HARDENING LAB

Dennis Keritsis

I. Metasploitable Server

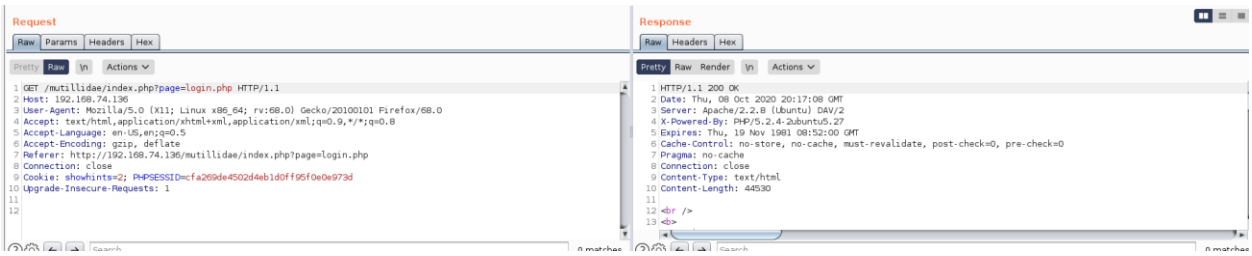
I.(A) Scan

Runs	High[1]	Med	Low
1	24	34	2
2	18	31	2
3	15	33	2
4	14	32	2

I had four (4) runs. With each run, I attempted save the state and remedy specific vulnerabilities. The first run was the first system test. I attempted to patch the Ubuntu Sever with sudo apt-get updates and sudo apt-get upgrade. This will be discussed below in Vulnerabilities.

Additionally, I went through the report and try to knock out some low hanging fruit. There were some issues I couldn't resolve. This is discussed below.

Throughout my probing I used Burpsuite (also discussed below) to verify and understand the vulnerabilities, *see* Banner Grabbing Fig. Also, after my fixes I verified the fix with Burpsuite which is also discussed below.



I. (B) Vulnerabilities

- OS End of Life Detection
- PostSQLgres password
- Root password

[1] My Exploits are probably higher than others because I added some backdoors to the server with Metasploit. I didn't remedy this.

- Root User Password for MYSQL
- VNC Password
- **Phpinfo.php**
- **Banner** displaying during HTTP Responses along with Response enumerating system information
- HTTP dangerous methods such as PUT and DELETE
- HTTP methods such as TRACE/TRACK

I. (C) Fixes

I. (C) (i) <u>OS End of Life and Patching</u>

Before trying to do anything in detail, we need to patch and/or try to update the OS to the best of our abilities. I failed miserably to update the OS. After I didn't patch things, upon restart the system was totally inert. We have to be super careful when updating as not to break things.

This is why we have the "aptitude" system when updating and going from one LTS to another LTS. It is suppose to safely upgrade due to all the packages and inter-dependencies being related. Still with "aptitude," I couldn't get the OS to upgrade to 10.04 from 8.04.[2]

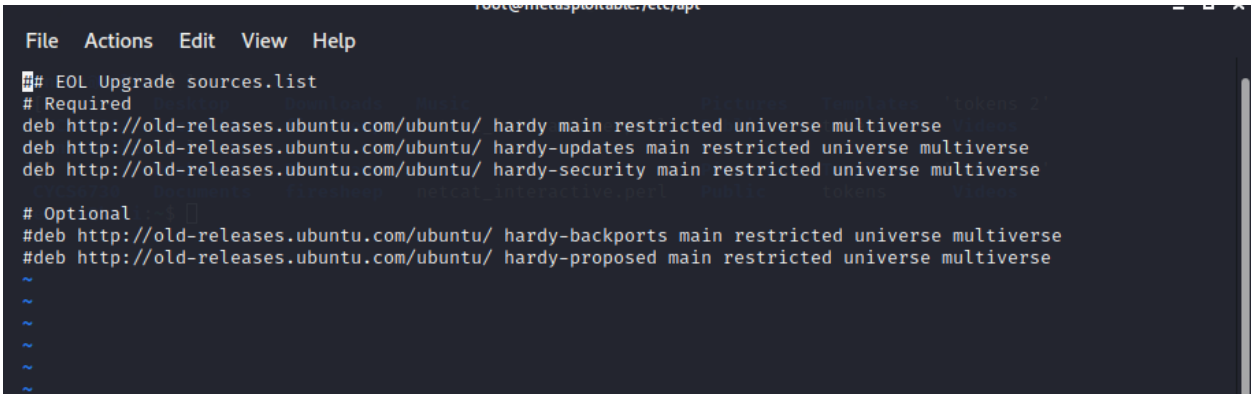
On a brighter side, I was able to use sudo apt-get upgrade && sudo apt-get update. Also, I found sudo get dist upgrade to be useful. I will note that this makes the system upon restart act very wanky and possibly even defund. So, I wouldn't recommend a "dist" upgrade.

After patching I found: (i) "high" warnings went from 24 down to 18, (ii) "medium" warnings went down to 31 from 31, and (ii) "low" warning stayed the same.

I will note that I needed to update the .sources file.

Specifically, I needed to source from "old-releases" as seen below.

[2] We can't jump to the lastest version. We have to hop from one LTS to the next LTS till we get to Ubuntu 20+.



And we are not suppose to source from "archive" according to the ubuntu.com.[3] I also noted that "aptitude" does not seem to be of much help.

```
## EOL Upgrade sources.list
# Required
deb http://archive.ubuntu.com/ubuntu/ hardy main restricted universe multiverse
deb http://archive.ubuntu.com/ubuntu/ hardy-updates main restricted universe multiverse
deb http://security.ubuntu.com/ubuntu/ hardy-security main restricted universe multiverse

# Optional
#deb http://archive.ubuntu.com/ubuntu/ hardy-backports main restricted universe multiverse
#deb http://archive.ubuntu.com/ubuntu/ hardy-proposed main restricted universe multiverse
```

You can make use of -backports, -proposed repositories if you want. For more information about repositories see Repositories/Ubuntu.

1. Update the package list and upgrade all the installed packages

```
sudo aptitude update && sudo aptitude safe-upgrade
```

1. Perform the release upgrade.

```
sudo do-release-upgrade
```

I. (C) (ii) Low Hanging Fruit

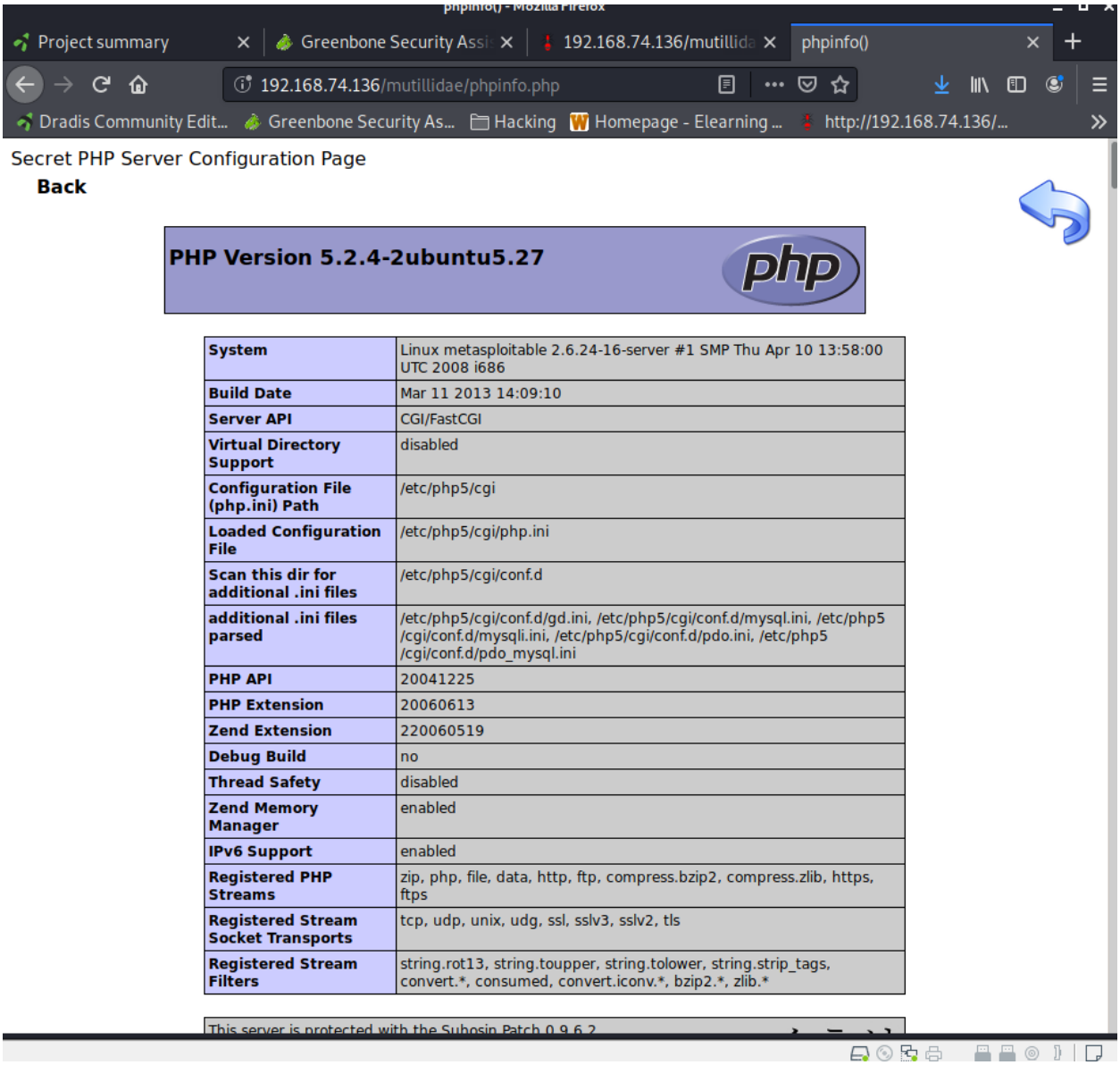
- PostSQLgres password
- Root password
- Root User Password for MYSQL
- VNC Password

These items are low hanging fruit. Just update the passwords. I had to do some research on how to fix some of these items. But I won't bother with the details.

