Build an IP Captive Portal from Scratch

(For Fun and Education, but Not for Profit)

Gilbert Detillieux, Computer Science

Presented to MUUG, 13 November 2018

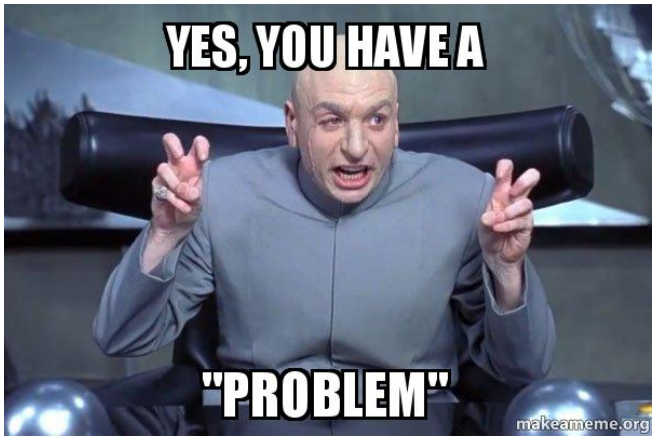
University of Manitoba

Warnings, Disclaimers, etc…

- This is a How-To talk
- Not mainly focused on security
- Not a “Pwn the Portal” presentation
- YMMV; not responsible for you getting hacked

We Have a Problem…

- Users plugging unknown devices into our Ethernet ports
- Policy is to not give network access to unknown devices
- Policy is documented, but… tl;dr…
- Want to help facilitate compliance
- Don’t want to inconvenience users

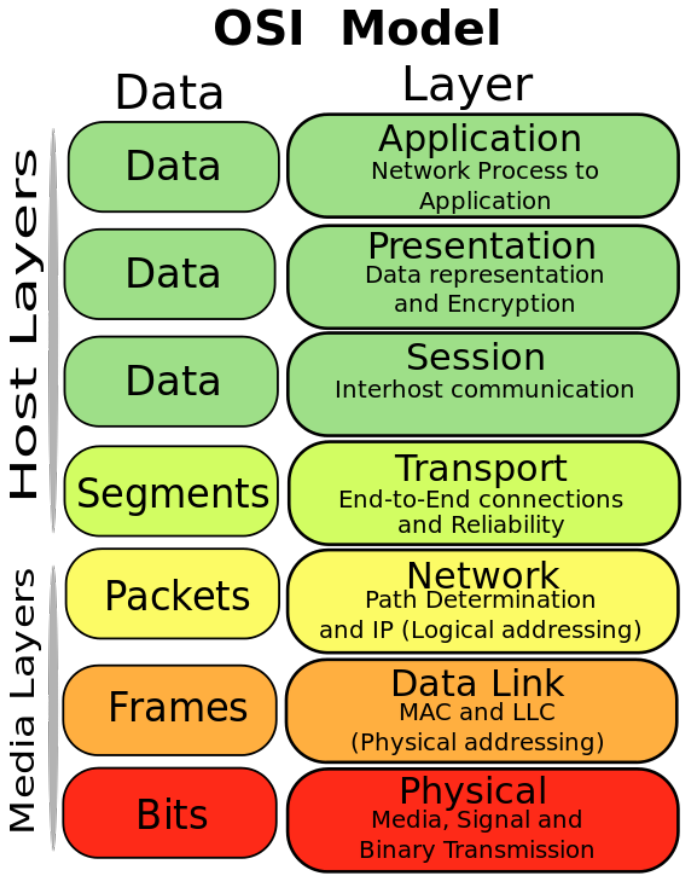


What is a Captive Portal?

- A **captive portal** is a web page that is displayed to newly connected users before they are granted broader access to network resources. Captive portals are commonly used to present a landing or log-in page which may require authentication, payment, acceptance of EULA/accepted use policies, or other valid credentials that both the host and user agree to adhere by. …
- The captive portal is presented to the client and is stored either at the gateway or on a web server hosting that page. Depending on the feature set of the gateway, websites or TCP ports can be white-listed so that the user would not have to interact with the captive portal in order to use them. The MAC address of attached clients can also be used to bypass the login process for specified devices.

Where to Put Captive Portal?

