DNS Poisoner Testing

William and Benny

Table of Contents

Table of Contents 1

ARP Poison 2

- Config File Settings 2
- Victim Actions 2
- Results 2
  - Attacker: 2
  - Victim: 3
- Pass? 3

Non-Targeted Websites 4

- Config File Settings 4
- Victim Actions 4
- Results 4
  - fedoraproject.org: 4
  - google.ca: 5
- Pass? 5

Targeted Websites 6

- Config File Settings 6
- Victim Actions 6
- Results 6
  - webview: 6
  - curl: 7
- Pass? 7

ARP Poison

The ARP table of the gateway and the victim machine should be poisoned with the MAC address specified in the config file. The wireshark capture for this test case can be found at captures/arp-poison.pcapng.

Config File Settings

```
# poisoner.conf
victimIp=192.168.0.20
gatewayIp=192.168.0.100
attackerMac=e4:b9:7a:ef:63:8c
interfaceName=eno1

# spoofed_domains.conf
milliways.bcit.ca=192.168.0.19
```

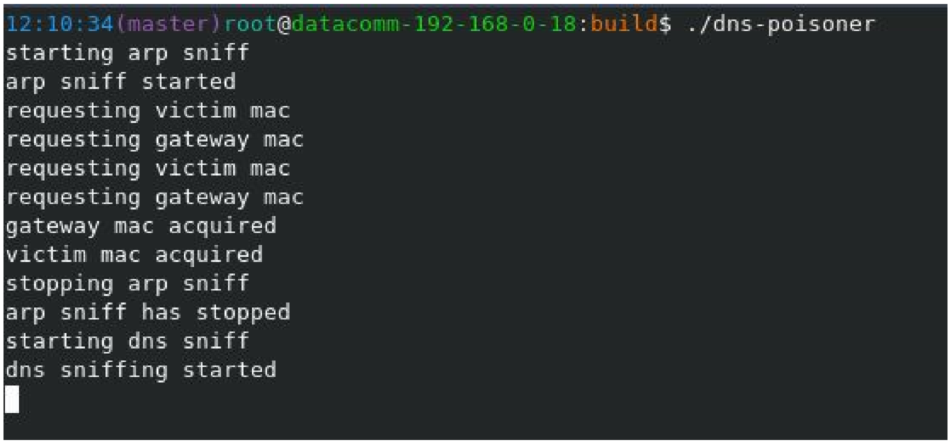
Victim Actions

The victim does nothing.

Results

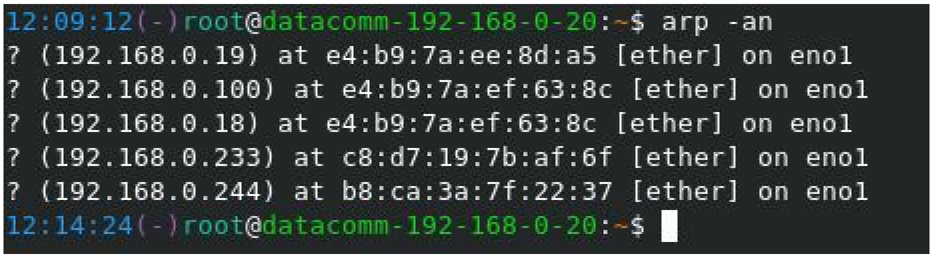
The ARP table entry for 192.168.0.100(gateway) on host 192.168.0.20(victim) is set to the attacker MAC address.

Attacker:



```
12:10:34(master)root@datacomm-192-168-0-18:build$ ./dns-poisoner
starting arp sniff
arp sniff started
requesting victim mac
requesting gateway mac
requesting victim mac
requesting gateway mac
gateway mac acquired
victim mac acquired
stopping arp sniff
arp sniff has stopped
starting dns sniff
dns sniffing started
```

Victim:



```
12:09:12(-)root@datacomm-192-168-0-20:~$ arp -an
? (192.168.0.19) at e4:b9:7a:ee:8d:a5 [ether] on eno1
? (192.168.0.100) at e4:b9:7a:ef:63:8c [ether] on eno1
? (192.168.0.18) at e4:b9:7a:ef:63:8c [ether] on eno1
? (192.168.0.233) at c8:d7:19:7b:af:6f [ether] on eno1
? (192.168.0.244) at b8:ca:3a:7f:22:37 [ether] on eno1
12:14:24(-)root@datacomm-192-168-0-20:~$ 
```

Pass?

