black hat® USA 2013

Universal DDoS Mitigation Bypass

Network Threats Information Sharing and Analysis Center

BLOODSPEAR LABORATORIES

NEXUSGUARD™

DDoS Mitigation Lab

About Us

Network Threats Information Sharing and Analysis Center

BLOODSPEAR LABORATORIES

Industry body formed to foster synergy among stakeholders to promote advancement in DDoS defense knowledge.

NEXUSGUARD™

DDoS Mitigation Lab

Independent academic R&D division of Nexusguard building next generation DDoS mitigation knowledge and collaborate with the defense community.

Outline

- DDoS Attack Categories
- DDoS Detection and Mitigation Techniques
  - How they work?
  - How to bypass / take advantage?
- DDoS Mitigation Bypass
  - How to use our PoC tool?
  - PoC tool capability
- Next-Generation Mitigation

Financial Impact

VOLUME:
> 20GBPS

FREQUENCY:
> 2.5MIL
PER YEAR

COMPLEXITY:
APP LEVEL > 30%

COST:
> US$6MIL
PER HOUR

Source: NTT Communications,
“Successfully Combating DDoS Attacks”, Aug 2012

Volumetric Attacks

- Packet-Rate-Based
- Bit-Rate-Based

Semantic Attacks

APPLICATION LEVEL ATTACKS!

API attacks

Hash DoS

Apache Killer

Teardrop

(old textbook example)

Slowloris / RUDY

SYN Flood

(old textbook example)

Smurf

(old textbook example)

PROTOCOL ATTACKS!