- Best implemented at layer 2 (i.e. Ethernet link layer)
- Not the same as 802.1X
- Can isolate devices/ports to a VLAN that is not routable
- Requires managed switches that support that functionality
- May not provide much flexibility or customisability



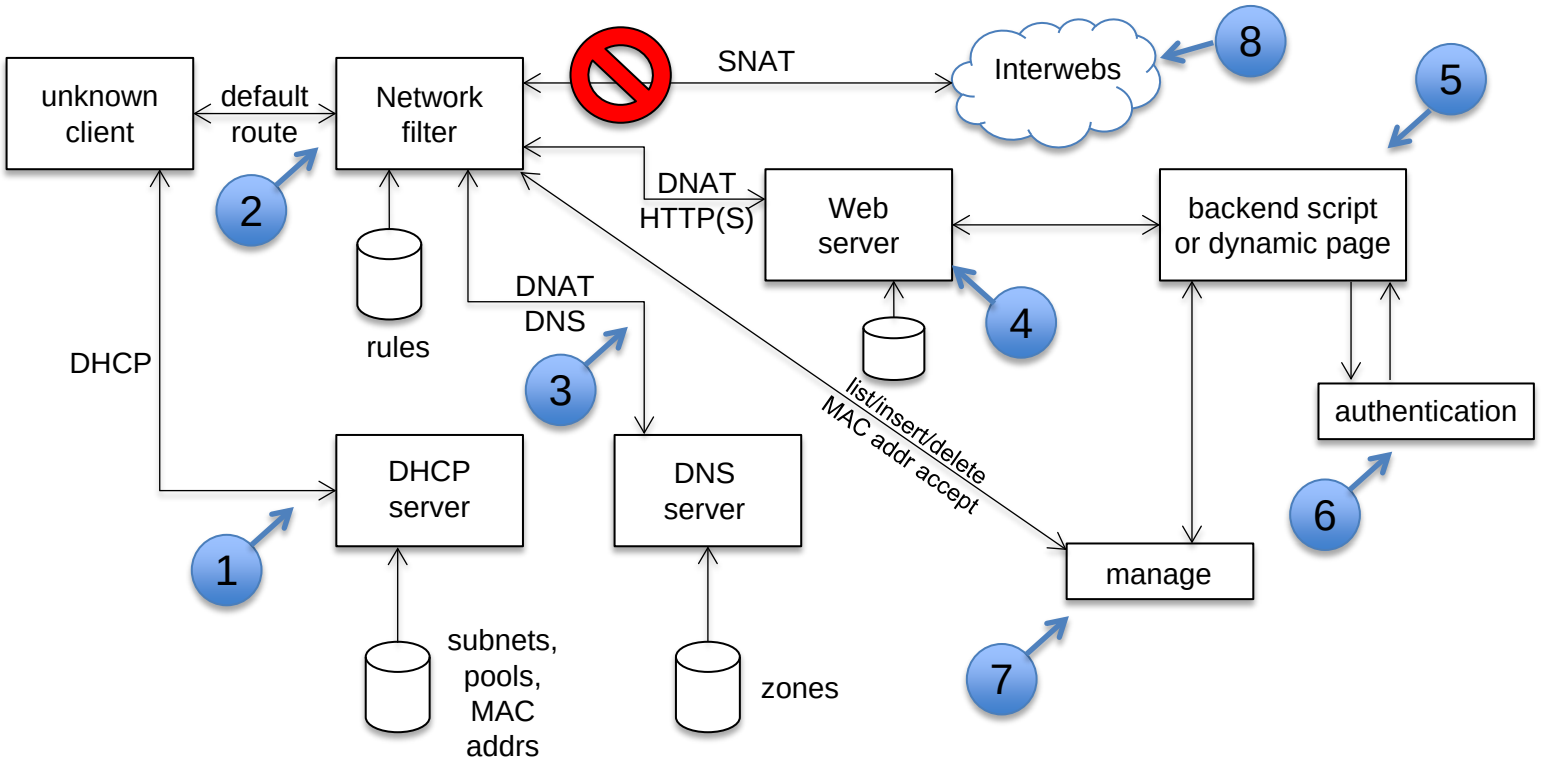
7-Layer Model

- 7
- 6
- 5
- 4 (TCP, UDP)
- 3 (IP, Routers)
- 2 (Ethernet, Switches, Bridges)
- 1 (100BaseT, Hubs, Repeaters)