Pass

Non-Targeted Websites

Once the victim is ARP poisoned, the victim should still be able to get correct DNS responses normally. The wireshark capture for this test case can be found at captures/non-targeted-websites.pcapng.

Config File Settings

```
# poisoner.conf
victimIp=192.168.0.20
gatewayIp=192.168.0.100
attackerMac=e4:b9:7a:ef:63:8c
interfaceName=eno1

# spoofed_domains.conf
milliways.bcit.ca=192.168.0.19
```

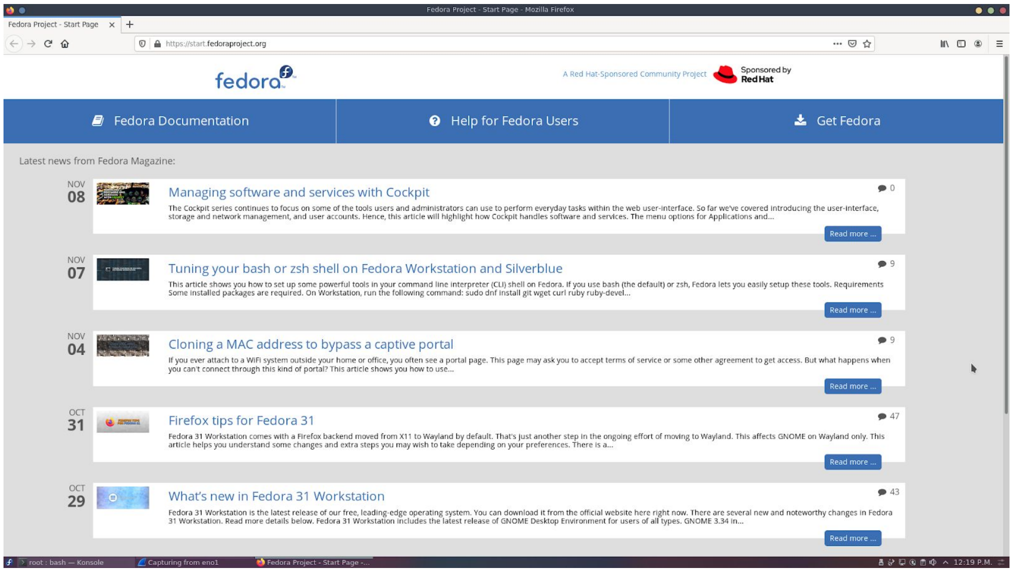
Victim Actions

The victim browses various websites not specified in the config file.

Results

The victim is able normally view websites.

fedoraproject.org:


Fedora Project - Start Page - Mozilla Firefox
Fedora Project - Start Page
https://start.fedoraproject.org
fedora
A Red Hat-Sponsored Community Project
Sponsored by Red Hat
Fedora Documentation
Help for Fedora Users
Get Fedora
root : bash — Konsole
Capturing from eno1
Fedora Project - Start Page -...
12:19 P.M.

Latest news from Fedora Magazine:

NOV 08 Managing software and services with Cockpit 0

The Cockpit series continues to focus on some of the tools users and administrators can use to perform everyday tasks within the web user-interface. So far we've covered introducing the user-interface, storage and network management, and user accounts. Hence, this article will highlight how Cockpit handles software and services. The menu options for Applications and...

Read more ...

