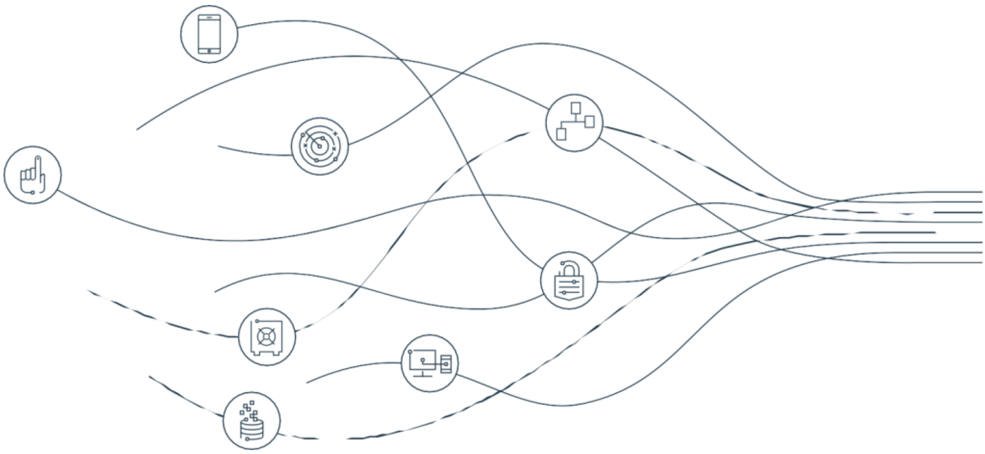
Endpoint Security Practices

Lab 3

Version: 2021.02.08



The information contained in this document has not been submitted to any formal IBM test and is distributed on an “as is” basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer’s ability to evaluate and integrate them into the customer’s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will result elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Contents

Preface

Overview

In this lab, we are going to put ourselves into the shoes of the attacker, and Footprint a network. We will then implant ourselves as a new user in the system to begin taking control. In the latter half of the lab, we will cover some defences and industry best practices that can keep us safe.

Estimated Time to Complete: 120 mins

Objectives:

This lab requires you to complete six Milestones:

1. Unsecured DVR and DDOS Attacks
2. Footprinting
3. Misconfiguration / Bruteforce
4. Take Control
5. Network Protection Practices
6. X-Force Exchange

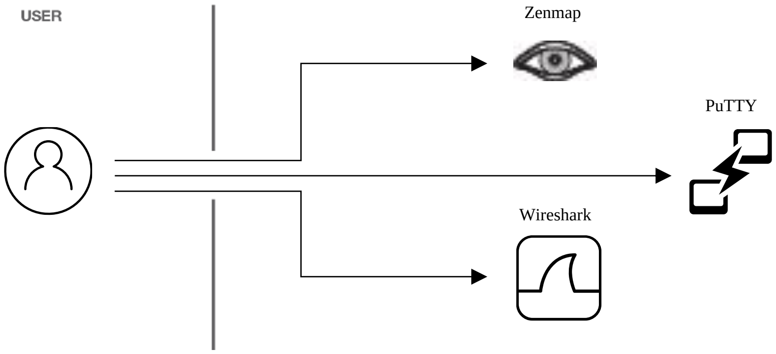
Tools

Zenmap

Wireshark

PuTTY

Flow



1. The User will follow the steps of an online attack by utilizing both Zenmap and Wireshark to find security flaws.
2. We will then defend ourselves from these types of attacks by implementing a Secure Shell with PuTTY.

Milestone 1: Unsecured DVR and DDOS Attacks

How often have you had an app or system push an update without any input from yourself? Maybe at some point you enabled automatic updates and forgot about it, or maybe you fell victim to a forced update. The reality is that everyday thousands of devices connected to the internet go through unmonitored updates. These devices, though they may not contain much sensitive data themselves, are targets for Cybercriminals as they can easily invade the device and, with a little malware, turn the device into a weapon. The weapon is ultimately known as a Distributed Denial of Service (DDoS) Attack, which uses thousands of internet devices to access one server at the same time, resulting in the inevitable collapse of the server.

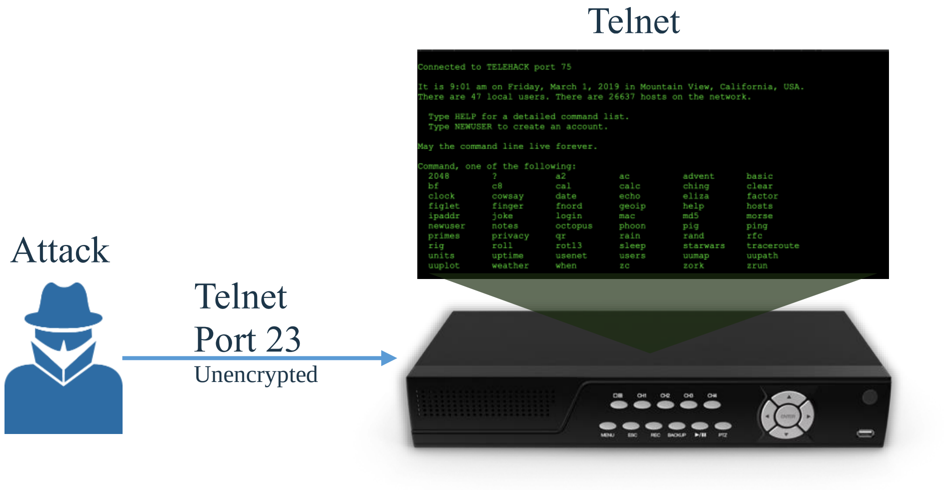
In this scenario we will cover the first three steps the cybercriminal implements to perform a DDoS attack as well as cover some industry best practices to defend yourself.

Steps to Implement a Malicious DDoS Attack

1. **Footpinting**
2. **Misconfiguration** / Bruteforce
3. **Take control**
4. Plant Botnet
5. Run Command and Control
6. Launch DDoS attack
7. Ransomware

The victim is an avid tv watcher and a loyal customer to his entertainment company of choice. So loyal they rent their DVR from them without any thought of security for themselves. Unfortunately for the victim, this company also held security as an afterthought.

One night while the victim is sleeping his DVR pushes an automatic update through an unsecured Telnet connection. This leaves a vulnerability in the victim's network that he may be unaware of, but a searching cybercriminal will soon discover.



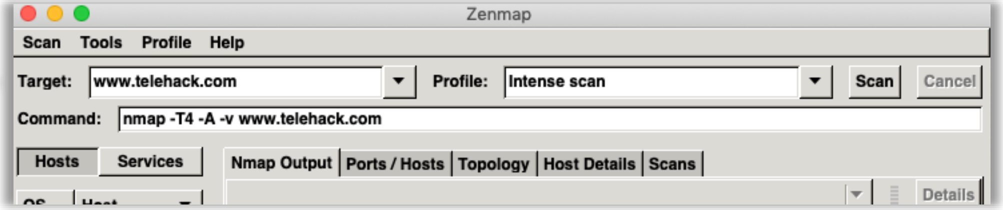
```
Connected to TELEHACK port 75

It is 9:01 am on Friday, March 1, 2019 in Mountain View, California, USA.
There are 47 local users. There are 26637 hosts on the network.

  Type HELP for a detailed command list.
  Type NEWUSER to create an account.

May the command line live forever.

Command, one of the following:
  2048        ?           a2          ac          advent      basic
  bf          c8          cal         calc        ching       clear
  clock       cowsay      date        echo        eliza       factor
  figlet      finger      fnord       geoip       help        hosts
  ipaddr      joke        login       mac         md5         morse
  newuser     notes       octopus     phoon       pig         ping
  primes      privacy     qr          rain        rand        rfc
  rig         roll        rot13       sleep       starwars    traceroute
  units       uptime      usenet      users       uumap       uupath
  uuplot      weather     when        zc          zork        zrun
```

Milestone 2: Footprinting

Network Mapping

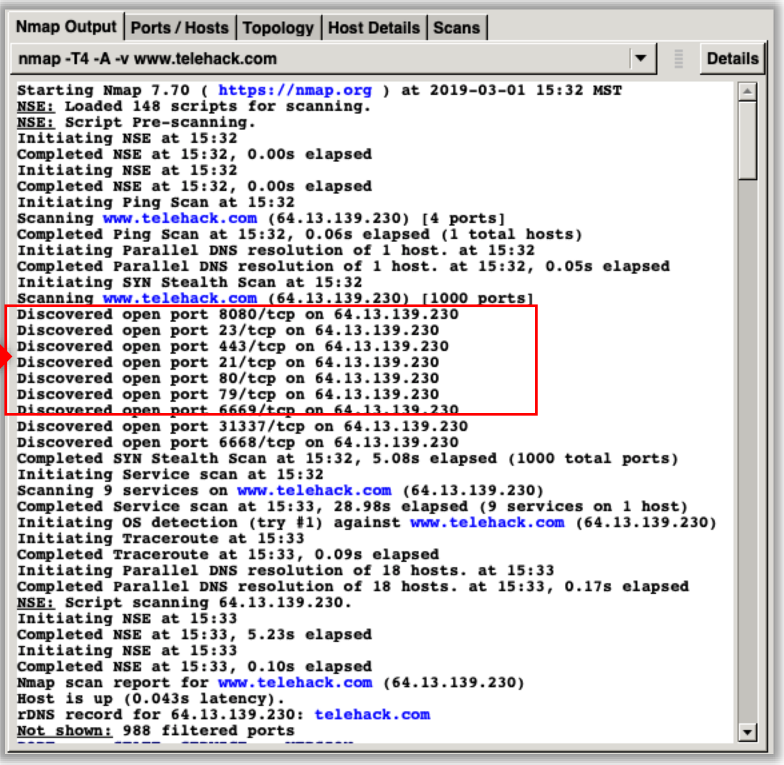
To be able to pull off a successful cyberattack, the attacker needs to know where to strike. This online reconnaissance is often referred to as "Footprinting." Hackers will use tools such as Zenmap to scan networks and discover unsecured open ports.