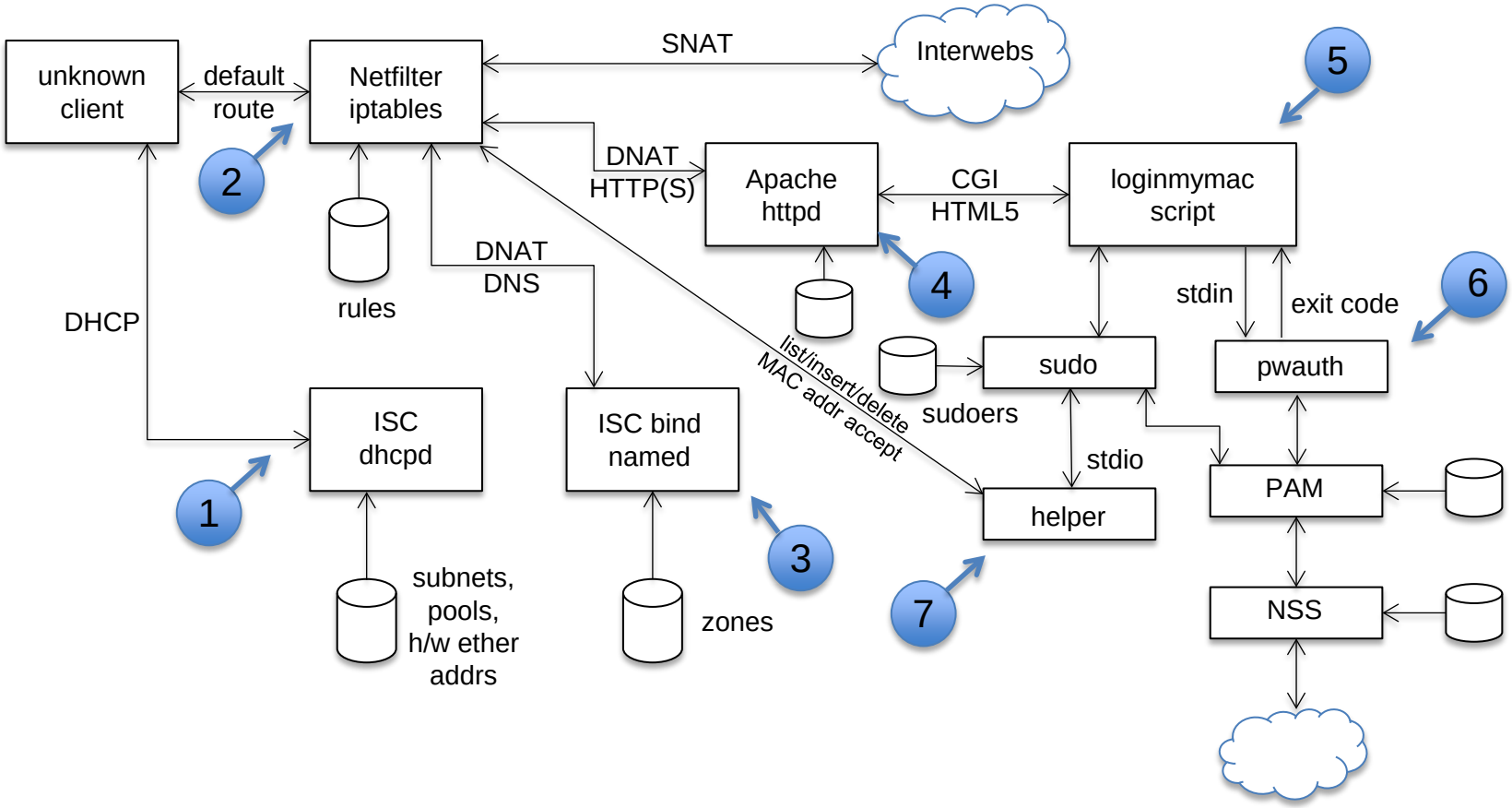
We Have Another Problem…

- Mix of different switches
- Some unmanaged workgroups switches in labs
- Switch ports on our VLAN, but not on switches we manage

