**Student Name:** **Weight: \_\_\_2.0\_\_\_\_\_%**

**Student ID:** **Marks: \_\_\_\_\_\_\_\_\_\_**

Lab 5: Web Proxies

# Learning Outcomes

* Install and configure an explicit web proxy.
* Create basic rules to allow web access from a subnet.
* Demonstrate the use of Blacklists and Whitelists.

# Purpose

In this lab, you will look at accessing the web using a web proxy, Squid. Using a web proxy provides an extra layer of security for the client computer, since there is no direct connection from the client computer to the Internet. Additionally, it is simpler to manage outbound Internet web access using firewall rules, because only one rule is allowed for outbound web access from the web proxy.

# Part 1: Burp

# Tools

* Kali
  + Burp

# Topology

Kali w/Burp

SAIT Internet

VM

# Setup

Before you begin the lab activities, perform the steps below to set up your computer.

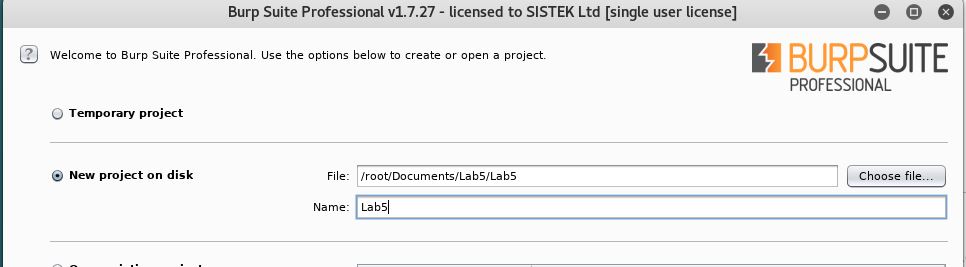
1. Set up a Kali workstation in a VM using ISO with the following parameters:

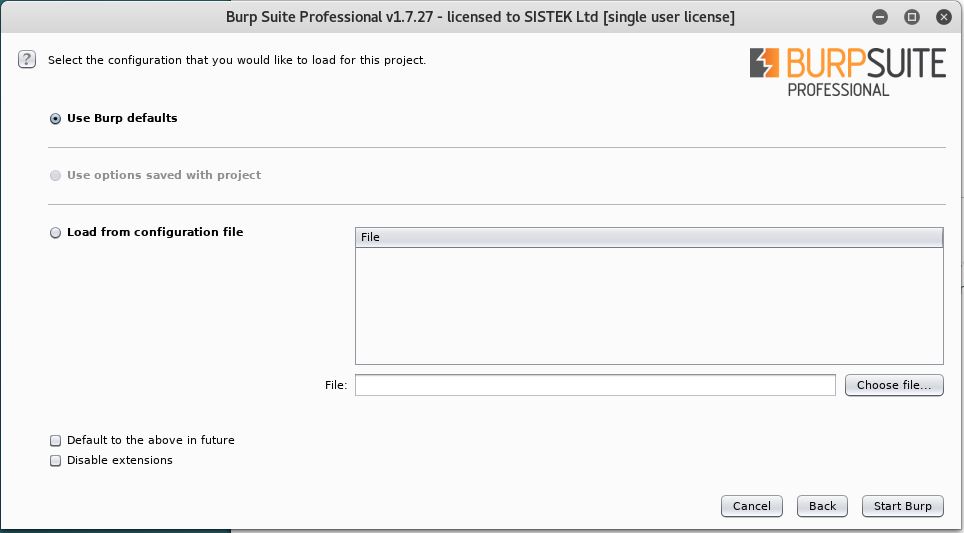
* Network Adapter: NAT
* Firefox Network Proxy Configuration (Options->General->Network Proxy-> Settings, Manual proxy configuration, 127.0.0.1 Port 8080

