

Colby Heilner

Professor Torres

3/21

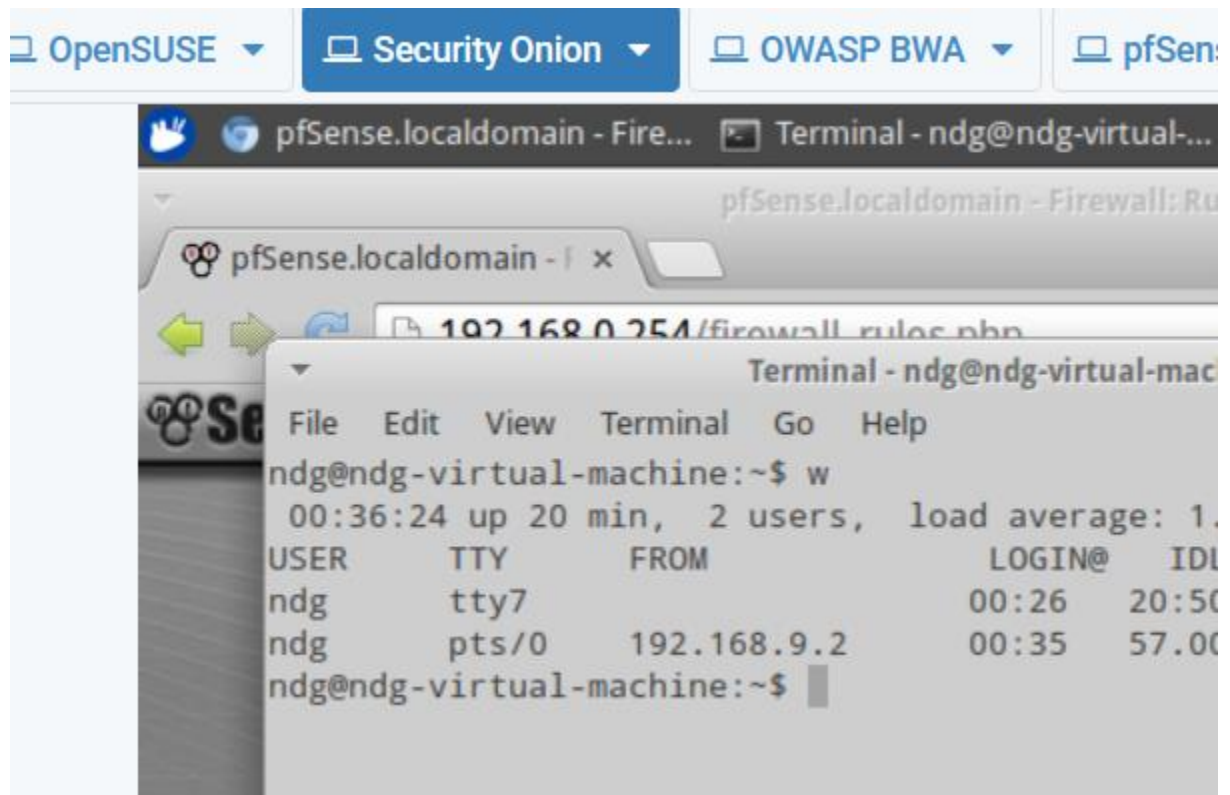
IT 145

Lab 8

Part A:

- Log on to Netlab: NDG Ethical Hacking- Lab 01
- Tunneling. On your kali box, **after the setup**, we are going to do some tunneling/port forwarding. Kali (our hacker) cannot ping anything. Kali can only SSH to security onion. We will be tunneling everything via SSH so that -from kali i can access web interfaces, etc. This will be one of the trickiest labs yet. **Take your time**. Chart out what you need to do.
- 99.9999 of the commands needed to complete this lab are done on kali (our hacker) NDG Ethical Hacking- Lab 01
- **SETUP:** Change pfSense rules. Test that you can only access Security Onion via SSH,
- Make sure that you cannot ping or access anything else from Kali
- Also: setup NAT SSH to Security Onion, in WAN rules pointing to Security Onion,
- there should only be one rule (your SSH), delete the other rules

