#sf21vus

School from Home: Watching the Wire with Wireshark

Tony E. - @showipintbri

Hello!

I am Tony E.

I am here because I 💖packets.

You can find me on Twitter: @showipintbri

#sf21vus

About Me

Network Engineer by Day...

- CCIE #64908
- PCNSA
- Consultant focused on security architectures, engineering & implementation

Packet Analyst by Night! 🌙

- GIAC Network Forensic Analyst
- Full PCAP at home (Arkime)
- Inline IPS (Suricata)
- ...and more ;)

Blog: https://showipintbri.github.io
Twitter: @showipintbri

Covid-19 Pandemic == * from home

- Work from home & School from home?

A packet hunters dream🌈 & security person's nightmare.😱

- 2 New (managed) Chromebooks
- Lots of new traffic to inspect

HTTP Method: Anna Molly ?

#sf21vus

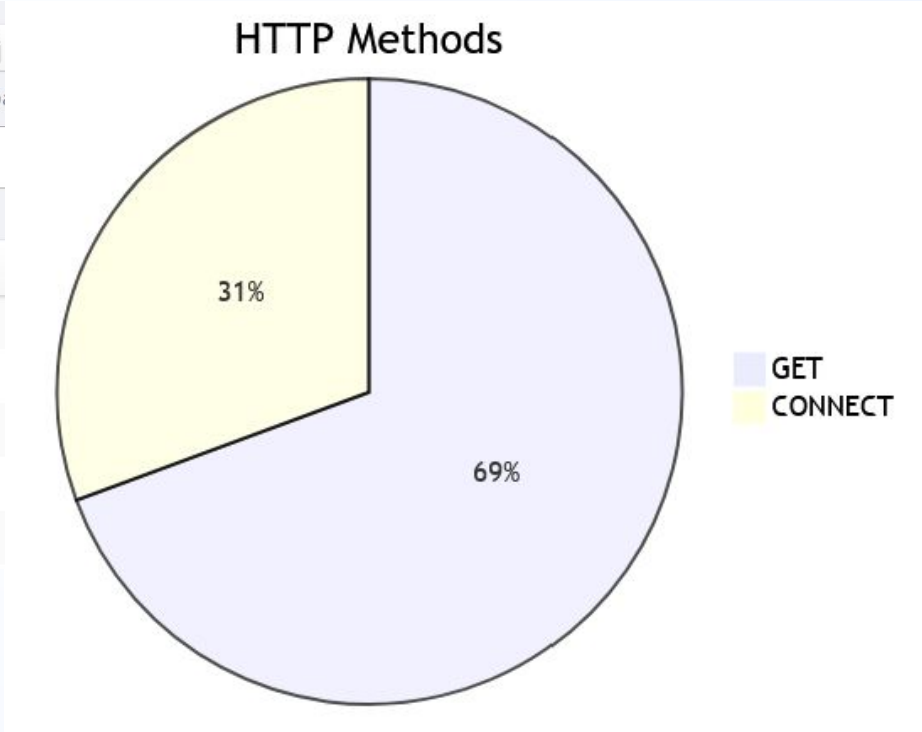
chromebook-1.pcapng

470.5 KB 2 WK

Subsp

```
_path="http" | count() by method,id.resp_p
```

method	id.resp_p	count
GET	8060	15
GET	80	584
CONNECT	8009	271
GET	7080	11
GET	8009	4



#sf21vus

HTTP URI: [host]:[port] wah?

chromebook-1.pcapng

470.5 KB 2 WK

Subspace Packets Export

```
_path="http" method="CONNECT" | count() by uri | sort -r count
```

uri	count
www.google.com:443	91
lh3.googleusercontent.com:443	11
cms-tc.pbskids.org:443	11
play.google.com:443	10
www.google-analytics.com:443	9
bam-cell.nr-data.net:443	8
blackboard.[redacted].org:443	8
webcdn.prodigygame.com:443	7

HTTP URI: cleartext *.pac file ?

#sf21vus

- MIME Type: text file
- ...over clear text HTTP
- ...same destination
- ...different chromebooks

method	host	uri	referrer	version	user_agent
GET	cloud[redacted]-swg.ibosscloud.com	/ibreports/web/pac/[redacted]/v2/proxy.pac		1.1	Mozilla/5.0 (X11; CrOS x86_64 13904.6
GET	cloud[redacted]-swg.ibosscloud.com	/ibreports/web/pac/[redacted]/v2/proxy.pac		1.1	Mozilla/5.0 (X11; CrOS x86_64 13904.6
GET	cloud[redacted]-swg.ibosscloud.com	/ibreports/web/pac/[redacted]/v2/proxy.pac		1.1	Mozilla/5.0 (X11; CrOS x86_64 13904.6
GET	cloud[redacted]-swg.ibosscloud.com	/ibreports/web/pac/[redacted]/v2/proxy.pac		1.1	Mozilla/5.0 (X11; CrOS x86_64 13904.6
GET	cloud[redacted]-swg.ibosscloud.com	/ibreports/web/pac/[redacted]/v2/proxy.pac		1.1	Mozilla/5.0 (X11; CrOS x86_64 13904.6
GET	cloud[redacted]-swg.ibosscloud.com	/ibreports/web/pac/[redacted]/v2/proxy.pac		1.1	Mozilla/5.0 (X11; CrOS x86_64 13904.6
GET	cloud[redacted]-swg.ibosscloud.com	/ibreports/web/pac/[redacted]/v2/proxy.pac		1.1	Mozilla/5.0 (X11; CrOS x86_64 13904.6
GET	cloud[redacted]-swg.ibosscloud.com	/ibreports/web/pac/[redacted]/v2/proxy.pac		1.1	Mozilla/5.0 (X11; CrOS x86_64 13904.6
GET	cloud[redacted]-swg.ibosscloud.com	/ibreports/web/pac/[redacted]/v2/proxy.pac		1.1	Mozilla/5.0 (X11; CrOS x86_64 13904.6
GET	cloud[redacted]-swg.ibosscloud.com	/ibreports/web/pac/[redacted]/v2/proxy.pac		1.1	Mozilla/5.0 (X11; CrOS x86_64 13904.6
GET	cloud[redacted]-swg.ibosscloud.com	/ibreports/web/pac/[redacted]/v2/proxy.pac		1.1	Mozilla/5.0 (X11; CrOS x86_64 13904.6

Network Tell-All: BGPstuff.net

#sf21vus

BGPSTUFF.NET

home route origin aspath roa asname invalids sourced totals whereami faq

Route is 149.19.33.0/24 for 149.19.33.22

The origin AS for 149.19.33.22 is AS396253

The AS name for AS396253 is IBOSS-8-ASN

AS396253 is sourcing 66 prefixes. 50 IPv4 prefixes and 16 IPv6 prefixes.

Twitter: @mellowdrifter

Network Tell-All: IANA

#sf21vus

Whois IP 138.43.105.135

Updated 1 second ago

```
NetRange:       138.43.96.0 - 138.43.111.255
CIDR:           138.43.96.0/20
NetName:        IBOSS-8
NetHandle:      NET-138-43-96-0-1
Parent:         NET138 (NET-138-0-0-0-0)
NetType:        Direct Assignment
OriginAS:
Organization:   iboss,inc (IBOSS-8)
RegDate:        2019-12-12
Updated:        2019-11-20
Ref:            https://rdap.arin.net/regi
```

Whois IP 149.19.32.103

Updated 1 second ago

```
NetRange:       149.19.32.0 - 149.19.63.255
CIDR:           149.19.32.0/19
NetName:        IBOSS-8
NetHandle:      NET-149-19-32-0-1
Parent:         NET149 (NET-149-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   iboss,inc (IBOSS-8)
RegDate:        2020-11-04
Updated:        2020-11-04
Ref:            https://rdap.arin.net/registry/ip/149.19.32.0
```

#sf21vus

File Analysis:

- text file
- ...over clear text HTTP
- ...same file size
- ...different MD5 hashes?

ts	_path	tx_hosts	rx_hosts	source	mime_type	filename	total_bytes	md5
2021-08-16T00:03:30.711	files	149.19.33.49	192.168.1.105	HTTP	text/plain	proxy.pac	19,885	5a7cfabb50fa3e1d72fb2512bdb90ea1
2021-08-16T00:03:30.717	files	149.19.33.48	192.168.1.105	HTTP	text/plain	proxy.pac	19,885	4f34f3f709d0fc296116ea3cc8fe6755
2021-08-16T00:03:30.751	files	149.19.32.103	192.168.1.105	HTTP	text/plain	proxy.pac	19,885	4e6f7c5f7b871025b4387af6efdf1a79
2021-08-16T00:03:40.877	files	149.19.33.49	192.168.1.105	HTTP	text/plain	proxy.pac	19,885	2d336d2f0721e0eadba9c3284016d6ab
2021-08-16T00:14:00.851	files	138.43.105.135	192.168.1.105	HTTP	text/plain	proxy.pac	19,885	39e99b07a0de0c9b528911f3c5d25bcf
2021-08-16T00:24:20.792	files	149.19.33.82	192.168.1.105	HTTP	text/plain	proxy.pac	19,885	6917e3c94a11c3335d7380da4619581c
2021-08-29T21:14:19.680	files	149.19.33.22	192.168.1.105	HTTP	text/plain	proxy.pac	19,885	f8802bc2f85286efa5479ce7196b7087
2021-08-29T21:14:19.683	files	149.19.33.22	192.168.1.105	HTTP	text/plain	proxy.pac	19,885	8a122877da628c2d00c4c1bb20617385
2021-08-29T21:14:19.739	files	138.43.105.135	192.168.1.105	HTTP	text/plain	proxy.pac	19,885	9321deb174143e9f684850895efe2299
2021-08-29T21:14:30.038	files	138.43.105.135	192.168.1.105	HTTP	text/plain	proxy.pac	19,885	4b4f4261d1f60ea29630c701eb65f46a
2021-08-29T21:24:50.052	files	138.43.106.214	192.168.1.105	HTTP	text/plain	proxy.pac	19,885	21ab0de968ba0d45a104d8ee6a062f79

PAC Files Oh My! 😲

#sf21vus

```
function FindProxyForURL(url, host) {

var hostIP = "";
var ibsrcip = "[redacted]";
var ibcountry = "US"; // ([redacted])";
/*  */
if ((shExpMatch(host, "msftncsi.com") || shExpMatch(host, "*.msftncsi.com")) ||
    (shExpMatch(host, "meet.google.com") || shExpMatch(host, "*.meet.google.com")) ||
    (shExpMatch(host, "accounts.google.com") || shExpMatch(host, "*.accounts.google.com")) ||
    (shExpMatch(host, "classroom.google.com") || shExpMatch(host, "*.classroom.google.com")) ||
    (shExpMatch(host, "classlink.com") || shExpMatch(host, "*.classlink.com")) ||
    (shExpMatch(host, "classlink.io") || shExpMatch(host, "*.classlink.io")) ||
    (shExpMatch(host, "connectivitycheck.android.com") || shExpMatch(host, "*.connectivitycheck.android.com")) ||
    (shExpMatch(host, "1e100.net") || shExpMatch(host, "*.1e100.net")) ||
    (shExpMatch(host, "accounts.google.com") || shExpMatch(host, "*.accounts.google.com")) ||
    (shExpMatch(host, "accounts.google") || shExpMatch(host, "*.accounts.google")) ||
    (shExpMatch(host, "accounts.gstatic.com") || shExpMatch(host, "*.accounts.gstatic.com")) ||
    (shExpMatch(host, "accounts.youtube.com") || shExpMatch(host, "*.accounts.youtube.com")) ||
    (shExpMatch(host, "gstatic.com") || shExpMatch(host, "*.gstatic.com")) ||
    (shExpMatch(host, "chromeos-ca.gstatic.com") || shExpMatch(host, "*.chromeos-ca.gstatic.com")) ||
    (shExpMatch(host, "clients1.google.com") || shExpMatch(host, "*.clients1.google.com")) ||
    (shExpMatch(host, "clients2.google.com") || shExpMatch(host, "*.clients2.google.com")) ||
    (shExpMatch(host, "clients3.google.com") || shExpMatch(host, "*.clients3.google.com")) ||
    (shExpMatch(host, "clients4.google.com") || shExpMatch(host, "*.clients4.google.com")) ||
```

Questions to Answer...

- The 5- “W”s and an “H”
- “Data in Context”

Let the Research Comence

Oh, I see you're using a forward proxy, and transferring your PAC file in the clear… Profit.

