26)

3. Under the projects tab go to the project "FGCU SCADA" click on it and scroll down. If the project has not been created yet, follow these steps. Go to the projects tab and click on "Create New Project" in the dropdown menu (Figure 27 and Figure 28)

4. First scan for IP addresses. Click on the Scan button under the Discovery section. Enter the IP address of the SCADA server and then click the Launch Scan button. The SCADA server IP address is 69.88.163.30 (Figure 29)

5. Next go back to Overview and run a bruteforce test by clicking the Bruteforce button under the Penetration section. Make sure the only IP address in the target addresses box is the SCADA server address. Click Toggle All services to select all options and then click the Launch Bruteforce button at the bottom (Figure 30)

6. Last go back to Overview and run an exploit test by clicking the Exploit button under the Penetration section. Make sure the only IP address in the target addresses box is the SCADA server address. Start the test by clicking the exploit button.(Figure 31)

7. Refer to the implementation section for the experimentation results.

Figures for metasploit user manual

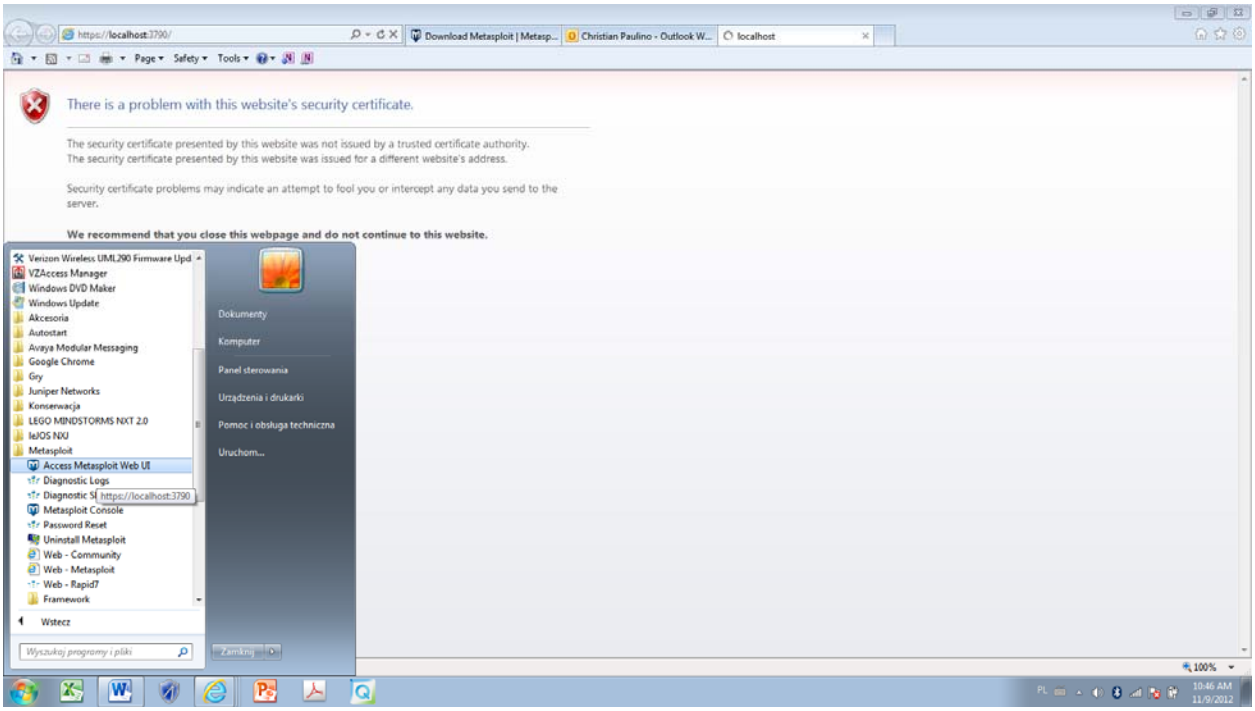

Fig.25Opening Metasploit

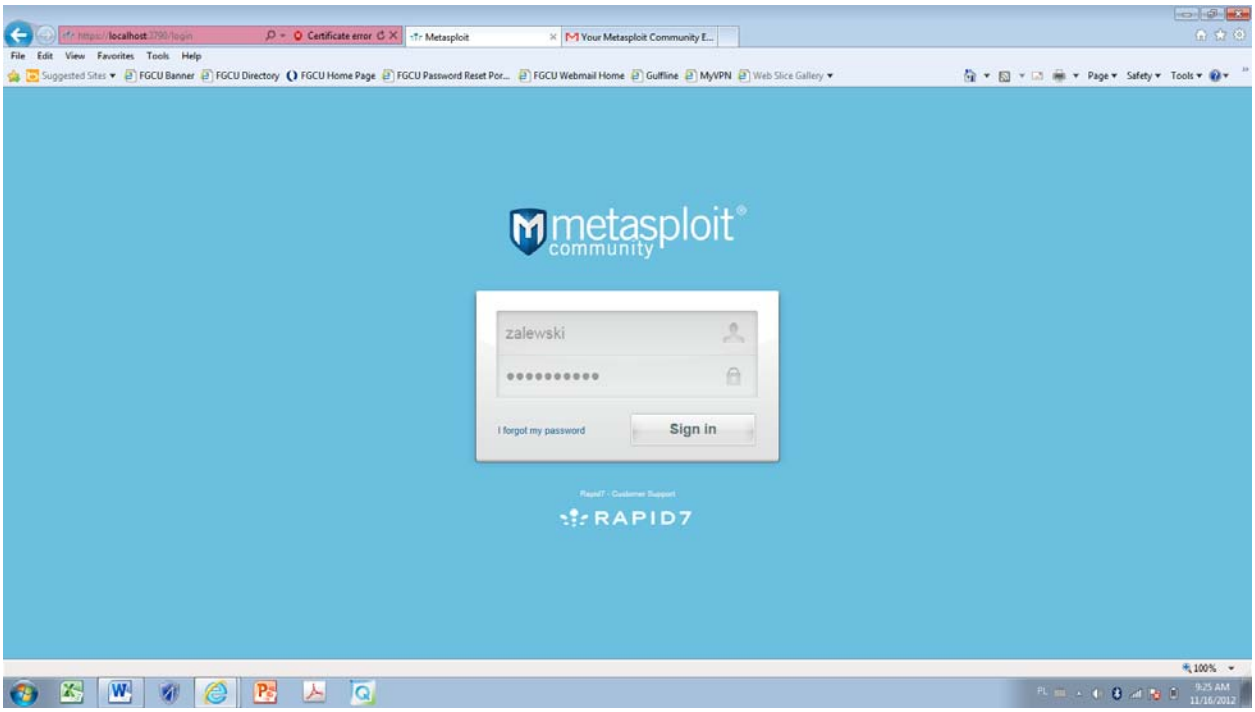

Fig.26 Log into Metasploit

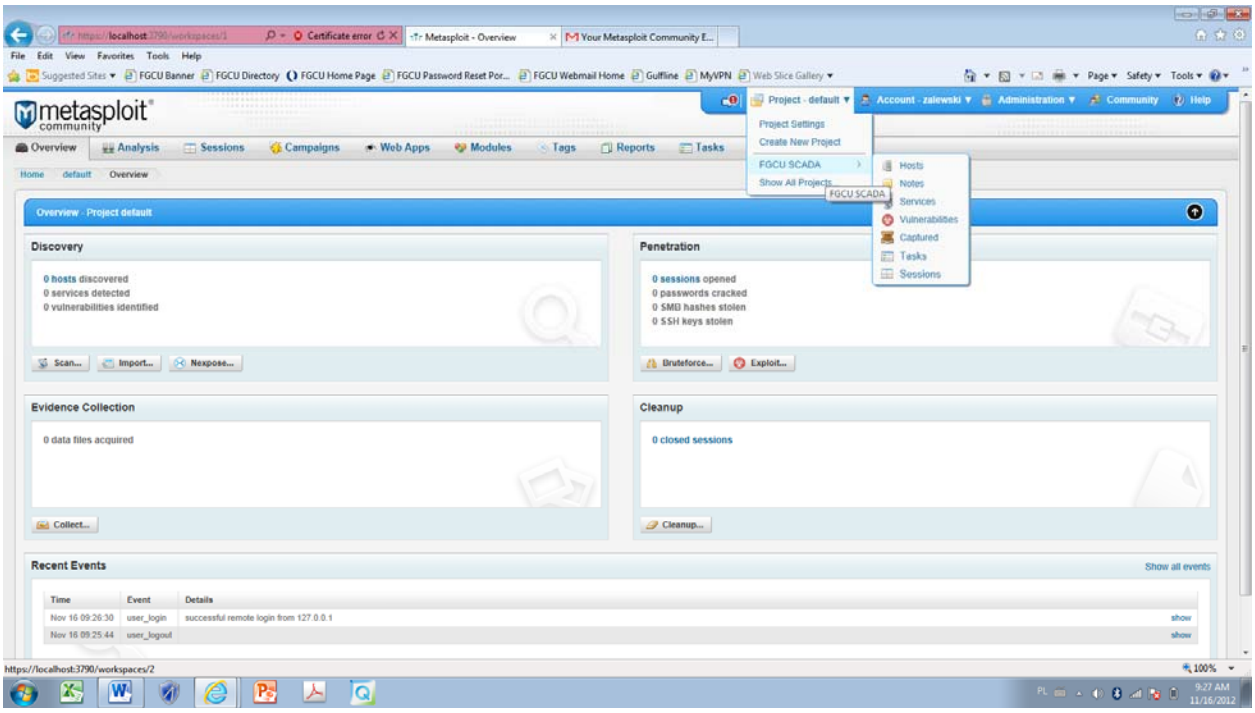

Fig.27 Opening FGCU SCADA project in Metasploit

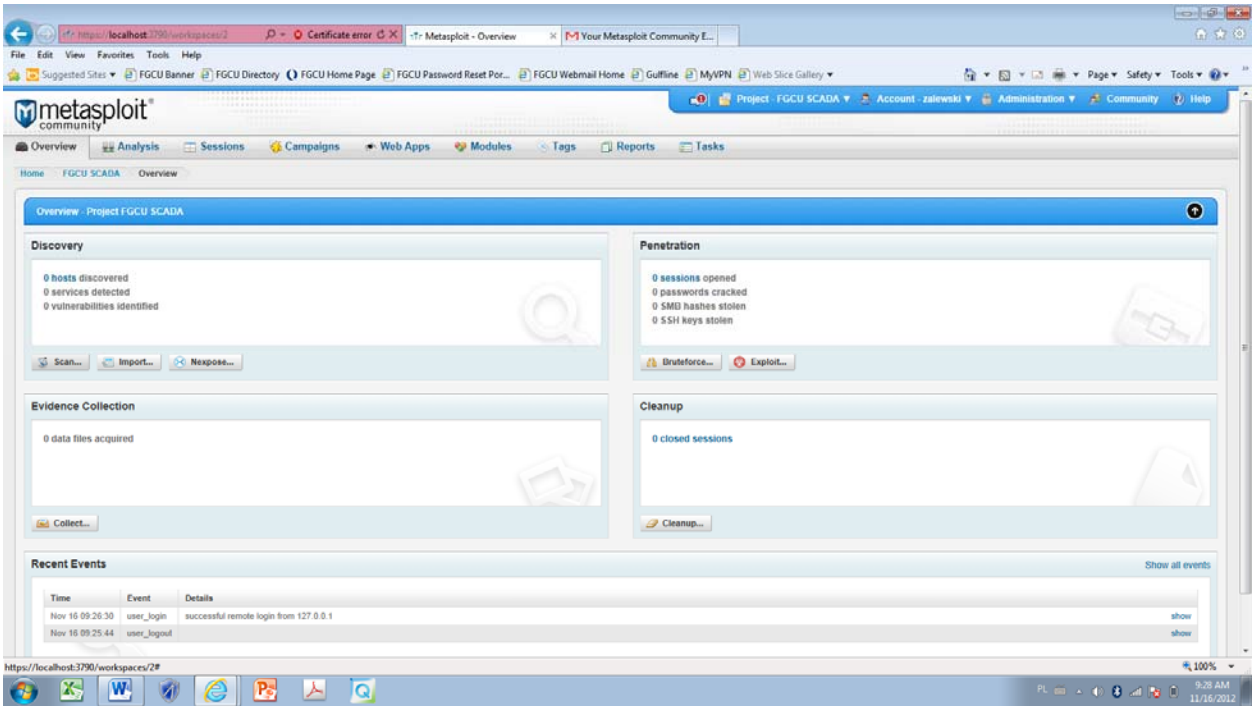

Fig.28 FGCU SCADA project page in Metasploit

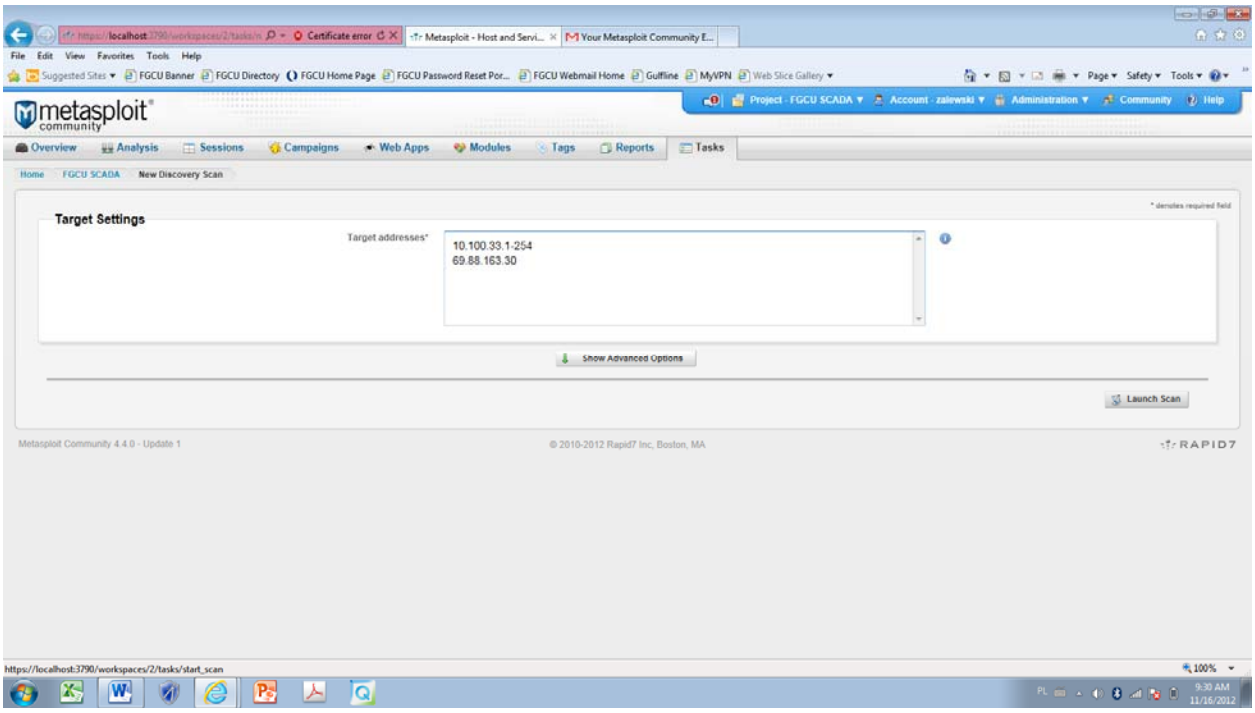

Fig.29 Target address box for Metasploit scan