Made the NAT ssh rule the only rule and was able to connect and not ping



- and finally add a user in Security Onion (student/hacker)

```
root@ndg-virtual-machine:/home/ndg# adduser student
adduser: The user `student' already exists.
root@ndg-virtual-machine:/home/ndg# adduser student1
Adding user `student1' ...
Adding new group `student1' (1004) ...
Adding new user `student1' (1003) with group `student1' .
Creating home directory `/home/student1' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for student1
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n]
root@ndg-virtual-machine:/home/ndg#
```

- From kali, tunnel security onion web interface via port 22- access on kali
Took some trial and error but was able to get in.

```

File Edit View Search Terminal Help
sed home
channel 3: open failed: connect failed: Connection refused
sed

student1@ndg-virtual-machine:~$
student1@ndg-virtual-machine:~$
student1@ndg-virtual-machine:~$
student1@ndg-virtual-machine:~$ quit
No command 'quit' found, did you mean:
  Command 'quilt' from package 'quilt' (main)
  Command 'luit' from package 'x11-utils' (main)
  Command 'quot' from package 'quota' (main)
  Command 'quiz' from package 'bsdgames' (universe)
  Command 'qgit' from package 'qgit' (universe)
quit: command not found
student1@ndg-virtual-machine:~$ exit
logout
Connection to 192.168.9.1 closed.
root@Kali2:~# ssh -L 5601:127.0.0.1:443 student1@192.168.9.1
student1@192.168.9.1's password:
Permission denied, please try again.
student1@192.168.9.1's password:
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-63-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

0 packages can be updated.
0 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2017.

Last login: Fri Mar 21 00:54:57 2025 from 192.168.9.2
student1@ndg-virtual-machine:~$

```

Kali Linux, an Offensive ... x Security Onion: HOME x

https://127.0.0.1:5601

Most Visited Offensive Security Kali Linux Kali Docs

Security Onion

<http://www.securityonion.net>
<http://www.securityonionsolutions.com>

What is it?
 Security Onion is a Linux distro for intrusion detection, network security monitoring, and log management. It's based on Ubuntu 12.04 and contains Snort, Suricata, Sguil, Squert, Snorby, Bro, NetworkMiner, Xplico, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!

How do I install and configure it?
 Please follow the [Installation guides](#) on our [Wiki](#).

Local Server
 Links to quickly access your local Squert, Snorby, ELSA, and Xplico instances:

- * [Squert](#): View NIDS/HIDS alerts and HTTP logs
- * [Snorby](#): View and annotate IDS alerts
- * [ELSA](#): Search logs (IDS, Bro, and syslog)
- * [Xplico](#): Carve PCAP files (please note that [port 9876 is not open to the outside world by default](#))

Useful Links
 Links to useful Security Onion information:

- * [Blog](#): Get the latest news and updates
- * [Wiki](#): Table of Contents
- * [Installation](#): Installation guides
- * [Tools](#): List of included security tools
- * [Mailing Lists](#): Join the list(s) to get help and help others

- From kali run Nikto via localhost after establishing tunnel to port 443

```

root@Kali2:~# nikto -h https://127.0.0.1:5601
- Nikto v2.1.6

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 5601

+ SSL Info: Subject: /CN=securityonion
            Ciphers: ECDHE-RSA-AES256-GCM-SHA384
            Issuer: /CN=securityonion
+ Start Time: 2025-03-20 20:07:32 (GMT-5)

+ Server: Apache/2.2.22 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.19
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint

```

- From kali run whatweb via localhost after establishing tunnel to port 443

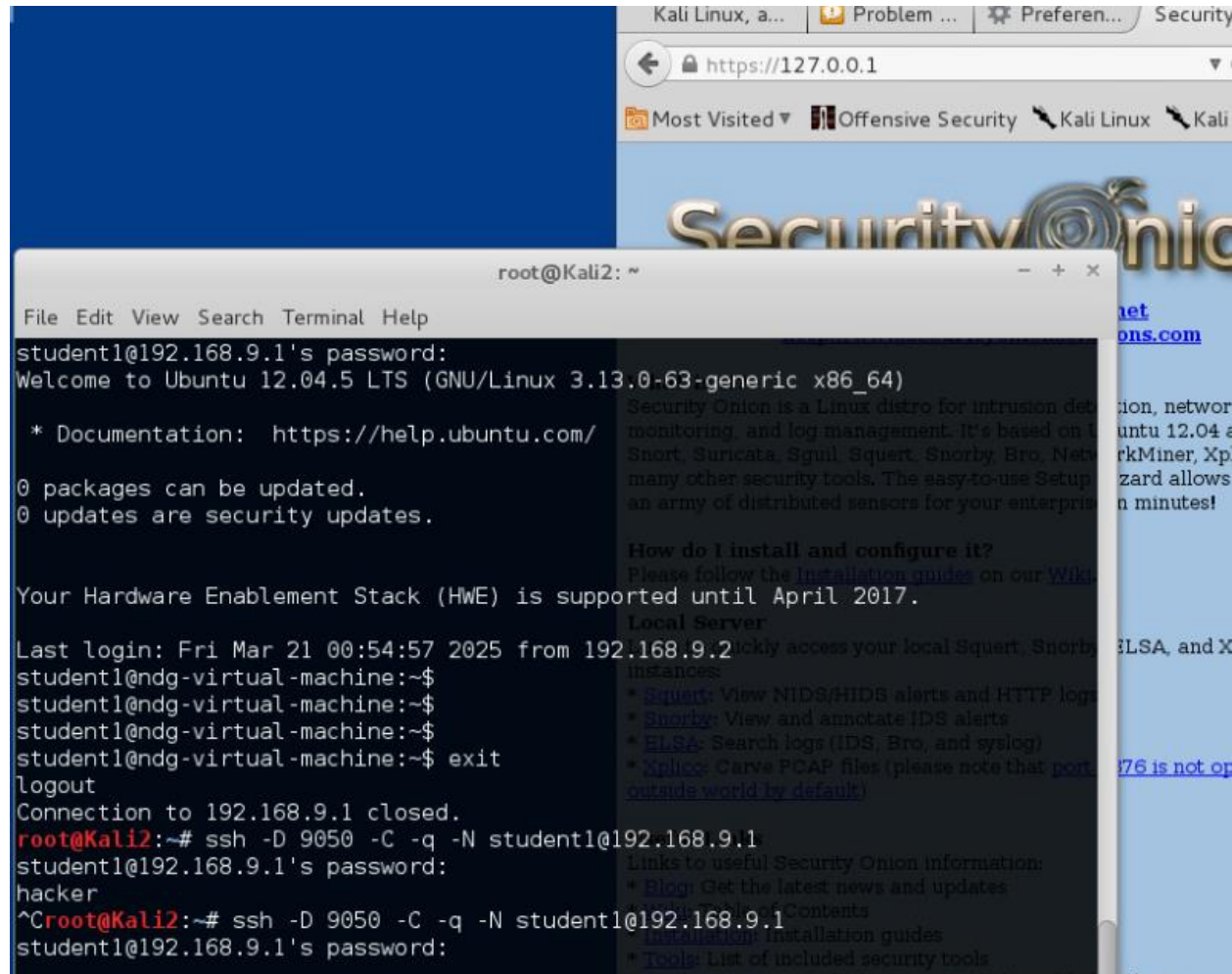
```

root@Kali2:~# whatweb https://127.0.0.1:5601
https://127.0.0.1:5601 [200] Apache[2.2.22], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.2.22 (Ubuntu)], IP[127.0.0.1], PHP[5.3.10-1ubuntu3.19], X-Powered-By[PHP/5.3.10-1ubuntu3.19]
root@Kali2:~#

```

- From kali use dynamic port forwarding and sox proxy to tunnel via port 22 (access browser via ip of security onion and openSUSE)

I was able to eventually get this to work aswell, had to add proxy in Iceweasel settings.