Proxies are used for:

- URL filtering
- Content filtering
- Security
- Content Caching
- Secure Web Gateway's
- SASE Architectures pronounced "sassy" :)

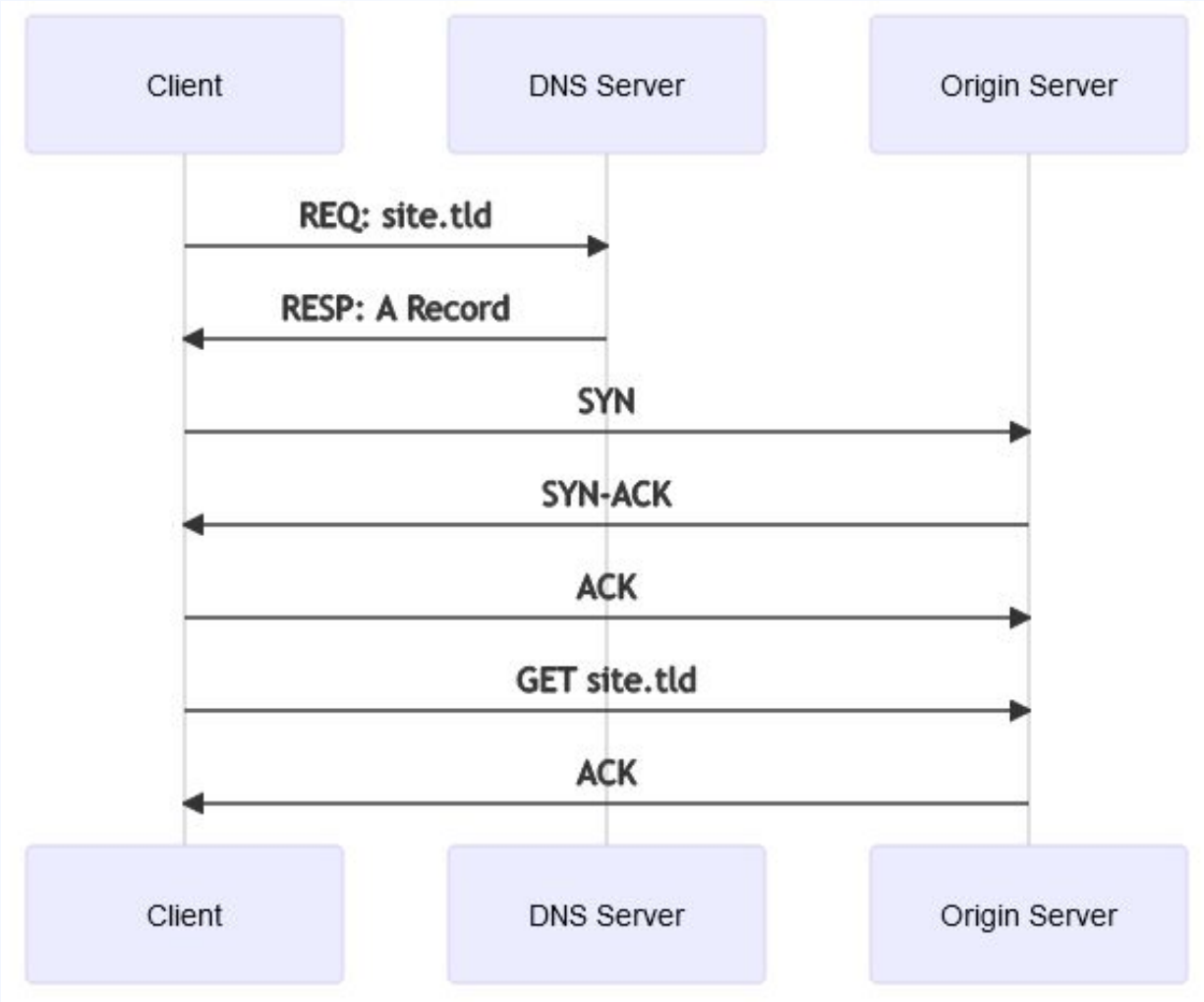
#sf21vus

Scientific Method

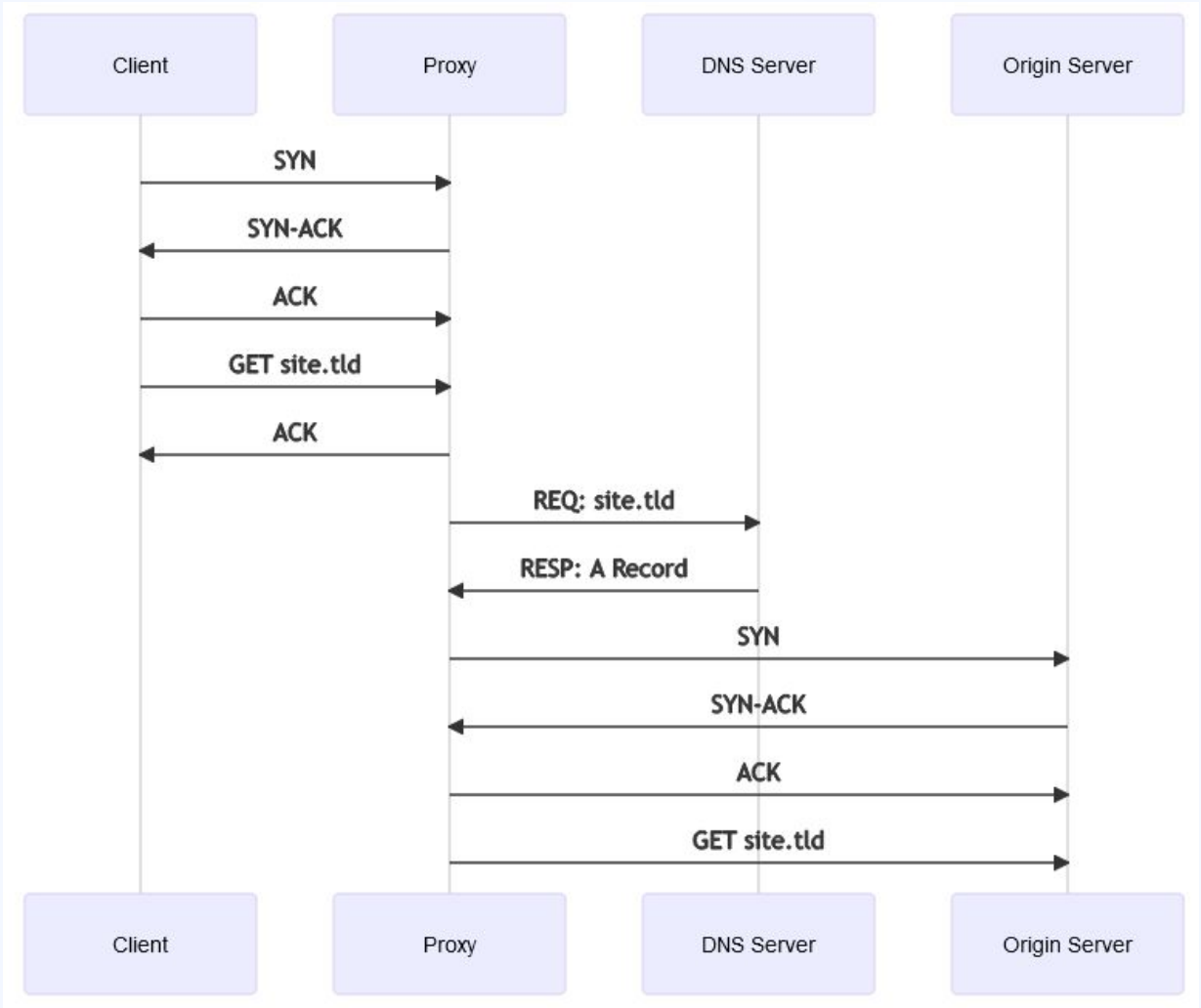
Hypothesis:

It is possible to circumvent the web controls on a managed Chromebook using only the network?

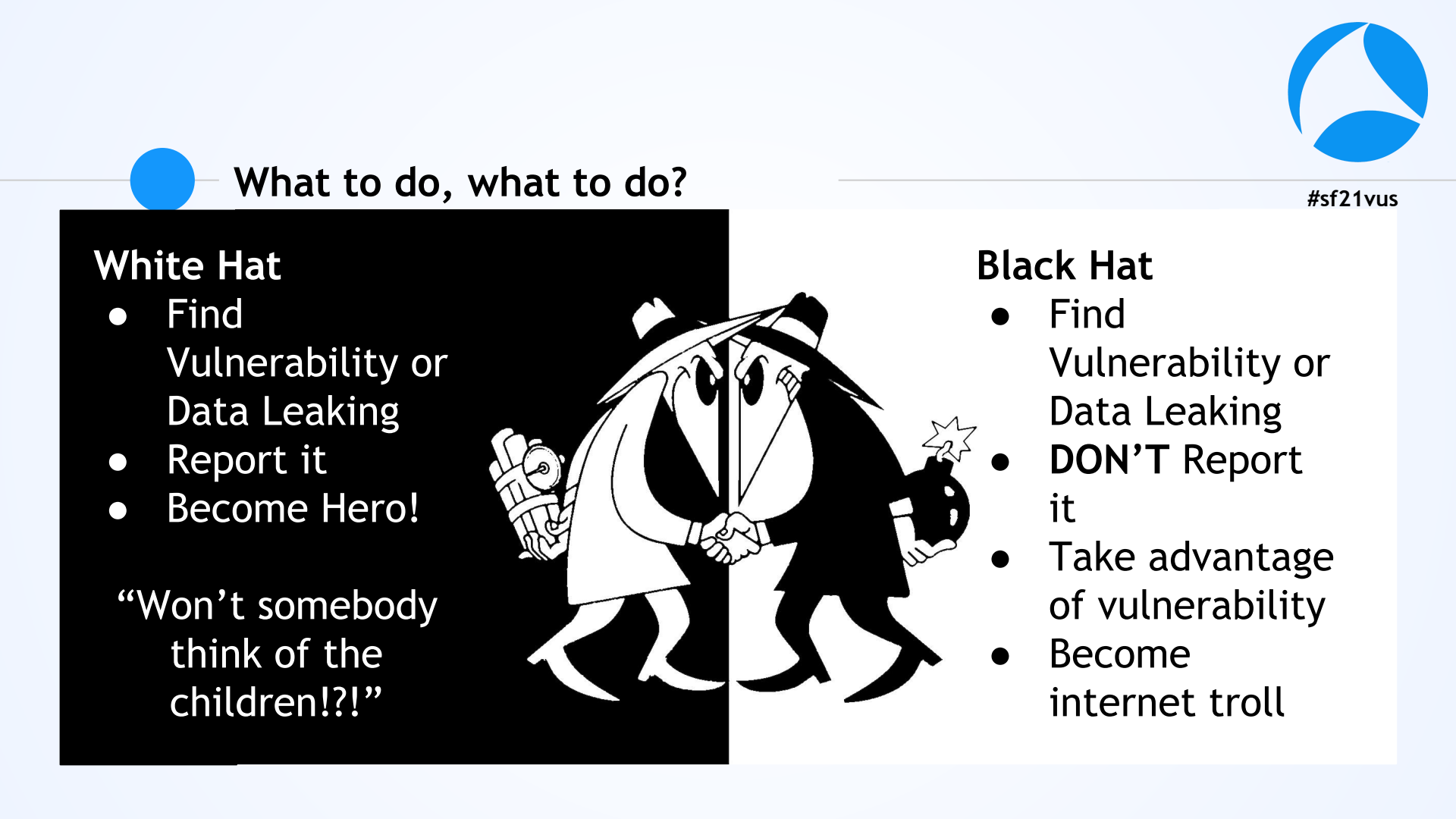
Prove *or* **Disprove**


Client
DNS Server
Origin Server
REQ: site.tld
RESP: A Record
SYN
SYN-ACK
ACK
GET site.tld
ACK
Client
DNS Server
Origin Server

#sf21vus


Client
Proxy
DNS Server
Origin Server
SYN
SYN-ACK
ACK
GET site.tld
ACK
REQ: site.tld
RESP: A Record
SYN
SYN-ACK
ACK
GET site.tld
Client
Proxy
DNS Server
Origin Server

#sf21vus



What to do, what to do?

White Hat

- Find Vulnerability or Data Leaking
- Report it
- Become Hero!

"Won't somebody think of the children!?!"

Black Hat

- Find Vulnerability or Data Leaking
- **DON'T** Report it
- Take advantage of vulnerability
- Become internet troll

What's the Goal?

Affect the operation of the configured proxy.

(self-imposed)Rules:

- Cannot touch the endpoint configuration
- All affects must be from the network!

