Applied Exploits & Hacking - Final Project

SS[ghost]

The University

Abstract

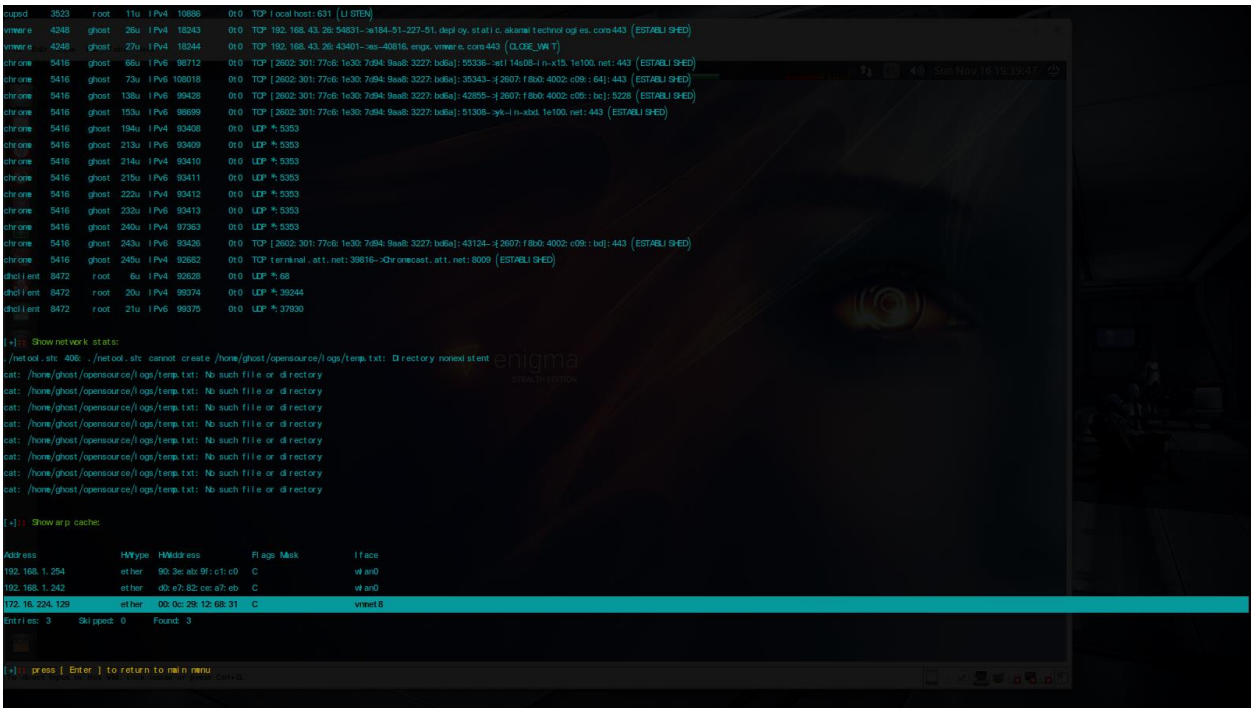
This project starts off running Nmap to find the host address and available ports. From there, the test precedes to use multiple tactics to penetrate the target VM, Ubuntu 14.04, from ARP spoofing to running exploits with Metasploit on numerous ports of the target machine. From trying DoS and ping-of-death attacks to failing to penetrate the apache2 web server. After seeing the tight security of the VM, I installed PIA VPN and MHN.

Keywords: Nmap, host, address, port, target VM, ARP spoofing, exploit, Metasploit, DoS, ping-of-death, attack, Apache2, VPN, MHN.