IP Captive Portal Components



Linux Captive Portal Components



University of Manitoba

1. dhcpd.conf

```
1.  # Pool of dynamic addresses for registered clients (routed for NAT by default)...
2.  pool {
3.      option routers 192.168.0.1;
4.      option domain-name-servers 192.168.0.1;
5.      max-lease-time  7200;
6.      range dynamic-bootp 192.168.0.192 192.168.0.223;
7.      deny unknown-clients;    …
8.  }
9.  # Pool of dynamic addresses for non-registered clients...
10. # (routed to captive portal until they authenticate, after which, they get NAT access)
11. pool {
12.     option routers 192.168.0.99;
13.     option domain-name-servers 192.168.0.99;
14.     max-lease-time  1800;
15.     range dynamic-bootp 192.168.0.224 192.168.0.239;
16.     allow unknown-clients;
17. }
```

1. dhcpd.conf, multi-subnet

```
1.  shared-network example.com {
2.      subnet 192.168.0.0 netmask 255.255.255.0 {
3.          pool {
4.              option routers 192.168.0.1;
5.              option domain-name-servers 192.168.0.1;
6.              …
7.          }
8.      }
9.      subnet 192.168.99.0 netmask 255.255.255.0 {
10.         pool {
11.             option routers 192.168.99.1;
12.             option domain-name-servers 192.168.99.1;
13.             …
14.         }
15.     }
16. }
```

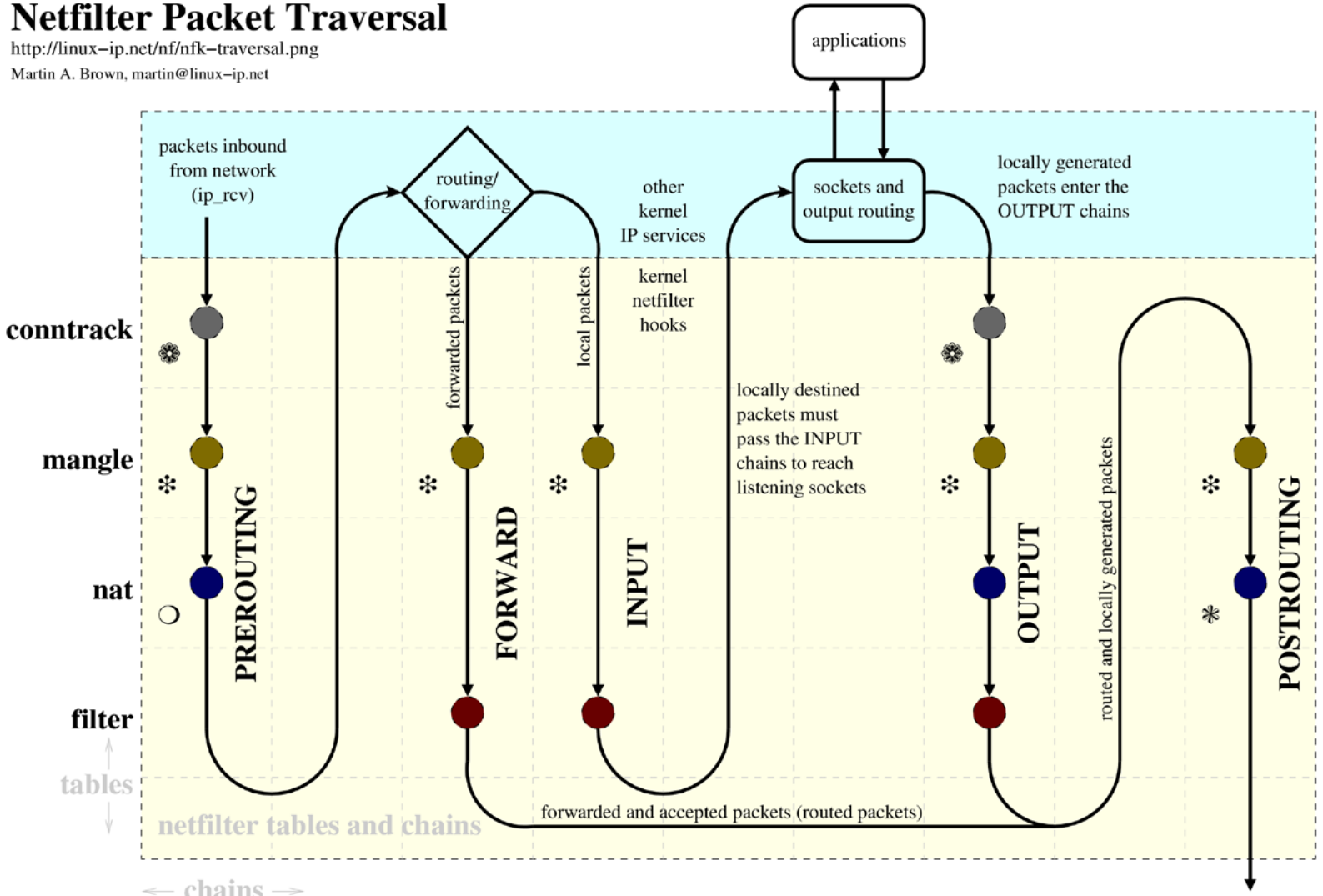
1. dhcpd.conf, RFC 7710 Option

```
1.  option captive-portal-rfc7710 code 160 = string;
2.  …
3.      pool {
4.          option routers 192.168.0.1;
5.          option domain-name-servers 192.168.0.1;
6.          …
7.      }
8.      pool {
9.          option routers 192.168.0.99;
10.         option domain-name-servers 192.168.0.99;
11.         option captive-portal-rfc7710 "https://192.168.0.99/captive/portal.html";
12.         …
13.       }
14.   }
```