Baseline Tests (Scientific Control)

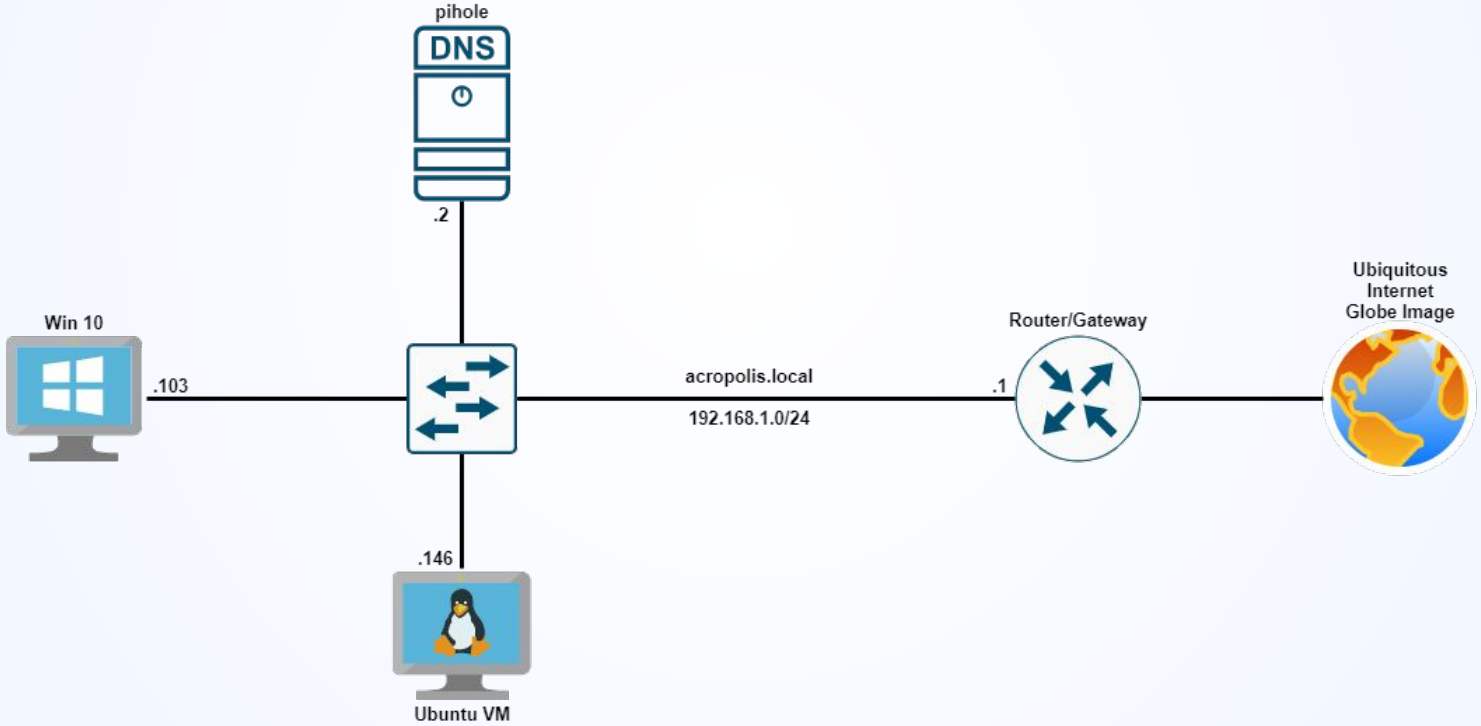
1. From Workstation to local web server using local DNS

2. From Workstation using explicit proxy on local network making a GET request for a remote origin server

3. From Workstation using explicit proxy on local network making a CONNECT request for a remote origin server

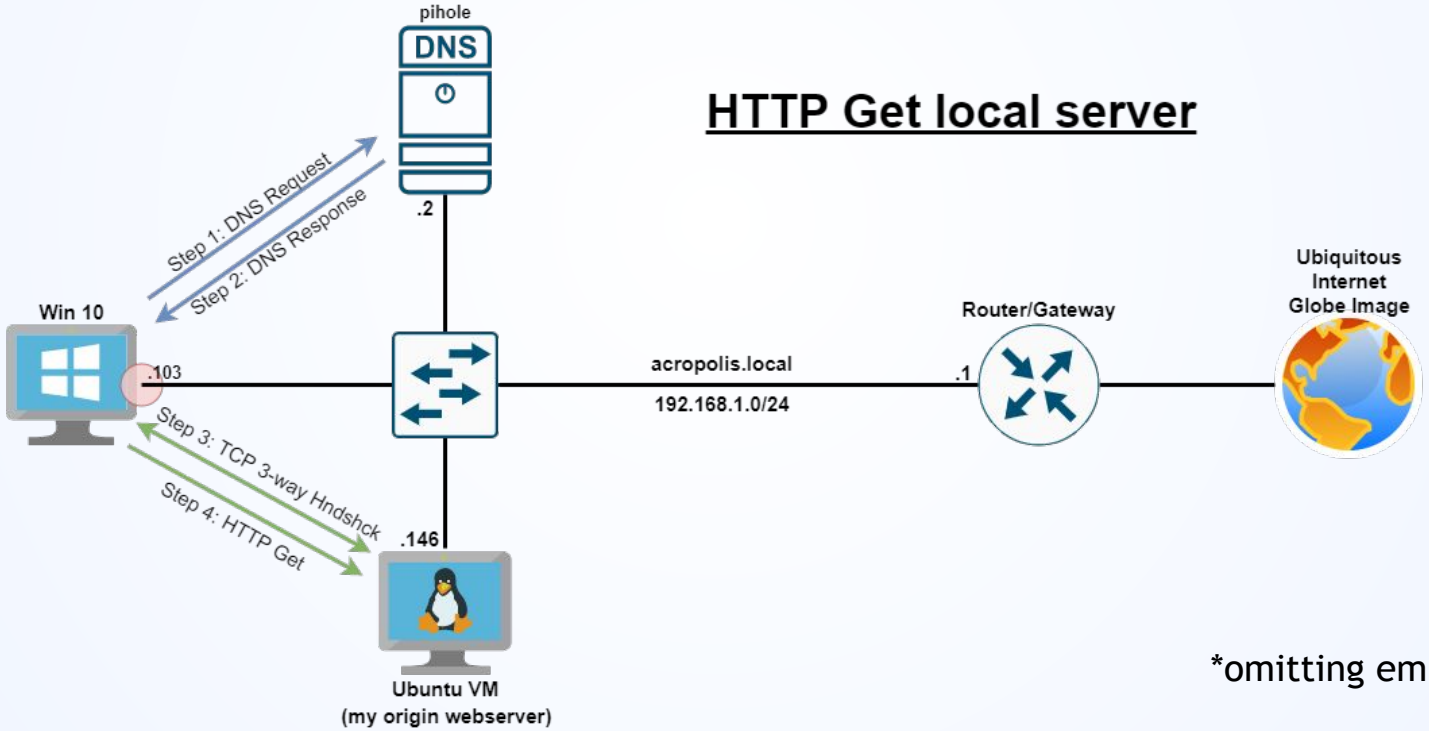
The Lab (home network)

#sf21vus



Test #1: Local Webserver, Local DNS, NO Proxy

#sf21vus



*omitting empty ACKs

What is the role of a Proxy?

#sf21vus

Forward Proxies:

- Makes requests on behalf of the clients.
- Typically many clients are behind a single Proxy.

Reverse Proxies:

- Receive requests on behalf of the servers.
- Typically many servers are behind a single proxy.

  (this functionality normally combined with a load-balancer)

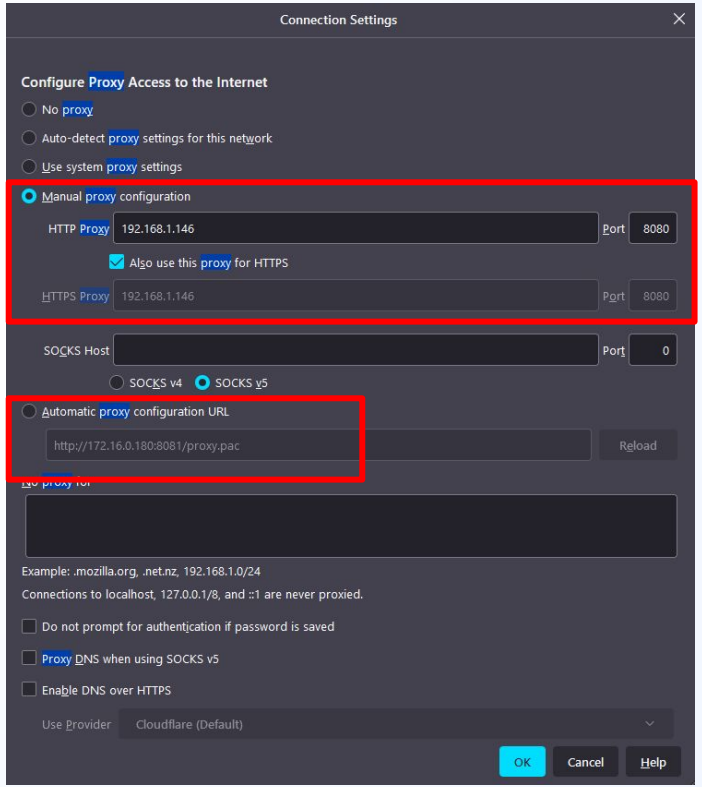
Browser vs. System Config

Browser Settings

- Explicit Browser config
- PAC file Browser config

OS Settings

- Explicitly configured via system configuration
- Proxy Auto Configuration via system settings



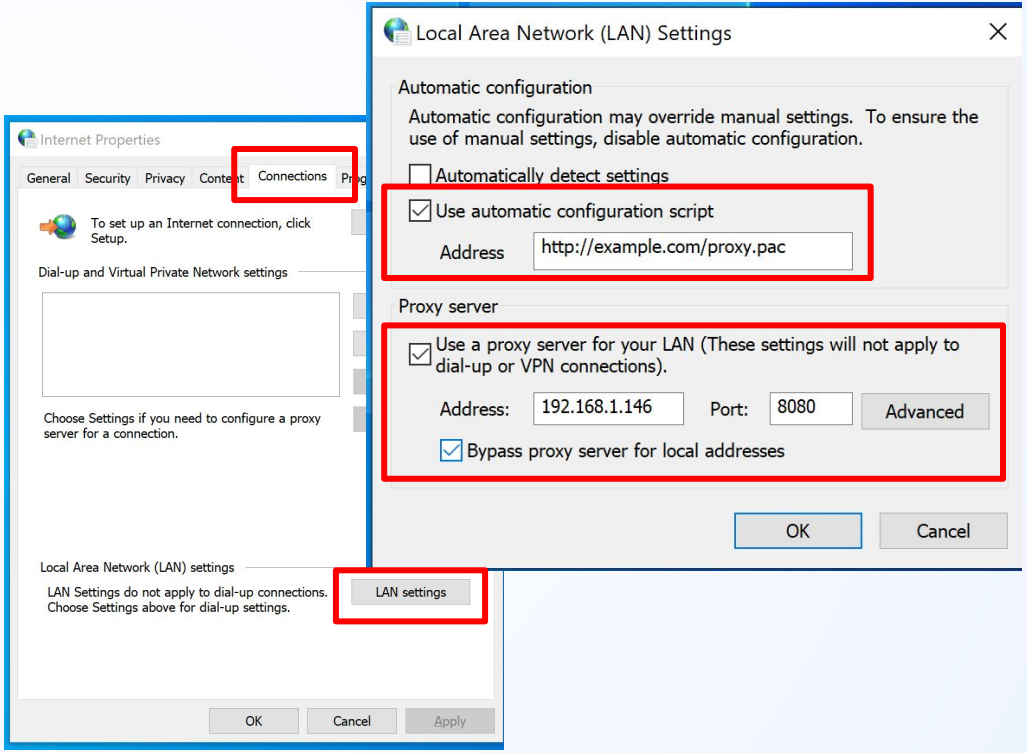
Browser vs. System Config

Browser Settings

- Explicit Browser config
- PAC file Browser config

OS Settings

- Explicitly configured via system configuration
- Proxy Auto Configuration via system settings



#sf21vus

What does a PAC file look like: Anatomy of a PAC File

```
function FindProxyForURL(url, host) {

if ((shExpMatch(host, "msftncsi.com") || shExpMatch(host, "*.msftncsi.com")))
{
    return "DIRECT";
}

    return "PROXY proxy.proxycloud.com:8009";
}
```

For more information about PAC files: http://findproxyforurl.com/

Explicit vs. PAC

Explicit: (static)

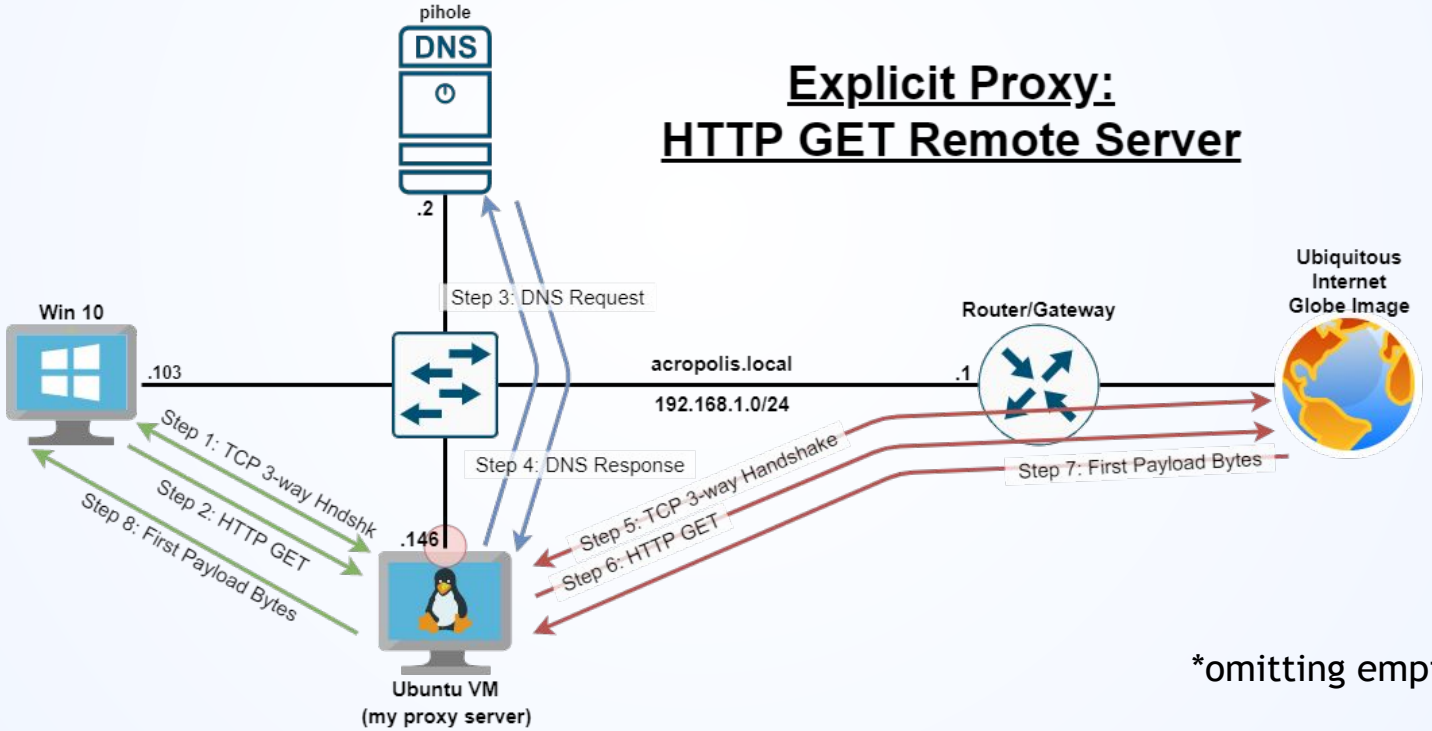
- Send All Requests to the configured PROXY address
- Manually specified explicit exclusions
- Hard to maintain at scale