- after setting up sox proxy, use proxychains to scan for live host
After setting up proxychains conf file we can run commands like this to go through the proxy

```

root@Kali2:~# proxychains nmap -sn 192.168.0.9/24
ProxyChains-3.1 (http://proxychains.sf.net)

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2025-03-21 15:50 CDT
Stats: 0:00:58 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan

```

- after setting up sox proxy, use proxychains with whatweb against security onion and openSUSE


```
root@Kali2:~# proxychains whatweb -v https://192.168.0.100
ProxyChains-3.1 (http://proxychains.sf.net)
|D-chain|-<-127.0.0.1:9050-<->-192.168.0.100:443-<->-OK
https://192.168.0.100/ [200] Apache[2.2.22], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.2.22 (Ubuntu)], IP[192.168.0.100], PHP[5.3.10-1ubuntu3.19], X-Powered-By[PHP/5.3.10-1ubuntu3.19]
URL : https://192.168.0.100
Status : 200

Apache
Description: The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.
Website : http://httpd.apache.org/
Version : 2.2.22 (from HTTP Server Header)

root@Kali2:~# proxychains whatweb -v https://192.168.0.2
ProxyChains-3.1 (http://proxychains.sf.net)
|D-chain|-<-127.0.0.1:9050-<->-192.168.0.2:443-<->-timeout
https://192.168.0.2 ERROR: Connection refused - connect(2) for "192.168.0.2" port 443
root@Kali2:~# proxychains whatweb -v http://192.168.0.2
ProxyChains-3.1 (http://proxychains.sf.net)
|D-chain|-<-127.0.0.1:9050-<->-192.168.0.2:80-<->-OK
http://192.168.0.2 ERROR: uninitialized constant Class::HTTPBadResponse
root@Kali2:~#
```

- set up a tunnel that allows you to view OWASP webpage in kali via security onion. (tricky one, look at network diagram)

- ```
ssh -L 8080:192.168.68.12:80 student@192.168.0.100
```



| TRAINING APPLICATIONS                                 |                                     |
|-------------------------------------------------------|-------------------------------------|
| <a href="#">OWASP WebGoat</a>                         | <a href="#">OWASP WebGoat.NET</a>   |
| <a href="#">OWASP ESAPI Java SwingSet Interactive</a> | <a href="#">OWASP Mutillidae II</a> |
| <a href="#">OWASP RailsGoat</a>                       | <a href="#">OWASP Bricks</a>        |
| <a href="#">OWASP Security Shepherd</a>               | <a href="#">Ghost</a>               |

- using the above configuration, execute whatweb to OWASP and Nikto against OWASP

```
root@Kali2:~# whatweb -v http://127.0.0.1:8080
http://127.0.0.1:8080/ [200]
http://127.0.0.1:8080 [200] Apache[2.2.14][mod_mono/2.4.3
hon/3.3.1,mod_ssl/2.2.14,proxy_html/3.0.1], Country[RU
untu Linux][Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP
ecin Patch proxy_html/3.0.1 mod_authen/3.3.1 Authen/2.

root@Kali2:~# nikto -h http://127.0.0.1:8080
- Nikto v2.1.6

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 8080
+ Start Time: 2025-03-21 16:13:29 (GMT-5)

+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP
```

- From kali tunnel openSUSE web interface via port 22- access on kali

```
root@Kali2:~# ssh -R 9090:127.0.0.1:22 root@192.168.9.2
root@192.168.9.2's password:
ent-Type-Options header is not set. This could allow the user agent
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
2008/05/crossdomainxml-invites-cross-site.html
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@Kali2:~# ss -tulpn | grep :9090
tcp LISTEN 0 128 127.0.0.1:9090
users:(("sshd",pid=2051,fd=10))
tcp LISTEN 0 128 :::9090
users:(("sshd",pid=2051,fd=9))
root@Kali2:~#
```