Sources: https://en.wikipedia.org/wiki/Captive_portal
https://sources.open-infrastructure.net/software/captive-portal/commit/share/doc/examples/isc-dhcp-server.conf?id=acbed62669206f2aa5bd05f21403a315259cfc9f&context=15

Netfilter Packet Traversal

http://linux-ip.net/nf/nfk-traversal.png
Martin A. Brown, martin@linux-ip.net



❁ The conntrack table is used (if the module is loaded) and is not directly user-manipulable.

❇ The targets MARK, TOS, and TTL are available only in the mangle table.

❍ The nat PREROUTING table supports the DNAT target.

✻ The nat POSTROUTING table supports SNAT and MASQUERADE targets.

cf. http://www.docum.org/qos/kptd/
cf. http://open-source.arkoon.net/kernel/kernel_net.png
cf. http://iptables-tutorial.frozentux.net/

2. Iptables DNAT & SNAT

- iptables -A PREROUTING –i eth0
  -j DNAT --to-destination 192.168.0.99
  # For a static destination address (can be other than host itself)
- iptables -A PREROUTING -i eth0 -j REDIRECT
  # DNAT to incoming address of host itself
- iptables -A POSTROUTING –o eth1
  -j SNAT --to-source 192.168.1.99
  # For a static source address (i.e. outward-facing IP of host itself)
- iptables -A POSTROUTING -o eth1
  -j MASQUERADE
  # SNAT from a dynamic source address (of host itself)

Sources: http://www.andybev.com/index.php/Using_iptables_and_PHP_to_create_a_captive_portal
https://unix.stackexchange.com/questions/132130/iptables-based-redirect-captive-portal-style
https://serverfault.com/questions/514116/how-to-set-mark-on-packet-when-forwarding-it-in-nat-prerouting-table

2. Iptables Script

1. # Accept all traffic destined for private net...
2. iptables -A PREROUTING -d 192.168.0.0/24 -j ACCEPT
3. # Allow access to internal web server(s), if needed...
4. iptables -A PREROUTING -d 192.168.20.40 -m tcp -p tcp -m multiport --dports 80,443 -j ACCEPT
5. iptables -A PREROUTING -d 192.168.20.41 -m tcp -p tcp -m multiport --dports 80,443 -j ACCEPT
6. # Re-route only DNS, HTTP and HTTPS, for entire private net...
7. iptables -A PREROUTING -s 192.168.0.0/24 -m udp -p udp --dport 53 -j DNAT --to-destination 192.168.0.99
8. iptables -A PREROUTING -s 192.168.0.0/24 -m tcp -p tcp -m multiport --dports 53,80,443 -j DNAT --to-destination 192.168.0.99
9. # ... and drop everything else (by marking it to drop in FORWARD filter)...
10. iptables -A PREROUTING -s 192.168.0.0/24 -j MARK --set-mark 86
11. Iptables -A FORWARD -m mark --mark 86 -j DROP
12. # … then SNAT all allowed outbound traffic…
13. iptables -A POSTROUTING -o eth1 -j MASQUERADE

Sources: http://www.andybev.com/index.php/Using_iptables_and_PHP_to_create_a_captive_portal
https://unix.stackexchange.com/questions/132130/iptables-based-redirect-captive-portal-style
https://serverfault.com/questions/514116/how-to-set-mark-on-packet-when-forwarding-it-in-nat-prerouting-table