PAC: (semi-dynamic)

- Apply some logic
- Resolvable exclusions
- Lists of exclusions can be updated
- Lends itself to scaling much better (MSSP, SASE, SWG)

Test #2: Remote Origin Server, GET Proxy, Local DNS

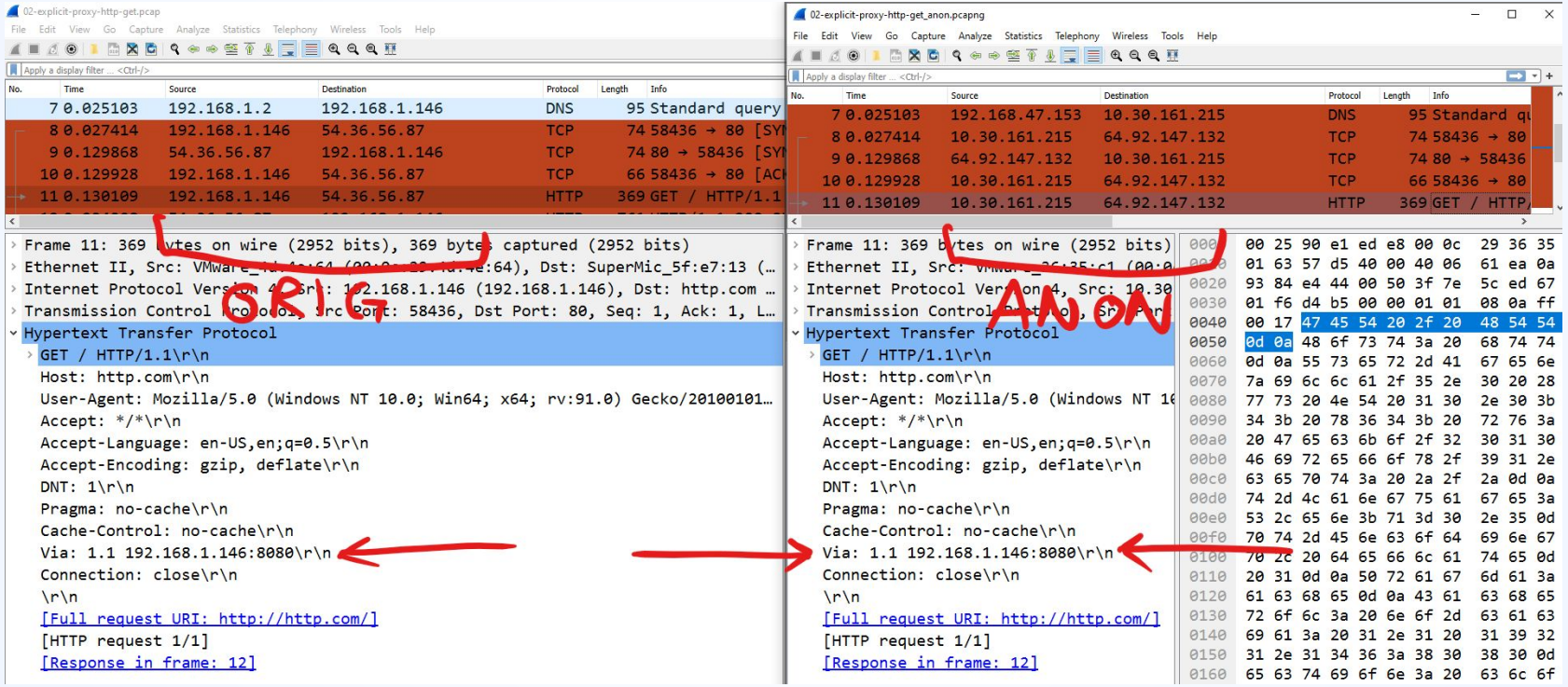
#sf21vus



*omitting empty ACKs

Packets ala TraceWrangler

#sf21vus



Twitter: @PacketJay

#sf21vus

A Word about the “Via: “ Header

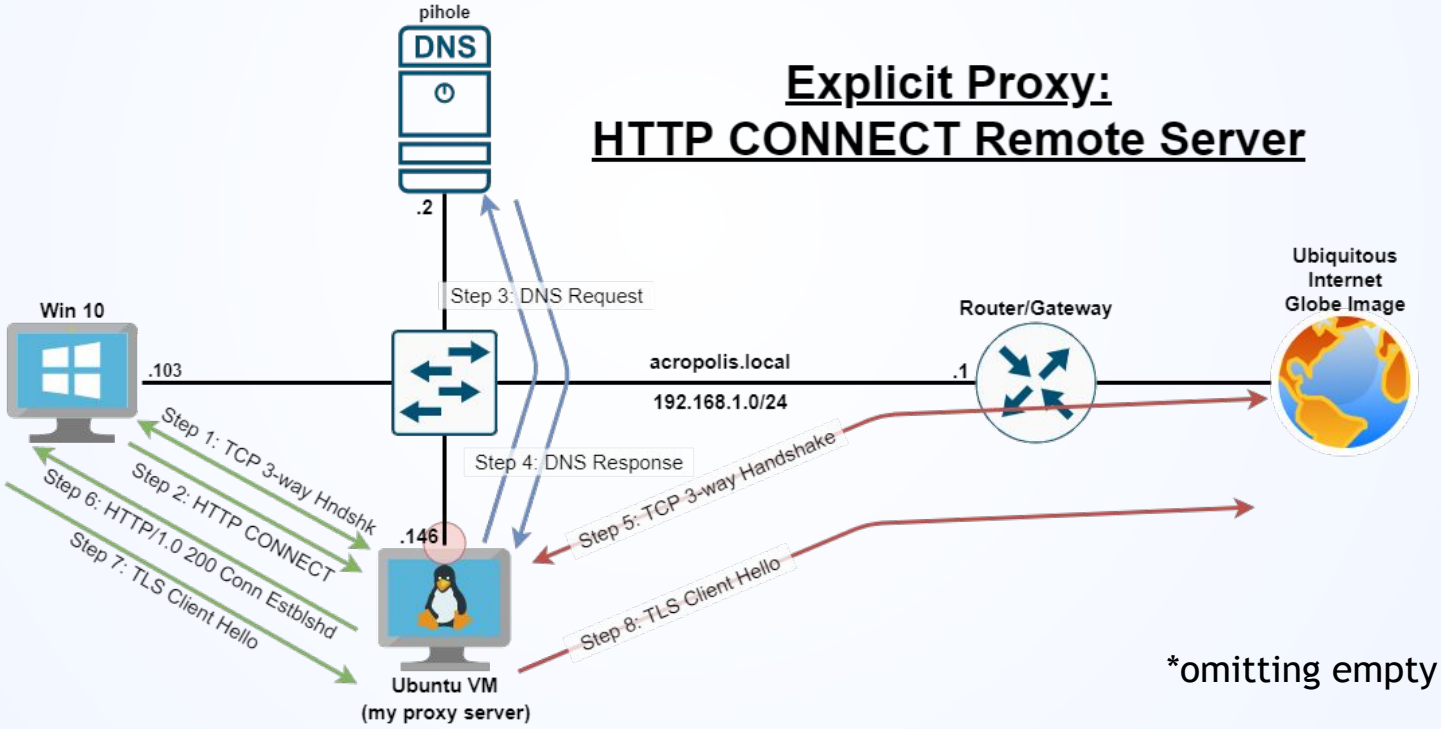
ProxyVia Directive

Description:	Information provided in the `Via` HTTP response header for proxied requests
Syntax:	`ProxyVia On|Off|Full|Block`
Default:	`ProxyVia Off`
Context:	server config, virtual host
Status:	Extension
Module:	mod_proxy

This directive controls the use of the `Via:` HTTP header by the proxy. Its intended use is to control the flow of proxy requests along a chain of proxy servers.

- If set to `Off`, which is the default, no special processing is performed. If a request or reply contains a `Via:` header, it is passed through unchanged.
- If set to `On`, each request and reply will get a `Via:` header line added for the current host.
- If set to `Full`, each generated `Via:` header line will additionally have the Apache httpd server version shown as a `Via:` comment field.
- If set to `Block`, every proxy request will have all its `Via:` header lines removed. No new `Via:` header will be generated.

Test #3: Remote Origin Server, CONNECT Proxy, Local DNS



*omitting empty ACKs

Why is there a PROXY to start with?

- **Assumption:** URL and Content Filtering
- **Liability (Logging and Visibility):** School provided Chromebook, it can't just wild and free exposing all our children to the naught bits.

What's being blocked? (Just a few examples)

- CartoonNetwork.com, showipintbri.com, malware.com

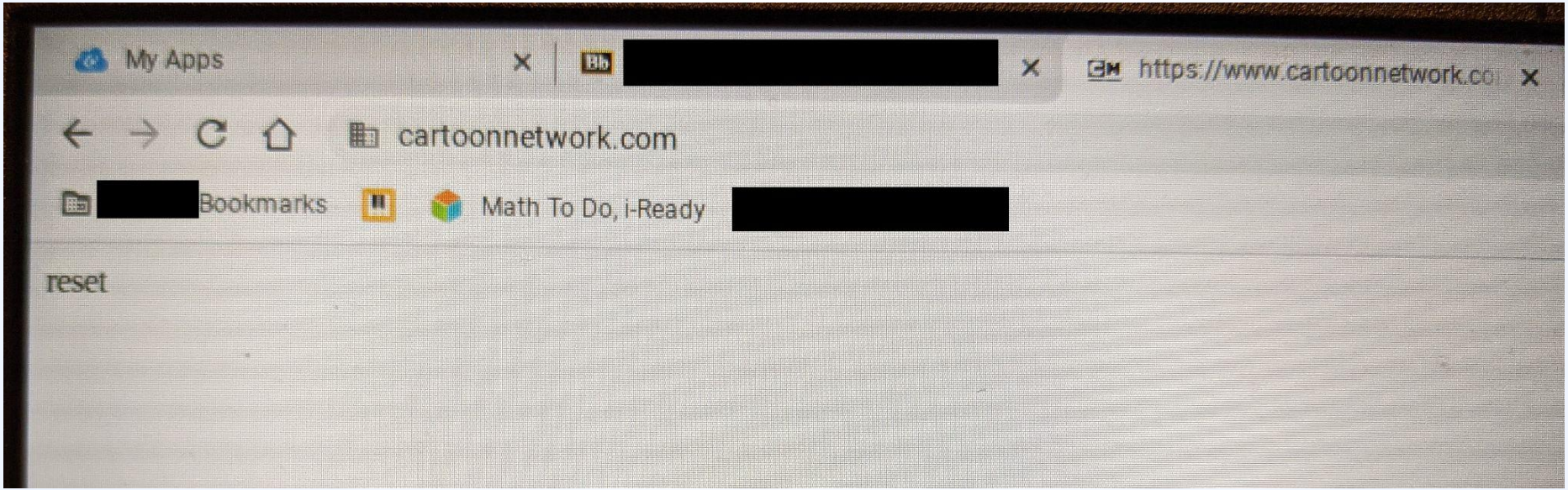
CartoonNetwork.com

#sf21vus

1	0.000000	Chromebook	192.168.1.2	DNS	86	Standard query 0xcada A www.cartoonnetwork.com
2	0.019933	192.168.1.2	Chromebook	DNS	182	Standard query response 0xcada A www.cartoonnetwork
3	0.140406	Chromebook	Cloud Proxy Server	TCP	78	39866 → 8009 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
4	0.170514	Cloud Proxy Server	Chromebook	TCP	78	8009 → 39866 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0
5	0.172512	Chromebook	Cloud Proxy Server	TCP	70	39866 → 8009 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSva
6	0.175511	Chromebook	Cloud Proxy Server	HTTP	910	CONNECT www.cartoonnetwork.com:443 HTTP/1.1
7	0.205619	Cloud Proxy Server	Chromebook	TCP	70	8009 → 39866 [ACK] Seq=1 Ack=841 Win=30720 Len=0 TS
8	0.261622	Cloud Proxy Server	Chromebook	HTTP	109	HTTP/1.1 200 Connection established
9	0.264049	Chromebook	Cloud Proxy Server	TCP	70	39866 → 8009 [ACK] Seq=841 Ack=40 Win=29312 Len=0
10	0.269888	Chromebook	Cloud Proxy Server	TLSv…	587	Client Hello
11	0.298368	Cloud Proxy Server	Chromebook	TCP	70	8009 → 39866 [ACK] Seq=40 Ack=1358 Win=32768 Len=0
12	0.320041	Cloud Proxy Server	Chromebook	TLSv…	169	Hello Retry Request, Change Cipher Spec
13	0.324930	Chromebook	Cloud Proxy Server	TLSv…	593	Change Cipher Spec, Client Hello
14	0.357898	Cloud Proxy Server	Chromebook	TLSv…	1518	Server Hello, Application Data
15	0.357949	Cloud Proxy Server	Chromebook	TCP	1518	8009 → 39866 [ACK] Seq=1587 Ack=1881 Win=34304 Len=
16	0.357951	Cloud Proxy Server	Chromebook	TLSv…	1033	Application Data, Application Data, Application Dat
17	0.360173	Chromebook	Cloud Proxy Server	TCP	70	39866 → 8009 [ACK] Seq=1881 Ack=3998 Win=36992 Len=
18	0.381449	Chromebook	Cloud Proxy Server	TLSv…	128	Application Data