- From security onion- ssh to kali (outbound connection) (**another tricky one, use your diagram**). For the next three connections, you are executing your command on the **victim** machine. You can then access the victim from your kali (hacker box)
- port forward the web-browser from security onion to kali  
This just would not work?
- port forward the openSUSE web browser from security onion to kali

```

root@Kali2:~# ssh -L 8081:192.168.0.2:80 -p 9090 root@127.0.0.1
root@127.0.0.1's password:
Permission denied, please try again.
root@127.0.0.1's password:
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Mar 21 16:28:55 2025 from 192.168.9.2
root@Kali2:~#

```

- port forward the OWASP web browser from security onion to kali

```

root@Kali2:~# ssh -L 8082:192.168.68.12:80 -p 9090 root@127.0.0.1
root@127.0.0.1's password:
Permission denied, please try again.
root@127.0.0.1's password:
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Mar 21 16:35:26 2025 from localhost
root@Kali2:~#

```

Also for all of these it was not letting me actually view the websites after I let it sit for a while? I'm not sure but I gave up on troubleshooting after two separate lab attempts.

**\*\*\*tcpdump all of your connections. See if you can understand the strange output.\*\*\***

**-On the 12 steps above, what tcpdump command would you use on each of the assignments above in order to capture relevant data**

**I would use tcpdump with the port associated with my tunnel forward.**

**8081 or 8082**

### Part B:

Netlab: NISGTC Network Security Setup:

- On the Windows 2008 Firewall, open up port 50000 point the firewall to port 50000 on 192.168.1.200 -the Windows 8 box has this port closed
- On the Windows 2008 Firewall, open up port 50001 point the firewall to port 50001 on 192.168.1.200 -the Windows 8 box has this port closed
- On the Windows 2008 and the Windows 8- disable the firewall
- On the Windows 2008 and the Windows 8 enable RDP
- On the Backtrack internal, add the user hacker with password student



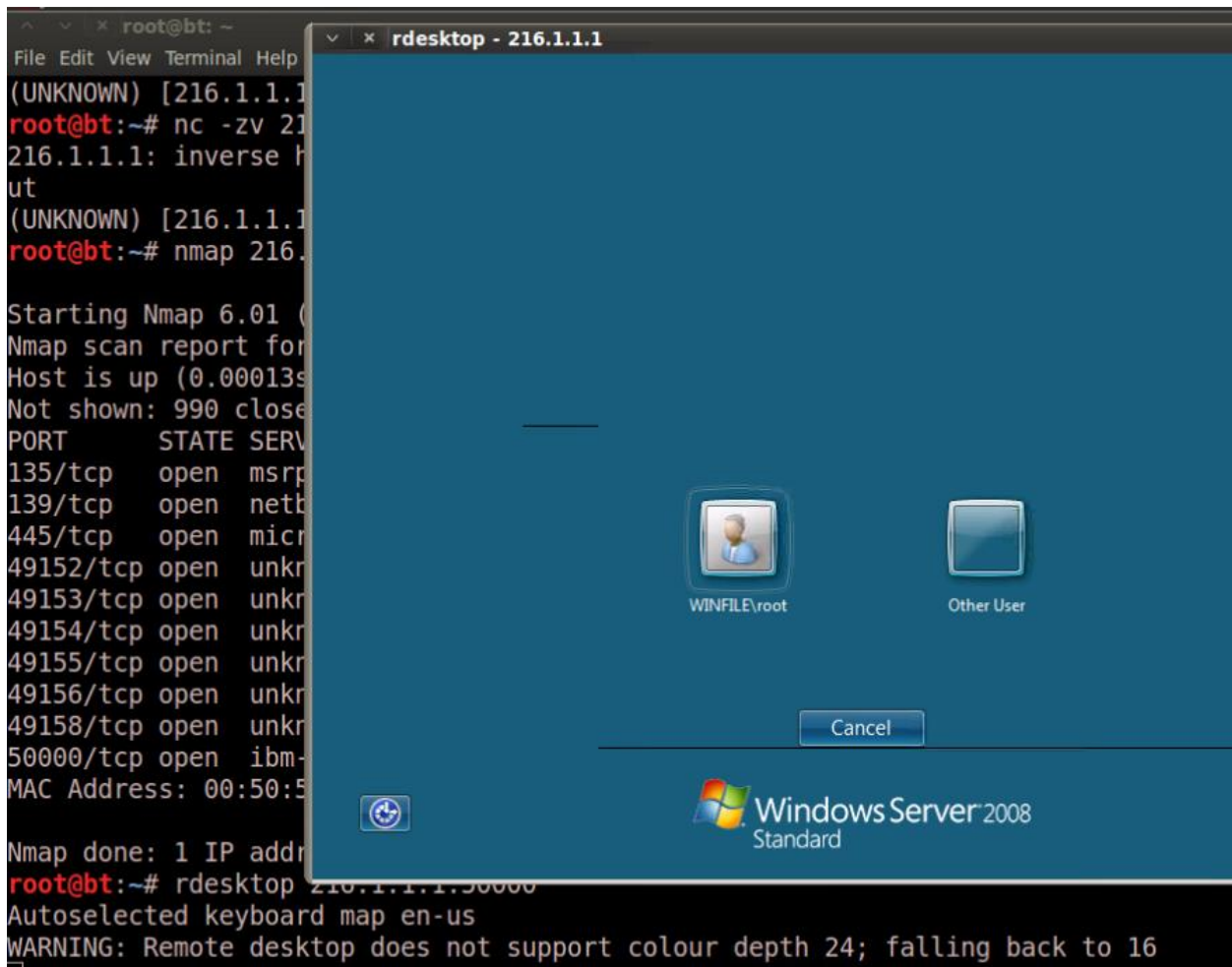
- On the Backtrack internal, run the following command as root: dpkg-reconfigure openssh-server (ensure SSH is running)