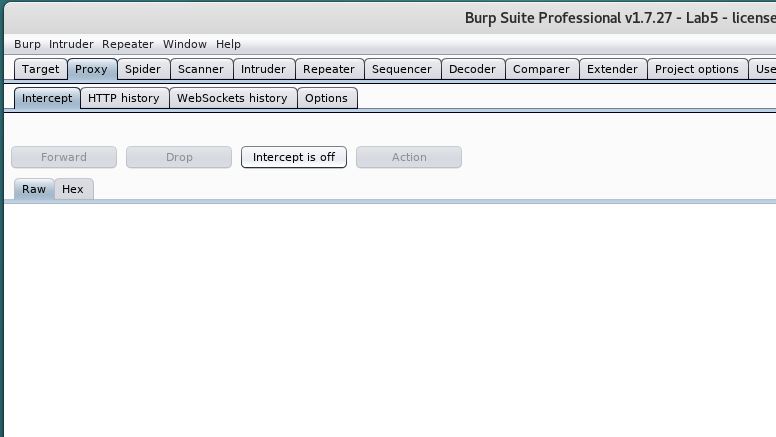
# Activities

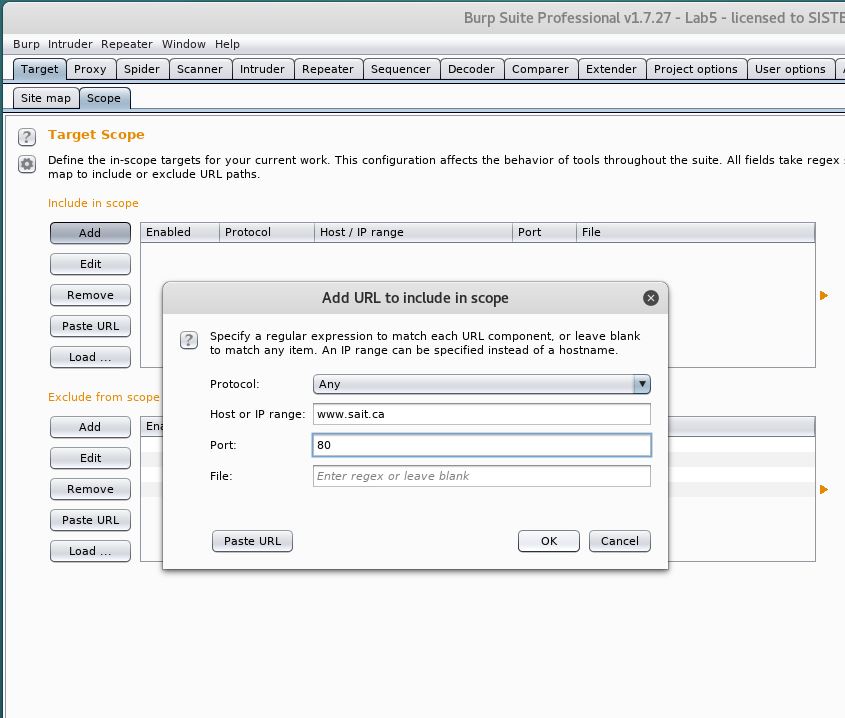
## Explore Burp

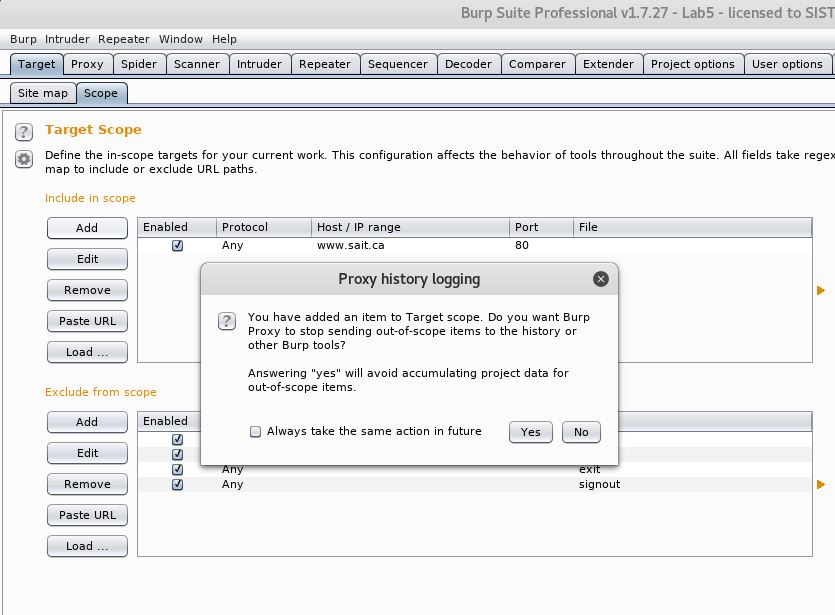
Open Burp, start a project,

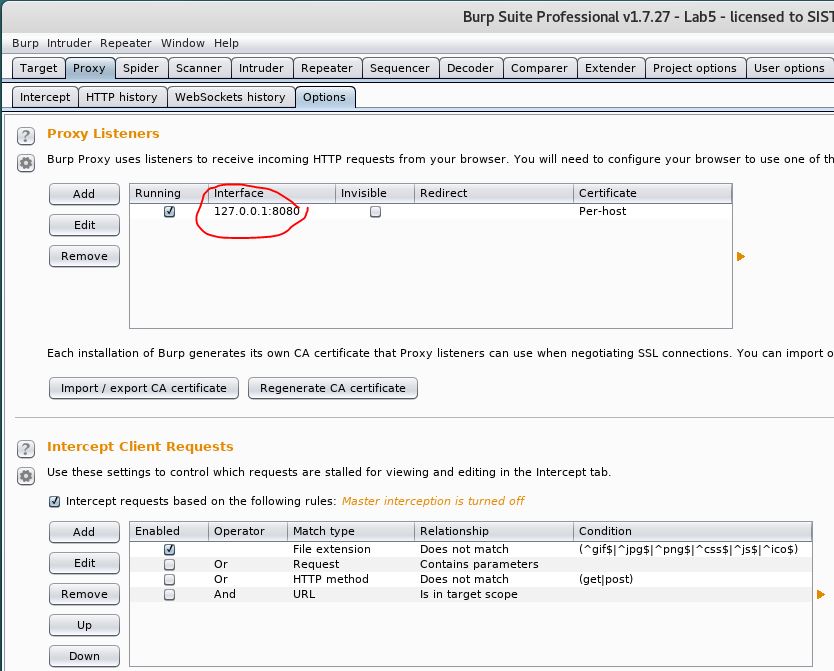