File: DUT-PROXY-cartoonnetwork.pcapng (not included)

CartoonNetwork.com



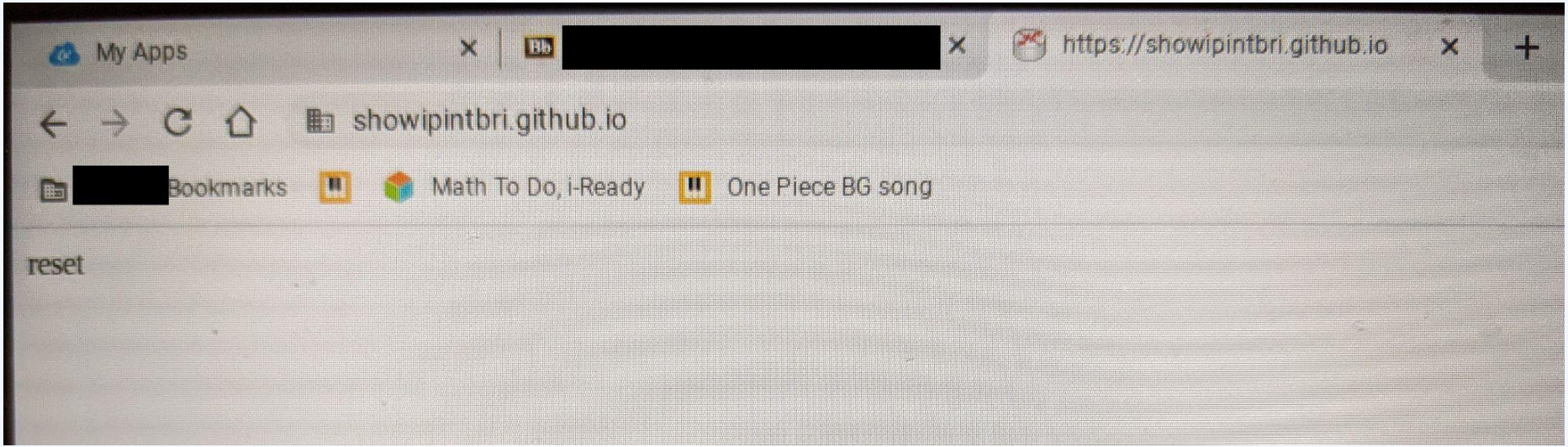
showipintbri.com

#sf21vus

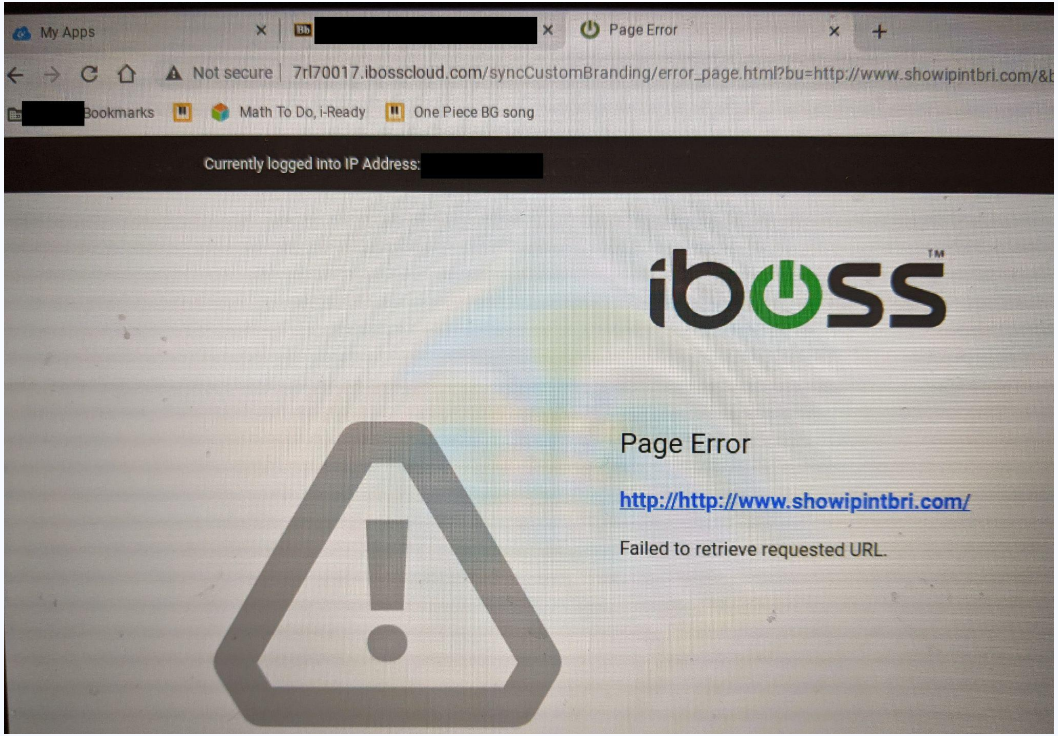
No.	Time	Source	Destination	Protocol	Length	Stream index	Info
1	0.000000	192.168.1.105	192.168.1.2	DNS	80		Standard query 0x8084 A showipintbri.com
2	0.000004	192.168.1.105	192.168.1.2	DNS	86		Standard query 0xe78a A showipintbri.github.io
3	0.000489	192.168.1.2	192.168.1.105	DNS	150		Standard query response 0xe78a A showipintbri.g
4	0.013582	192.168.1.105	149.19.33.56	TCP	78	0	39914 → 8009 [SYN] Seq=0 Win=29200 Len=0 MSS=14
5	0.023215	192.168.1.2	192.168.1.105	DNS	96		Standard query response 0x8084 A showipintbri.c
6	0.036198	149.19.33.56	192.168.1.105	TCP	78	0	8009 → 39914 [SYN, ACK] Seq=0 Ack=1 Win=28960 L
7	0.038063	192.168.1.105	149.19.33.56	TCP	70	0	39914 → 8009 [ACK] Seq=1 Ack=1 Win=29312 Len=0
8	0.043281	192.168.1.105	149.19.33.56	HTTP	910	0	CONNECT showipintbri.github.io:443 HTTP/1.1
9	0.048157	192.168.1.105	149.19.33.56	TCP	78	1	39920 → 8009 [SYN] Seq=0 Win=29200 Len=0 MSS=14
10	0.065013	149.19.33.56	192.168.1.105	TCP	70	0	8009 → 39914 [ACK] Seq=1 Ack=841 Win=30720 Len=
11	0.072271	149.19.33.56	192.168.1.105	TCP	78	1	8009 → 39920 [SYN, ACK] Seq=0 Ack=1 Win=28960 L
12	0.074633	192.168.1.105	149.19.33.56	TCP	70	1	39920 → 8009 [ACK] Seq=1 Ack=1 Win=29312 Len=0
13	0.083019	192.168.1.105	149.19.33.56	HTTP	1153	1	GET http://showipintbri.com/ HTTP/1.1
14	0.093562	149.19.33.56	192.168.1.105	HTTP	109	0	HTTP/1.1 200 Connection established
15	0.095896	192.168.1.105	149.19.33.56	TCP	70	0	39914 → 8009 [ACK] Seq=841 Ack=40 Win=29312 Len
16	0.098287	192.168.1.105	149.19.33.56	TLSv…	587	0	Client Hello
17	0.106739	149.19.33.56	192.168.1.105	TCP	70	1	8009 → 39920 [ACK] Seq=1 Ack=1084 Win=31232 Len
18	0.150985	149.19.33.56	192.168.1.105	TLSv…	169	0	Hello Retry Request, Change Cipher Spec

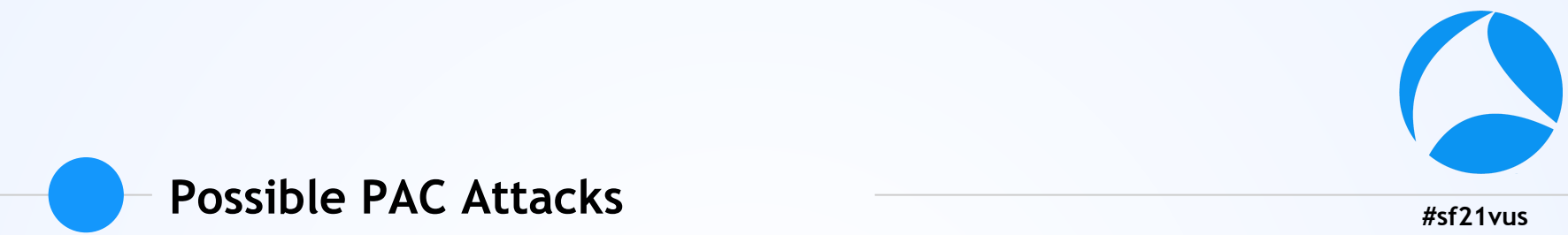
File: DUT-PROXY-showipintbri.pcapng (not included)

showipintbri.com

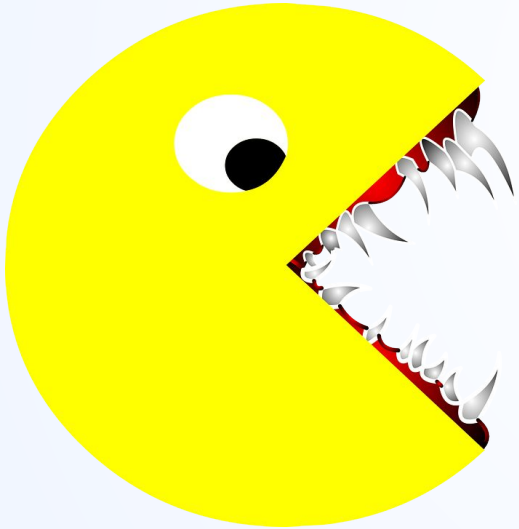


Error Pages


My Apps
Page Error
Not secure
7rl70017.ibosscloud.com/syncCustomBranding/error_page.html?bu=http://www.showipintbri.com/&
Bookmarks
Math To Do, i-Ready
One Piece BG song
Currently logged into IP Address:
iboss
Page Error
http://http://www.showipintbri.com/
Failed to retrieve requested URL.