Blended Attacks

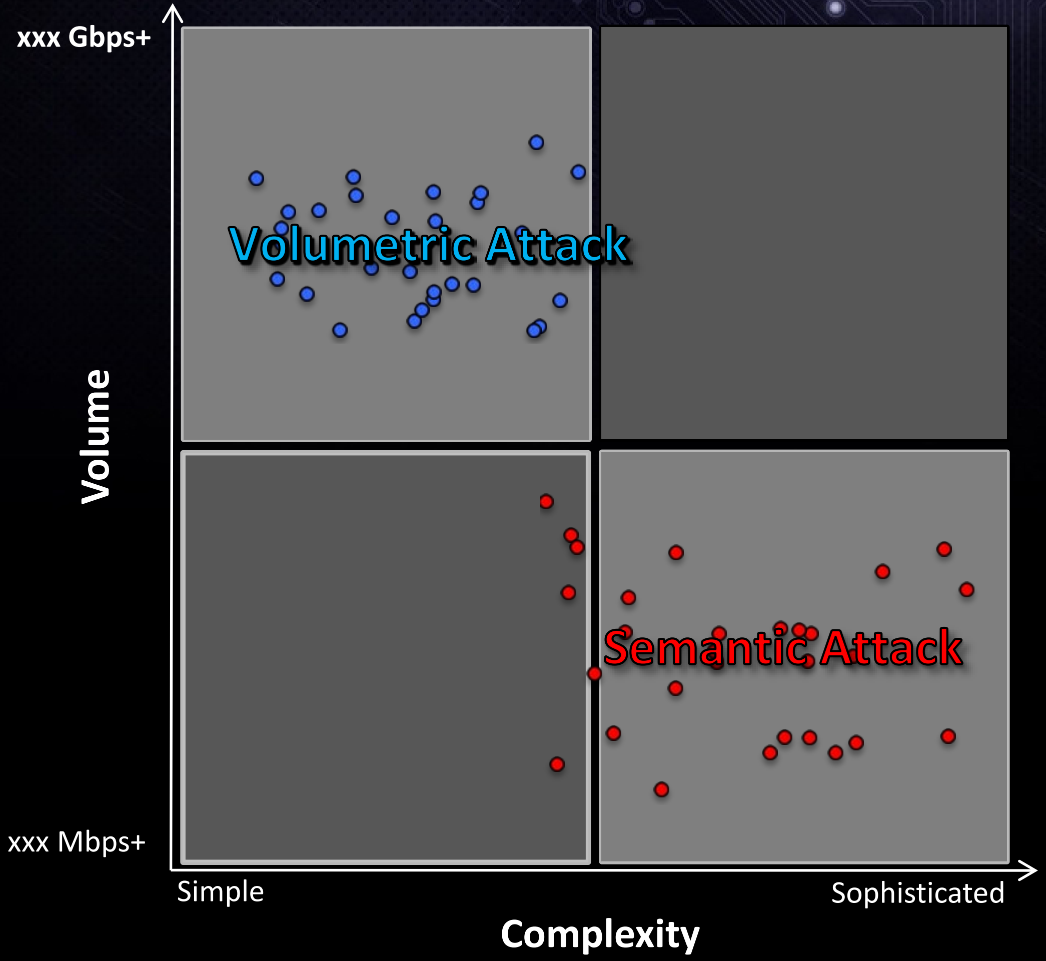
© Mike Boike

BLENDING

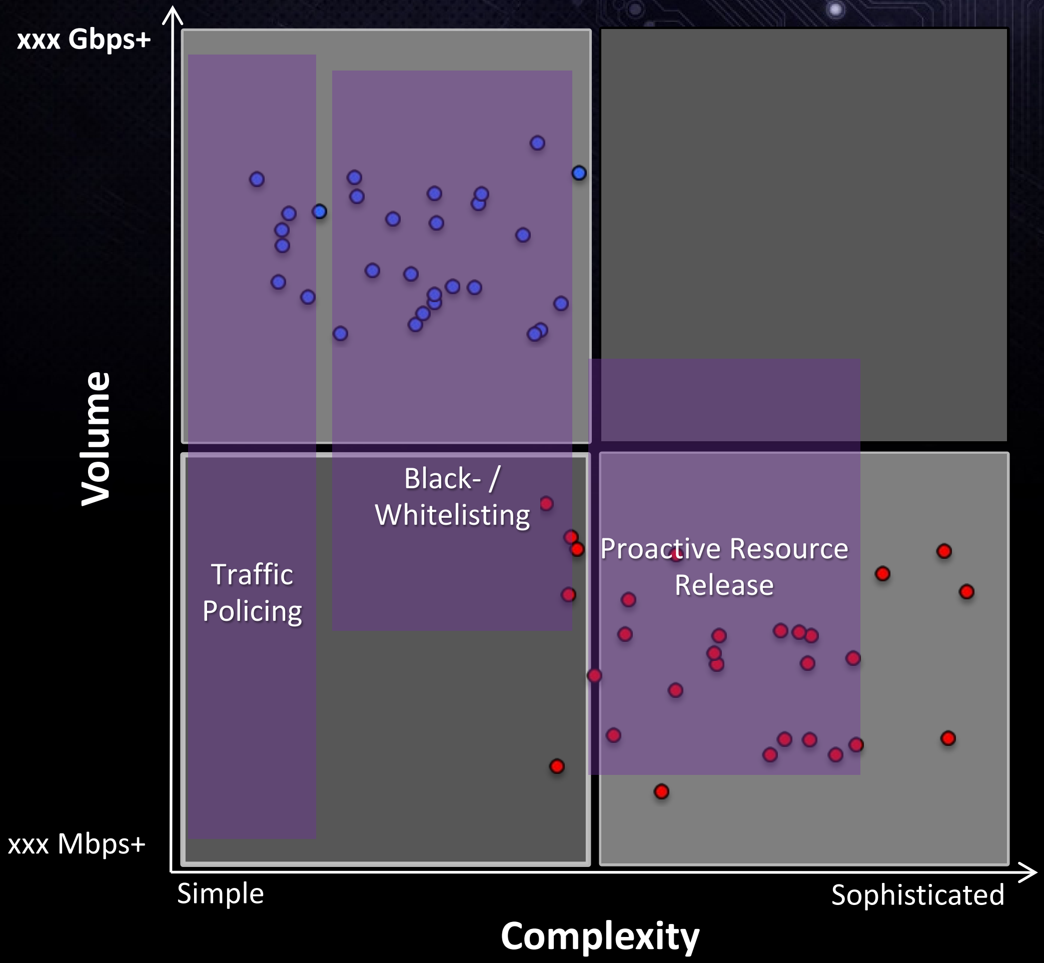
IT REALLY WORKS!