NOV 07 Tuning your bash or zsh shell on Fedora Workstation and Silverblue 9

This article shows you how to set up some powerful tools in your command line interpreter (CLI) shell on Fedora. If you use bash (the default) or zsh, Fedora lets you easily setup these tools. Requirements Some installed packages are required. On Workstation, run the following command: sudo dnf install git wget curl ruby ruby-devel...

Read more ...

NOV 04 Cloning a MAC address to bypass a captive portal 9

If you ever attach to a WiFi system outside your home or office, you often see a portal page. This page may ask you to accept terms of service or some other agreement to get access. But what happens when you can't connect through this kind of portal? This article shows you how to use...

Read more ...

OCT 31 Firefox tips for Fedora 31 47

Fedora 31 Workstation comes with a Firefox backend moved from X11 to Wayland by default. That's just another step in the ongoing effort of moving to Wayland. This affects GNOME on Wayland only. This article helps you understand some changes and extra steps you may wish to take depending on your preferences. There is a...

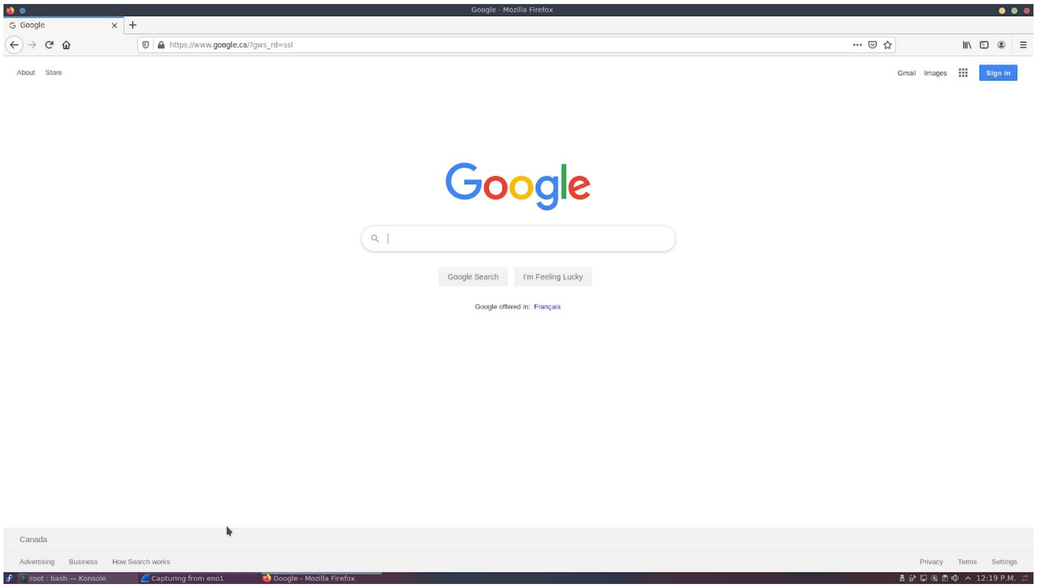
Read more ...

OCT 29 What's new in Fedora 31 Workstation 43

Fedora 31 Workstation is the latest release of our free, leading-edge operating system. You can download it from the official website here right now. There are several new and noteworthy changes in Fedora 31 Workstation. Read more details below. Fedora 31 Workstation includes the latest release of GNOME Desktop Environment for users of all types. GNOME 3.34 in...

Read more ...

google.ca:



Pass?

Pass

Targeted Websites

Once the victim is ARP poisoned, when the victim makes a query for a targeted domain name, the victim should receive a poisoned response. The wireshark capture for this test case can be found at captures/target-website.pcapng.