1. Open Zenmap (Installation instructions can be found in the previous lab if needed)



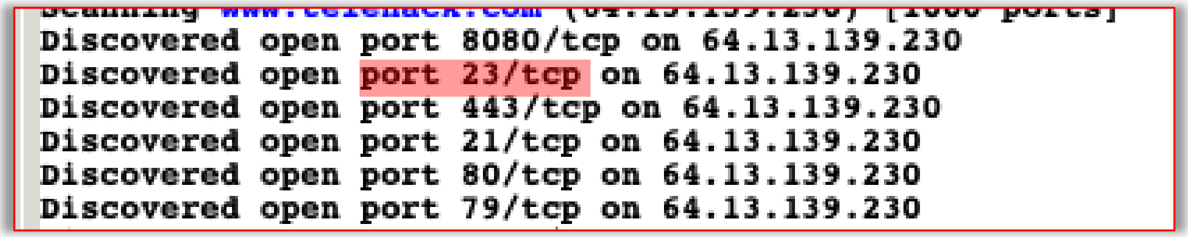
Target: www.telehack.com
Profile: Intense scan
Command: nmap -T4 -A -v www.telehack.com

2. In the Target field input www.telehack.com
3. Click "Scan"
4. Notice the discovered open ports, you may have to scroll back to the top of the generated report
5. We can see that this security system is misconfigured because Port 23, the port Telnet uses for unsecure communications, is still open.



```
nmap -T4 -A -v www.telehack.com
```

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-01 15:32 MST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:32
Completed NSE at 15:32, 0.00s elapsed
Initiating NSE at 15:32
Completed NSE at 15:32, 0.00s elapsed
Initiating Ping Scan at 15:32
Scanning www.telehack.com (64.13.139.230) [4 ports]
Completed Ping Scan at 15:32, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:32
Completed Parallel DNS resolution of 1 host. at 15:32, 0.05s elapsed
Initiating SYN Stealth Scan at 15:32
Scanning www.telehack.com (64.13.139.230) [1000 ports]
Discovered open port 8080/tcp on 64.13.139.230
Discovered open port 23/tcp on 64.13.139.230
Discovered open port 443/tcp on 64.13.139.230
Discovered open port 21/tcp on 64.13.139.230
Discovered open port 80/tcp on 64.13.139.230
Discovered open port 79/tcp on 64.13.139.230
Discovered open port 6669/tcp on 64.13.139.230
Discovered open port 31337/tcp on 64.13.139.230
Discovered open port 6668/tcp on 64.13.139.230
Completed SYN Stealth Scan at 15:32, 5.08s elapsed (1000 total ports)
Initiating Service scan at 15:32
Scanning 9 services on www.telehack.com (64.13.139.230)
Completed Service scan at 15:33, 28.98s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against www.telehack.com (64.13.139.230)
Initiating Traceroute at 15:33
Completed Traceroute at 15:33, 0.09s elapsed
Initiating Parallel DNS resolution of 18 hosts. at 15:33
Completed Parallel DNS resolution of 18 hosts. at 15:33, 0.17s elapsed
NSE: Script scanning 64.13.139.230.
Initiating NSE at 15:33
Completed NSE at 15:33, 5.23s elapsed
Initiating NSE at 15:33
Completed NSE at 15:33, 0.10s elapsed
Nmap scan report for www.telehack.com (64.13.139.230)
Host is up (0.043s latency).
rDNS record for 64.13.139.230: telehack.com
Not shown: 988 filtered ports
```

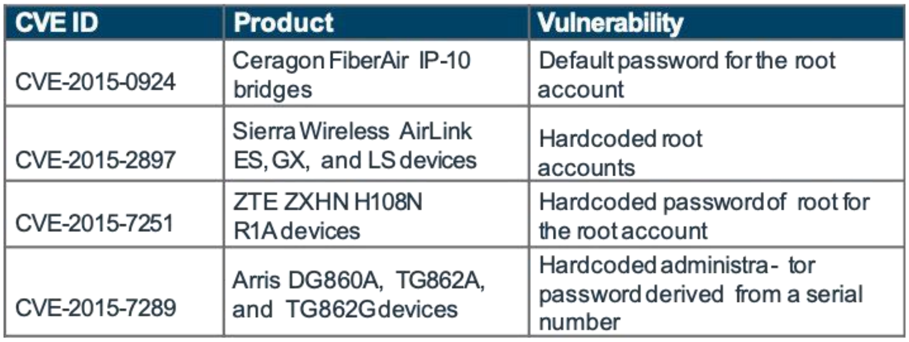


```
Scanning www.telehack.com (64.13.139.230) [1000 ports]
Discovered open port 8080/tcp on 64.13.139.230
Discovered open port 23/tcp on 64.13.139.230
Discovered open port 443/tcp on 64.13.139.230
Discovered open port 21/tcp on 64.13.139.230
Discovered open port 80/tcp on 64.13.139.230
Discovered open port 79/tcp on 64.13.139.230
```

Milestone 3: Misconfiguration / Bruteforce

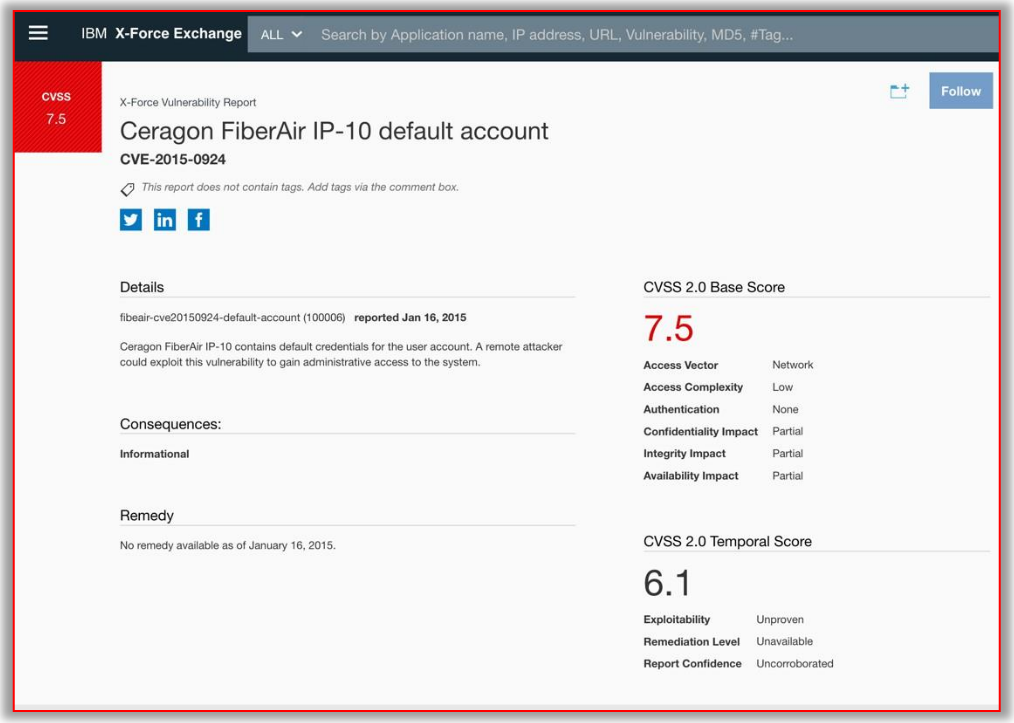
In the following section, we will describe a general methodology to take advantage of a specific IOT misconfiguration:

- Now that we have confirmed that TCP port 23 for Telnet is open on the IOT device, the next step would be to investigate more details about any potential vulnerabilities disclosed for this specific device.
- As an example, let’s say an attacker found an open port on Ceragon FiberAir IP-10 bridges, as we reviewed in the lecture, those devices have a known vulnerability with the following identifier: CVE-2015-0924. Please refer to the following table:



CVE ID	Product	Vulnerability
CVE-2015-0924	Ceragon FiberAir IP-10 bridges	Default password for the root account
CVE-2015-2897	Sierra Wireless AirLink ES, GX, and LS devices	Hardcoded root accounts
CVE-2015-7251	ZTE ZXHN H108N R1A devices	Hardcoded password of root for the root account
CVE-2015-7289	Arris DG860A, TG862A, and TG862G devices	Hardcoded administra- tor password derived from a serial number

- By searching on X-Force Exchange (XFE) and other Threat Intelligence platforms, you can find all the technical details about CVE-2015-0924. Click on the link below to review this information on XF: https://exchange.xforce.ibmcloud.com/vulnerabilities/cve-2015-0924


IBM X-Force Exchange
ALL
Search by Application name, IP address, URL, Vulnerability, MD5, #Tag...
CVSS
7.5
Follow

X-Force Vulnerability Report

Ceragon FiberAir IP-10 default account

CVE-2015-0924

This report does not contain tags. Add tags via the comment box.

Details

fibeair-cve20150924-default-account (100006) **reported Jan 16, 2015**

Ceragon FiberAir IP-10 contains default credentials for the user account. A remote attacker could exploit this vulnerability to gain administrative access to the system.

Consequences:

Informational

Remedy

No remedy available as of January 16, 2015.

CVSS 2.0 Base Score

7.5

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality Impact	Partial
Integrity Impact	Partial
Availability Impact	Partial

CVSS 2.0 Temporal Score

6.1

Exploitability	Unproven
Remediation Level	Unavailable
Report Confidence	Uncorroborated

- As a result of your investigation, you might be able to find the “root” password to get access to the device or you can just try to Bruteforce the root password using the Telnet service we discovered using Nmap.

Milestone 4: Take Control

Create New User

Once the attacker has successfully entered into the DVR Network, the first thing he will do is create himself as a new user.

1. Navigate to telehack.com to simulate the user gaining access to an unsecured device.

In the command line input:

```
newuser
```

2. You will need to verify that you 13 years or older as well as read the privacy policy.
3. Enter your desired Username. Your Username must be within 2-9 characters, begin with a lowercase letter, and may contain letters or numbers.
4. Once you have decided on a Username, input the password. It must be at least 6 characters long.

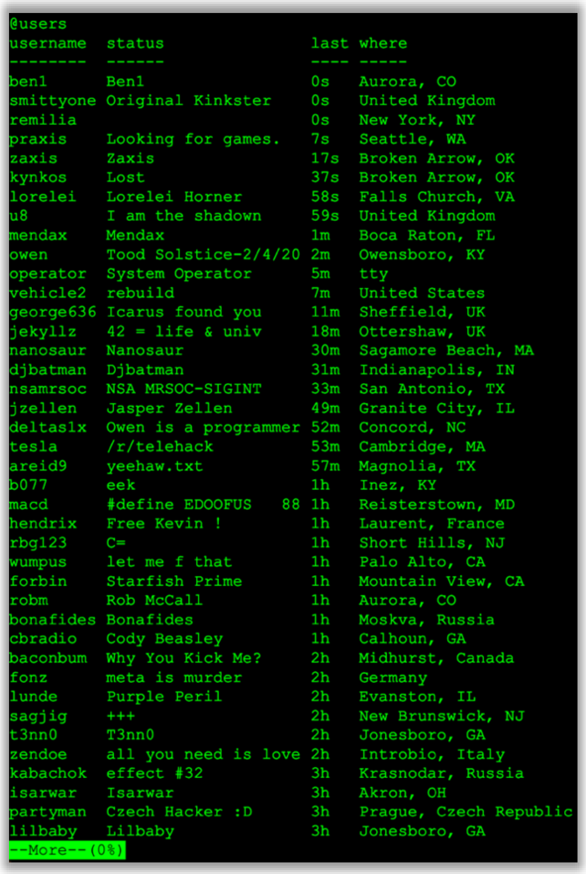
View Other Users

Now that the attacker has made himself a completely legitimate user profile, he now has access to sensitive information such as User data.

In the command line input:

```
users
```

1. You can scroll down the list to see all of the users on the network as well as their last status, when they were last online, and where they are located.
2. When long lists like this are generated, you can hit enter to move line by line or spacebar to move quickly
3. Hold “Control” and hit “c” to stop a list or command



```
@users
username  status               last where
--------  ------               ---- -----
ben1      Ben1                 0s   Aurora, CO
smittyone Original Kinkster    0s   United Kingdom
remilia                        0s   New York, NY
praxis    Looking for games.   7s   Seattle, WA
zaxis     Zaxis                17s  Broken Arrow, OK
kynkos    Lost                 37s  Broken Arrow, OK
lorelei   Lorelei Horner       58s  Falls Church, VA
u8        I am the shadown     59s  United Kingdom
mendax    Mendax               1m   Boca Raton, FL
owen      Tood Solstice-2/4/20 2m   Owensboro, KY
operator  System Operator      5m   tty
vehicle2  rebuild              7m   United States
george636 Icarus found you     11m  Sheffield, UK
jekyllz   42 = life & univ     18m  Ottershaw, UK
nanosaur  Nanosaur             30m  Sagamore Beach, MA
djbatman  Djbatman             31m  Indianapolis, IN
nsamrsoc  NSA MRSOC-SIGINT     33m  San Antonio, TX
jzellen   Jasper Zellen        49m  Granite City, IL
deltas1x  Owen is a programmer 52m  Concord, NC
tesla     /r/telehack          53m  Cambridge, MA
areid9    yeehaw.txt           57m  Magnolia, TX
b077      eek                  1h   Inez, KY
macd      #define EDOOFUS   88 1h   Reisterstown, MD
hendrix   Free Kevin !         1h   Laurent, France
rbg123    C=                   1h   Short Hills, NJ
wumpus    let me f that        1h   Palo Alto, CA
forbin    Starfish Prime       1h   Mountain View, CA
robm      Rob McCall           1h   Aurora, CO
bonafides Bonafides            1h   Moskva, Russia
cbradio   Cody Beasley         1h   Calhoun, GA
baconbum  Why You Kick Me?     2h   Midhurst, Canada
fonz      meta is murder       2h   Germany
lunde     Purple Peril         2h   Evanston, IL
sagjig    +++                  2h   New Brunswick, NJ
t3nn0     T3nn0                2h   Jonesboro, GA
zendoe    all you need is love 2h   Introbio, Italy
kabachok  effect #32           3h   Krasnodar, Russia
isarwar   Isarwar              3h   Akron, OH
partyman  Czech Hacker :D      3h   Prague, Czech Republic
lilbaby   Lilbaby              3h   Jonesboro, GA
--More--(0%)
```

Finger

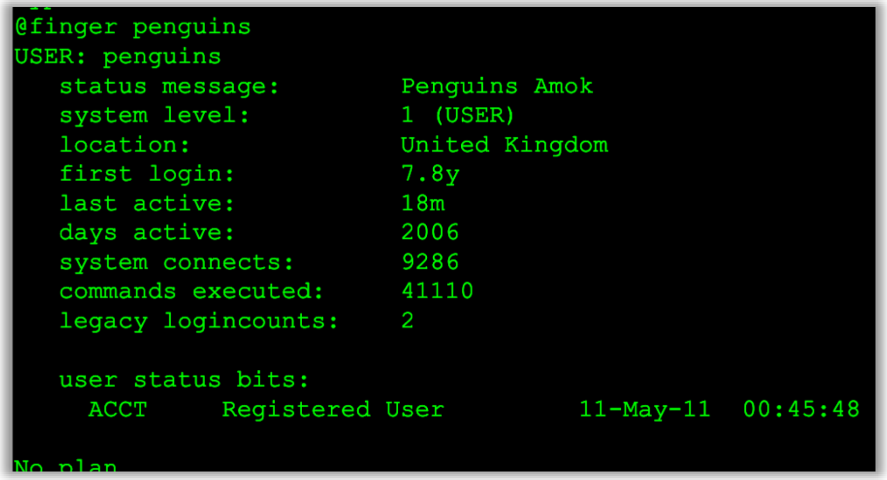
With access to all the users on the network the attacker can use the finger command to pull extra information from each of those users.

1. Find a lab partner or grab a random name from the user list and in the command line input:

```
Finger <user>
```

With <user> replaced by the actual username of your choice.

2. Using this command, you will not only pull location and last login of the user, but also when they first made their account, how many times they have connected to the system, and the number of commands the user has executed. Some users even have status bits connected to their account so you can see what they were last working on.



```
@finger penguins
USER: penguins
   status message:         Penguins Amok
   system level:           1 (USER)
   location:               United Kingdom
   first login:            7.8y
   last active:            18m
   days active:            2006
   system connects:        9286
   commands executed:      41110
   legacy logincounts:     2

   user status bits:
     ACCT     Registered User         11-May-11  00:45:48

No plan
```

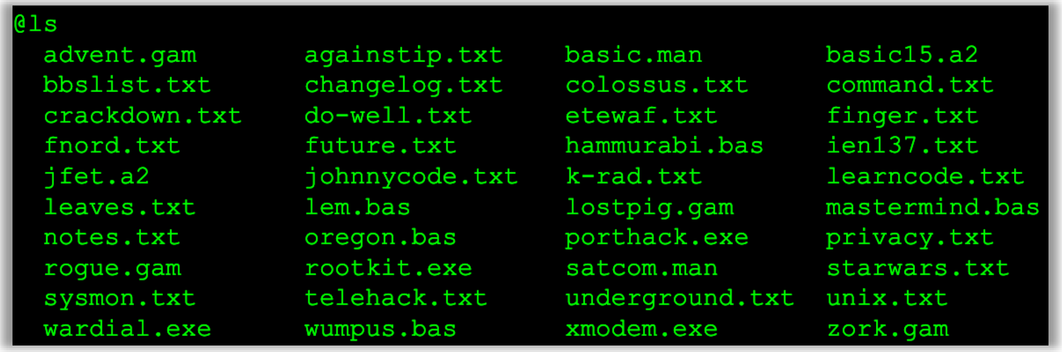
View Files

Once connected to the network, it isn’t only user information that is in danger, but also any documents, paperwork, even programs and services kept on that network are now fair game to the attacker.

1. When logged in as a user, in the command line input:

```
ls
```

2. A list of all the files and services stored on that network will display

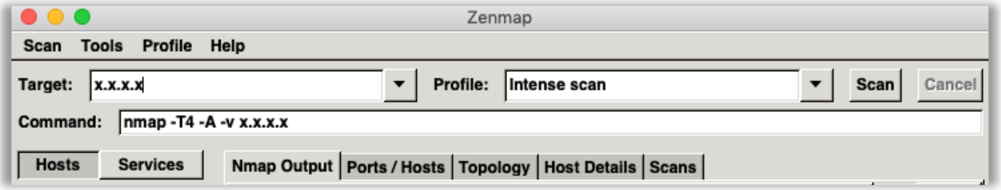