I. (C) (iii) PHP

[3] *See* https://help.ubuntu.com/community/EOLUpgrades/Hardy

This is a joke. Hopefully no one in the real world would find this or even leave this enabled on the server. But I guess it can happen. From my research, this is typically used in development to help the web development get information about the server running in real time. It should be disabled or totally removed upon deployment. This was an easy fix.

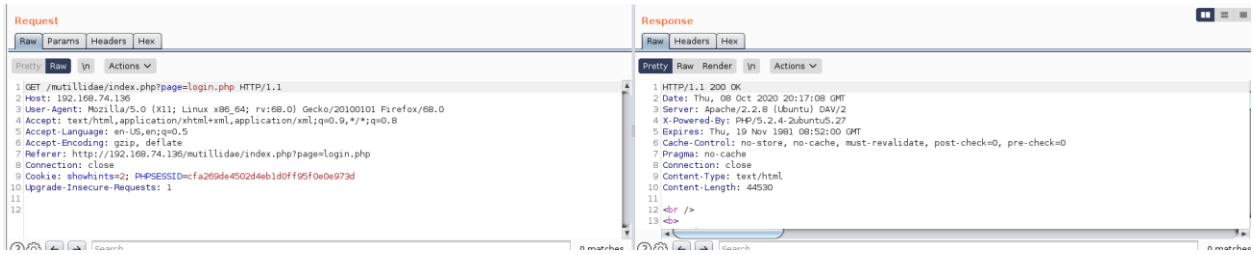


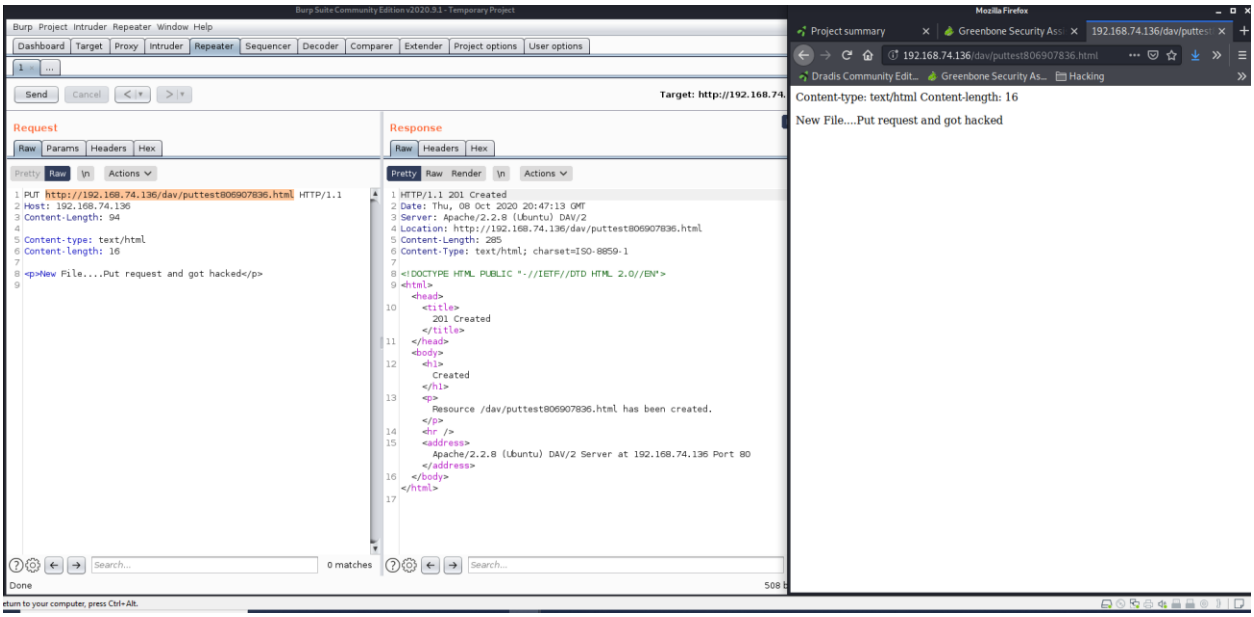
System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Mar 11 2013 14:09:10
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.*

I. (C) (iv) <u>Banner HTTP</u>

The first figure below is a GET HTTP request. From the 200 Response, we can see a plurality of information as our disposal. Actually, when I found this, I was able to a Metasploit exploit based on the Apache Version and add a backdoor (which is still on my server). This is part of the Recon and/or Foot phase of Blackbox testing.

The second figure uses a PUT method. We see first that PUT is allow. (This is bad and discussed below.) Also, we see a 201 Create Response with a ton of banner information.





This last figure is just me being a nerd and boasting about my leet hackorzing on Team. Here, I added a backdoor with the banner grabbed information based on the old version of Apache 2.2.8 on port 80. I was able to place a “Reverse Shell” on the server (which is actually still running).

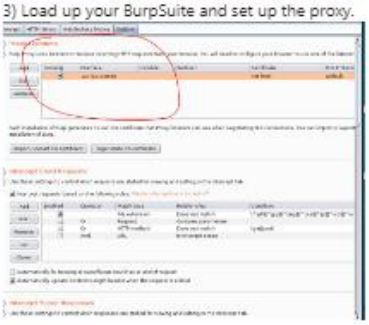
Dennis George Keritsis 10/5 10:26 PM Edited

—How to Hack your Metasploit Apache 2.2.8 Server on port 80—

1) Have your metasploit server running.

2) Ensure your metasploit server Apache is running.

3) Load up your BurpSuite and set up the proxy.



4) Attempt to login into multillidae webpage and while doing so, "intercept" the http POST message.

5) Get the POST message and with right click sent it to the "repeater"

6) Check the Response...OOO Yummy Apache 2.2.8 is running:

7) Open up metasploit and exploit with the following youtube video....https://www.youtube.com/watch?v=FGUydmaEiU0Should be straight forward. You set up a "reverse shell" which will get around firewalls.

8) Now you can see I own the machine:

New conversation

With the banner grabbing fix, it would make it more difficult for a hacker to do Recon and Exploit accordingly since they wouldn't know what specific version of Apache I would have running.

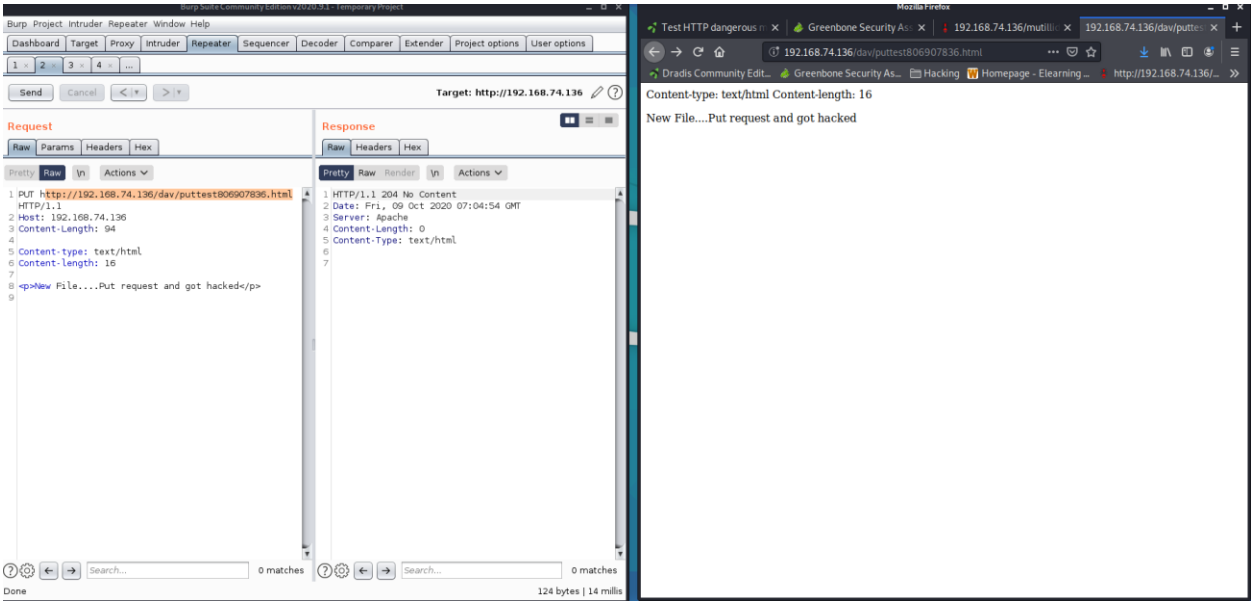
The fix was simple (but it took me a while to learn about .conf files in APACHE). I changed to the ServerSignature Off (disable signature) and ServerTokens Prod (Disables the Banner)

```
#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
# If you are behind a reverse proxy, you might want to change %h into %{X-Forwarded-For}i
#
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

#
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of:  Full | OS | Minor | Minimal | Major | Prod
# where Full conveys the most information, and Prod the least.
#
ServerTokens Prod

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of:  On | Off | EMail
#
ServerSignature Off



#
# Customizable error responses come in three flavors:
# 1) plain text 2) local redirects 3) external redirects
#
# Some examples:
#ErrorDocument 500 "The server made a boo boo."
```