Applied Exploits & Hacking - Final Project

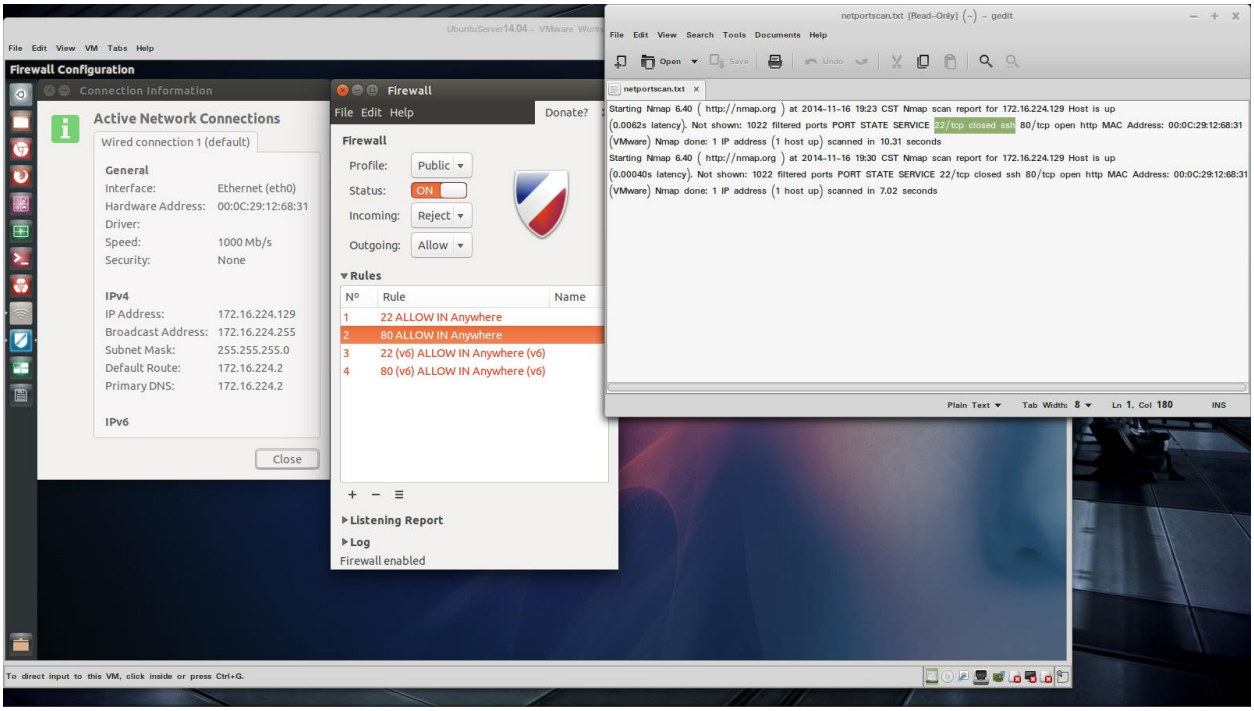
Nmap

The first tool used that utilizes Nmap was Net Tools, as known as Netool.sh, which is a MiTM penetration testing tool with Nmap, Driftnet, SSLstrip, Ettercap, and more. Upon running a scan of all local hosts, the target server, Ubuntu 14.04, was listed with IP address 172.16.224.129.



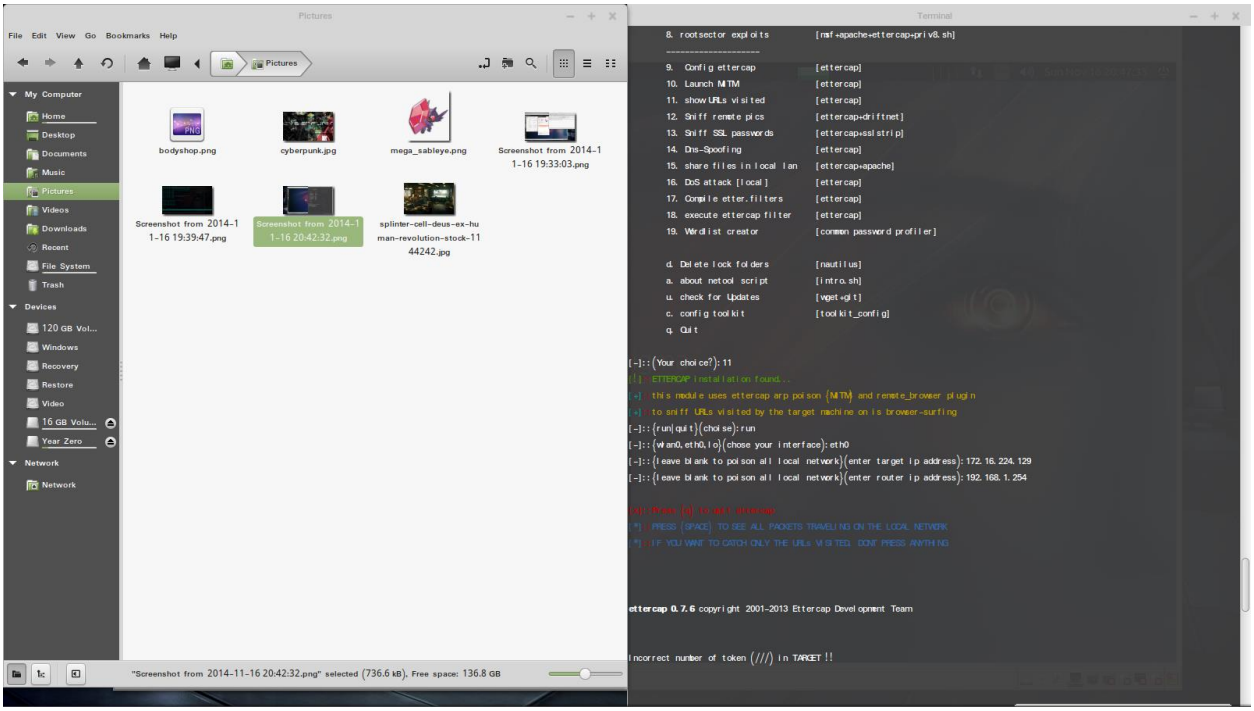
Then I used my own Nmap script from Cloaks&&Daggers to run two ICMP echo pings, one TCP SYN port scan, and one TCP ACK port scan. The first three scans came back with 1,022 of the first 1,024 ports scanned as filtered, that port 22 for SSH was closed, and that port HTTP was open. The TCP ACK scan also returned with 1,022 filtered ports but that the other two were unfiltered. I saw on the target machine that UFW (Uncomplicated FireWall) didn't just have rules for port 80 remaining open to any connection but port 22 as well. Either the Samhain IDS blocked port 22 connection or the port scans are faulty.