```
@ls
  advent.gam       againstip.txt    basic.man        basic15.a2
  bbslist.txt      changelog.txt    colossus.txt     command.txt
  crackdown.txt    do-well.txt      etewaf.txt       finger.txt
  fnord.txt        future.txt       hammurabi.bas    ien137.txt
  jfet.a2          johnnycode.txt   k-rad.txt        learncode.txt
  leaves.txt       lem.bas          lostpig.gam      mastermind.bas
  notes.txt        oregon.bas       porthack.exe     privacy.txt
  rogue.gam        rootkit.exe      satcom.man       starwars.txt
  sysmon.txt       telehack.txt     underground.txt  unix.txt
  wardial.exe      wumpus.bas       xmodem.exe       zork.gam
```

Milestone 5: Network Protection Practices

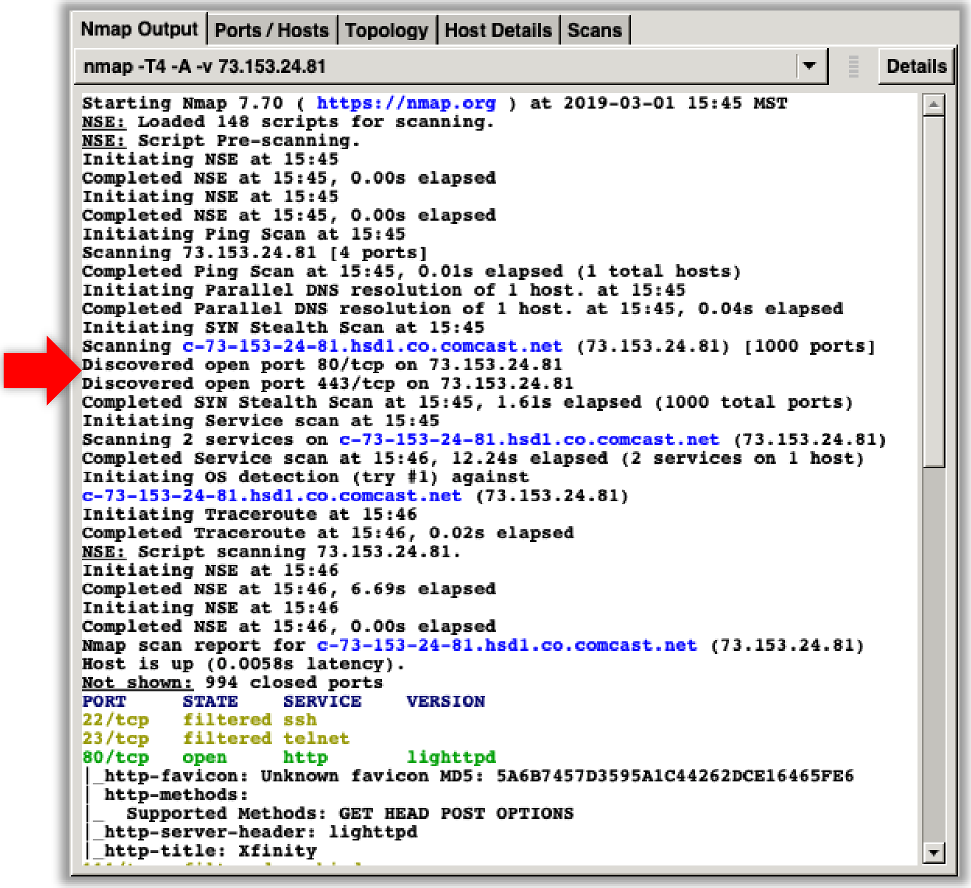
We know that Telnet is an unsecured connection that can be used to access your network. In order to ensure we are not susceptible to this vulnerability, we can utilize a Secure Shell (SSH) and ensure port 23 is not open. In the next steps we are going to monitor a protected network and verify that information is encrypted.

1. Find your IP Address.
2. This time input your personal IP Address into the Target for Zenmap and hit "Scan".



Target: x.x.x.x
Profile: Intense scan
Command: nmap -T4 -A -v x.x.x.x

3. Review the generated report. Do you still see an open port 23? What ports do you have open?



nmap -T4 -A -v 73.153.24.81

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-01 15:45 MST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:45
Completed NSE at 15:45, 0.00s elapsed
Initiating NSE at 15:45
Completed NSE at 15:45, 0.00s elapsed
Initiating Ping Scan at 15:45
Scanning 73.153.24.81 [4 ports]
Completed Ping Scan at 15:45, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:45
Completed Parallel DNS resolution of 1 host. at 15:45, 0.04s elapsed
Initiating SYN Stealth Scan at 15:45
Scanning c-73-153-24-81.hsd1.co.comcast.net (73.153.24.81) [1000 ports]
Discovered open port 80/tcp on 73.153.24.81
Discovered open port 443/tcp on 73.153.24.81
Completed SYN Stealth Scan at 15:45, 1.61s elapsed (1000 total ports)
Initiating Service scan at 15:45
Scanning 2 services on c-73-153-24-81.hsd1.co.comcast.net (73.153.24.81)
Completed Service scan at 15:46, 12.24s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against
c-73-153-24-81.hsd1.co.comcast.net (73.153.24.81)
Initiating Traceroute at 15:46
Completed Traceroute at 15:46, 0.02s elapsed
NSE: Script scanning 73.153.24.81.
Initiating NSE at 15:46
Completed NSE at 15:46, 6.69s elapsed
Initiating NSE at 15:46
Completed NSE at 15:46, 0.00s elapsed
Nmap scan report for c-73-153-24-81.hsd1.co.comcast.net (73.153.24.81)
Host is up (0.0058s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE    VERSION
22/tcp   filtered ssh
23/tcp   filtered telnet
80/tcp   open     http       lighttpd
|_http-favicon: Unknown favicon MD5: 5A6B7457D3595A1C44262DCE16465FE6
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: lighttpd
|_http-title: Xfinity
```

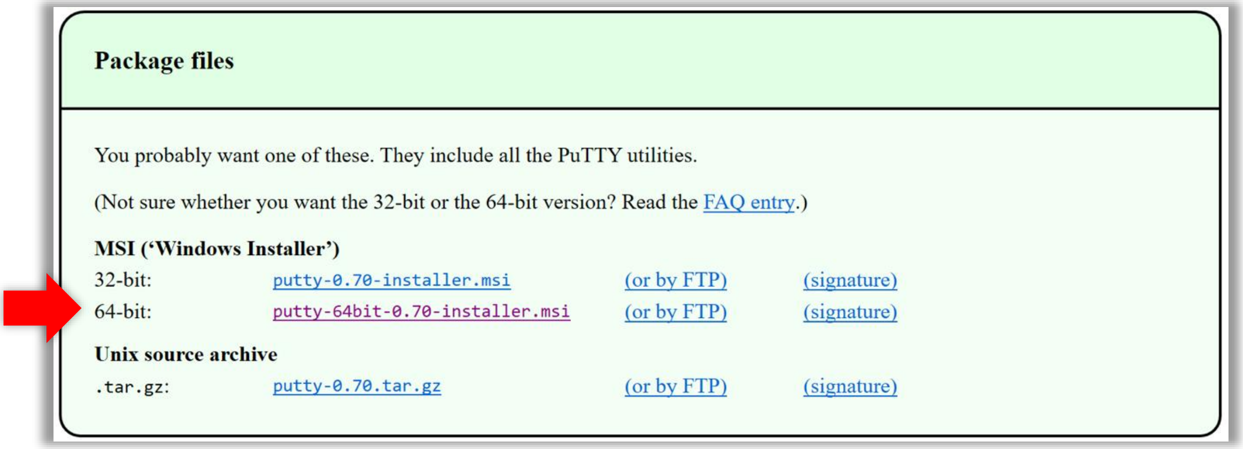
SSH

A Secure Shell (SSH) wraps your connection in an encrypted layer so even if an attacker can sniff the packet sent, they will not be able to acquire any useful information.

SSH Windows Installation and Use

Windows does not have a built in Secure Shell so we will need to download a third-party program. For this lab we recommend PuTTY.

1. Navigate to the PuTTY download link found here.
2. Scroll down the page to find the correct download package for your operating system.



Package files

You probably want one of these. They include all the PuTTY utilities.

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

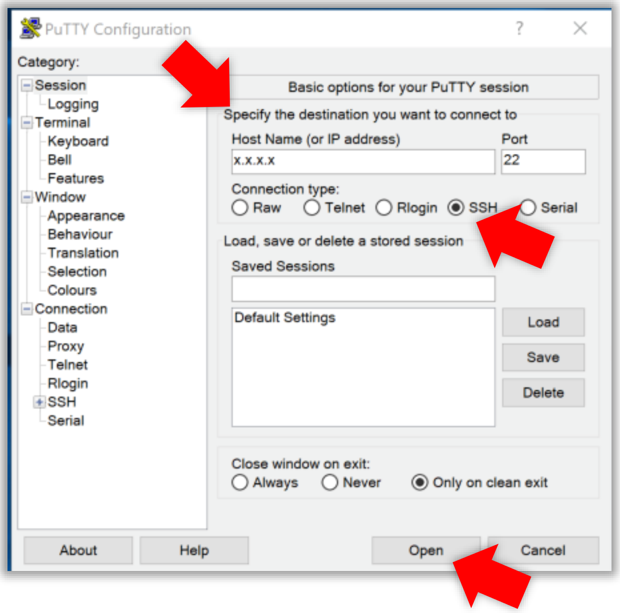
MSI ('Windows Installer')

32-bit:	putty-0.70-installer.msi	(or by FTP)	(signature)
64-bit:	putty-64bit-0.70-installer.msi	(or by FTP)	(signature)

Unix source archive

.tar.gz:	putty-0.70.tar.gz	(or by FTP)	(signature)

3. Download and run the installer.
4. Click through the installer and read through the ReadMe.
5. PuTTY is ready for use! Open the program, input the IP Address of device you wish to connect with, and hit "open."



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): x.x.x.x

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

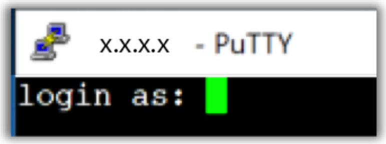
Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

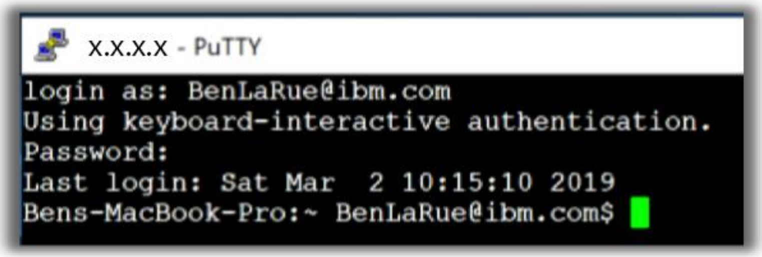
Double-check that the connection type is set to SSH.