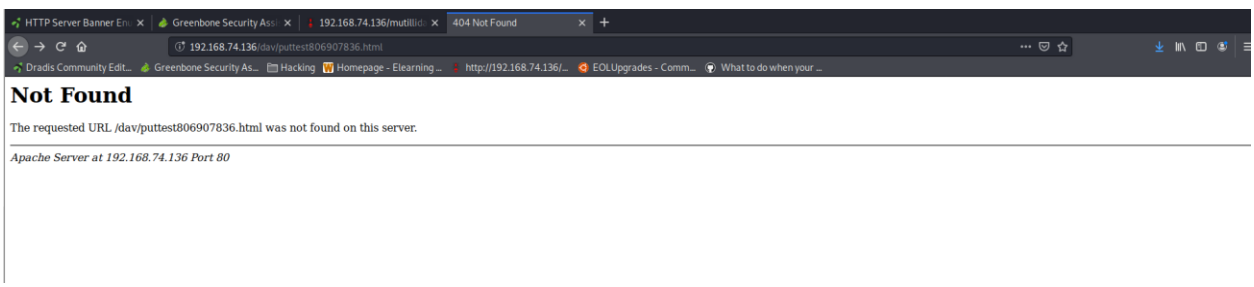
I. (C) (v) <u>Dangerous Methods —Not Fixed But Tried</u>

PUT and DELETE are dangerous methods because we do not want people adding pages and removing pages as they see fit. PUT for example could be used to create a XSS attack or CSRF attack. These method should be disabled, and if enable, should be allow on a very, very limited basis.

I used BurpSuite with the PUT method to add “New File…Put request and got hacked.”



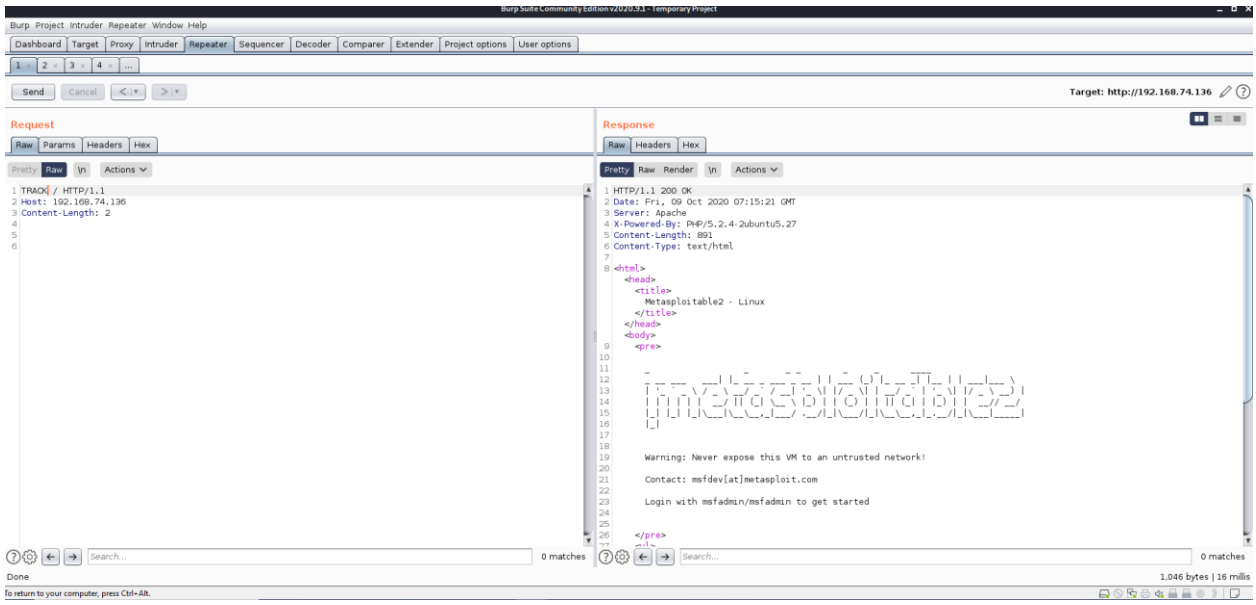
I was also able to use the “DELETE” method. And I cycled with PUT and DELETE to engage in some experimentation. I also found that VAS add a PUT test file and I DELETED what was PUT by VAS.

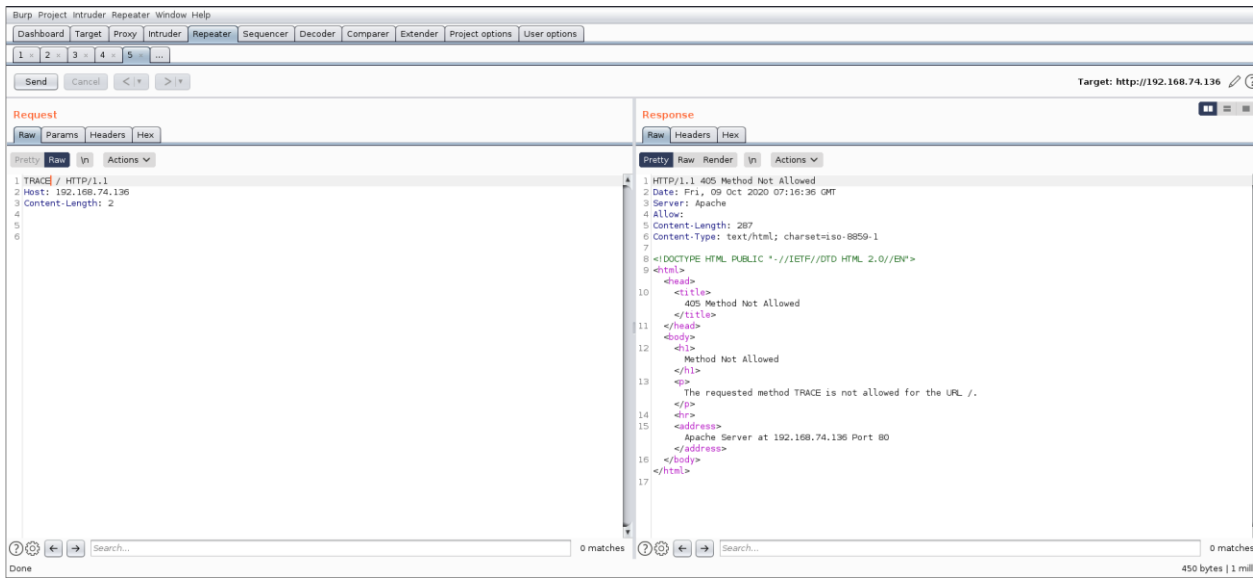


However, I could NOT fix this. I did my best with Google. I couldn’t figure out how to fix this because there are other .conf files. More work needs to be done.

I. (C) (vi) <u>TRACE/TRACK/OPTIONS — Not Fixed but Tried</u>

I worked again with Burpsuite and played around with TRACE and TRACK methods.