NOTE: Screenshot doesn't show the TCP-SYN or -ACK scans.

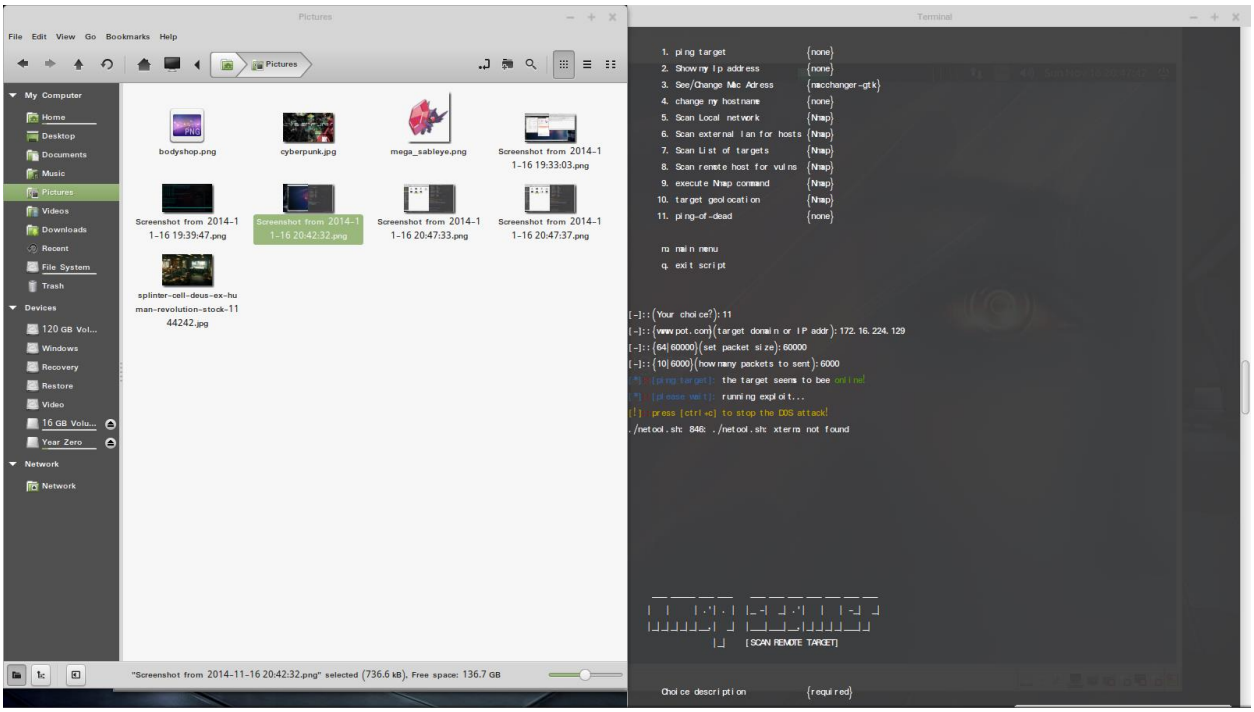


Net Tools

Before closing out Net Tools, I decided to make use of its functionalities to use ping-of-death, DoS, and ARP poisoning. Viewing remote pics or visited URLs of the target with Driftnet and Ettercap both failed with invalid tokens and Ettercap's GUI and CLI refused to run after starting both as root.