6. You will be prompted for the user login information just like any connection request.



```
login as: 
```

7. Once connected you will have the same capabilities that the Telnet connection provided.

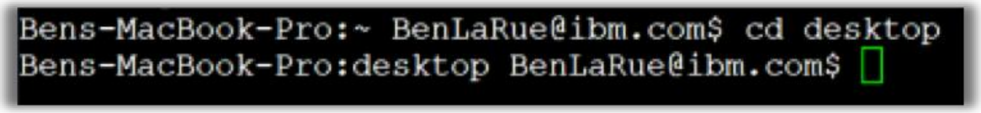


```
login as: BenLaRue@ibm.com
Using keyboard-interactive authentication.
Password:
Last login: Sat Mar  2 10:15:10 2019
Bens-MacBook-Pro:~ BenLaRue@ibm.com$ 
```

8. Select the desktop as the chosen directory and look at all the files stored.
   To do this, Input

```
cd desktop
```

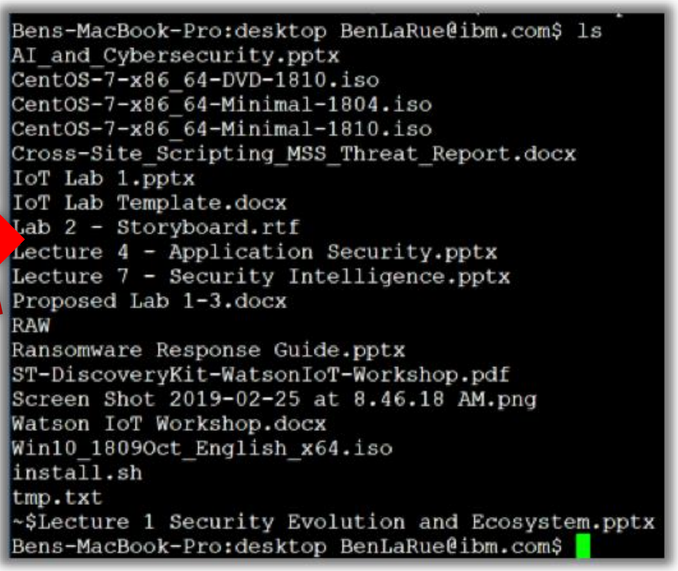
You will know you are in the chosen directory by it being displayed before your username.



```
Bens-MacBook-Pro:~ BenLaRue@ibm.com$ cd desktop
Bens-MacBook-Pro:desktop BenLaRue@ibm.com$ 
```

9. Now we will look at the files just as we did with the Telnet connection.
   In the command line input:

```
ls
```



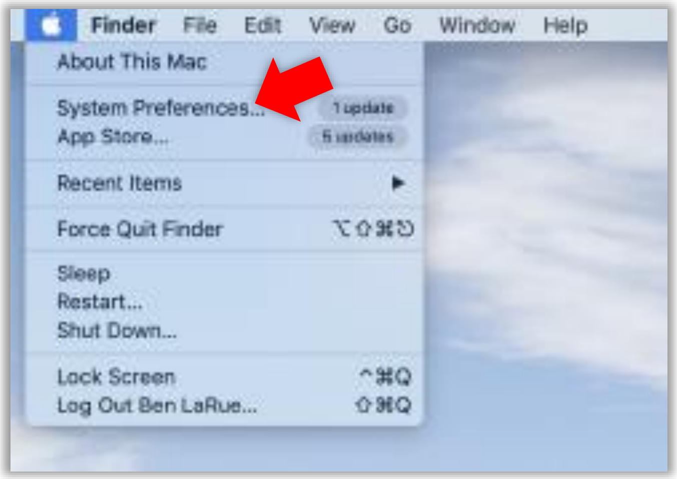
```
Bens-MacBook-Pro:desktop BenLaRue@ibm.com$ ls
AI_and_Cybersecurity.pptx
CentOS-7-x86_64-DVD-1810.iso
CentOS-7-x86_64-Minimal-1804.iso
CentOS-7-x86_64-Minimal-1810.iso
Cross-Site_Scripting_MSS_Threat_Report.docx
IoT Lab 1.pptx
IoT Lab Template.docx
Lab 2 - Storyboard.rtf
Lecture 4 - Application Security.pptx
Lecture 7 - Security Intelligence.pptx
Proposed Lab 1-3.docx
RAW
Ransomware Response Guide.pptx
ST-DiscoveryKit-WatsonIoT-Workshop.pdf
Screen Shot 2019-02-25 at 8.46.18 AM.png
Watson IoT Workshop.docx
Win10_1809Oct_English_x64.iso
install.sh
tmp.txt
~$Lecture 1 Security Evolution and Ecosystem.pptx
Bens-MacBook-Pro:desktop BenLaRue@ibm.com$ 
```

All the files stored in that directory are displayed to us, exactly like the Telnet connection.

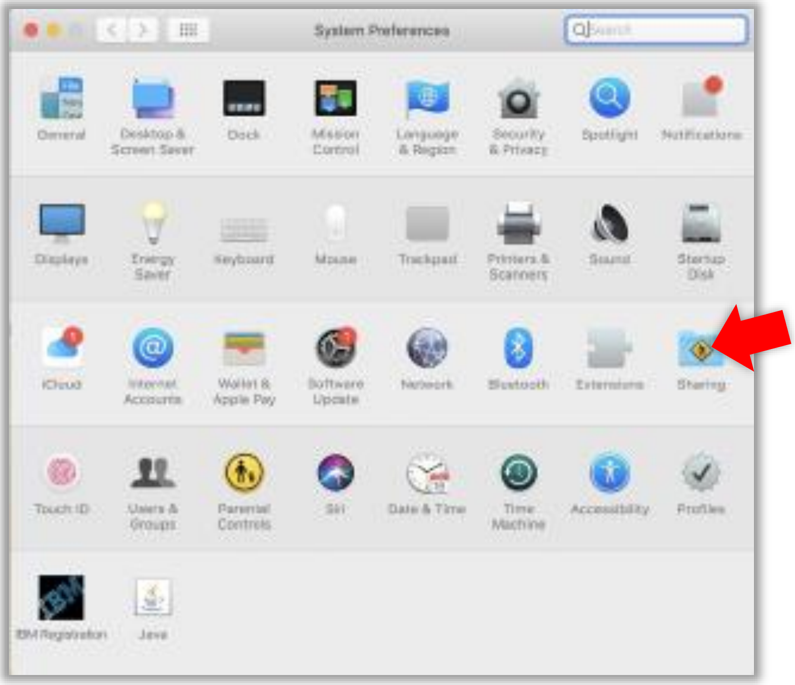
SSH Mac Activation

Mac has a built in Secure Shell connection, so we simply need to go through the steps to activate it. However, we do need to enable Remote Login through Sharin in System Preferences in order to enable the SSH Server.

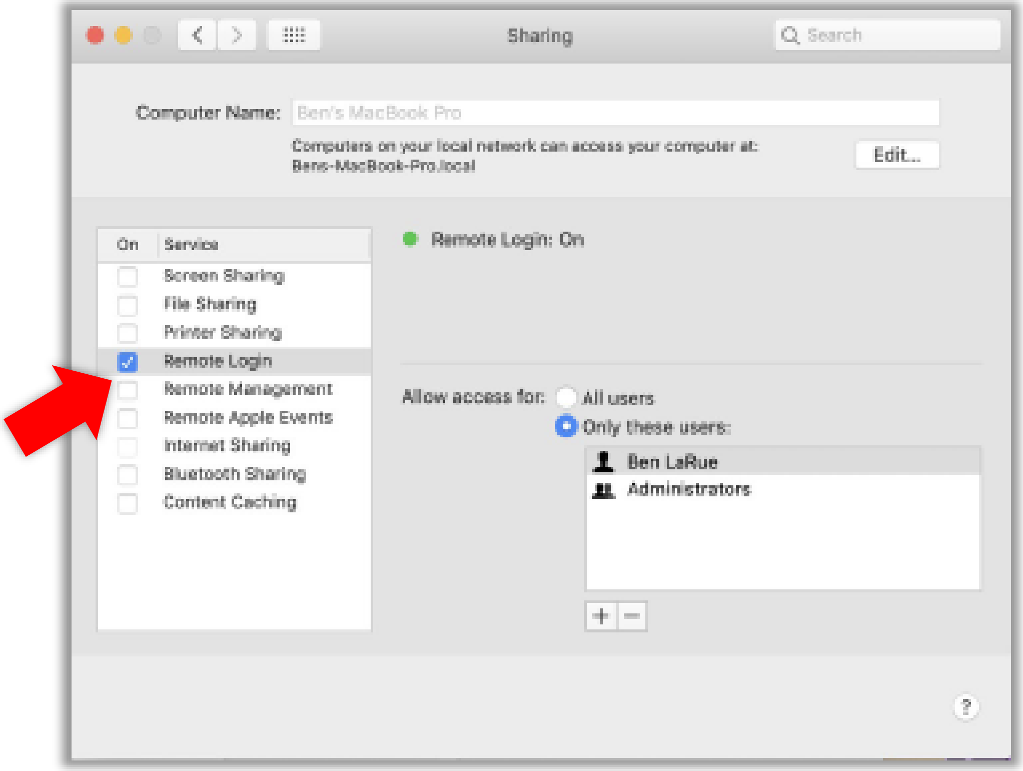
1. Navigate to “System Preferences”.