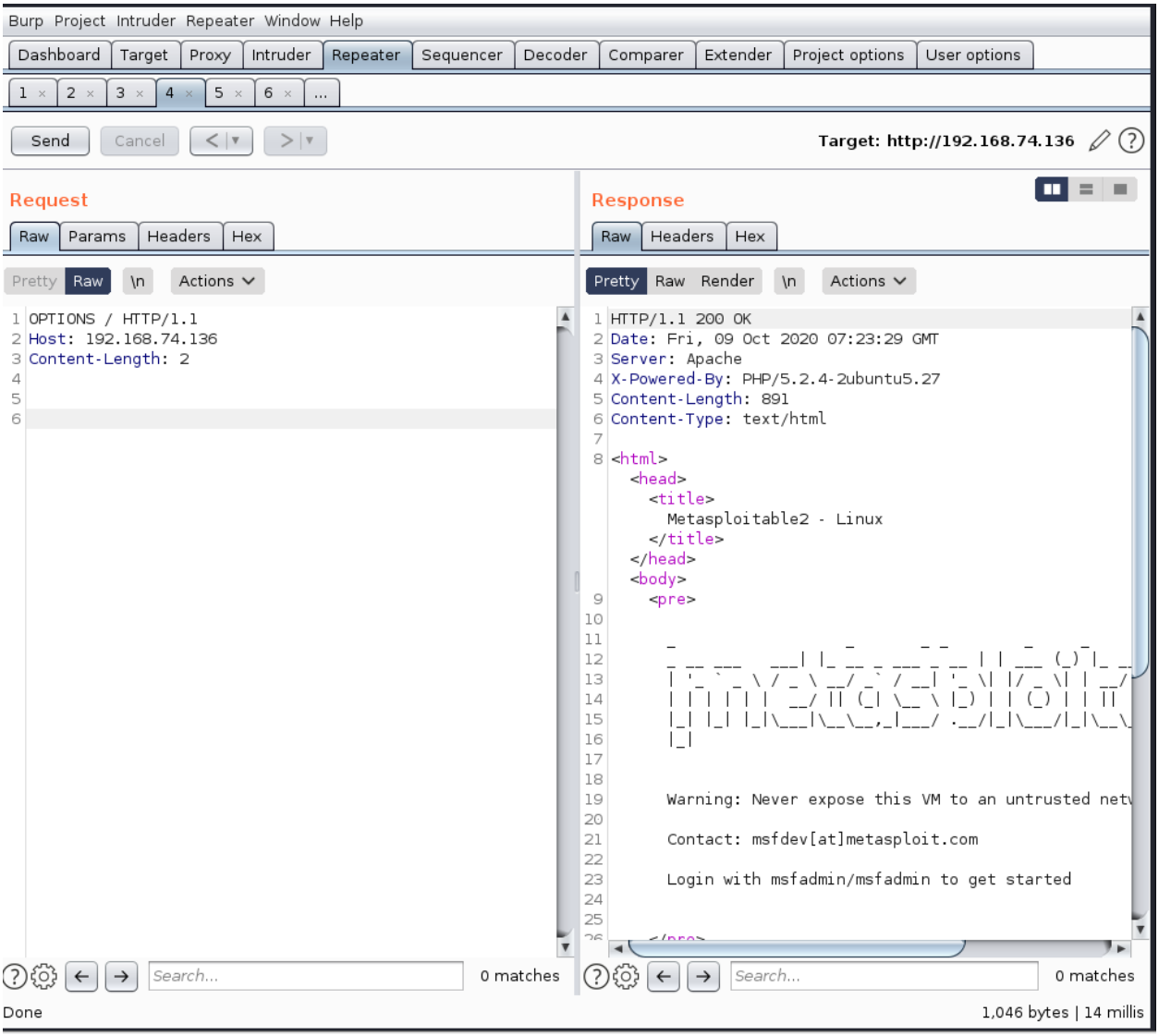




As can be seen, the TRACK method is enabled given the “200 OK” response whereas the TRACE method is disabled given the “405 Method Not Allowed” response.

I couldn’t figure out how disable the TRACK method but I tried.

I also used the OPTIONS method. This gave a HTTP 200 response. I couldn’t figure out how to disable this.

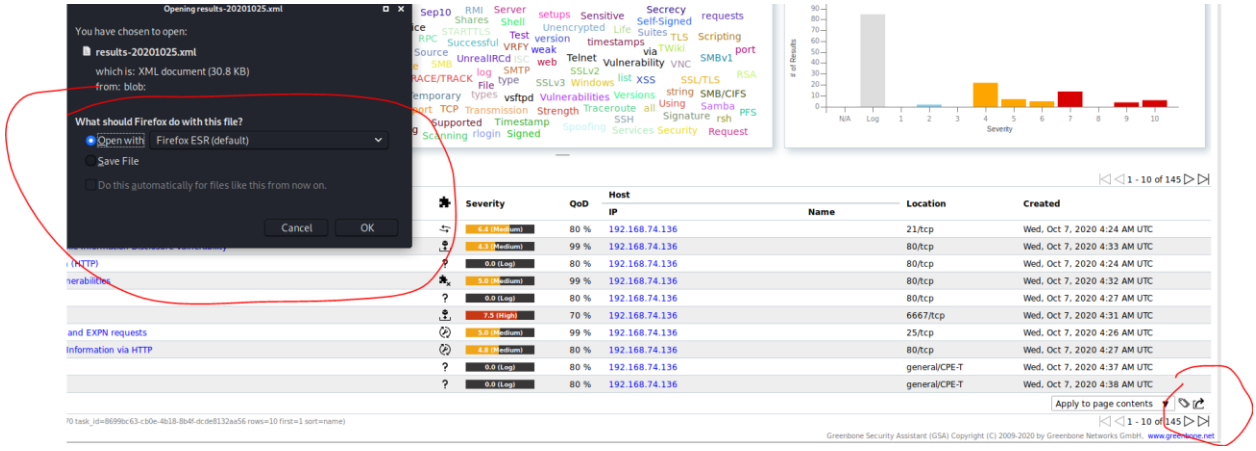


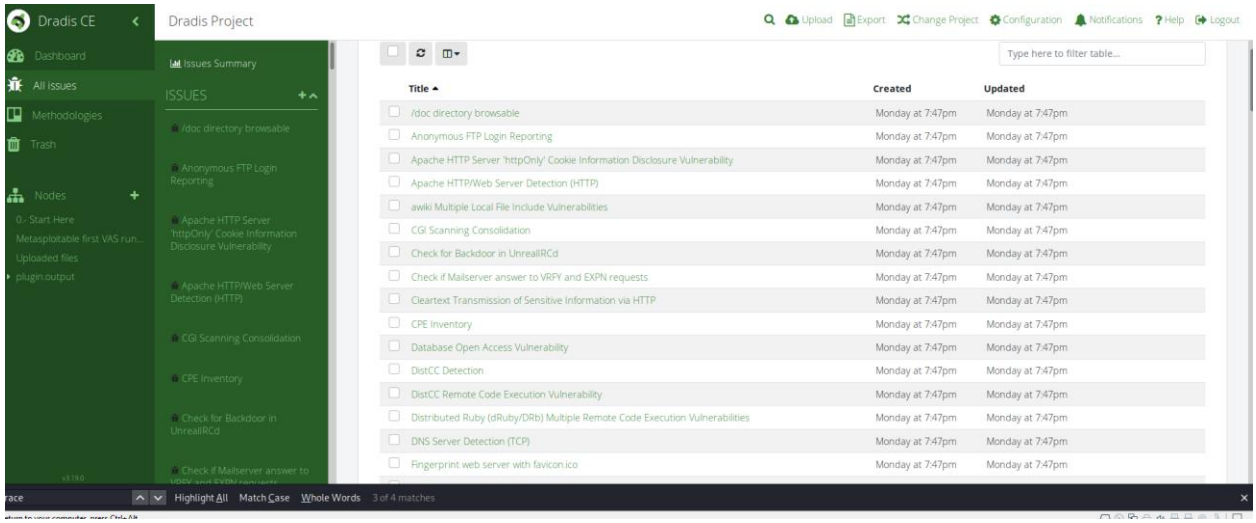
I. (D) Dradis

I. (D) (i) Adding

First figure is exporting using XML.

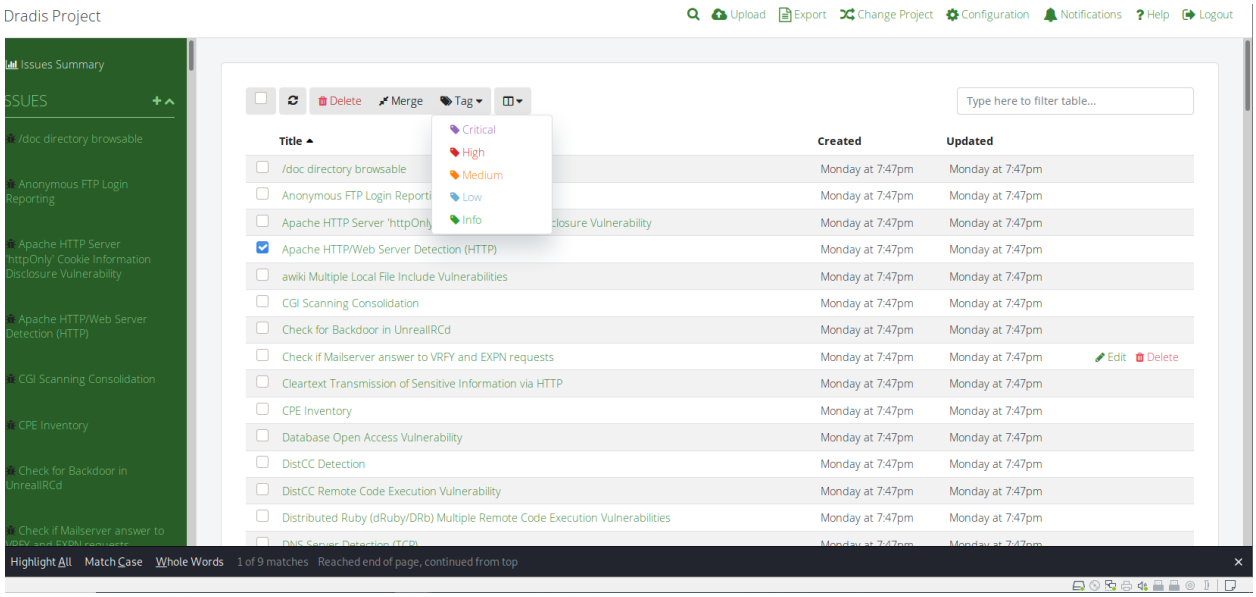
Second figure is shows that exported vulnerabilities.