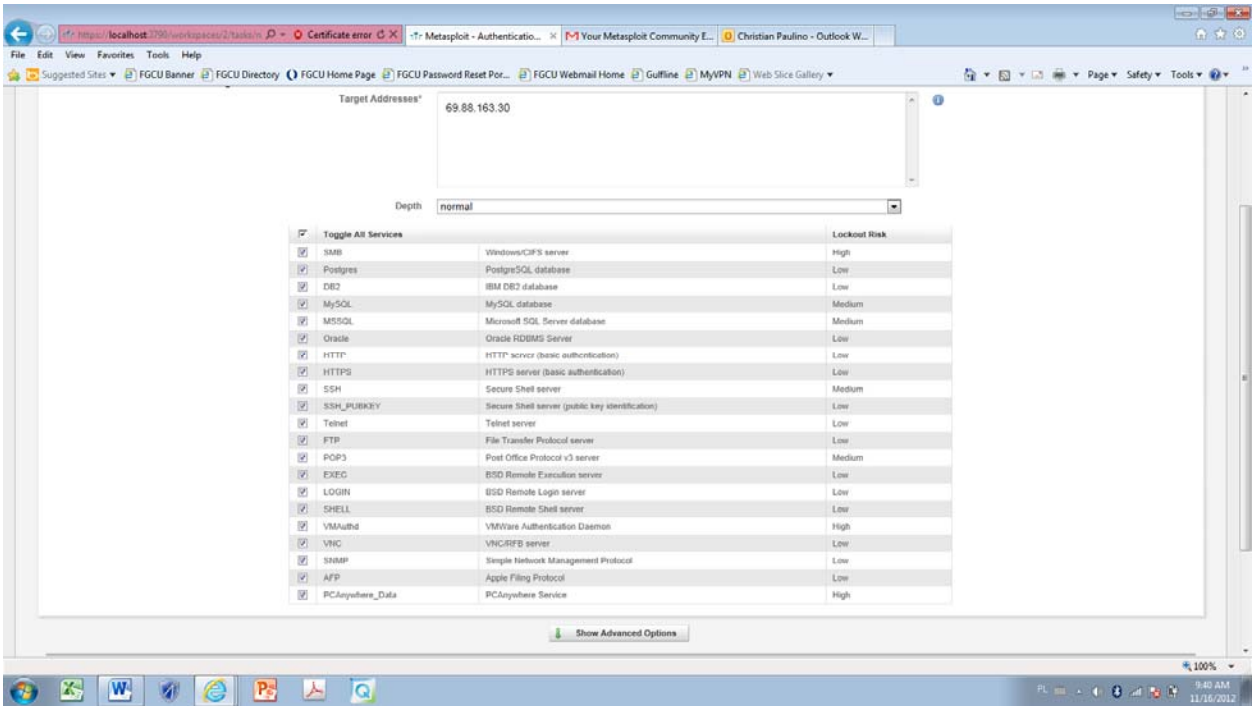

Fig.30 Target address box and services for bruteforce test

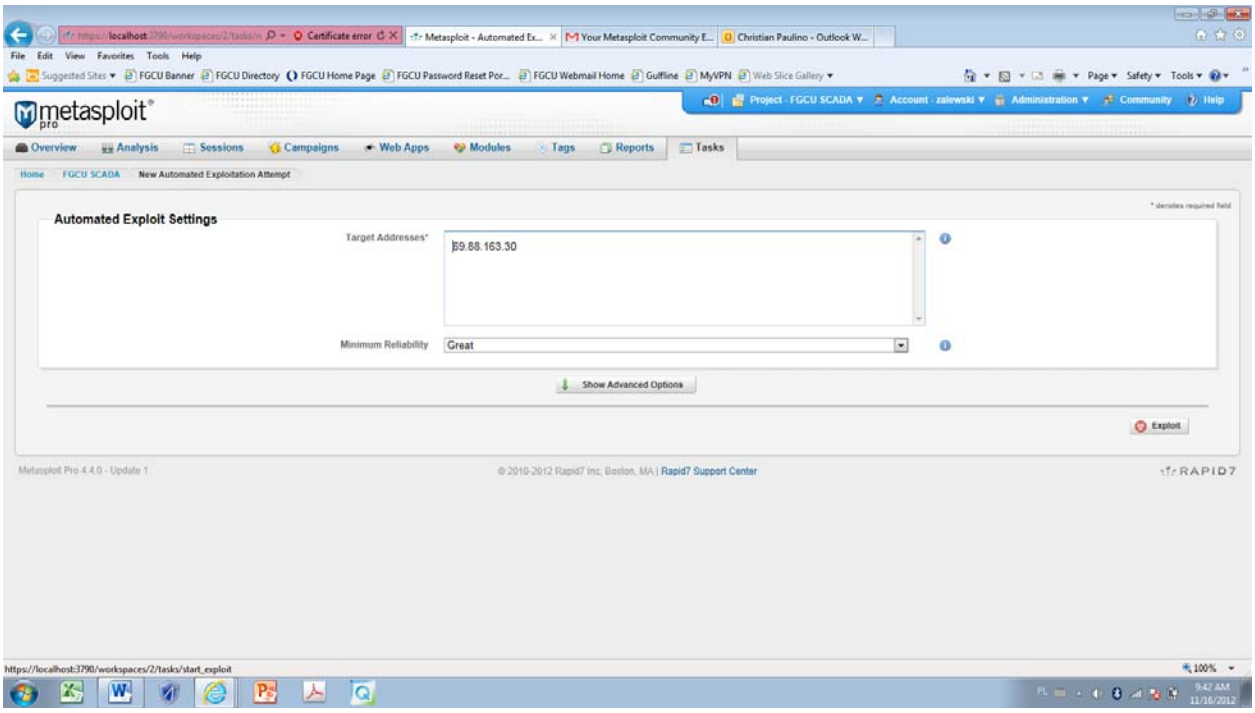

Fig.31 Target address box for exploit test

References

[1] T. Bennet. "Security in SCADA Applications".Florida Gulf Coast Unviersity. Fort Myers, FL 2010

[2] M. Humphries. "Remote Control and Reporting using SCADA".Florida Gulf Coast University.Fort Myers, 2011.