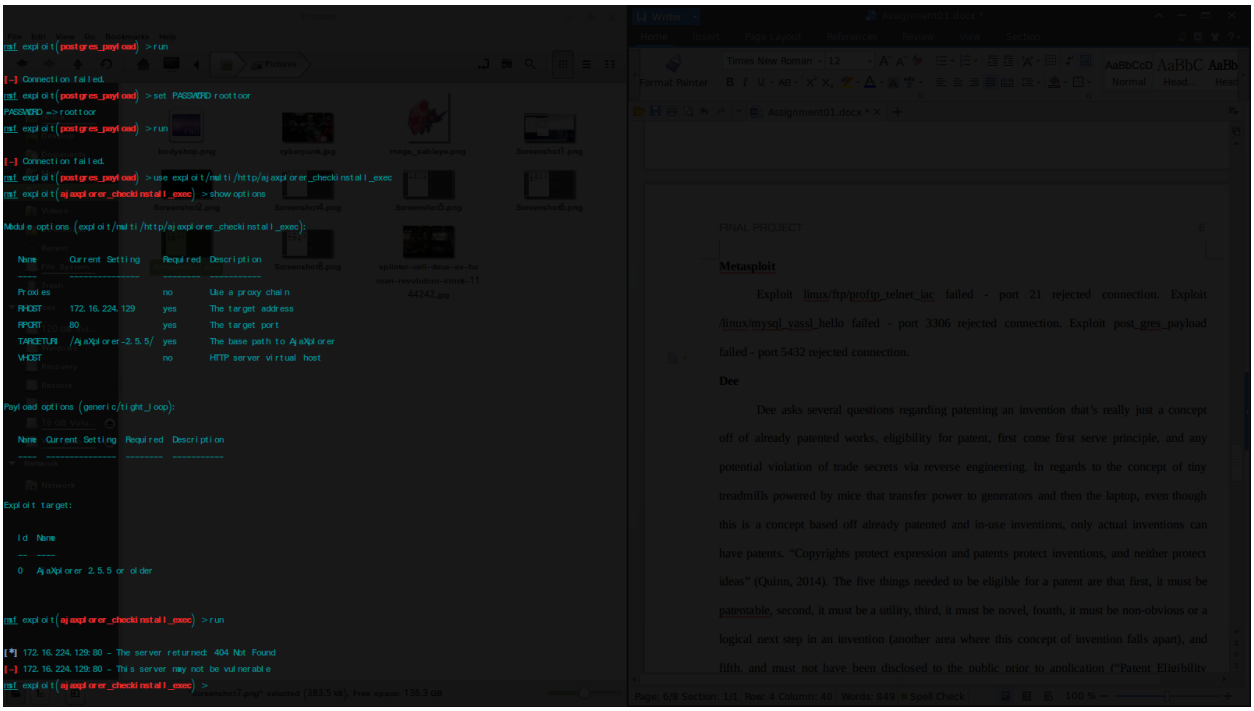


Ping-of-death, DoS, and running ARP poisoning with Ettercap through Net Tools all failed with syntax errors from the coder ending its use. However, the script did find Apache2 running since 5/5, even though all attempts to connect from attack machine were blocked despite UFW.