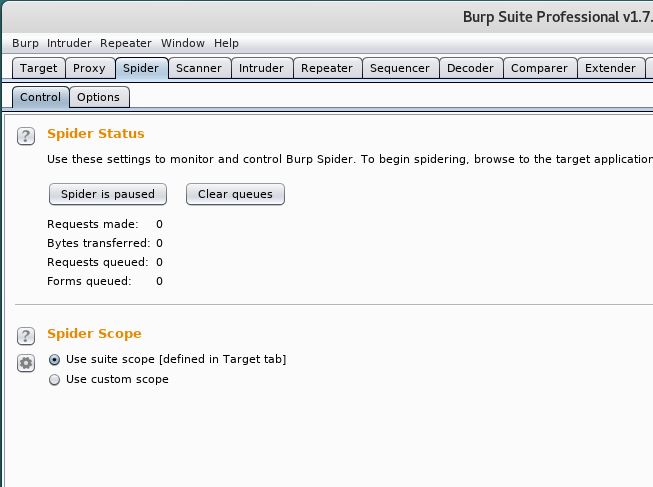




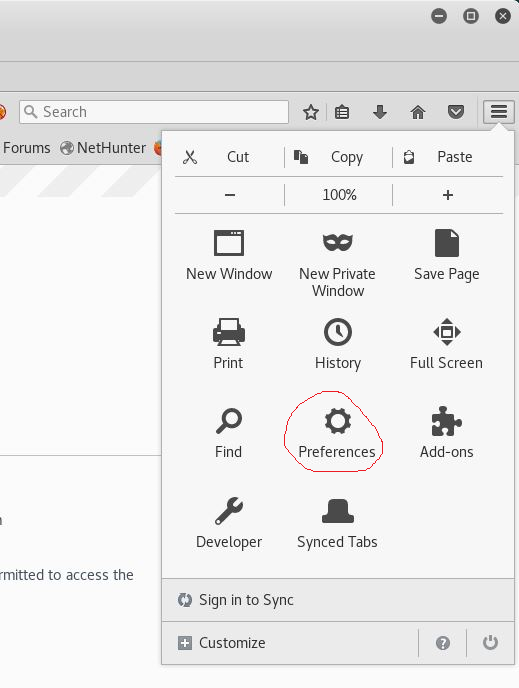




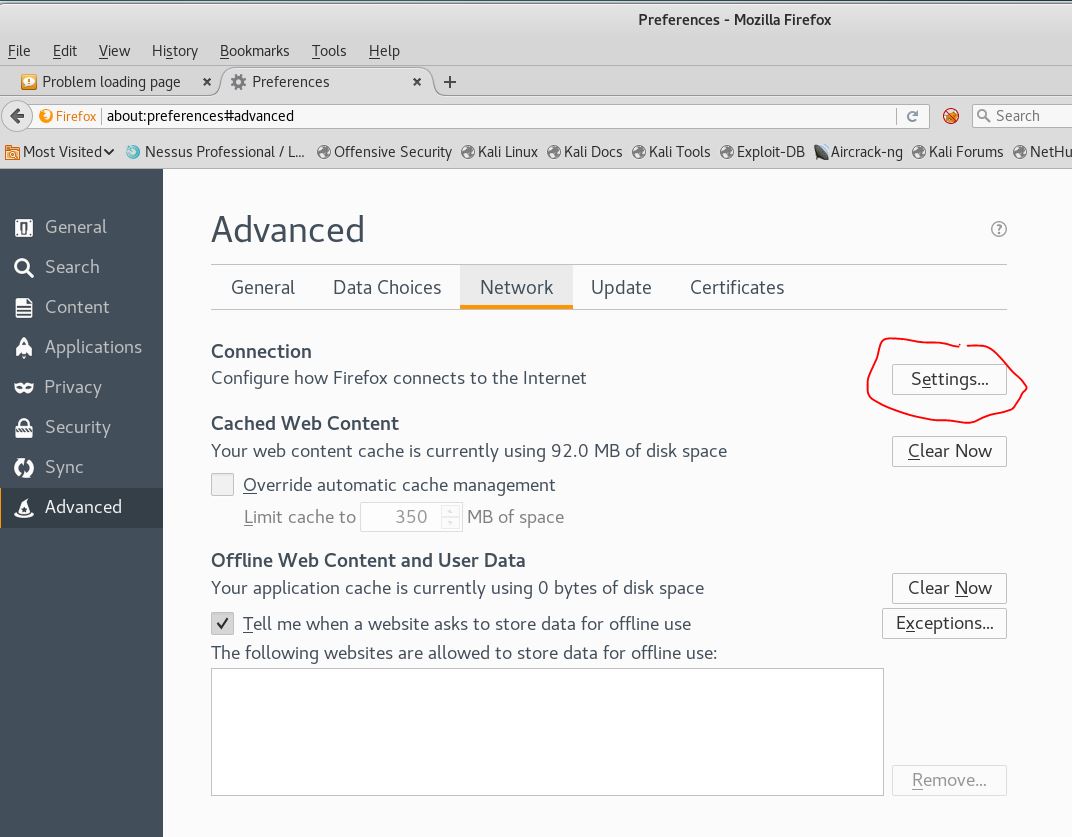




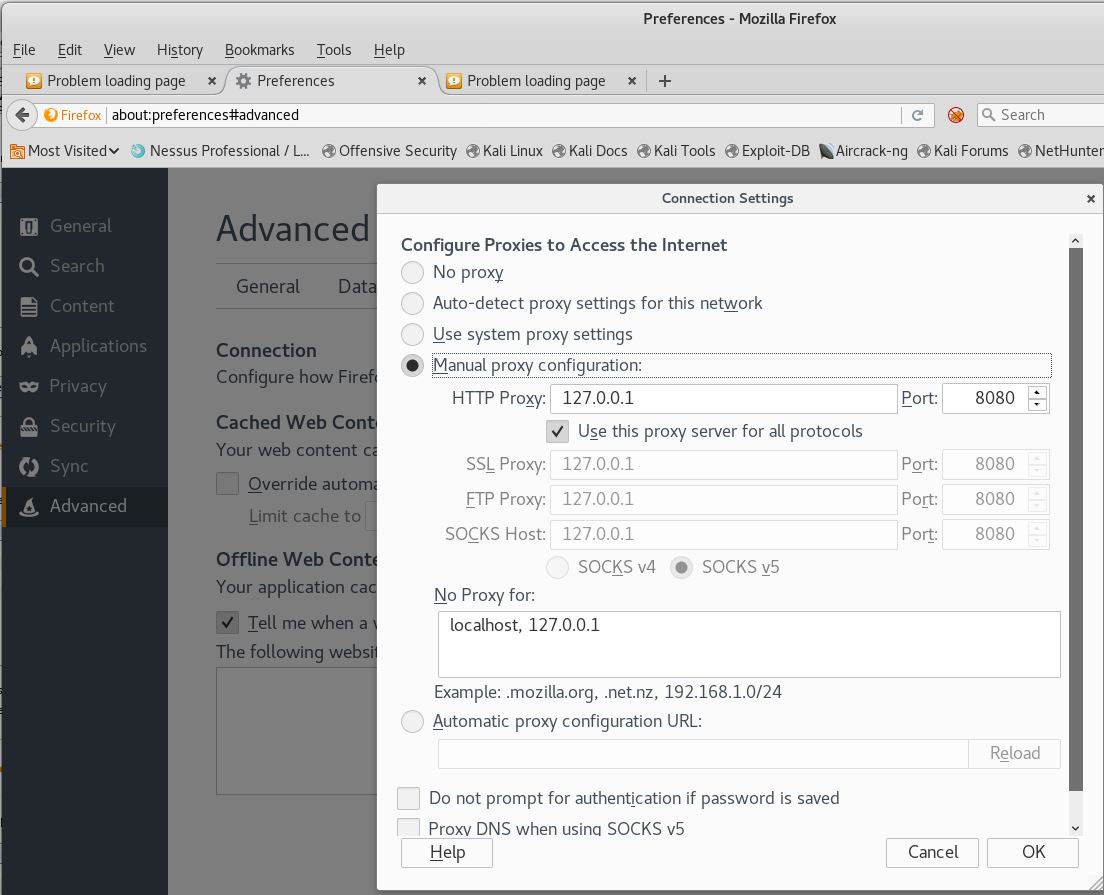
Open Firefox, change network settings



Click on advanced settings and click on network



Enter manual proxy configuration setting and click ok

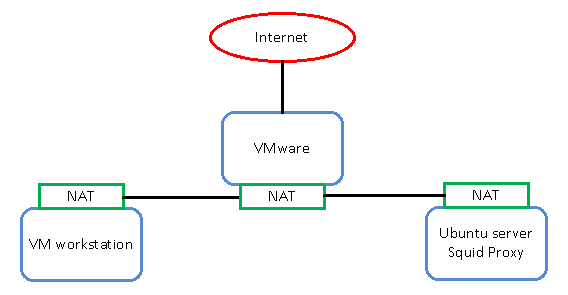


# Part 2: Squid Proxy

# Tools

* Squid proxy on Ubuntu server
* VM workstation

# Topology



© 2017, Southern Alberta Institute of Technology

# Setup

Before you begin the lab activities, perform the steps below to set up your computer.