3. named.conf

- Nothing specific to portal in our configuration
- Might want to restrict access to external domains…
- Can give “fake” DNS back to captive clients (like ad blockers do)
- Should set TTL to 0 on redirected responses

4. Apache …/portal.conf

```
1.  <VirtualHost 192.168.0.99:80>
2.      ServerName portal.example.com
3.      DocumentRoot "/var/www/portal"
4.      <IfModule mod_rewrite.c>
5.          RewriteEngine on
6.          RewriteOptions inherit
7.          # Apple (iOS & macOS):
8.          RewriteEngine on
9.          RewriteCond %{HTTP_USER_AGENT} ^CaptiveNetworkSupport(.*)$ [NC]
10.         RewriteCond %{HTTP_HOST} !^192.168.0.99$
11.         RewriteRule ^(.*)$ http://192.168.0.99/captive/portal.html [L,R=302]
12.     </IfModule>
13.     …
14.     # whatever we missed...
15.     ErrorDocument 404 /captive/portal.html
16. </VirtualHost>
```

Sources: https://thinkincredible.intraway.com/blog-post/how-browser-identify-captive-portals
https://unix.stackexchange.com/questions/386242/captive-portal-using-apache/386243

4. Apache …/portal.conf (cont.)

```
1.  # Android, Chrome:
2.  RedirectMatch 302 /generate_204 http://192.168.0.99/captive/portal.html
3.  # Windows 7 & 8:
4.  RedirectMatch 302 /ncsi.txt http://192.168.0.99/captive/portal.html
5.  # Windows 10:
6.  RedirectMatch 302 /connecttest.txt http://192.168.0.99/captive/portal.html
7.  # Firefox
8.  RedirectMatch 302 /success.txt http://192.168.0.99/captive/portal.html
9.  # whatever we missed...
10. ErrorDocument 404 /captive/portal.html
```

Sources: https://thinkincredible.intraway.com/blog-post/how-browser-identify-captive-portals
https://unix.stackexchange.com/questions/386242/captive-portal-using-apache/386243
https://blogs.technet.microsoft.com/netgeeks/2018/02/20/why-do-i-get-an-internet-explorer-or-edge-popup-open-when-i-get-connected-to-my-corpnet-or-a-public-network/
http://support.moonpoint.com/network/web/browser/firefox/detect_portal/

5. Backend Web Processing

- Can use any kind of dynamic content (ASP, PHP, CGI)
- If no input (via POST), or if errors, send HTML form
- If input is OK, authorize user, register MAC address
- Provide link to allow de-registration (i.e. logout)
- Have some kind of expiry and forced de-registration (at or cron job)

5. Backend Web Processing

```
1.  <form method="POST" action="$SCRIPT_NAME">
2.  <table align="center" border=0>
3.  <tr><td valign="top"><label for="user">Username:</label></td>
4.      <td><input name="user" id="user" type="text" value="" autofocus></td></tr>
5.  <tr><td valign="top"><label for="passwd">Password:</label></td>
6.      <td><input name="passwd" id="passwd" type="password" value=""></td></tr>
7.  <tr><td valign="top"><label for="agree">Agreement:</label></td>
8.      <td><input name="agree" id="agree" type="checkbox" value="yes">
9.      <font size=-2>I'm agree to abide by The Company's
10.     <a href="http://example.com/governance/computer-use/policy.htm" target="_blank">
11.     Computer Use Policy</a> and
12.     <a href="http://dept.example.com/guidelines.html" target="_blank">
13.     Department Guidelines</a>.</font></td></tr>
14. <tr><td><input type=submit value="Login"></td><td></td></tr>
15. </table>
16. </form>
```

Sources: https://www.w3schools.com/tags/tag_input.asp
https://www.w3schools.com/tags/att_input_autofocus.asp

UNIVERSITY OF MANITOBA

6. pwauth

- Standard pam.d config file:

```
#%PAM-1.0
auth        include      password-auth
account     include      password-auth
```

- No need to customize if system's PAM-based auth is fine
- Setuid-root to allow full PAM access (including shadow files)
- Only executable by web user (apache)
- Reads userid and password from 2 lines of stdin
- Exit code indicates success or failure(s)