Config File Settings

```
# poisoner.conf
victimIp=192.168.0.20
gatewayIp=192.168.0.100
attackerMac=e4:b9:7a:ef:63:8c
interfaceName=eno1

# spoofed_domains.conf
milliways.bcit.ca=192.168.0.19
```

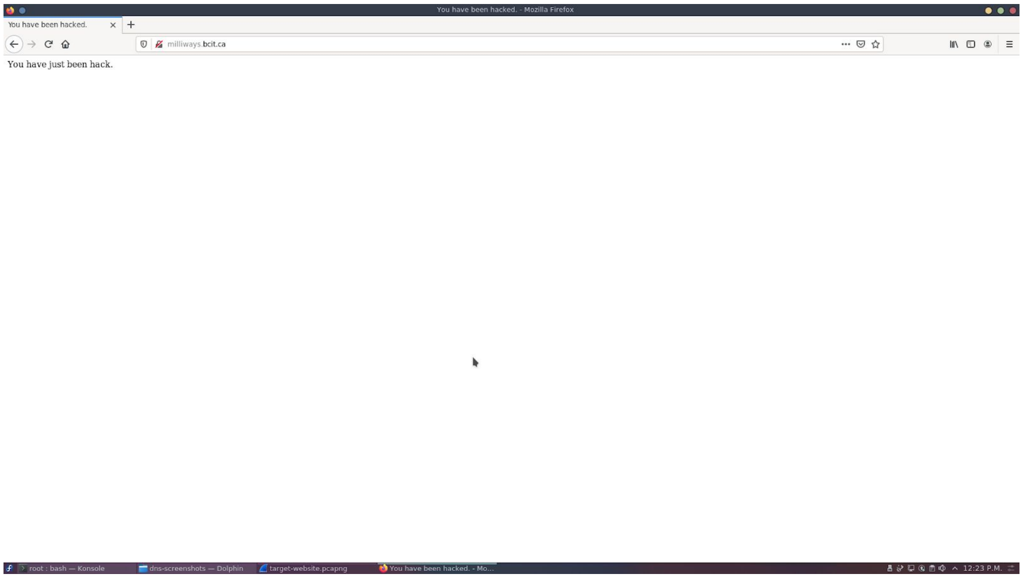
Victim Actions

The victim visits milliways.bcit.ca.

Results

The victim is redirected to our own Apache server when they visit milliways.bcit.ca.

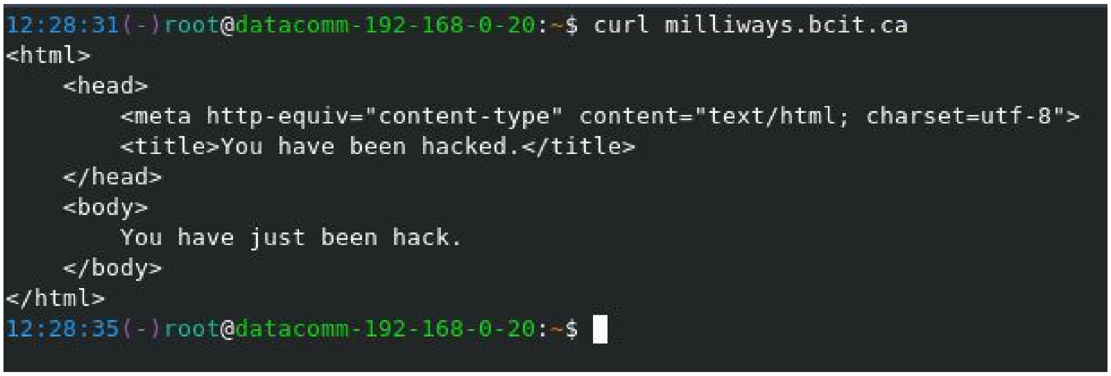
webview:



You have just been hack.

You have been hacked. - Mozilla Firefox
You have been hacked.
milliways.bcit.ca
root : bash — Konsole
dns-screenshots — Dolphin
target-website.pcapng
You have been hacked. - Mo...
12:23 P.M.

curl:



```
12:28:31(-)root@datacomm-192-168-0-20:~$ curl milliways.bcit.ca
<html>
    <head>
        <meta http-equiv="content-type" content="text/html; charset=utf-8">
        <title>You have been hacked.</title>
    </head>
    <body>
        You have just been hack.
    </body>
</html>
12:28:35(-)root@datacomm-192-168-0-20:~$
```

Pass?

Pass