1. Set up a Windows workstation in a VM using ISO with the following parameters:

* 1 CPU
* 1 GB of RAM
* 80 GB HDD
* Network Adapter: NAT
* Latest version of Wireshark with Winpcap

1. Set up an Ubuntu server in the VM using ISO with the following parameters.

* 1 CPU
* 1 GB of RAM
* 80 GB HDD
* Network Adapter: NAT

1. Install wireshark on the Ubuntu server by entering the following command:
   * $ sudo apt-get install wireshark
2. Install apache2-utils on the Ubuntu server by entering the following command:
   * $ sudo apt-get install apache2-utils
3. Install the Squid proxy on Ubuntu server by entering the following command:
   * $ sudo apt install squid

Note the server IP address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The Squid proxy default port is TCP 3128.

Start Wireshark on Squid proxy server.

# Activities

## Troubleshooting

Demonstrate in Wireshark the TCP connection to 3128 is being RST by proxy server.

Enter the command on proxy$ sudo tail -f /var/log/squid/access.log to see what addresses were denied access.

Show the results of above by insert screen shot: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Web access

1. Change the Windows browser proxy setting to use an explicit web proxy.
2. Note the browser VM IP address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
   Address: <Squid Proxy IP> Port: 3128
3. Access [www.sait.ca](http://www.sait.ca) and write the error received below or insert screenshot:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Define an access rule to allow the use of server proxy from local networks

1. Edit /etc/squid/squid.conf with the following commands:

* acl localnet src 10.0.0.0/8
* acl localnet src 172.16.0.0/12
* acl localnet src 192.168.0.0/16
* http\_access allow localnet

1. Restart the Squid server using the command:

$ sudo service squid restart

1. Test web access and check the access log. Web access should be open to any website.
2. Demonstrate the allowed web access in access.log. Place screenshot here:\_\_\_\_\_\_\_

## Configure basic user authentication

1. Use the following commands:

* $ sudo htpasswd -c /etc/squid/passwords webuser

Password: webuser

* chown proxy /etc/squid/passwords
* chgrp proxy /etc/squid/passwords

1. Test Squid’s basic authentication:

* $ /usr/lib/squid/basic\_ncsa\_auth /etc/squid/passwords webuser webuser

OK ^C

1. In /etc/squid/squid.conf set the configuration as follows:

* auth\_param basic program /usr/lib/squid/basic\_ncsa\_auth /etc/squid/passwords
* auth\_param basic children 5 startup=5 idle=1
* auth\_param basic realm Squid proxy-caching web server
* auth\_param basic credentialsttl 2 hours
* acl basic\_ncsa\_users proxy\_auth REQUIRED
* http\_access allow basic\_ncsa\_users
* Remove http\_access allow localnet

1. Demonstrate the allowed web access in access.log, screenshot of authentication pop up here:\_\_\_\_\_\_\_
2. Test web access and check the access log. Web access should prompt for username and password authentication.

User webuser:webuser for proxy authentication

Demonstrate allowed web access in access.log with username. Place screenshot of access log here:\_\_\_\_\_\_\_

## Configure a Blacklist and a Whitelist

1. Use the following commands:

* $ sudo vi /etc/squid/blacklists.txt

Add **.google.com** and **.google.ca**

* $ sudo vi /etc/squid/whitelists.txt

Add **.amd.com** and **.cnn.com**

1. Change file ownership:

* $ sudo chown proxy ./whitelists.txt ./blacklists.txt
* $ sudo chgrp proxy ./whitelists.txt ./blacklists.txt

1. In /etc/squid/squid.conf, add:

* acl blacklists dstdomain "/etc/squid/blacklists.txt”
* acl whitelists dstdomain "/etc/squid/whitelists.txt”
  1. At the top of http\_access, add:
* http\_access allow whitelists
* http\_access deny blacklists

1. Restart Squid, test web access and check the access log.

Demonstrate blacklists and whitelists without authentication, place screenshot of access log here:\_\_\_\_\_\_\_