2. Click on “Sharing”.



3. Check the box next to “Remote Login”. This will allow an external login to our system.



Computer Name: Ben's MacBook Pro

Computers on your local network can access your computer at: Bens-MacBook-Pro.local

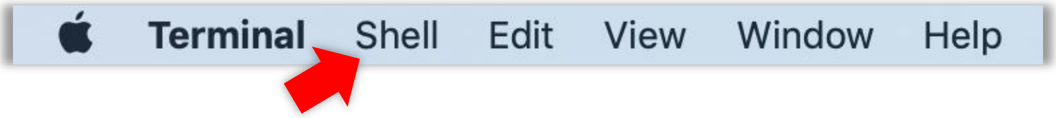
- □ Screen Sharing
- □ File Sharing
- □ Printer Sharing
- ☑ Remote Login
- □ Remote Management
- □ Remote Apple Events
- □ Internet Sharing
- □ Bluetooth Sharing
- □ Content Caching

● Remote Login: On

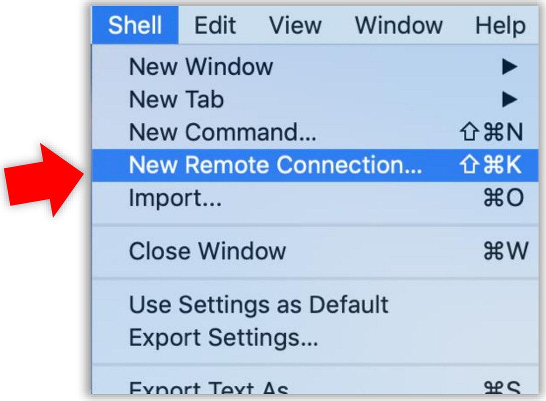
Allow access for: ○ All users ● Only these users:

Ben LaRue
Administrators

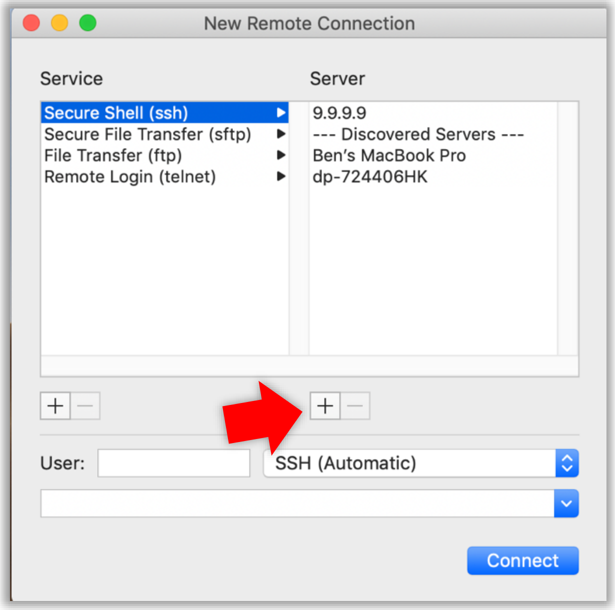
4. Open your Terminal. Click on the magnifying glass at the top right and type Terminal.
5. With the Terminal open, at the top left of your screen click “Shell.”



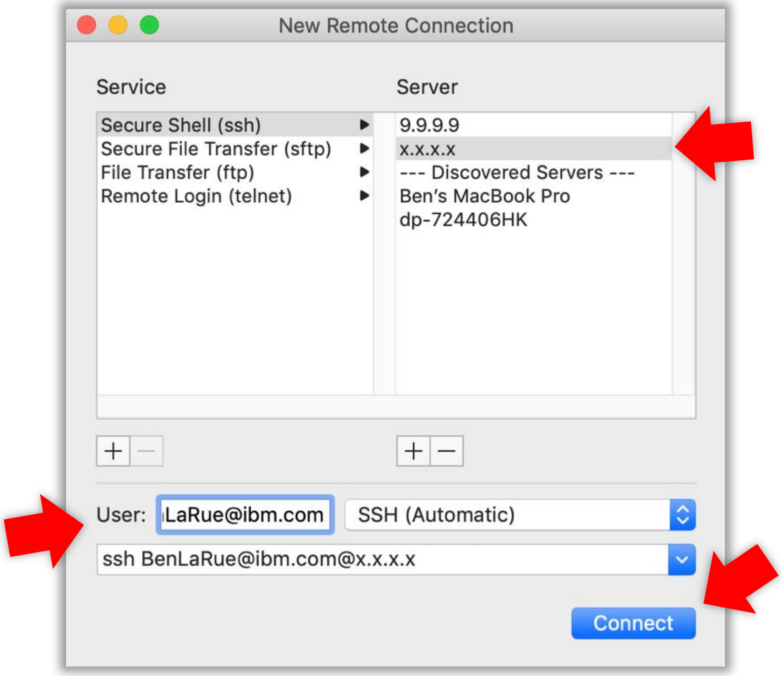
6. Then choose “New Remote Connection.”



7. Select the "Secure Shell (ssh)" service and then under the Server column hit the "+" to enter a new IP.



8. Enter the IP Address of the device you wish to connect to. Now enter the user and with the correct IP selected hit "Connect."



User: LaRue@ibm.com

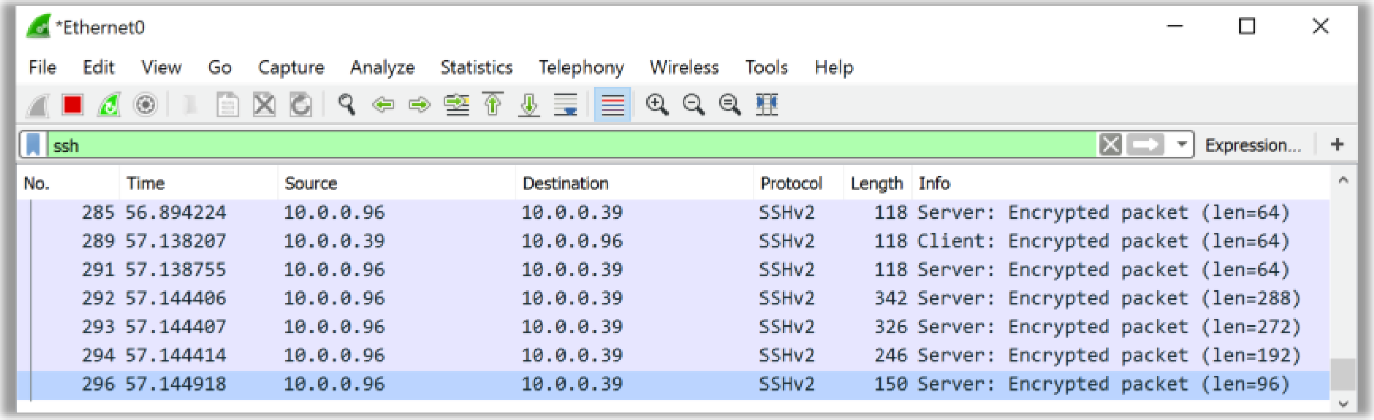
ssh BenLaRue@ibm.com@x.x.x.x

9. Enter the password and you have gained remote access. Follow steps 8 and 9 from the previous Windows section to choose a directory and look at stored files.

SSH Capabilities – Data is Encrypted

We’ve shown that SSH provides the same capabilities as Telnet, but Telnet is an old form of connection that is riddled with vulnerabilities. The Secure Shell wraps all of your communication and other data in layers of encryption so even when an attacker is using a sniffer on your data packets, they won’t be able to see any sensitive information.

1. Open Wireshark (installation instructions can be found in previous lab).
2. Point at your network and capture the data packets transferred during the SSH connection



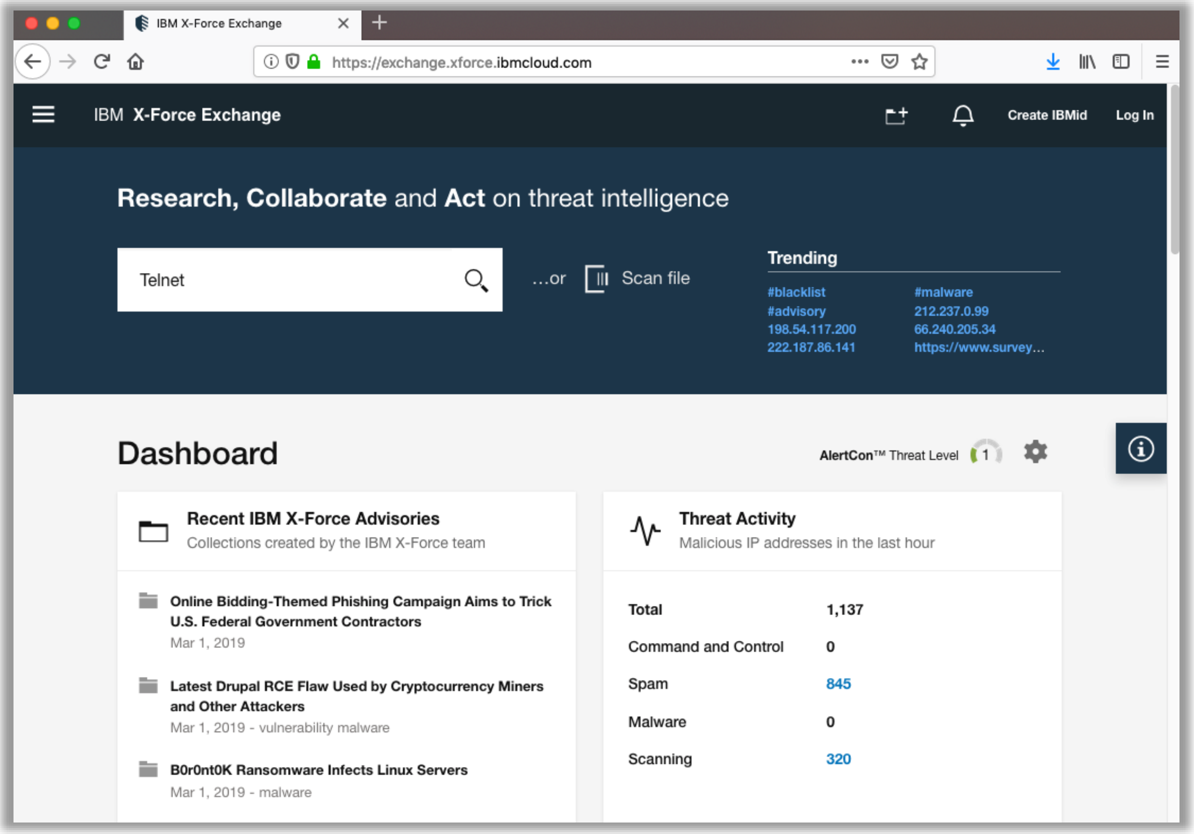
```
No.     Time       Source      Destination  Protocol  Length  Info
   285 56.894224   10.0.0.96   10.0.0.39    SSHv2        118 Server: Encrypted packet (len=64)
   289 57.138207   10.0.0.39   10.0.0.96    SSHv2        118 Client: Encrypted packet (len=64)
   291 57.138755   10.0.0.96   10.0.0.39    SSHv2        118 Server: Encrypted packet (len=64)
   292 57.144406   10.0.0.96   10.0.0.39    SSHv2        342 Server: Encrypted packet (len=288)
   293 57.144407   10.0.0.96   10.0.0.39    SSHv2        326 Server: Encrypted packet (len=272)
   294 57.144414   10.0.0.96   10.0.0.39    SSHv2        246 Server: Encrypted packet (len=192)
   296 57.144918   10.0.0.96   10.0.0.39    SSHv2        150 Server: Encrypted packet (len=96)
```

3. Notice all data packets are encrypted!

Milestone 6: X-Force Exchange

Other than using programs like Secure Shells to keep us safe we can utilize services who, 24/7, monitor cyber threats. IBM's X-Force Exchange is just one such company.