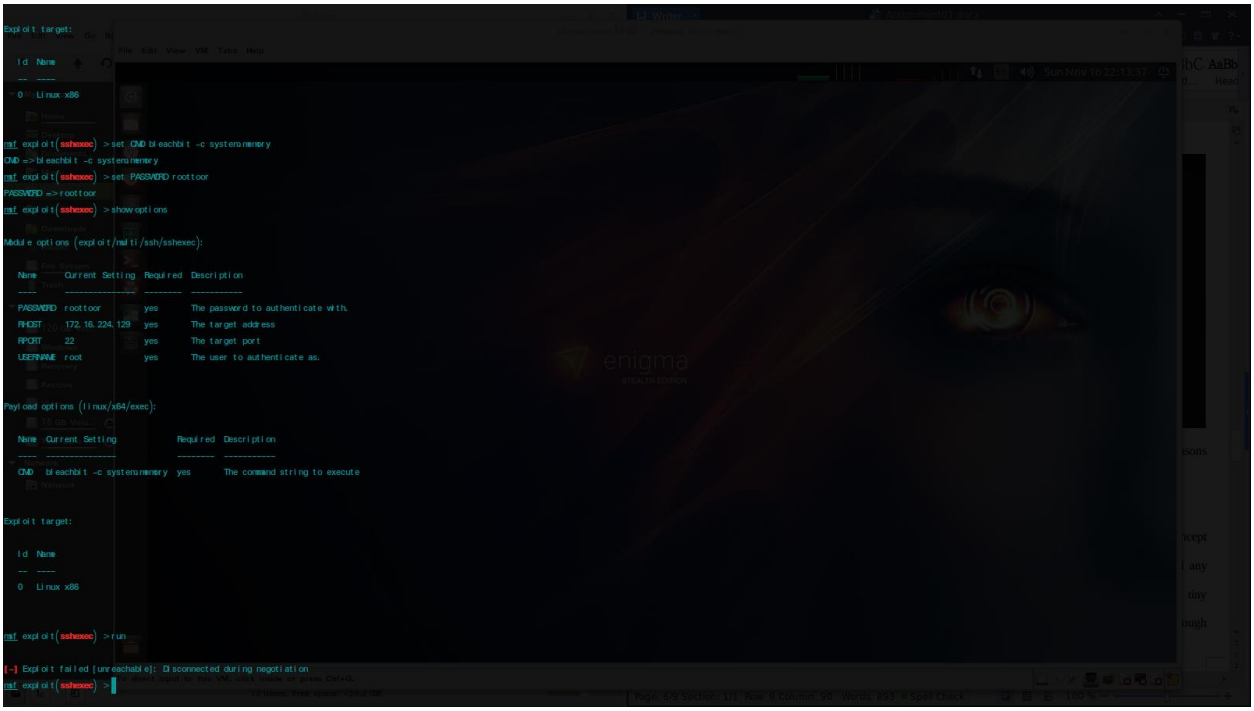


Metasploit

Exploit linux/ftp/proftp_telnet_iac failed - port 21 rejected connection. Exploit /linux/mysql_yassl_hello failed - port 3306 rejected connection. Exploit linux/postgres/postgres_payload failed - port 5432 rejected connection. Exploit multi/ajaxplorer_check_install failed - port 80 rejected connection. Results: “This server may not be vulnerable.” Exploit multi/http/op5_welcome failed - port 80 rejected connection.