[3] R. L. Krutz. "Securing SCADA Systems". Wiley Publishing, Inc. Indianapolis, IN,2006.

[4] E. D. Knapp."Industrial Network Security".Elsevier Inc. Waltham, MA. 2011

[5] PA Consulting Group and CPNI. "Good Practice Guide – Process Control and SCADA Security". PA Consulting Group and CPNI.London.

[6] P.Aubin. "SCADA Communications Security Authentication, Encryption, Integration".www.controlmicrosystems.com

[7] G. A. Cagalaban, Y. So, S. Kim "SCADA Network Insecurity: Securing Critical Infrastructures through SCADA Security Exploitation" Journal of Security Engineering.

[8] D.Kilman, J. Stamp. "Framework for SCADA Security Policy" Sandia National Laboratories. Albuquerque, NM

[9] C.Neuman. "Understanding Trust and Security in SCADA Systems". Information Sciences Institute University of Southern California

[10] H.Ko. "Application of Asymmetric-key Encryption Method for Internet-based SCADA Security",Journal of Security Engineering

[11] J. Caswell. "Survey of Industrial Control Systems Security".www.cse.wustl.edu/~jain/cse571-11/ftp/ics/index.html

[12] S. Panguluri, W. R. Phillips Jr., R. M. Clark. "cyber threats and it/scada system vulnerability"www.digitalengineeringlibrary.com

[13] A. Saxena, O. Pal, Z.Saquib, D. Patel. “Customized PKI for SCADA System” Int. J. of Advanced Networking and Applications Volume: 01, Issue: 05, Pages: 282-289 (2010)

[14] T. Kim. “Securing Communication of SCADA Components in Smart Grid Environment”international journal of systems applications, engineering &development Issue 2, Vol 5, 2011

[15] R. J. Robles, M. Choi, E. Cho, S. Kim, G. Park, S. Yeo. “Vulnerabilities in SCADA and Critical Infrastructure Systems” International Journal of Future Generation Communication and Networking

[16] J. St.Sauver. “SCADA Security” NLANR/Internet2 Joint Techs MeetingColumbus OH, July 21, 2004

[17] A. N. Mahmood, C.Leckie, J. Hu, Z.Tari, M.Atiquzzaman. “Network Traffic Analysis and SCADA Security”

[18] The President’s Critical Infrastructure Protection Board. “21 Steps to Improve Cyber Security of SCADA Networks”.The President’s Critical Infrastructure Protection Board

[19] Riptech Inc. “Understanding SCADA System Security Vulnerabilities” Riptech Inc., 2001

[20] Intelligent Systems Research Laboratory Technical Report TR-ISRL-04-01 " Security Considerations in SCADA Communication Protocols" Dept. of Computer Engineering and Computer Science, University of Louisville Louisville, KY.2004

[21] PA Consulting Group and NISCC "Good Practice Guide Process Control and SCADA Security"PA Consulting Group, London.

[22] office of the manager national communications system. "Supervisory Control and Data Acquisition (SCADA) Systems".office of the manager national communications system Arlington, VA. 2004

[23] R. K. Fink, D. F. Spencer, R. A. Wells. "lessons learned from cyber security assessments of scada and energy management systems" National SCADA Test Bed. 2006

[24] W. F. Young, J. E. Stamp and J. D. Dillinger, M. A. Rumsey. "COMMUNICATION VULNERABILITIES AND MITIGATIONS IN WIND POWER SCADA SYSTEMS"Sandia National Laboratories, MS 0708Albuquerque, New Mexico. 2003

[25] J.Mamos. "SCADA Information Security Management Guide"

[26] E.Udassin. "control system attack vectors and examples: field site and coporate network". www.c4-security.com 2008

[27] R. K. Fink, D. F. Spencer, R. A. Wells. "lessons learned from cyber security assement of scada and energy management systems"U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, 2006

[28] A. McIntyre, B. Becker, R.Halbgewachs. "Security Metrics for Process Control Systems". Sandia National Laboratories Albuquerque, New Mexico, 2007

[29] R.E. Johnson. "Survey of SCADA security challenges and potential attack vectors". Internet Technology and Secured Transactions (ICITST), International Conference for Date, 8-11 Nov. 2010

[30] Riverbed Technology. "Wireshark".www.wireshark.com

[31] Rapid7. "Metasploit". www.metasploit.com