1. Navigate to X-Force Exchange and login with your IBM id.
2. Input Telnet into the search.



Research, Collaborate and Act on threat intelligence

Telnet

Trending

#blacklist	#malware
#advisory	212.237.0.99
198.54.117.200	66.240.205.34
222.187.86.141	https://www.survey...

Dashboard

Recent IBM X-Force Advisories
Collections created by the IBM X-Force team

Online Bidding-Themed Phishing Campaign Aims to Trick U.S. Federal Government Contractors
Mar 1, 2019

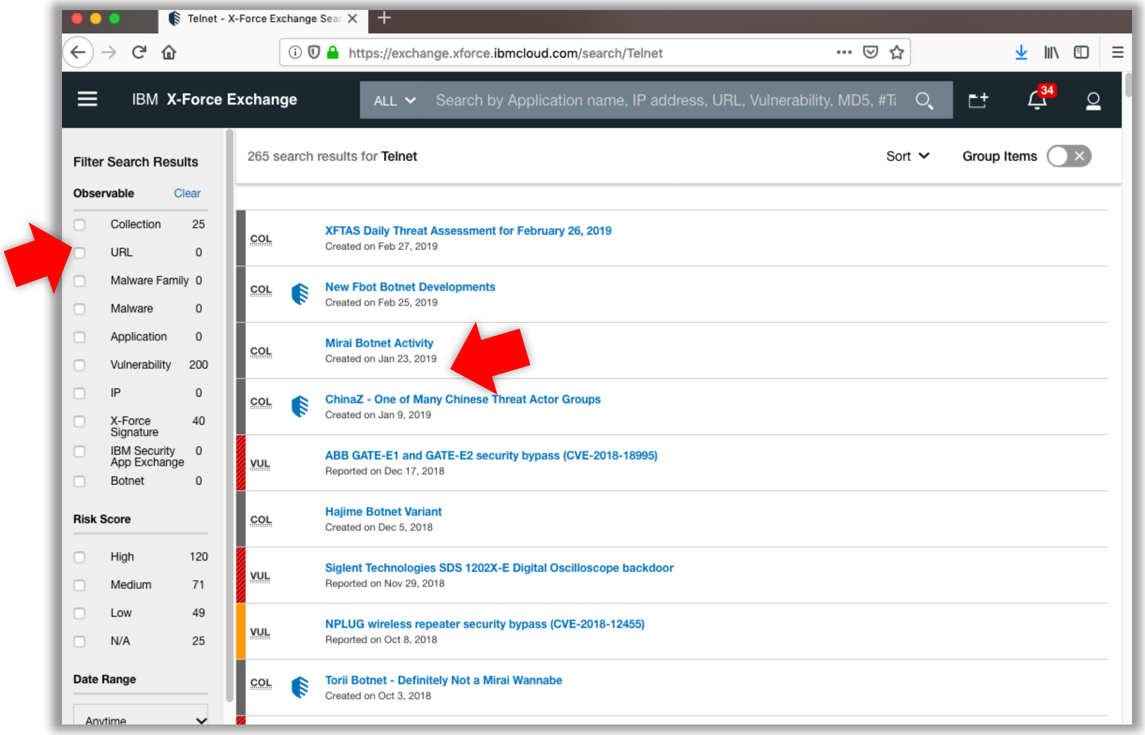
Latest Drupal RCE Flaw Used by Cryptocurrency Miners and Other Attackers
Mar 1, 2019 - vulnerability malware

B0r0nt0K Ransomware Infects Linux Servers
Mar 1, 2019 - malware

Threat Activity
Malicious IP addresses in the last hour

Total	1,137
Command and Control	0
Spam	845
Malware	0
Scanning	320

3. The “Collections” will show what type of attacks are happening.



Telnet - X-Force Exchange Sear
https://exchange.xforce.ibmcloud.com/search/Telnet
IBM X-Force Exchange
ALL
Search by Application name, IP address, URL, Vulnerability, MD5, #Ta
34

265 search results for **Telnet**

Sort

Group Items

Filter Search Results

Observable Clear

Observable	
□ Collection	25
□ URL	0
□ Malware Family	0
□ Malware	0
□ Application	0
□ Vulnerability	200
□ IP	0
□ X-Force Signature	40
□ IBM Security App Exchange	0
□ Botnet	0

Risk Score

Risk Score	
□ High	120
□ Medium	71
□ Low	49
□ N/A	25

Date Range

Anytime

COL XFTAS Daily Threat Assessment for February 26, 2019
Created on Feb 27, 2019

COL New Fbot Botnet Developments
Created on Feb 25, 2019

COL Mirai Botnet Activity
Created on Jan 23, 2019

COL ChinaZ - One of Many Chinese Threat Actor Groups
Created on Jan 9, 2019

VUL ABB GATE-E1 and GATE-E2 security bypass (CVE-2018-18995)
Reported on Dec 17, 2018

COL Hajime Botnet Variant
Created on Dec 5, 2018

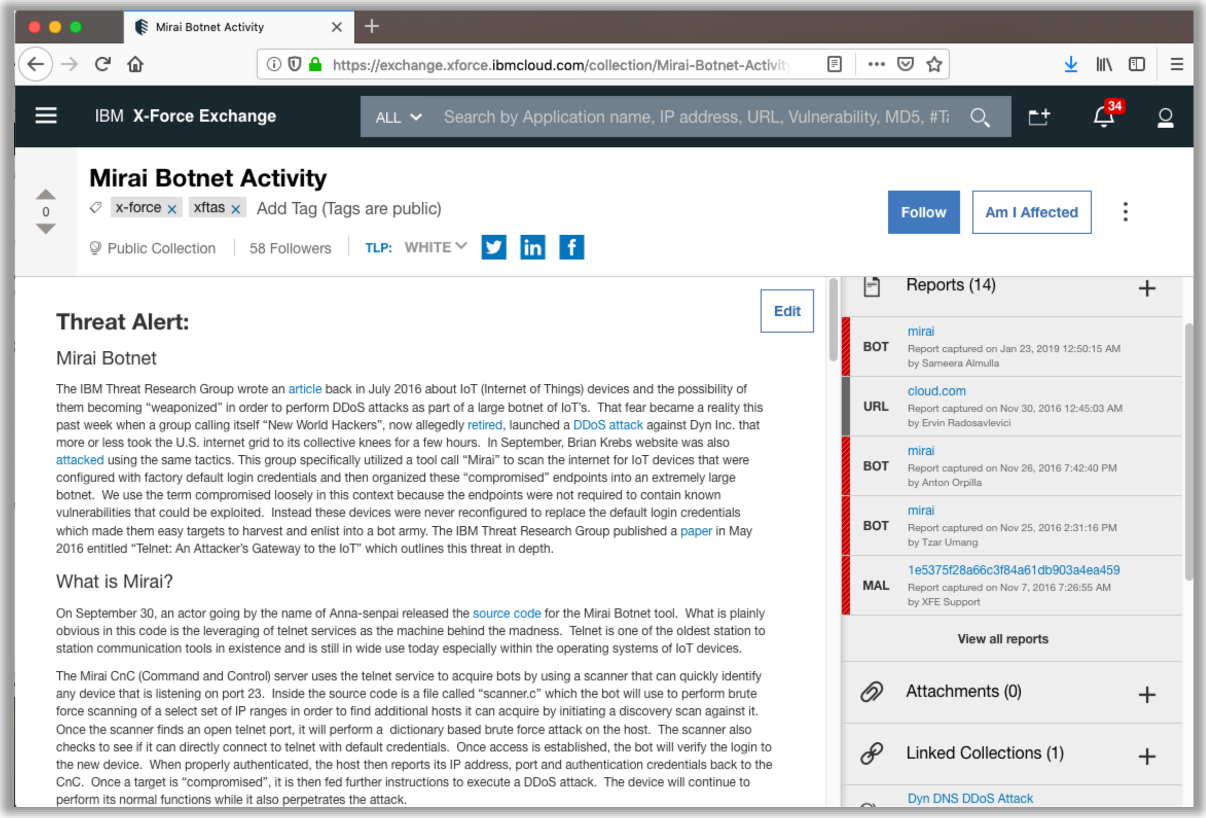
VUL Siglent Technologies SDS 1202X-E Digital Oscilloscope backdoor
Reported on Nov 29, 2018

VUL NPLUG wireless repeater security bypass (CVE-2018-12455)
Reported on Oct 8, 2018

COL Torii Botnet - Definitely Not a Mirai Wannabe
Created on Oct 3, 2018

We can see that Mirai is a botnet that attacks through Telnet and has been active recently.