ADMIT IT, YOU DID NOT NOTICE HIM AT FIRST.

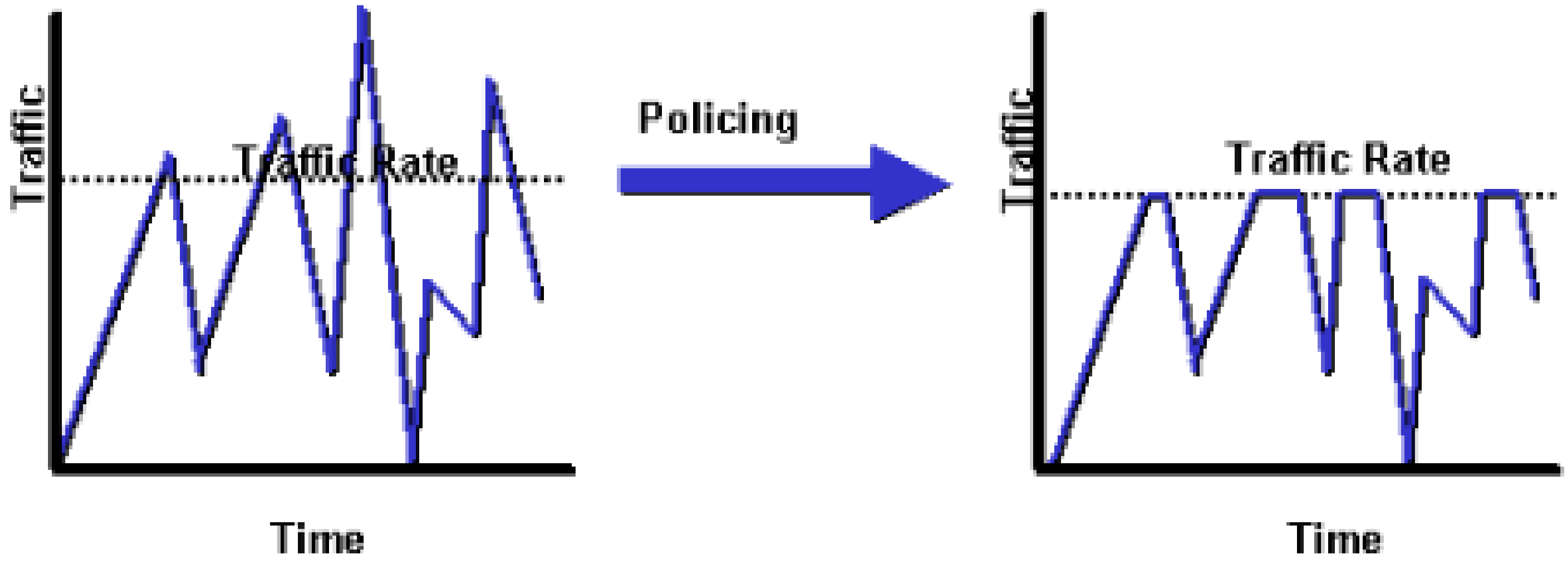
Attack Quadrant



DDoS Mitigations

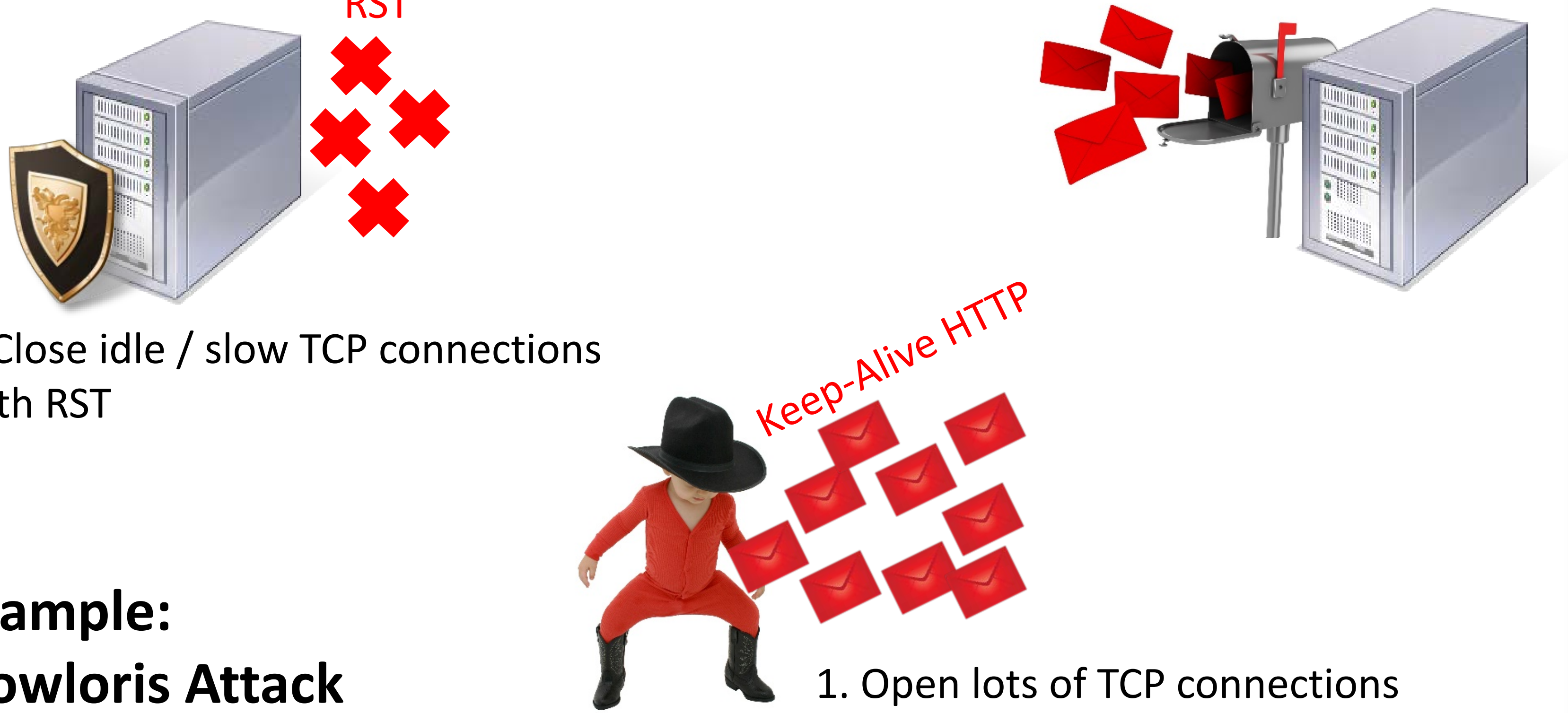


DDoS Mitigation: Traffic Policing