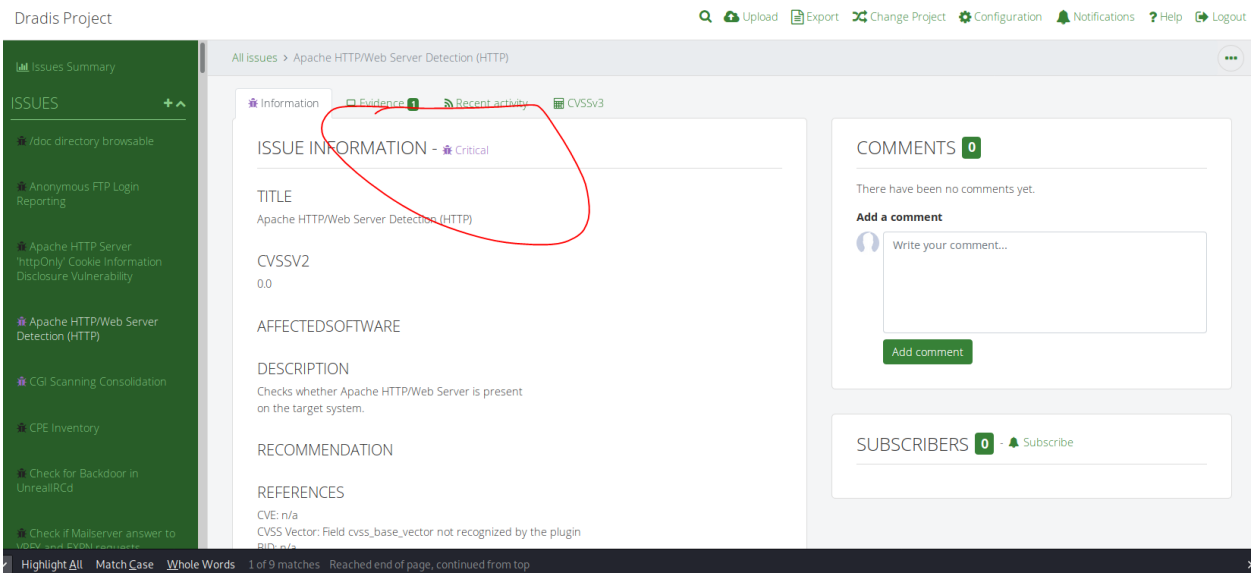




I. (D) (ii) Flagging

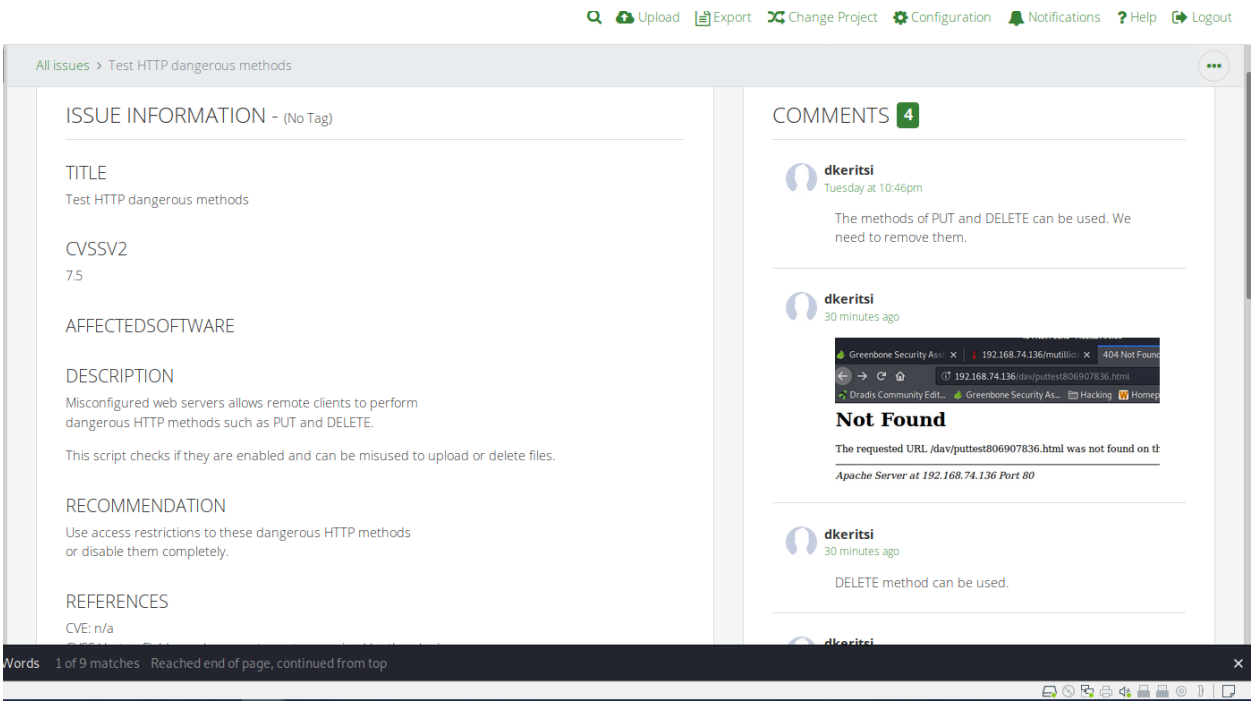
Figures below are show the Tagging method for classifying the issues.





I. (D) (iii) Evidence and Commenting

Pictures below show comments and evidence with the HTTP methods.



All issues > Test HTTP dangerous methods

RECOMMENDATION

Use access restrictions to these dangerous HTTP methods
or disable them completely.

REFERENCES

CVE: n/a
CVSS Vector: Field cvss_base_vector not recognized by the plugin
BID: n/a
Other: n/a

RAWDESCRIPTION

(note that some of the information below can change from instance to instance of this problem)
n/a

PLUGIN

open_vas

PLUGIN_ID

1.3.6.1.4.1.25623.1.0.10498

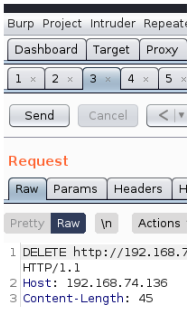
Author: Open vas upload plugin

dkeritsi
30 minutes ago

DELETE method can be used.

dkeritsi
27 minutes ago

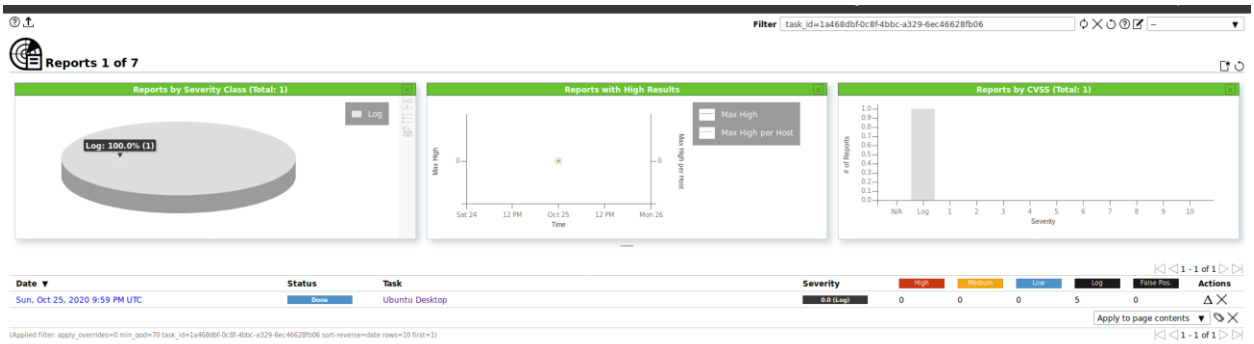
HTTP DELETE method used in BurpSuite



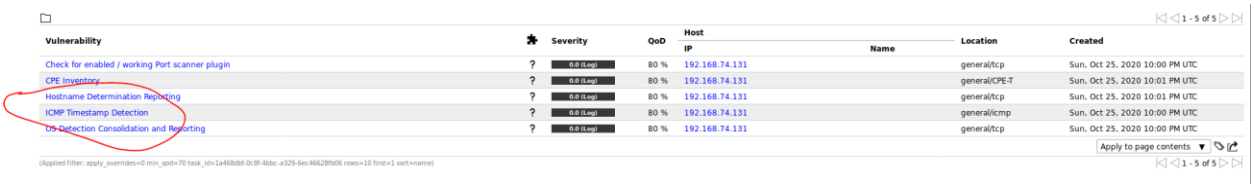
ords 1 of 9 matches Reached end of page, continued from top

II. Ubuntu Server

This is really no surprise. The Server is pretty hardened and it is the most up to date OS. This means that when sourced it will source only from the latest packages.



I did take a note that ICMP is enabled.



I verified this with a ping test.