Source: http://code.google.com/p/pwauth/

7. Helper Script

- Want to list, insert & delete accepted MAC addresses
- Need to run iptables commands as root:

```
iptables -L PREROUTING -t nat -n | fgrep -i "$MAC"
iptables -I PREROUTING 1 -t nat -m mac --mac-source "$MAC" -j ACCEPT
iptables -D PREROUTING -t nat -m mac --mac-source "$MAC" -j ACCEPT
```

- Will be invoked by web user (apache)
- Setuid binary would be an option (as for pwauth)
- Simple script run via sudo is another option

sudoers(5) Examples:

```
Cmnd_Alias    CGIHELPER = /usr/local/sbin/cgihelper

# Normally, require a tty, to not show password in clear…
# ... but override for specific commands run by CGI scripts...
Defaults!CGIHELPER          !requiretty

# Allows owner of particular CGI scripts to run
# “helper” command as other users...
webuser         ALL=(ALL) NOPASSWD: CGIHELPER
```

Source: RTFM: sudo(8) https://muug.ca/meetings/10-11.html#apr

We Still Have a Problem…

- SELinux goes into conniptions
- Can set up a custom module:

  setenforce 0 # then run the app…

  cat /var/log/audit/audit.log | audit2allow -M myapp

  semodule -i myapp.pp

  setenforce 1
- Still miss some audit events

  semodule –DB # do this first!
- This will generate a lot of output

  semodule –B # do this soon after!
- Also need…

  setsebool -P domain_kernel_load_modules=1

Sources: https://relativkreativ.at/articles/how-to-compile-a-selinux-policy-package
https://www.linuxquestions.org/questions/linux-security-4/selinux-unable-to-send-audit-message-4175591310/

SELinux myapp.te allow rules

1. allow fprintd_t httpd_sys_script_t:dbus send_msg;
2. allow httpd_sys_script_t fprintd_t:dbus send_msg;
3. allow httpd_sys_script_t httpd_log_t:dir { add_name write };
4. allow httpd_sys_script_t httpd_log_t:file create;
5. allow httpd_sys_script_t iptables_var_run_t:file { lock open read };
6. allow httpd_sys_script_t lastlog_t:file { open write };
7. allow httpd_sys_script_t pam_var_run_t:dir { add_name write };
8. allow httpd_sys_script_t pam_var_run_t:file { create getattr lock open read write };
9. allow httpd_sys_script_t proc_t:filesystem getattr;
10. allow httpd_sys_script_t self:capability { audit_write dac_override net_raw setgid setuid sys_resource };
11. allow httpd_sys_script_t self:netlink_audit_socket { create nlmsg_relay };
12. allow httpd_sys_script_t self:process setrlimit;
13. allow httpd_sys_script_t self:rawip_socket { create getopt setopt };
14. allow httpd_sys_script_t shadow_t:file { getattr open read };
15. allow httpd_sys_script_t sudo_db_t:dir getattr;
16. allow httpd_sys_script_t system_dbusd_t:dbus send_msg;
17. allow httpd_sys_script_t system_dbusd_t:unix_stream_socket connectto;
18. allow httpd_sys_script_t var_run_t:file { lock open read write };
19. allow httpd_sys_script_t hi_reserved_port_t:tcp_socket name_bind;
20. allow httpd_sys_script_t hi_reserved_port_t:udp_socket name_bind;
21. allow httpd_sys_script_t rndc_port_t:tcp_socket name_bind;
22. allow httpd_sys_script_t self:capability { net_admin net_bind_service };
23. allow httpd_sys_script_t self:netlink_audit_socket { read write };
24. allow httpd_t httpd_sys_script_t:process { noatsecure rlimitinh siginh };

What Did I Learn?

- Lots more about Linux Netfilter/iptables, including DNAT implementation
- Some weird stuff in ISC dhcpd.conf, including “option captive-portal-rfc7710”
- Apache VirtualHost with IP address
- Captive portal detection in different systems
- Some cool HTML5 extensions for form input
- More than I wanted to know about SELinux!

What's Left to Do?

- Sane HTTPS handling
- Better client detection & web redirection
- Better DNS handling (for security)
- Security audit and hardening

TRAILBLAZER ADVENTURER
INNOVATOR DEFENDER CHALLENGER
ADVENTURER TRAILBLAZER DEFENDER VISIONARY
VISIONARY ADVENTURER TRAILBLAZER CHALLENGER DEFENDER VISIONARY

Questions?

UNIVERSITY OF MANITOBA