Source: Cisco

DDoS Mitigation: Proactive Resource Release



3. Detect idle / slow TCP connections

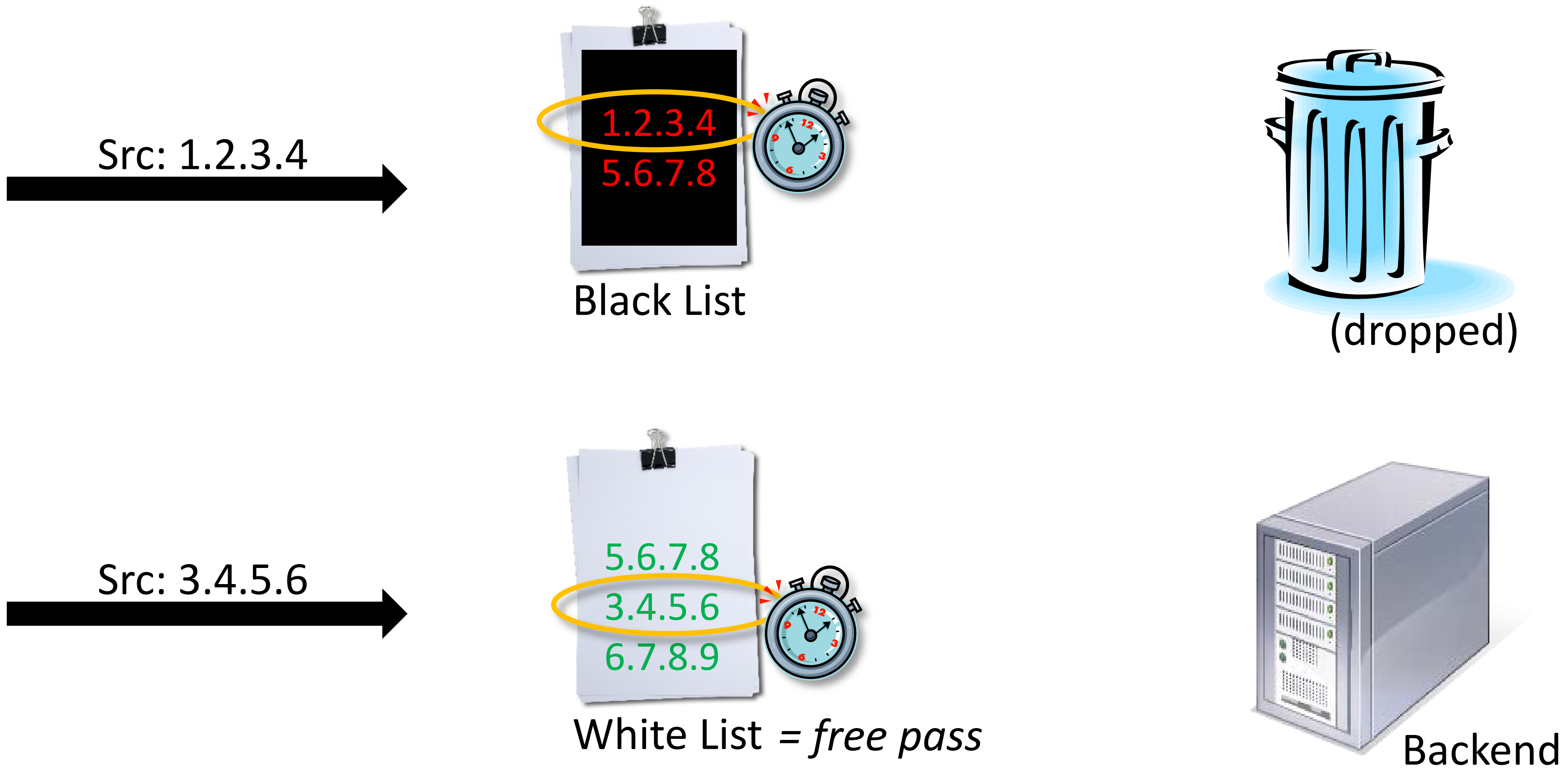
2. TCP connection pool starved

4. Close idle / slow TCP connections
With RST

1. Open lots of TCP connections

Example:
Slowloris Attack

DDoS Mitigation: Black- / Whitelisting



Src: 1.2.3.4

Black List

1.2.3.4
5.6.7.8

(dropped)