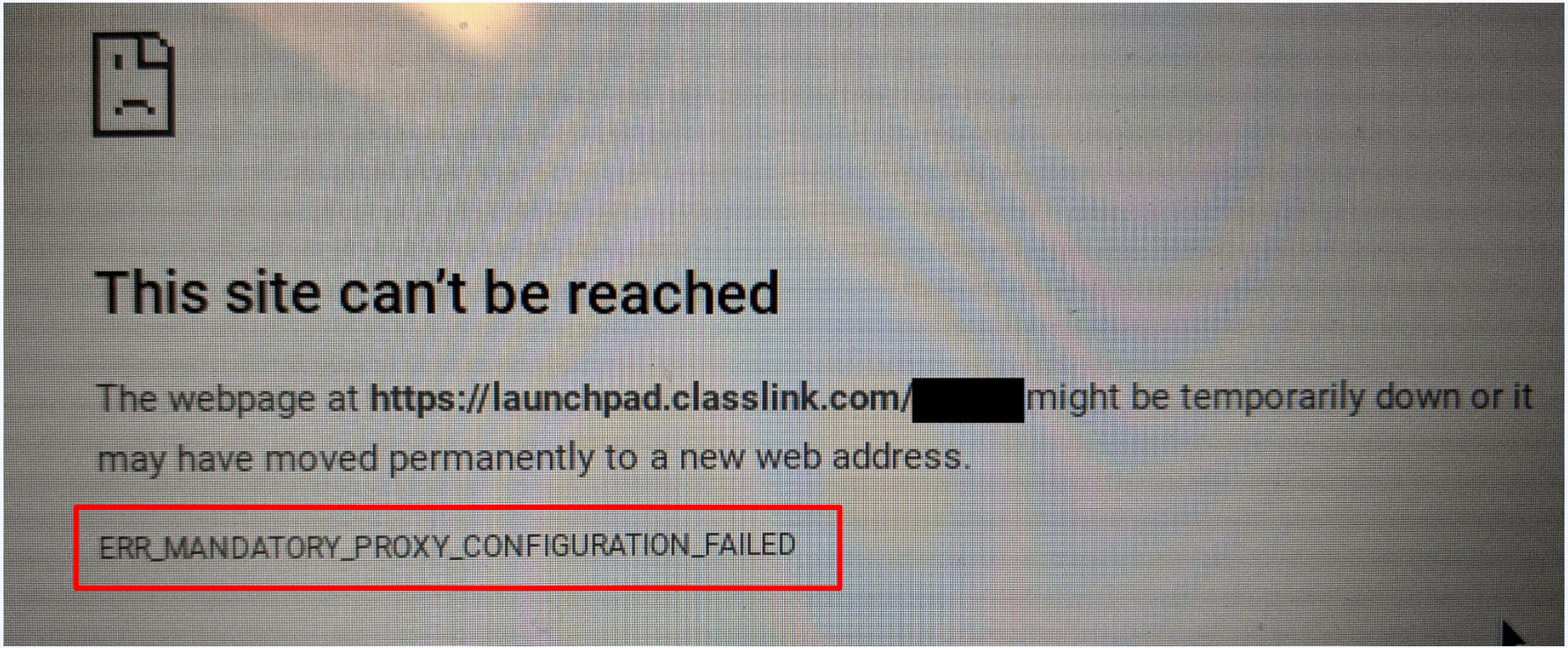


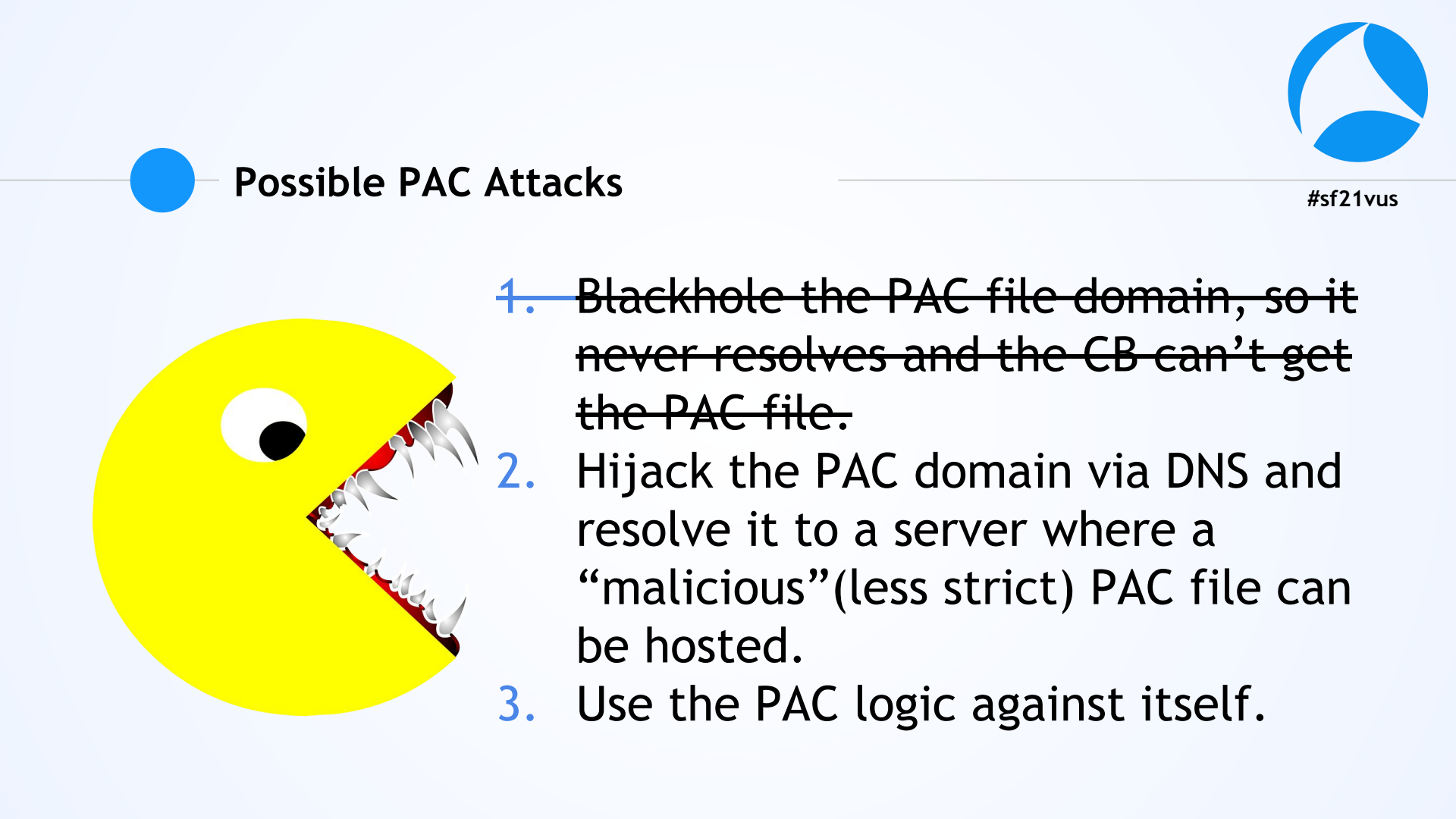
Possible PAC Attacks



1. Blackhole the PAC file domain, so it never resolves and the CB can’t get the PAC file.
2. Hijack the PAC domain via DNS and resolve it to a server where a “malicious”(less strict) PAC file can be hosted.
3. Use the PAC logic against itself.

PAC Attack #1: Blackhole PAC Domain

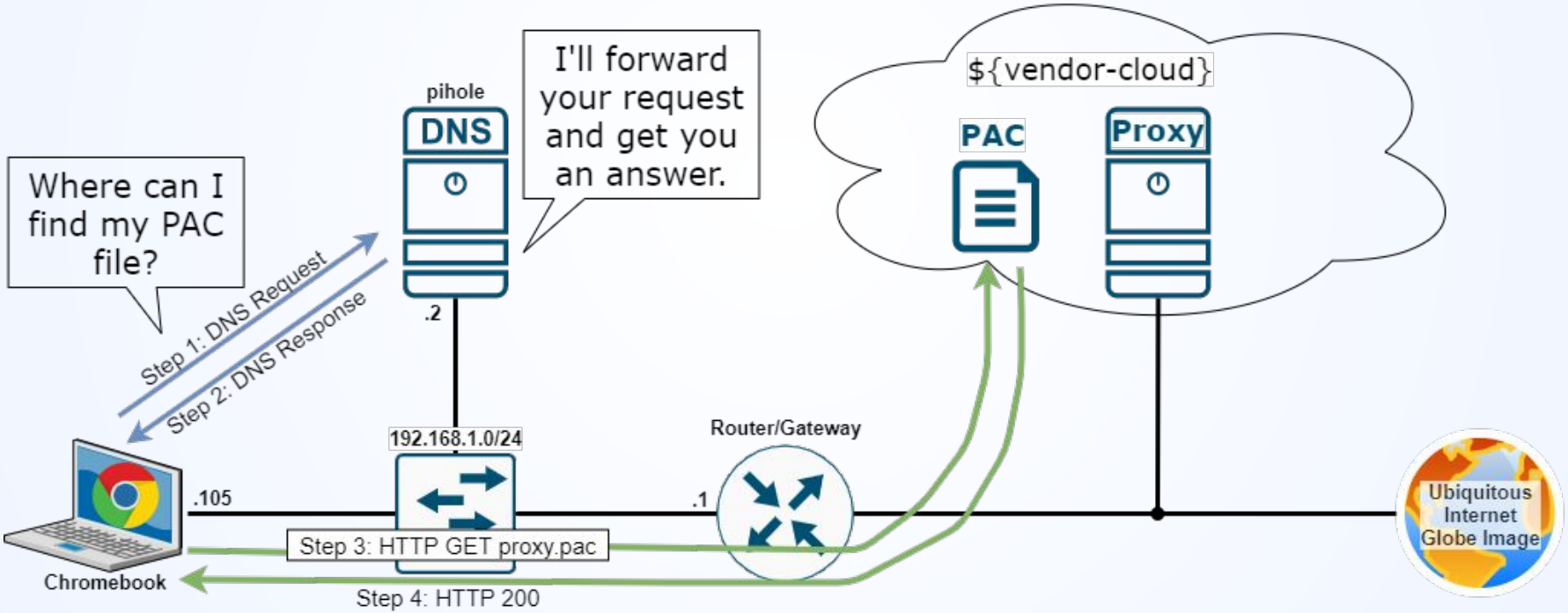




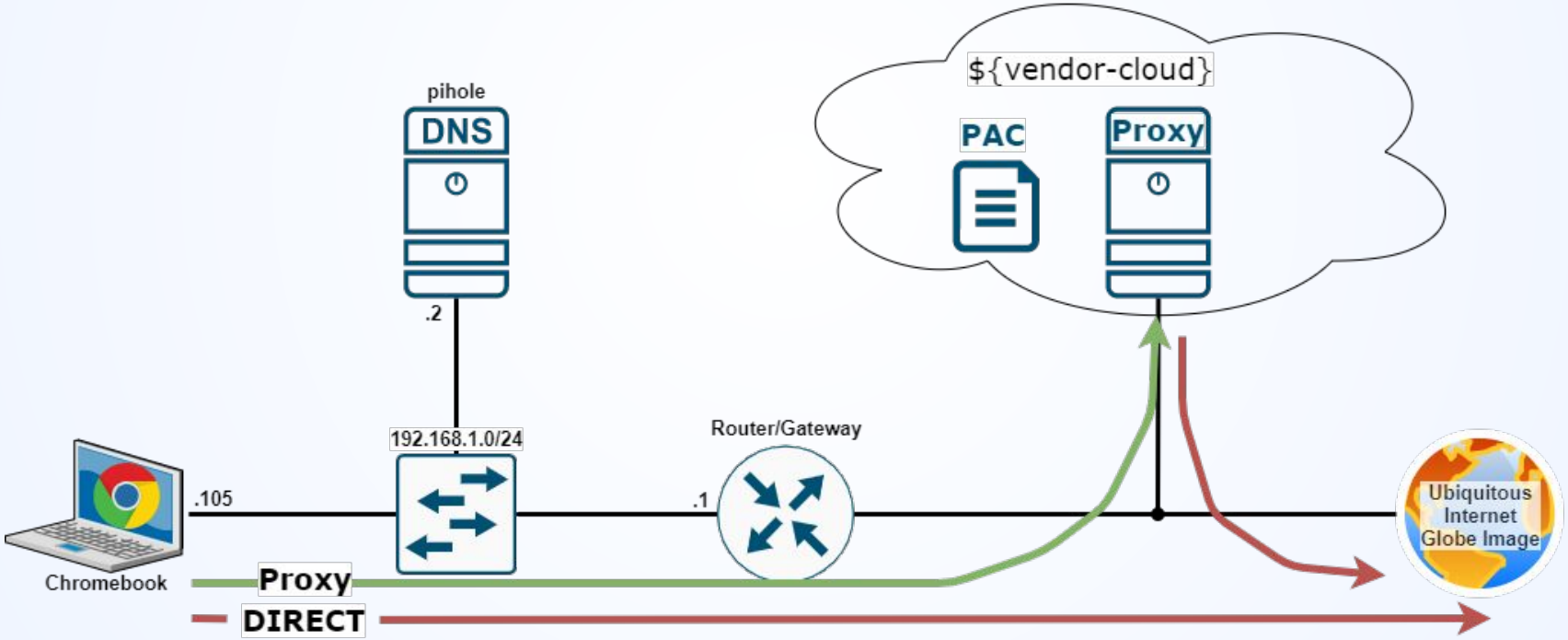
Possible PAC Attacks

1. ~~Blackhole the PAC file domain, so it never resolves and the CB can't get the PAC file.~~
2. Hijack the PAC domain via DNS and resolve it to a server where a "malicious"(less strict) PAC file can be hosted.
3. Use the PAC logic against itself.

PAC Attack #2: What Normally Happens

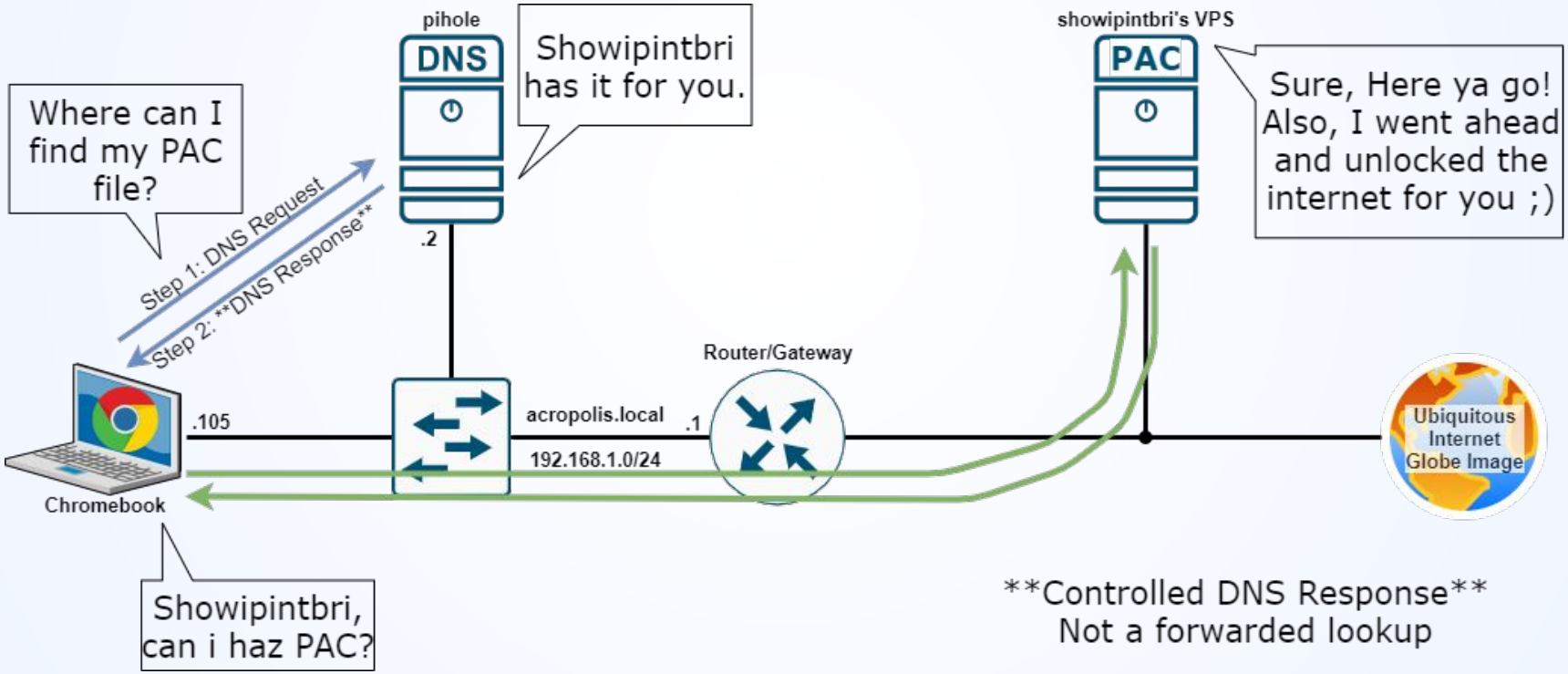


PAC Attack #2: What Normally Happens



PAC Attack #2: Hijack PAC Domain

#sf21vus



My Hosted PAC File :)