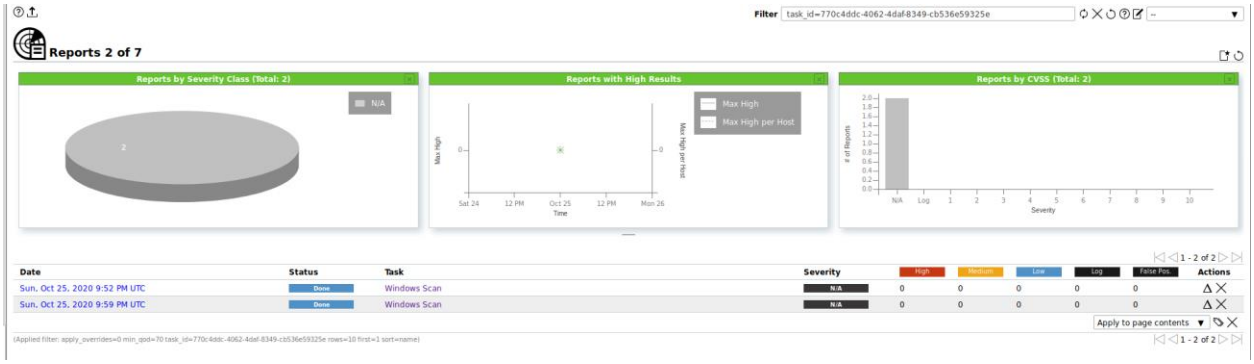
dennis@kali: ~

File Actions Edit View Help

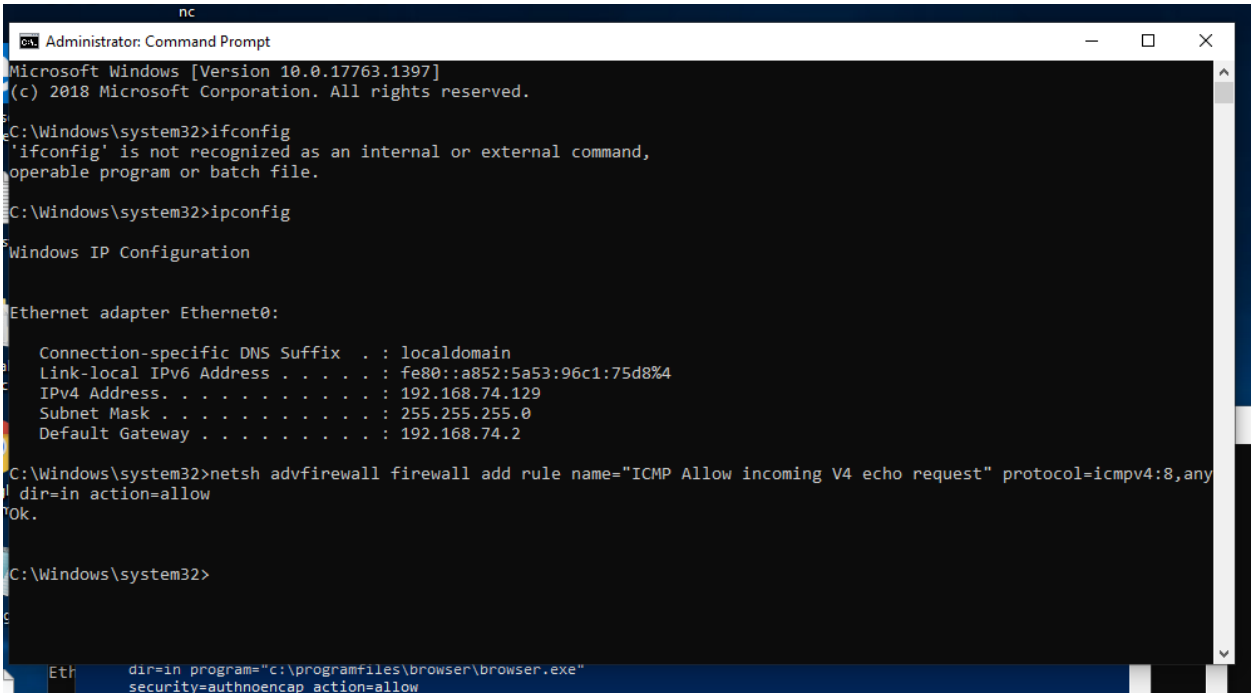
```
--- 192.168.74.131 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 0.220/0.845/1.681/0.614 ms
dennis@kali:~$ ipconfig
bash: ipconfig: command not found
dennis@kali:~$ ip -a
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { link | address | addrlabel | route | rule | neigh | ntable |
                   tunnel | tuntap | maddress | mroute | mrule | monitor | xfrm |
                   netns | l2tp | fou | macsec | tcp_metrics | token | netconf | ila |
                   vrf | sr | nexthop | mptcp }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                   -h[uman-readable] | -iec | -j[son] | -p[retty] |
                   -f[amily] { inet | inet6 | mpls | bridge | link } |
                   -4 | -6 | -I | -D | -M | -B | -0 |
                   -l[oops] { maximum-addr-flush-attempts } | -br[ief] |
                   -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename] |
                   -rc[vbuf] [size] | -n[etns] name | -N[umeric] | -a[ll] |
                   -c[olor]}
dennis@kali:~$ ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:15:30:f1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.74.130/24 brd 192.168.74.255 scope global dynamic noprefixroute eth0
       valid_lft 1367sec preferred_lft 1367sec
    inet6 fe80::20c:29ff:fe15:30f1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
dennis@kali:~$ ping 192.168.74.129
PING 192.168.74.129 (192.168.74.129) 56(84) bytes of data.
^C
--- 192.168.74.129 ping statistics ---
249 packets transmitted, 0 received, 100% packet loss, time 253949ms

dennis@kali:~$ ping 192.168.74.131
PING 192.168.74.131 (192.168.74.131) 56(84) bytes of data.
64 bytes from 192.168.74.131: icmp_seq=1 ttl=64 time=0.231 ms
64 bytes from 192.168.74.131: icmp_seq=2 ttl=64 time=0.188 ms
64 bytes from 192.168.74.131: icmp_seq=3 ttl=64 time=0.198 ms
64 bytes from 192.168.74.131: icmp_seq=4 ttl=64 time=0.268 ms
64 bytes from 192.168.74.131: icmp_seq=5 ttl=64 time=0.531 ms
64 bytes from 192.168.74.131: icmp_seq=6 ttl=64 time=0.259 ms
64 bytes from 192.168.74.131: icmp_seq=7 ttl=64 time=0.220 ms
```

III. Windows Server

Windows appears to be blocked off completely. I scanned two times.



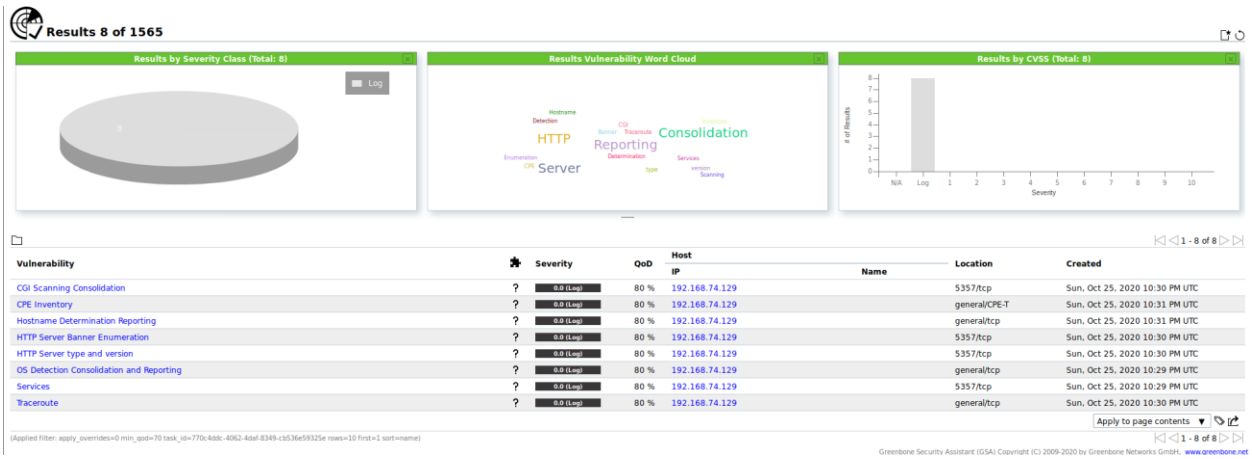
Allow ICMP from firewall incoming.



Ping now works.

```
dennis@kali:~$ ping 192.168.74.129
PING 192.168.74.129 (192.168.74.129) 56(84) bytes of data.
^C
--- 192.168.74.129 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8190ms

dennis@kali:~$ ping 192.168.74.129
PING 192.168.74.129 (192.168.74.129) 56(84) bytes of data.
64 bytes from 192.168.74.129: icmp_seq=1 ttl=128 time=0.430 ms
64 bytes from 192.168.74.129: icmp_seq=2 ttl=128 time=1.10 ms
64 bytes from 192.168.74.129: icmp_seq=3 ttl=128 time=1.03 ms
^C
--- 192.168.74.129 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.430/0.852/1.101/0.300 ms
dennis@kali:~$
```

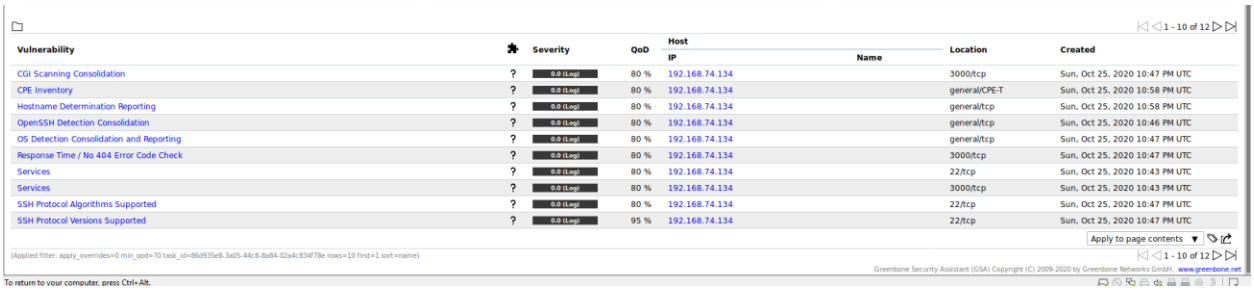
Let’s rescan and see what is different.