I added all of these settings! Trust!

Try to implement the following: **Take your time**. Chart out what you need to do.

A. Connect to 192.168.1.100 via RDP from the external systems--> rdesktop 216.1.1.1:50000

Took me a few hours working with others and trying to find alternate methods, but we got it to work



B. Connect to 192.168.1.50 via SSH from the external system--> SSH [hacker@216.1.1.1](#) - p50001

```

root@bt:~# ssh hacker@216.1.1.1 -p 50002
hacker@216.1.1.1's password:
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

System information as of Fri Mar 21 20:35:25 EDT 2025

System load: 0.0 Processes: 108
Usage of /: 58.0% of 19.06GB Users logged in: 1
Memory usage: 12% IP address for eth2: 192.168.1.50
Swap usage: 0%

=> There is 1 zombie process.

Graph this data and manage this system at https://landscape.canonical.co

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

hacker@bt:~$ whoami
hacker
hacker@bt:~$ pwd
/home/hacker

```

C. From Backtrack external, try to scan 192.168.1.100, 200 and 50

Works!

```

Starting Nmap 6.01 (http://nmap.org) at 2025-03-21 20:36 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00032s latency).
Nmap scan report for 192.168.1.50
Host is up (0.000052s latency).
Nmap scan report for 192.168.1.100
Host is up (0.00022s latency).
Nmap scan report for 192.168.1.175
Host is up (0.00045s latency).
Nmap scan report for 192.168.1.200
Host is up (0.00037s latency).

```

D. From the Windows 7 external box, try to do the below **"at the same time"**:

- access the windows 2008 web interface
- Even with correct rules this would not work.

Description of Service:

win880

Public address

☒ On this interface

☐ On this address pool entry:

Protocol

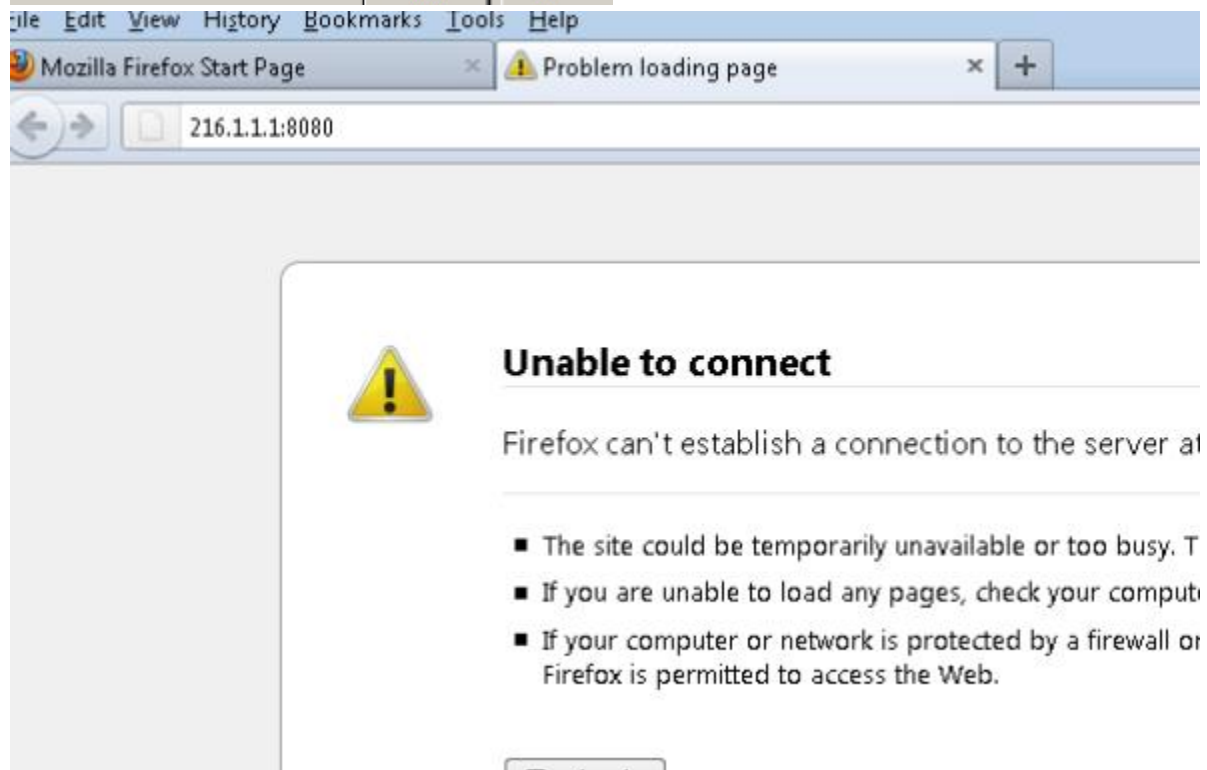
☐ TCP ☒ UDP

Incoming port: 8080

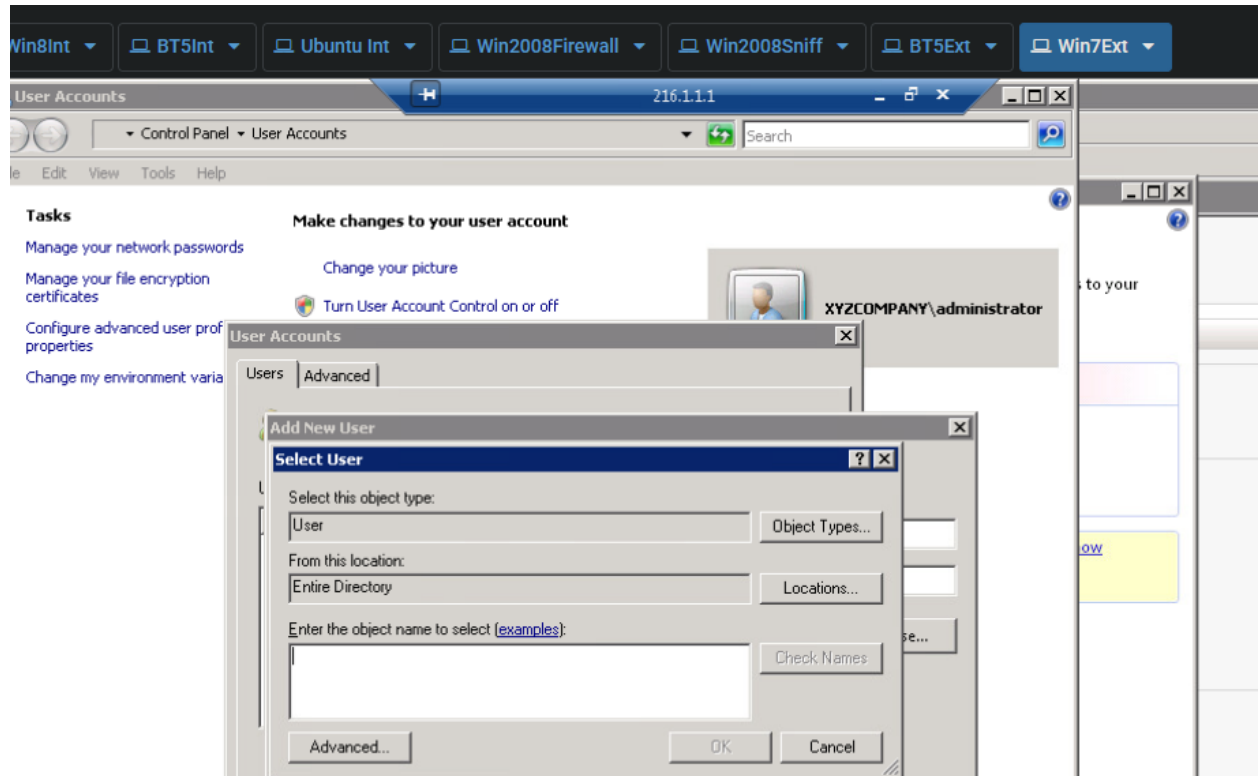
Private address: 192 . 168 . 1 . 100

Outgoing port: 80

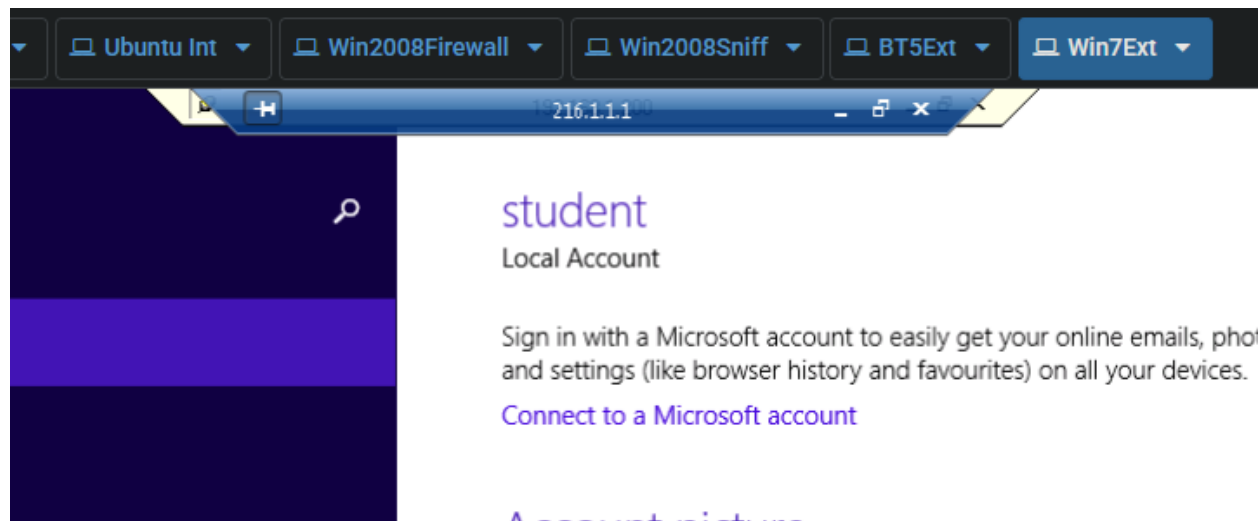
OK Cancel



- access the windows 2008 RDP



- access the windows 8 via RDP



- access the backtrack internal ftp server and copy nc.exe from BT-internal to you windows 7 box

I ftp in and grab the file