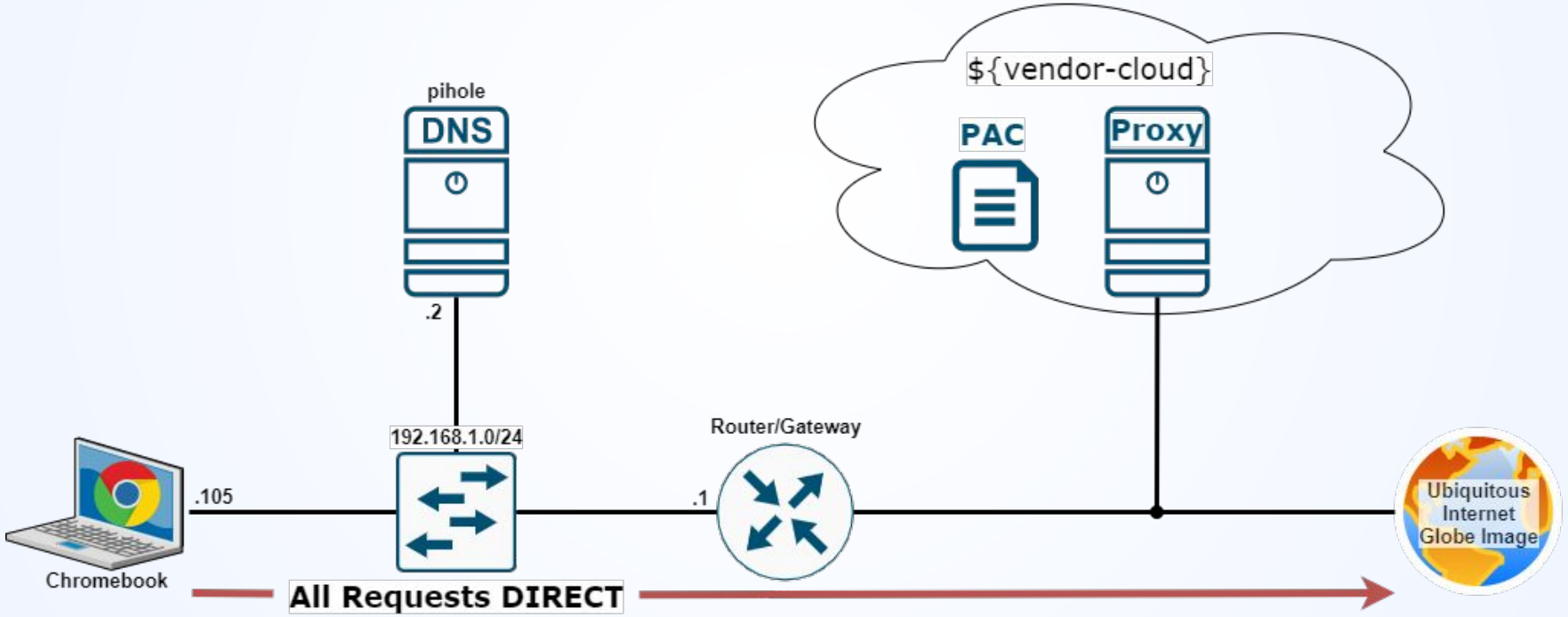

```
function FindProxyForURL(url, host) {

var hostIP = "";

        return "DIRECT";
}
~
```

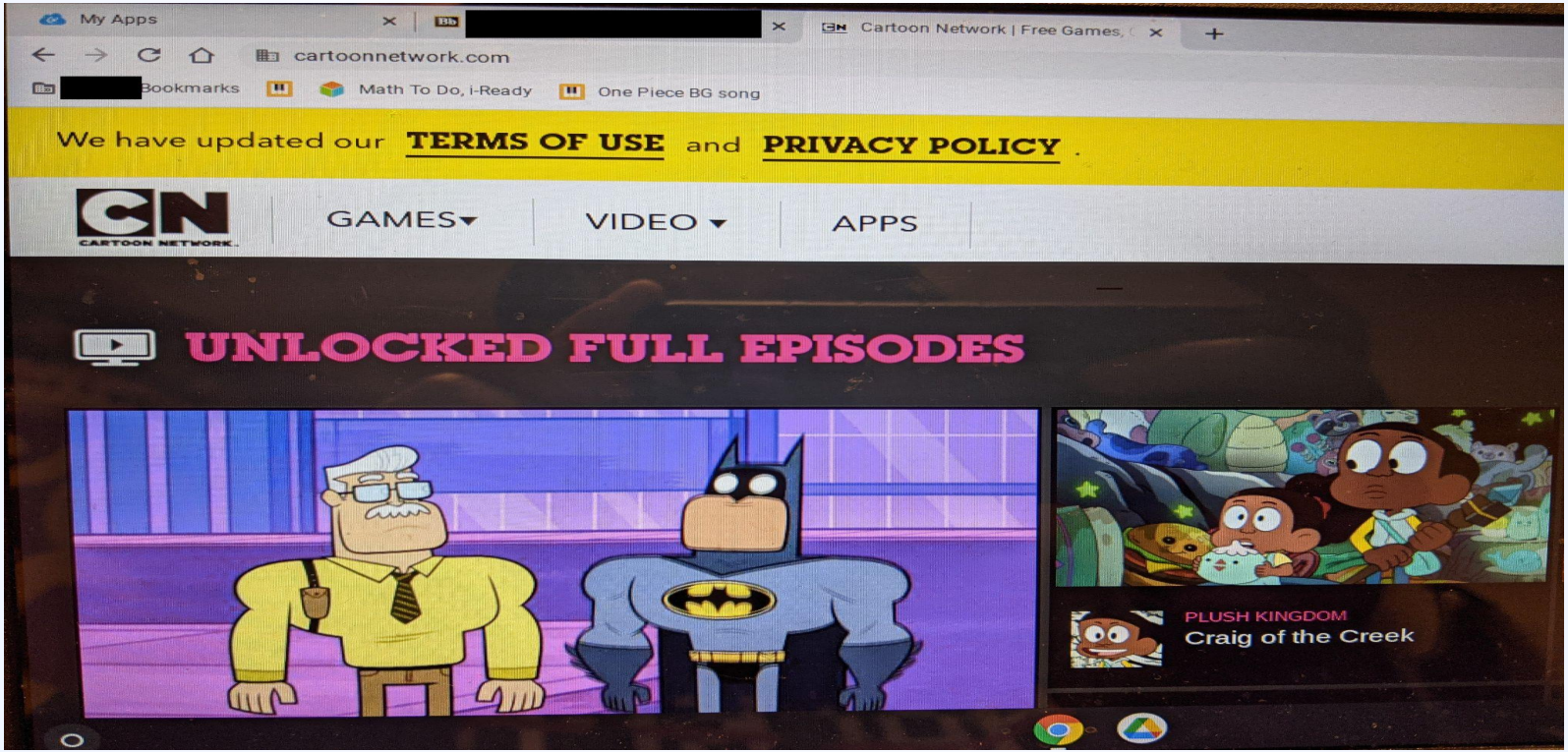
“Here are the keys to your new internet, sir.”

PAC Attack #2: Hijack PAC Domain



PAC Attack #2: CartoonNetwork.com

#sf21vus



#sf21vus

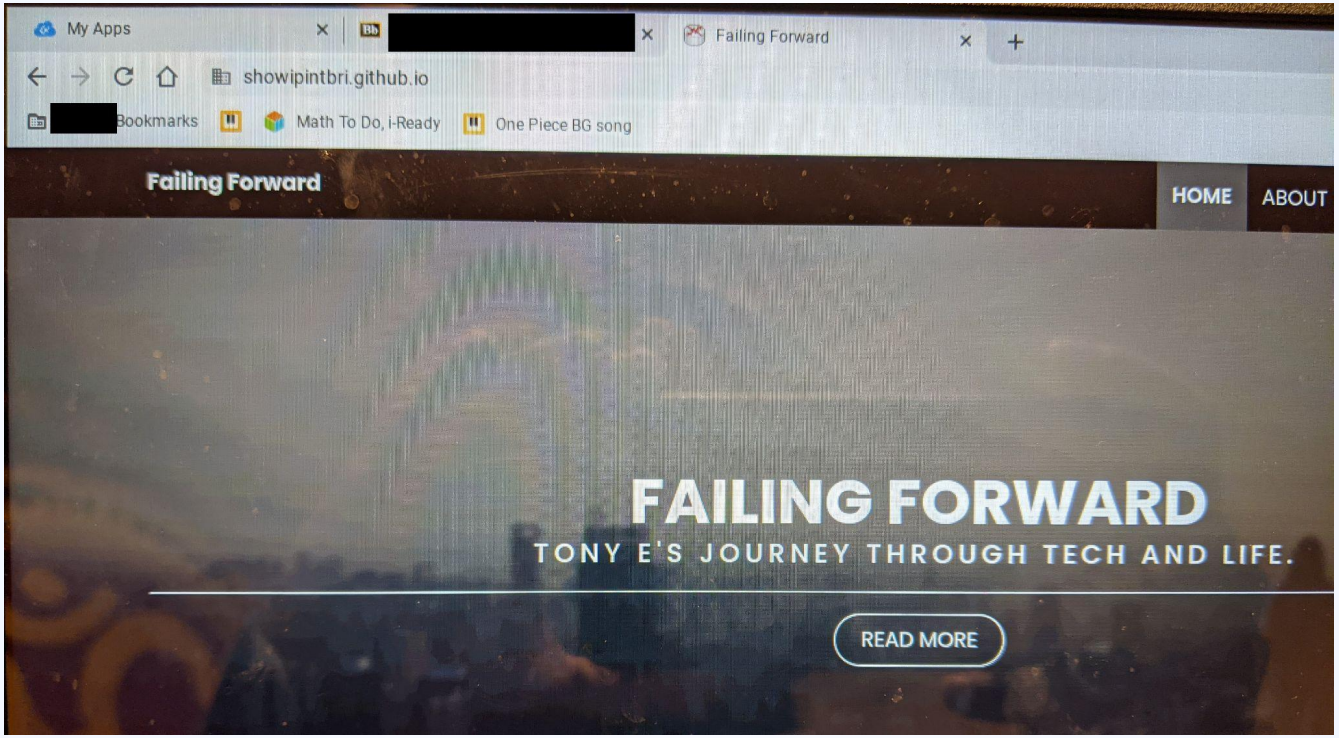
PAC Attack #2: CartoonNetwork.com

No.	Time	Source	Destination	Protocol	Length	Stream index	Info
1	0.000000	Chromebook	192.168.1.2	DNS	86		Standard query 0xfa15 A www.cartoonnetwork.com
2	0.018563	192.168.1.2	Chromebook	DNS	182		Standard query response 0xfa15 A www.cartoonne
3	0.024082	Chromebook	www.cartoonnetwork.com	TCP	78	0	38910 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=14
4	0.032462	www.cartoonnetwork.com	Chromebook	TCP	78	0	443 → 38910 [SYN, ACK] Seq=0 Ack=1 Win=65160 L
5	0.033766	Chromebook	www.cartoonnetwork.com	TCP	70	0	38910 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0
6	0.034963	Chromebook	www.cartoonnetwork.com	TLSv…	587	0	Client Hello
7	0.041003	www.cartoonnetwork.com	Chromebook	TCP	70	0	443 → 38910 [ACK] Seq=1 Ack=518 Win=64768 Len=
8	0.042029	www.cartoonnetwork.com	Chromebook	TLSv…	1518	0	Server Hello, Change Cipher Spec, Application
9	0.042034	www.cartoonnetwork.com	Chromebook	TCP	1518	0	443 → 38910 [PSH, ACK] Seq=1449 Ack=518 Win=64
10	0.042052	www.cartoonnetwork.com	Chromebook	TCP	1270	0	443 → 38910 [PSH, ACK] Seq=2897 Ack=518 Win=64
11	0.043278	www.cartoonnetwork.com	Chromebook	TCP	1518	0	443 → 38910 [ACK] Seq=4097 Ack=518 Win=64768 L
12	0.045177	Chromebook	www.cartoonnetwork.com	TCP	70	0	38910 → 443 [ACK] Seq=518 Ack=2897 Win=35072 L
13	0.045179	Chromebook	www.cartoonnetwork.com	TCP	70	0	38910 → 443 [ACK] Seq=518 Ack=4097 Win=37888 L
14	0.045180	Chromebook	www.cartoonnetwork.com	TCP	70	0	38910 → 443 [ACK] Seq=518 Ack=5545 Win=40832 L
15	0.052896	www.cartoonnetwork.com	Chromebook	TLSv…	1518	0	Application Data [TCP segment of a reassembled
16	0.052902	www.cartoonnetwork.com	Chromebook	TLSv…	263	0	Application Data, Application Data
17	0.054856	Chromebook	www.cartoonnetwork.com	TCP	70	0	38910 → 443 [ACK] Seq=518 Ack=7186 Win=44160 L
18	0.093309	Chromebook	www.cartoonnetwork.com	TLSv…	150	0	Change Cipher Spec, Application Data