Ok. We got something. Looks like a hacker might be able to get a small foot hold if part of the firewall is disabled.

III. Dradis Server

Looks like our Dradis Server is pretty solid.



1 - 10 of 12

Vulnerability		Severity	QoD	Host IP	Host Name	Location	Created
CGI Scanning Consolidation	?	0.0 (Log)	80 %	192.168.74.134		3000/tcp	Sun, Oct 25, 2020 10:47 PM UTC
CPE Inventory	?	0.0 (Log)	80 %	192.168.74.134		general/CPE-T	Sun, Oct 25, 2020 10:58 PM UTC
Hostname Determination Reporting	?	0.0 (Log)	80 %	192.168.74.134		general/tcp	Sun, Oct 25, 2020 10:58 PM UTC
OpenSSH Detection Consolidation	?	0.0 (Log)	80 %	192.168.74.134		general/tcp	Sun, Oct 25, 2020 10:46 PM UTC
OS Detection Consolidation and Reporting	?	0.0 (Log)	80 %	192.168.74.134		general/tcp	Sun, Oct 25, 2020 10:47 PM UTC
Response Time / No 404 Error Code Check	?	0.0 (Log)	80 %	192.168.74.134		3000/tcp	Sun, Oct 25, 2020 10:47 PM UTC
Services	?	0.0 (Log)	80 %	192.168.74.134		22/tcp	Sun, Oct 25, 2020 10:43 PM UTC
Services	?	0.0 (Log)	80 %	192.168.74.134		3000/tcp	Sun, Oct 25, 2020 10:43 PM UTC
SSH Protocol Algorithms Supported	?	0.0 (Log)	80 %	192.168.74.134		22/tcp	Sun, Oct 25, 2020 10:47 PM UTC
SSH Protocol Versions Supported	?	0.0 (Log)	95 %	192.168.74.134		22/tcp	Sun, Oct 25, 2020 10:47 PM UTC

Apply to page contents

(Applied filter: apply_overrides=0 min_qod=70 task_id=86d935e8-3a05-44c8-8a84-02a4c834f78e rows=10 first=1 sort=name)

1 - 10 of 12

Greenbone Security Assistant (GSA) Copyright (C) 2009-2020 by Greenbone Networks GmbH, www.greenbone.net

To return to your computer, press Ctrl+Alt.

IV. Bind9 DNS Server

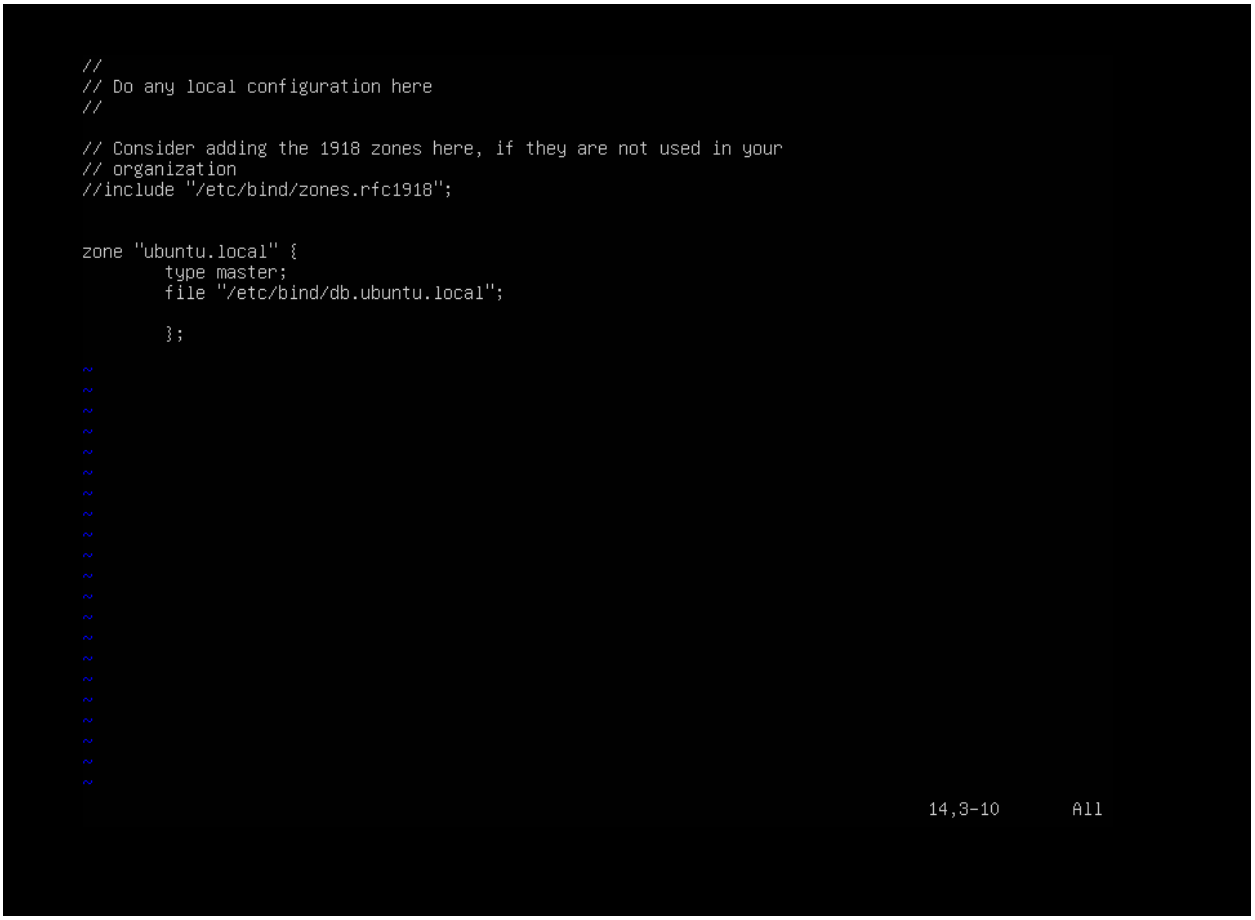
Set static IP.

```
# ifupdown has been replaced by netplan(5) on this system.  See
# /etc/netplan for current configuration.
# To re-enable ifupdown on this system, you can run:
#    sudo apt install ifupdown
#
#Primary Network Interface
auto eth0
iface eth0 inet static
address 192.168.74.128
netmask 255.0.0.0
dns-nameservers 127.0.0.1
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/network/interfaces" [readonly] 11L, 320C                    9,22          All
```

Set forwarder. Use google's.

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

         forwarders {
                8.8.8.8;
                8.8.4.4;
         };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };

        //hide version from client for security reasons
        version "not currently available";

        //optional - BIND default behavior is recursion
        recursion yes;

        //provision recursion to trusted clients only
        allow-recursion
        {
        192.168.74.130;
"named.conf.options" 46L, 1244C                                          14,3-17       Top
```

Configure the host. And set zones.



```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";


zone "ubuntu.local" {
        type master;
        file "/etc/bind/db.ubuntu.local";

        };

~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
                                                                  14,3-10       All
```

```
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    86400
@       IN      SOA     ubuntu.local. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                          86400 )       ; Negative Cache TTL
;
        IN      A       192.168.74.128
@       IN      NS      localhost.
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"db.ubuntu.local" 15L, 377C                                          14,20-38      All
```

I think loading is good.

```
dkeritsi@bind9_dns:/etc/bind$ ls
bind.keys  db.255    db.root          named.conf.default-zones  rndc.key
db.0       db.empty  db.ubuntu.local  named.conf.local          zones.rfc1918
db.127     db.local  named.conf       named.conf.options
dkeritsi@bind9_dns:/etc/bind$ tail /var/log/syslog
Oct 25 23:28:06 bind9_dns named[4858]: reloading configuration succeeded
Oct 25 23:28:06 bind9_dns named[4858]: reloading zones succeeded
Oct 25 23:28:06 bind9_dns named[4858]: zone ubuntu.local/IN: loaded serial 1
Oct 25 23:28:06 bind9_dns named[4858]: zone ubuntu.local/IN: sending notifies (serial 1)
Oct 25 23:28:06 bind9_dns named[4858]: all zones loaded
Oct 25 23:28:06 bind9_dns named[4858]: running
Oct 25 23:28:06 bind9_dns rndc[5439]: server reload successful
Oct 25 23:28:06 bind9_dns systemd[1]: Reloaded BIND Domain Name Server.
Oct 25 23:28:06 bind9_dns named[4858]: managed-keys-zone: Key 20326 for zone . acceptance timer comp
lete: key now trusted
Oct 25 23:28:06 bind9_dns named[4858]: resolver priming query complete
dkeritsi@bind9_dns:/etc/bind$ _
```

Using nslookup

```
dkeritsi@blind9ubuntu2004:~$ ls
dkeritsi@blind9ubuntu2004:~$ ls
dkeritsi@blind9ubuntu2004:~$ pwd
/home/dkeritsi
dkeritsi@blind9ubuntu2004:~$ ls
dkeritsi@blind9ubuntu2004:~$ sudo -u
sudo: option requires an argument -- 'u'
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout]
            [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout]
            [-u user] file ...
dkeritsi@blind9ubuntu2004:~$ sudo -i
[sudo] password for dkeritsi:
Sorry, try again.
[sudo] password for dkeritsi:
root@blind9ubuntu2004:~# cd /etc/bind
root@blind9ubuntu2004:/etc/bind# ls
bind.keys  db.192    db.local         named.conf.default-zones  rndc.key
db.0       db.255    db.ubuntu.local  named.conf.local          zones.rfc1918
db.127     db.empty  named.conf       named.conf.options
root@blind9ubuntu2004:/etc/bind# nslookup
> 192.168.74.137
137.74.168.192.in-addr.arpa     name = blind9ubuntu2004.
137.74.168.192.in-addr.arpa     name = blind9ubuntu2004.local.