4. Click into Mirai Botnet Activity. This gives us a more in depth description of the alert and what Mirai is.


Mirai Botnet Activity
https://exchange.xforce.ibmcloud.com/collection/Mirai-Botnet-Activit
IBM X-Force Exchange
ALL
Search by Application name, IP address, URL, Vulnerability, MD5, #Ta
34
Follow
Am I Affected
Edit

Mirai Botnet Activity

0

x-force × xftas × Add Tag (Tags are public)

Public Collection | 58 Followers | TLP: WHITE

Threat Alert:

Mirai Botnet

The IBM Threat Research Group wrote an article back in July 2016 about IoT (Internet of Things) devices and the possibility of them becoming “weaponized” in order to perform DDoS attacks as part of a large botnet of IoT’s. That fear became a reality this past week when a group calling itself “New World Hackers”, now allegedly retired, launched a DDoS attack against Dyn Inc. that more or less took the U.S. internet grid to its collective knees for a few hours. In September, Brian Krebs website was also attacked using the same tactics. This group specifically utilized a tool call “Mirai” to scan the internet for IoT devices that were configured with factory default login credentials and then organized these “compromised” endpoints into an extremely large botnet. We use the term compromised loosely in this context because the endpoints were not required to contain known vulnerabilities that could be exploited. Instead these devices were never reconfigured to replace the default login credentials which made them easy targets to harvest and enlist into a bot army. The IBM Threat Research Group published a paper in May 2016 entitled “Telnet: An Attacker’s Gateway to the IoT” which outlines this threat in depth.

What is Mirai?

On September 30, an actor going by the name of Anna-senpai released the source code for the Mirai Botnet tool. What is plainly obvious in this code is the leveraging of telnet services as the machine behind the madness. Telnet is one of the oldest station to station communication tools in existence and is still in wide use today especially within the operating systems of IoT devices.

The Mirai CnC (Command and Control) server uses the telnet service to acquire bots by using a scanner that can quickly identify any device that is listening on port 23. Inside the source code is a file called “scanner.c” which the bot will use to perform brute force scanning of a select set of IP ranges in order to find additional hosts it can acquire by initiating a discovery scan against it. Once the scanner finds an open telnet port, it will perform a dictionary based brute force attack on the host. The scanner also checks to see if it can directly connect to telnet with default credentials. Once access is established, the bot will verify the login to the new device. When properly authenticated, the host then reports its IP address, port and authentication credentials back to the CnC. Once a target is “compromised”, it is then fed further instructions to execute a DDoS attack. The device will continue to perform its normal functions while it also perpetrates the attack.

Reports (14) +

BOT	mirai Report captured on Jan 23, 2019 12:50:15 AM by Sameera Almulla
URL	cloud.com Report captured on Nov 30, 2016 12:45:03 AM by Ervin Radosavlevici
BOT	mirai Report captured on Nov 26, 2016 7:42:40 PM by Anton Orpilla
BOT	mirai Report captured on Nov 25, 2016 2:31:16 PM by Tzar Umang
MAL	1e5375f28a66c3f84a61db903a4ea459 Report captured on Nov 7, 2016 7:26:55 AM by XFE Support

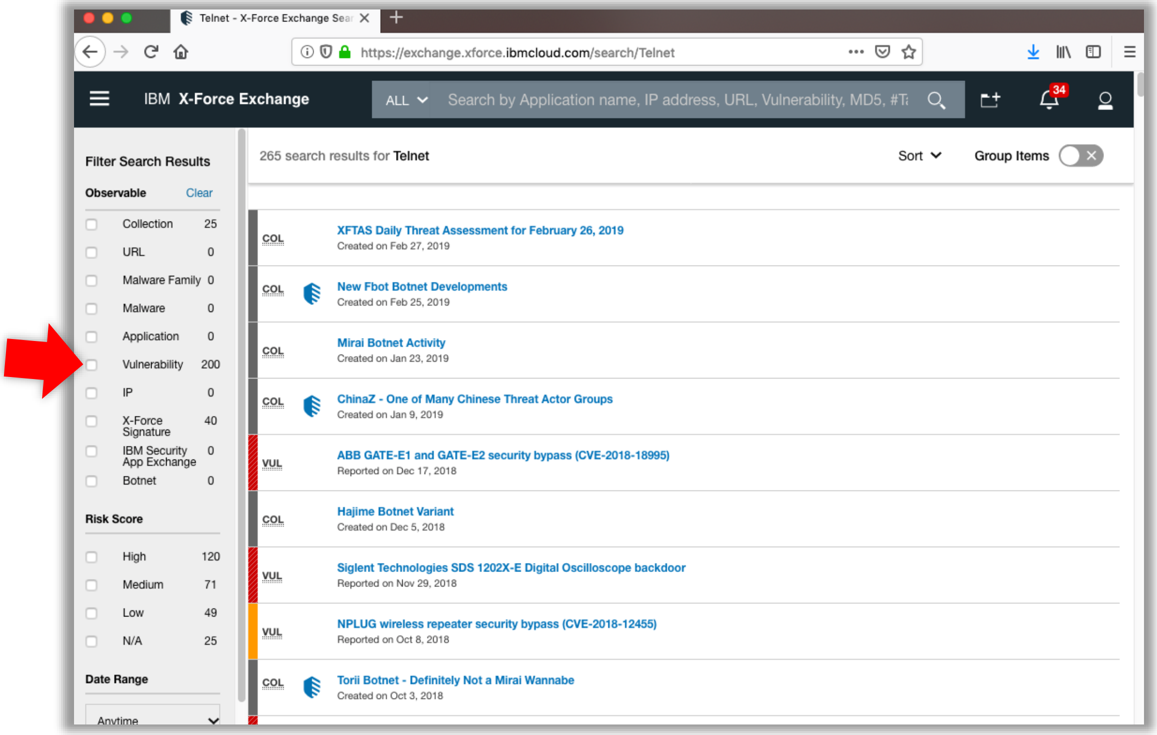
View all reports

Attachments (0) +

Linked Collections (1) +

Dyn DNS DDoS Attack

5. Return back to the Telnet search. This time we are going to take a look at vulnerabilites.



Telnet - X-Force Exchange Sea
https://exchange.xforce.ibmcloud.com/search/Telnet
IBM X-Force Exchange
ALL
Search by Application name, IP address, URL, Vulnerability, MD5, #T
34
Sort
Group Items

265 search results for **Telnet**

Filter Search Results

Observable Clear

□	Collection	25
□	URL	0
□	Malware Family	0
□	Malware	0
□	Application	0
□	Vulnerability	200
□	IP	0
□	X-Force Signature	40
□	IBM Security App Exchange	0
□	Botnet	0

Risk Score

□	High	120
□	Medium	71
□	Low	49
□	N/A	25

Date Range

Anytime

COL XFTAS Daily Threat Assessment for February 26, 2019
Created on Feb 27, 2019

COL New Fbot Botnet Developments
Created on Feb 25, 2019

COL Mirai Botnet Activity
Created on Jan 23, 2019

COL ChinaZ - One of Many Chinese Threat Actor Groups
Created on Jan 9, 2019

VUL ABB GATE-E1 and GATE-E2 security bypass (CVE-2018-18995)
Reported on Dec 17, 2018

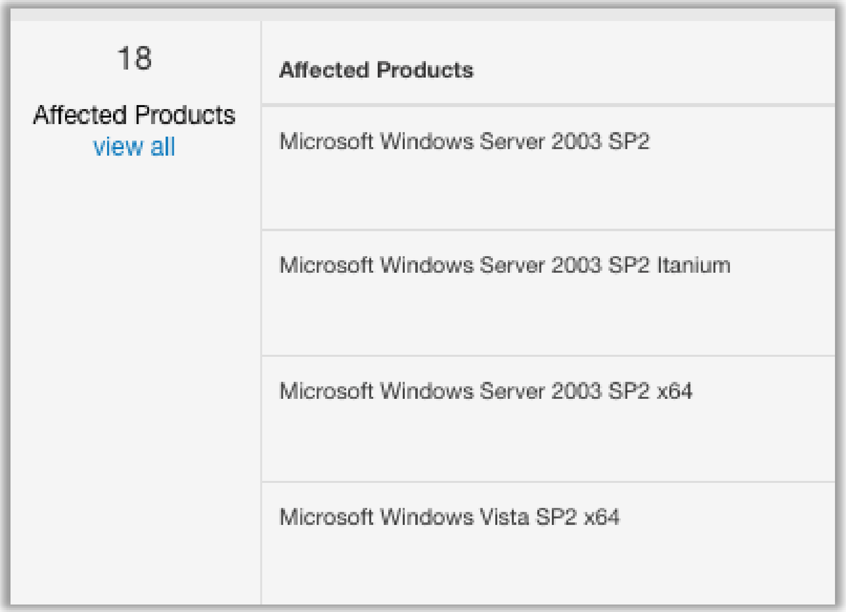
COL Hajime Botnet Variant
Created on Dec 5, 2018

VUL Siglent Technologies SDS 1202X-E Digital Oscilloscope backdoor
Reported on Nov 29, 2018

VUL NPLUG wireless repeater security bypass (CVE-2018-12455)
Reported on Oct 8, 2018

COL Torii Botnet - Definitely Not a Mirai Wannabe
Created on Oct 3, 2018

6. The vulnerabilites are reports detailing what systems are in the most danger from this type of attack.
7. Click into any vulnerability and scroll down to the "Affected Products"



18

Affected Products
view all

Affected Products
Microsoft Windows Server 2003 SP2
Microsoft Windows Server 2003 SP2 Itanium
Microsoft Windows Server 2003 SP2 x64
Microsoft Windows Vista SP2 x64

X-Force Exchange keeps track of the products that are vulnerable to a type of attack.

With 24/7 monitoring, collections, and reports on vulnerabilities; X-Force Exchange is an extremely useful tool for any security expert.

The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. This information is based on current IBM product plans and strategy, which are subject to change by IBM without notice. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way.