File: DUT-DIRECT-cartoonnetwork.pcapng

#sf21vus

PAC Attack #2: showipintbri.com

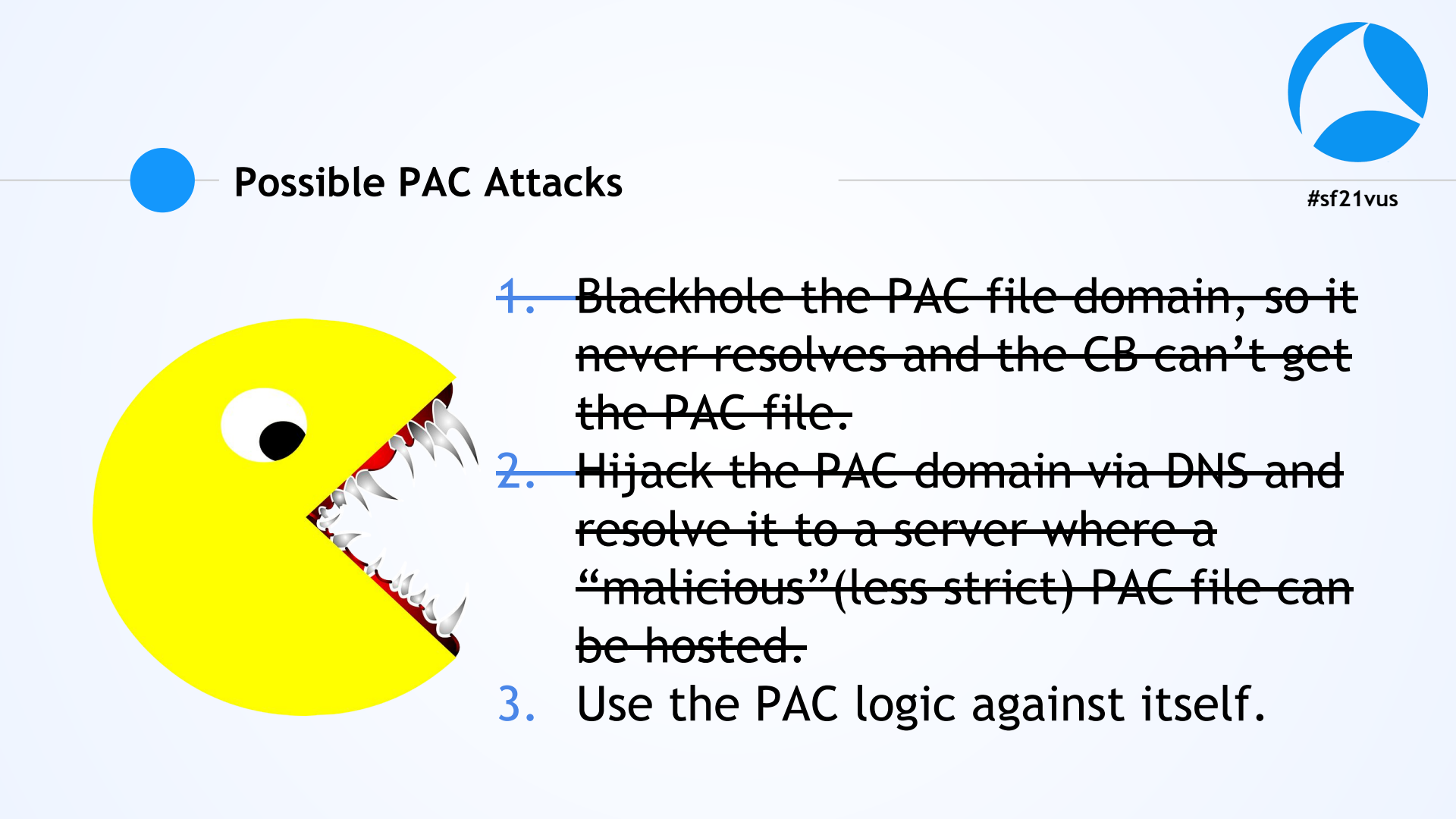


PAC Attack #2: showipintbri.com

#sf21vus

No.	Time	Source	Destination	Protocol	Length	Stream index	Info
1	0.000000	Chromebook	192.168.1.2	DNS	80		Standard query 0xe3a6 A showipintbri.com
2	0.000008	Chromebook	192.168.1.2	DNS	86		Standard query 0xc8bc A showipintbri.github.io
3	0.020680	192.168.1.2	Chromebook	DNS	96		Standard query response 0xe3a6 A showipintbri.c
4	0.020983	192.168.1.2	Chromebook	DNS	150		Standard query response 0xc8bc A showipintbri.g
5	0.034347	Chromebook	showipintbri.github.io	TCP	78	0	34962 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=146
6	0.034632	Chromebook	NameCheap Redirect	TCP	78	1	42170 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
7	0.042797	showipintbri.github.io	Chromebook	TCP	78	0	443 → 34962 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
8	0.044660	Chromebook	showipintbri.github.io	TCP	70	0	34962 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 T
9	0.046987	Chromebook	showipintbri.github.io	TLSv…	587	0	Client Hello
10	0.054482	showipintbri.github.io	Chromebook	TCP	70	0	443 → 34962 [ACK] Seq=1 Ack=518 Win=139776 Len=
11	0.056401	showipintbri.github.io	Chromebook	TLSv…	1450	0	Server Hello, Change Cipher Spec, Application D
12	0.056423	showipintbri.github.io	Chromebook	TCP	1450	0	443 → 34962 [ACK] Seq=1381 Ack=518 Win=139776 L
13	0.056424	showipintbri.github.io	Chromebook	TLSv…	1450	0	Application Data, Application Data, Application
14	0.056425	showipintbri.github.io	Chromebook	TLSv…	215	0	Application Data
15	0.058084	Chromebook	showipintbri.github.io	TCP	70	0	34962 → 443 [ACK] Seq=518 Ack=4286 Win=37888 Le
16	0.111712	NameCheap Redirect	Chromebook	TCP	78	1	80 → 42170 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len
17	0.113616	Chromebook	NameCheap Redirect	TCP	70	1	42170 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TS
18	0.157652	Chromebook	showipintbri.github.io	TLSv…	134	0	Change Cipher Spec, Application Data

File: DUT-DIRECT-showipintbri.pcapng



Possible PAC Attacks

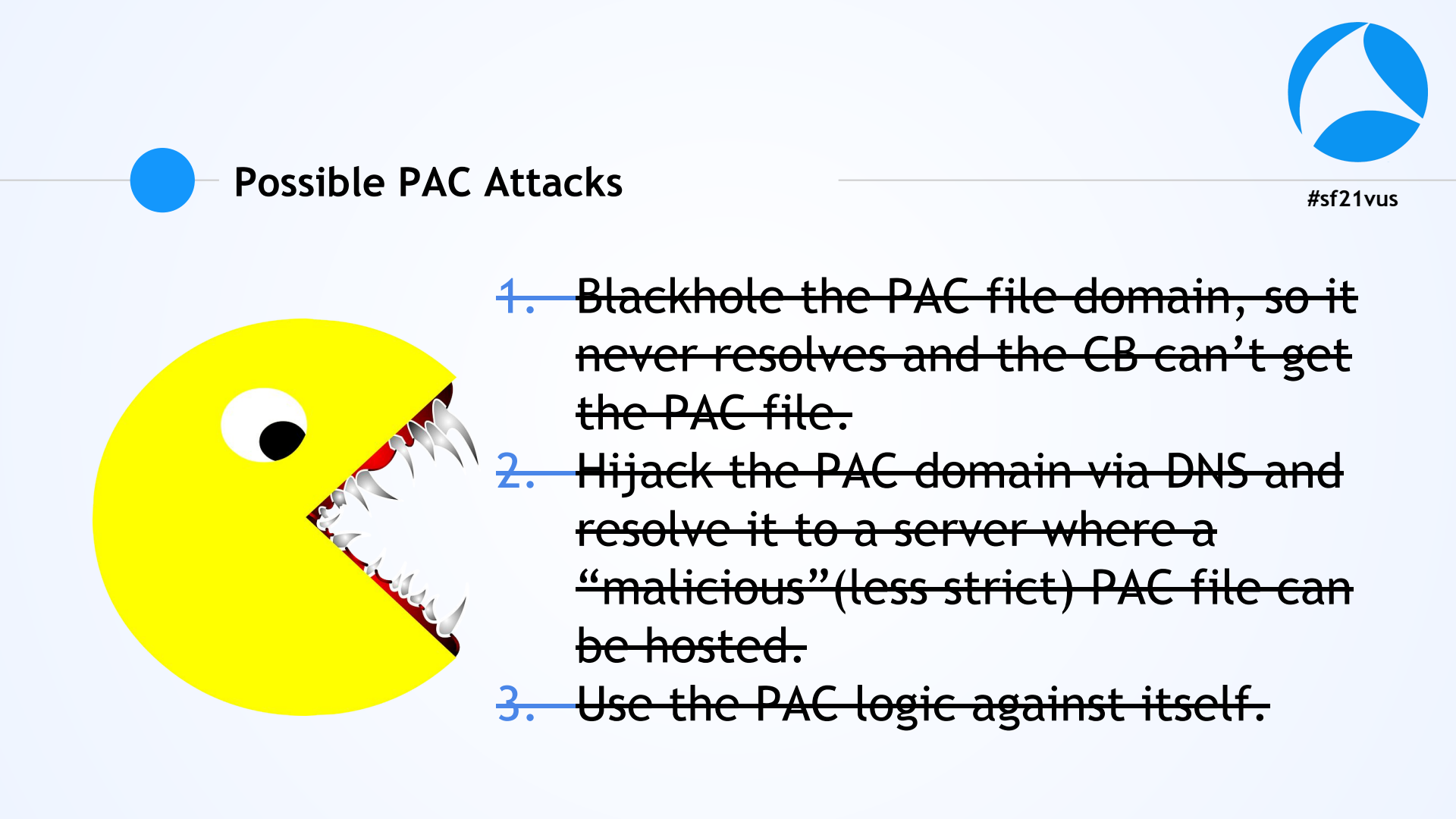
1. ~~Blackhole the PAC file domain, so it never resolves and the CB can't get the PAC file.~~
2. ~~Hijack the PAC domain via DNS and resolve it to a server where a "malicious"(less strict) PAC file can be hosted.~~
3. Use the PAC logic against itself.

Using the PAC Logic Against Itself


```
function FindProxyForURL(url, host) {

var hostIP = "";
var ibsrcip = "xx.xx.xx.xx";
var ibcountry = "US"; // (xx.xxx,-xx.xxx)";
/*  */
if ((shExpMatch(host, "msftncsi.com") || shExpMatch(host, "*.msftncsi.com")) ||
    (shExpMatch(host, "meet.google.com") || shExpMatch(host, "*.meet.google.com")) ||
    (shExpMatch(host, "accounts.google.com") || shExpMatch(host, "*.accounts.google.com")) |
    (shExpMatch(host, "classroom.google.com") || shExpMatch(host, "*.classroom.google.com"))
```

Example Misconfiguration: “*msftncsi.com”



Possible PAC Attacks

1. ~~Blackhole the PAC file domain, so it never resolves and the CB can't get the PAC file.~~
2. ~~Hijack the PAC domain via DNS and resolve it to a server where a "malicious"(less strict) PAC file can be hosted.~~
3. ~~Use the PAC logic against itself.~~

DNS Validity: Oops! 😜

- I made a mistake during preparation for this presentation and setup a test domain in my local resolver using an “_”.
- I could resolve it, ping it, browse the web page locally from my workstation.
- When trying from the chromebook it would resolve but wouldn’t even try to connect via HTTP

Assumption

- Your gateway is more permissive than your proxy server

Takeaways, Part 1

- Just because something is proxied, doesn’t mean we can’t see it, play with it, manipulate it.
- This is not exploiting a technical vulnerability, rather it is exploiting “implied trust”:
  - Chromebook trusts: DNS, PAC file server host, and data of the PAC file
  - There’s no validation or authentication.

I couldn’t have said it better...

#sf21vus

> Communication to HTTP proxy servers is insecure, meaning proxied http:// requests are sent in the clear. When proxying https:// requests through an HTTP proxy, the TLS exchange is forwarded through the proxy using the CONNECT method, so end-to-end encryption is not broken. However when establishing the tunnel, the hostname of the target URL is sent to the proxy server in the clear.

Reference: https://chromium.googlesource.com/chromium/src/+/main/net/docs/proxy.md

Takeaways, Part 2

- If you can control DNS, you can deliver an untrusted PAC file
- If you control the PAC file you can avoid the proxy, exposing a possibly less secure communications channel.
- If you can read the PAC file, you can use that data against itself.

In Conclusion...

#sf21vus

Hypothesis:

It is possible to circumvent the web controls on a managed Chromebook using only the network?

Cheers!

Links/Resources:

- http://findproxyforurl.com/pac-functions/
- https://chromium.googlesource.com/chromium/src/+/main/net/docs/proxy.md
- https://github.com/GrrrDog/weird_proxies
- https://showipintbri.github.io

#sf21vus

Thank You

FIN