Authoritative answers can be found from:
> ubuntu.local
Server:         127.0.0.53
Address:        127.0.0.53#53

** server can't find ubuntu.local: SERVFAIL
> _
```

Hmm. There appears to be a small problem with the “ubuntu.local” when I nslook up this.

I got my Bind9 Server running through.

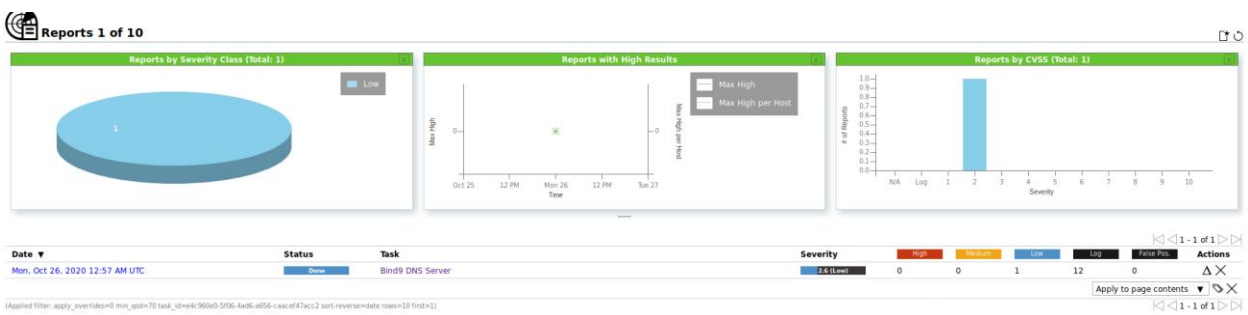
```
Setting up initramfs-tools (0.136ubuntu6.3) ...
update-initramfs: deferring update (trigger activated)
Setting up cryptsetup-initramfs (2:2.2.2-3ubuntu2.3) ...
update-initramfs: deferring update (trigger activated)
update-initramfs: deferring update (trigger activated)
Processing triggers for libc-bin (2.31-0ubuntu9.1) ...
Processing triggers for systemd (245.4-4ubuntu3.2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for plymouth-theme-ubuntu-text (0.9.4git20200323-0ubuntu6) ...
update-initramfs: deferring update (trigger activated)
Processing triggers for dbus (1.12.16-2ubuntu2.1) ...
Processing triggers for install-info (6.7.0.dfsg.2-5) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for initramfs-tools (0.136ubuntu6.3) ...
update-initramfs: Generating /boot/initrd.img-5.4.0-52-generic
root@blind9ubuntu2004:/etc/bind# systemctl status named
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2020-10-26 00:17:52 UTC; 8min ago
       Docs: man:named(8)
   Main PID: 798 (named)
      Tasks: 8 (limit: 4587)
     Memory: 23.2M
     CGroup: /system.slice/named.service
             └─798 /usr/sbin/named -f -u bind

Oct 26 00:17:52 blind9ubuntu2004 named[798]: network unreachable resolving './NS/IN': 2001:500:2d::>
Oct 26 00:17:52 blind9ubuntu2004 named[798]: network unreachable resolving './NS/IN': 2001:500:2::c>
Oct 26 00:17:52 blind9ubuntu2004 named[798]: network unreachable resolving './NS/IN': 2001:500:a8::>
Oct 26 00:17:52 blind9ubuntu2004 named[798]: network unreachable resolving './NS/IN': 2001:500:2f::>
Oct 26 00:17:52 blind9ubuntu2004 named[798]: network unreachable resolving './NS/IN': 2001:7fe::53#>
Oct 26 00:17:52 blind9ubuntu2004 named[798]: zone ubuntu.local/IN: sending notifies (serial 2)
Oct 26 00:17:52 blind9ubuntu2004 named[798]: network unreachable resolving './NS/IN': 2001:dc3::35#>
Oct 26 00:17:52 blind9ubuntu2004 named[798]: network unreachable resolving './NS/IN': 2001:500:1::5>
Oct 26 00:17:52 blind9ubuntu2004 named[798]: managed-keys-zone: Key 20326 for zone . is now trusted>
Oct 26 00:17:52 blind9ubuntu2004 named[798]: resolver priming query complete
lines 1-20/20 (END)
```

Hmm from what I understand we are suppose to be listening on port 53. But this should be UDP and not TCP.

```
"named.conf" 11L, 463C written
root@blind9ubuntu2004:/etc/bind# netstat -a -n -p tcp | grep -i ":53"
tcp        0      0 192.168.74.137:53       0.0.0.0:*               LISTEN      798/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      798/named
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      767/systemd-resolve
tcp6       0      0 fe80::20c:29ff:fe6c::53 :::*                    LISTEN      798/named
tcp6       0      0 ::1:53                  :::*                    LISTEN      798/named
udp        0      0 192.168.74.137:53       0.0.0.0:*                           798/named
udp        0      0 192.168.74.137:53       0.0.0.0:*                           798/named
udp        0      0 127.0.0.1:53            0.0.0.0:*                           798/named
udp        0      0 127.0.0.1:53            0.0.0.0:*                           798/named
udp        0      0 127.0.0.53:53           0.0.0.0:*                           767/systemd-resolve
udp6       0      0 ::1:53                  :::*                                798/named
udp6       0      0 ::1:53                  :::*                                798/named
udp6       0      0 fe80::20c:29ff:fe6c::53 :::*                                798/named
udp6       0      0 fe80::20c:29ff:fe6c::53 :::*                                798/named
root@blind9ubuntu2004:/etc/bind# nslookup
> 192.168.74.137
137.74.168.192.in-addr.arpa     name = blind9ubuntu2004.
137.74.168.192.in-addr.arpa     name = blind9ubuntu2004.local.

Authoritative answers can be found from:
> ubuntu.local
Server:         127.0.0.53
Address:        127.0.0.53#53

** server can't find ubuntu.local: SERVFAIL
> root@blind9ubuntu2004:/etc/bind# clearclear: command not found
root@blind9ubuntu2004:/etc/bind# ^C
root@blind9ubuntu2004:/etc/bind# _
To return to your computer, press Ctrl+Alt.
```

O well. I guess I do not get full credit. Not going to pretend I am elite. 😊

Time to Scan with VAS.



We have one low and 12 log in our report. **I would also image that I would have some low warning with UDP if I got my bind9 server to work. And we would leave those in place because we want port 53 to be listening**. As InfoSec, we would leave those alone since we want our DNS server to be listening. But as I said, not going to pretend I am elite and I got my DNS server to work. 😊

1 - 10 of 13

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
TCP timestamps	2.6 (Low)	80 %	192.168.74.137		general/tcp	Mon, Oct 26, 2020 12:58 AM UTC
ISC BIND 'named' Detection (Remote)	0.0 (Log)	80 %	192.168.74.137		53/tcp	Mon, Oct 26, 2020 12:59 AM UTC
ICMP Timestamp Detection	0.0 (Log)	80 %	192.168.74.137		general/icmp	Mon, Oct 26, 2020 1:00 AM UTC
CPE Inventory	0.0 (Log)	80 %	192.168.74.137		general/CPE-T	Mon, Oct 26, 2020 1:10 AM UTC
Hostname Determination Reporting	0.0 (Log)	80 %	192.168.74.137		general/tcp	Mon, Oct 26, 2020 1:10 AM UTC
Services	0.0 (Log)	80 %	192.168.74.137		22/tcp	Mon, Oct 26, 2020 12:57 AM UTC
Traceroute	0.0 (Log)	80 %	192.168.74.137		general/tcp	Mon, Oct 26, 2020 12:58 AM UTC
DNS Server Detection (TCP)	0.0 (Log)	80 %	192.168.74.137		53/tcp	Mon, Oct 26, 2020 12:59 AM UTC
SSH Server type and version	0.0 (Log)	80 %	192.168.74.137		22/tcp	Mon, Oct 26, 2020 12:59 AM UTC
OpenSSH Detection Consolidation	0.0 (Log)	80 %	192.168.74.137		general/tcp	Mon, Oct 26, 2020 12:59 AM UTC

Apply to page contents

(Applied filter: apply_overrides=0 min_qod=70 task_id=e4c960e0-5f06-4ad6-a656-caacef47acc2 rows=10 first=1 sort-reverse=severity)

1 - 10 of 13

TCP timestamps in detail.

			IP	Name		
TCP timestamps	2.6 (Low)	80 %	192.168.74.137		general/tcp	Mon, Oct 26, 2020 12:58 AM UTC

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Detection Result

```
It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1121919543
Packet 2: 1121920622
```

Insight

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: TCP timestamps OID: 1.3.6.1.4.1.25623.1.0.80091

Affected Software/OS

TCP implementations that implement RFC1323/RFC7323.

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

Solution Type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to