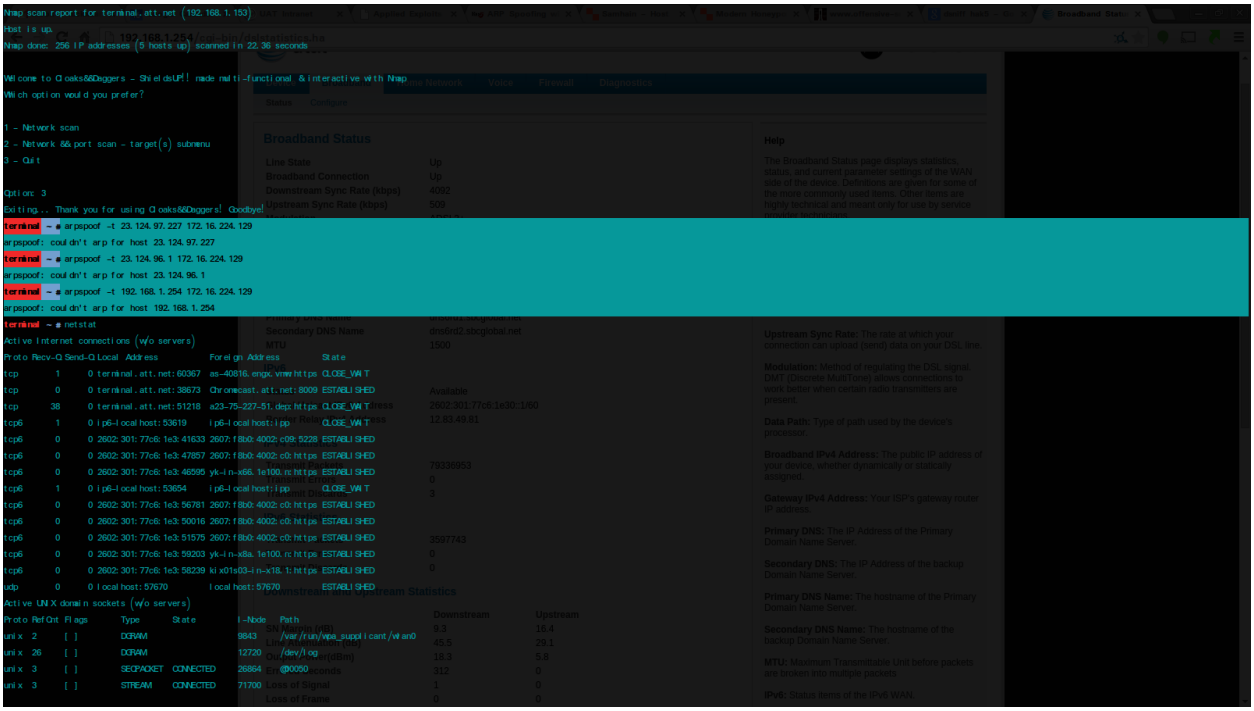


Exploit multi/misc/wireshark_lwres_getaddrbyname_loop bufferoverflow failed - reasons unknown. Target machine shows consistent network spikes of being pinged with no results. Exploit multi/ssh/sshexec with payload linux/x64/exec failed - port 22 refused connection. Even with password set and CMD “bleachbit -c system.memory” that caused a VM buffer overflow that even froze the host machine that was to attack. UFW rules aren’t working as listed. Samhain IDS has shown no logs so far. That means UFW is blocking the connections despite rules set.



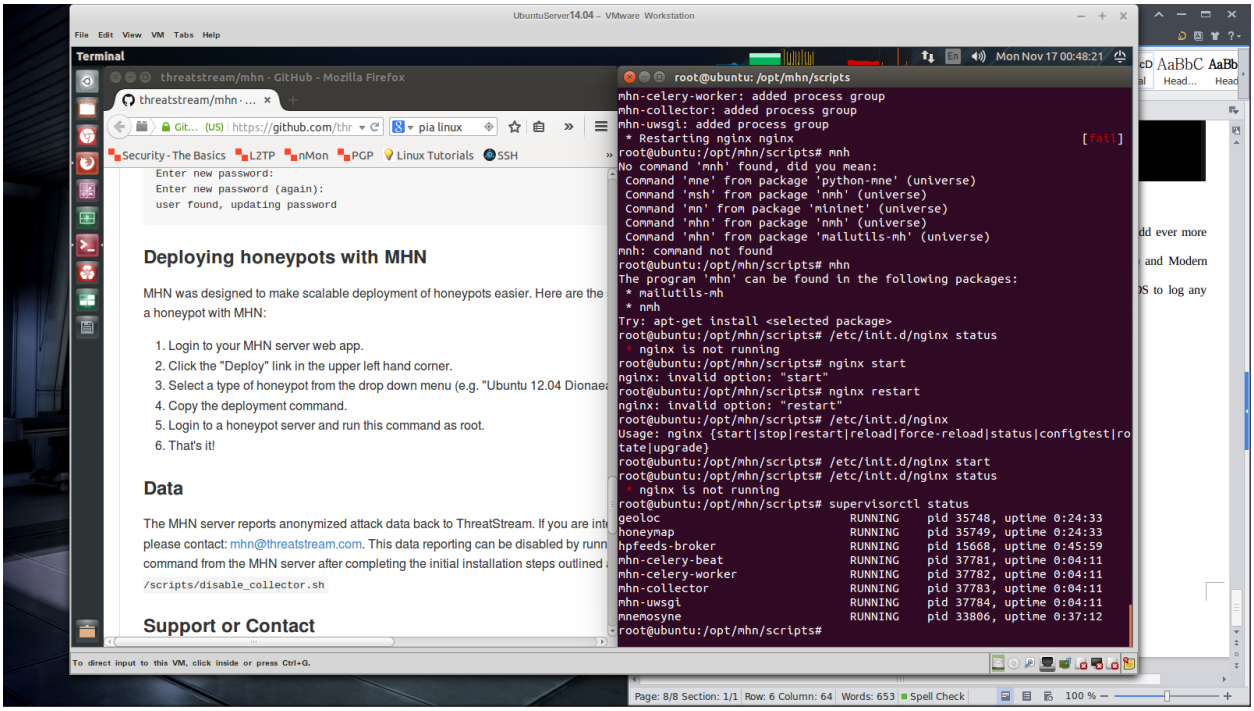
DSniff

Driftnet's DSniff wasn't able to function with ARP spoofing correctly for a MiTM as even the network these penetration tests are being run is not configured to run like a local network but as a class A network with static IP addresses and DNSs. Inconsequentially, I just managed to cause a ping-of-death to said network by trying to ping the router IP address to see if the IP was live, but I did so in an infinite loop of 60,000 byte packets.



Modern Honeypot Network

After the VM failed to be penetrated numerous times, I thought why not add ever more security? I installed Private Internet Access (PIA) VPN (virtual private network) and Modern Honeypot Network (MHN) I configured to work in conjunction with Samhain IDS to log any penetration attempts on any of the running honeypot instances. I've got another Ubuntu 14.04 Server instance running, Ubuntu 12.04, Debian 7.5, and Linux Mint 16.


UbuntuServer14.04 - VMware Workstation
File Edit View VM Tabs Help
Terminal
Mon Nov 17 00:48:21
threatstream/mhn · GitHub - Mozilla Firefox
threatstream/mhn · ...
https://github.com/thr
pia linux
Security - The Basics
L2TP
nMon
PGP
Linux Tutorials
SSH
Enter new password:
Enter new password (again):
user found, updating password
Deploying honeypots with MHN
MHN was designed to make scalable deployment of honeypots easier. Here are the
a honeypot with MHN:
1. Login to your MHN server web app.
2. Click the "Deploy" link in the upper left hand corner.
3. Select a type of honeypot from the drop down menu (e.g. "Ubuntu 12.04 Dionae
4. Copy the deployment command.
5. Login to a honeypot server and run this command as root.
6. That's it!
Data
The MHN server reports anonymized attack data back to ThreatStream. If you are int
please contact: mhn@threatstream.com. This data reporting can be disabled by runn
command from the MHN server after completing the initial installation steps outlined
/scripts/disable_collector.sh
Support or Contact
root@ubuntu: /opt/mhn/scripts
mhn-celery-worker: added process group
mhn-collector: added process group
mhn-uwsgi: added process group
* Restarting nginx nginx [fail]
root@ubuntu:/opt/mhn/scripts# mnh
No command 'mnh' found, did you mean:
Command 'mne' from package 'python-mne' (universe)
Command 'msh' from package 'nmh' (universe)
Command 'mn' from package 'mininet' (universe)
Command 'mhn' from package 'nmh' (universe)
Command 'mhn' from package 'mailutils-mh' (universe)
mnh: command not found
root@ubuntu:/opt/mhn/scripts# mhn
The program 'mhn' can be found in the following packages:
* mailutils-mh
* nmh
Try: apt-get install <selected package>
root@ubuntu:/opt/mhn/scripts# /etc/init.d/nginx status
* nginx is not running
root@ubuntu:/opt/mhn/scripts# nginx start
nginx: invalid option: "start"
root@ubuntu:/opt/mhn/scripts# nginx restart
nginx: invalid option: "restart"
root@ubuntu:/opt/mhn/scripts# /etc/init.d/nginx
Usage: nginx {start|stop|restart|reload|force-reload|status|configtest|ro
tate|upgrade}
root@ubuntu:/opt/mhn/scripts# /etc/init.d/nginx start
root@ubuntu:/opt/mhn/scripts# /etc/init.d/nginx status
* nginx is not running
root@ubuntu:/opt/mhn/scripts# supervisorctl status
geoloc RUNNING pid 35748, uptime 0:24:33
honeymap RUNNING pid 35749, uptime 0:24:33
hpfeeds-broker RUNNING pid 15668, uptime 0:45:59
mhn-celery-beat RUNNING pid 37781, uptime 0:04:11
mhn-celery-worker RUNNING pid 37782, uptime 0:04:11
mhn-collector RUNNING pid 37783, uptime 0:04:11
mhn-uwsgi RUNNING pid 37784, uptime 0:04:11
mnemosyne RUNNING pid 33806, uptime 0:37:12
root@ubuntu:/opt/mhn/scripts#
To direct input to this VM, click inside or press Ctrl+G.
Page: 8/8 Section: 1/1 Row: 6 Column: 64 Words: 653 Spell Check
100 %