Src: 3.4.5.6

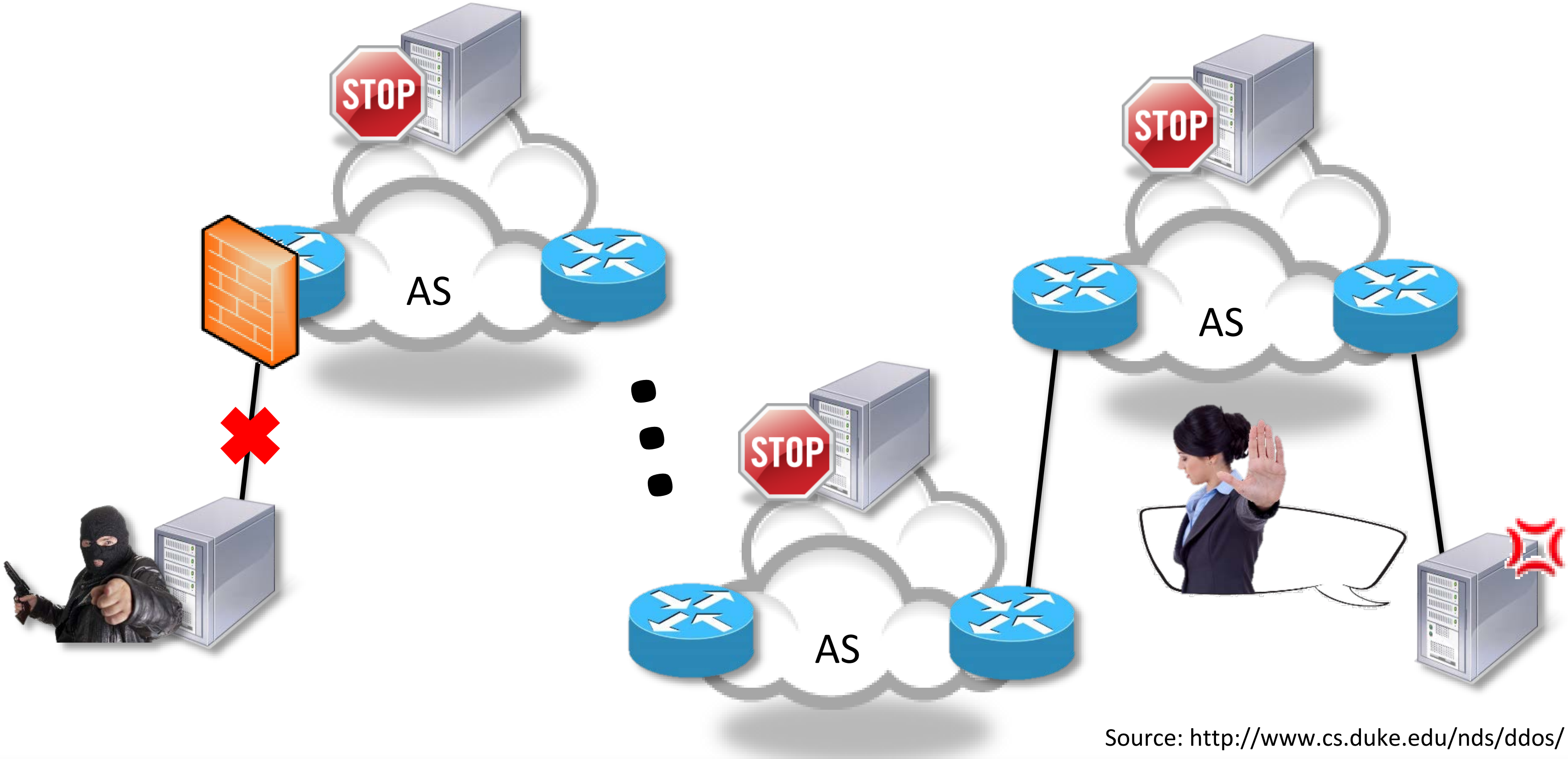
5.6.7.8
3.4.5.6
6.7.8.9

White List = *free pass*

Backend

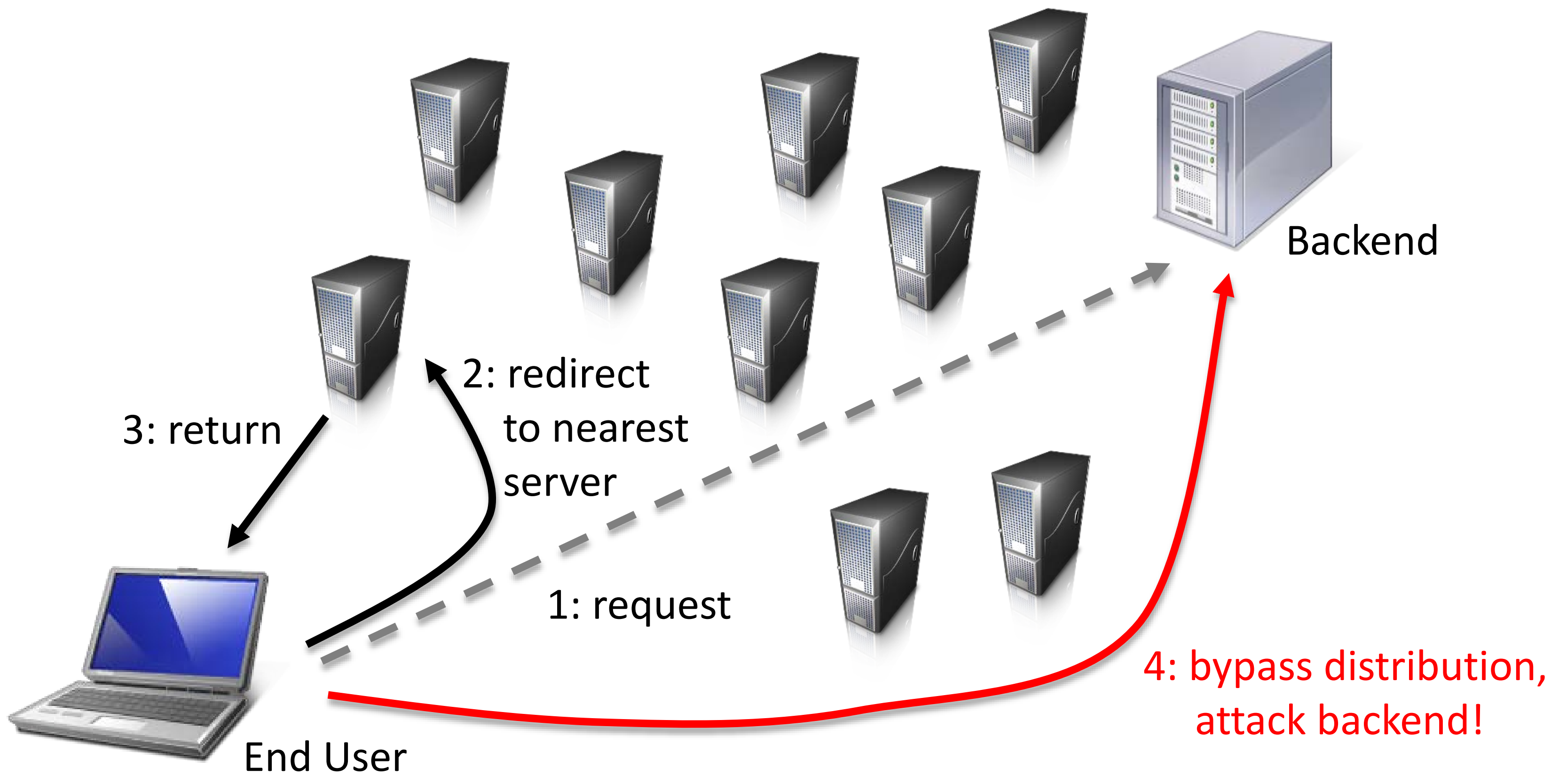
(for awhile / for x amount of volume)

DDoS Mitigation: Source Isolation



Source: http://www.cs.duke.edu/nds/ddos/

DDoS Solution: Secure CDN



Backend

2: redirect to nearest server

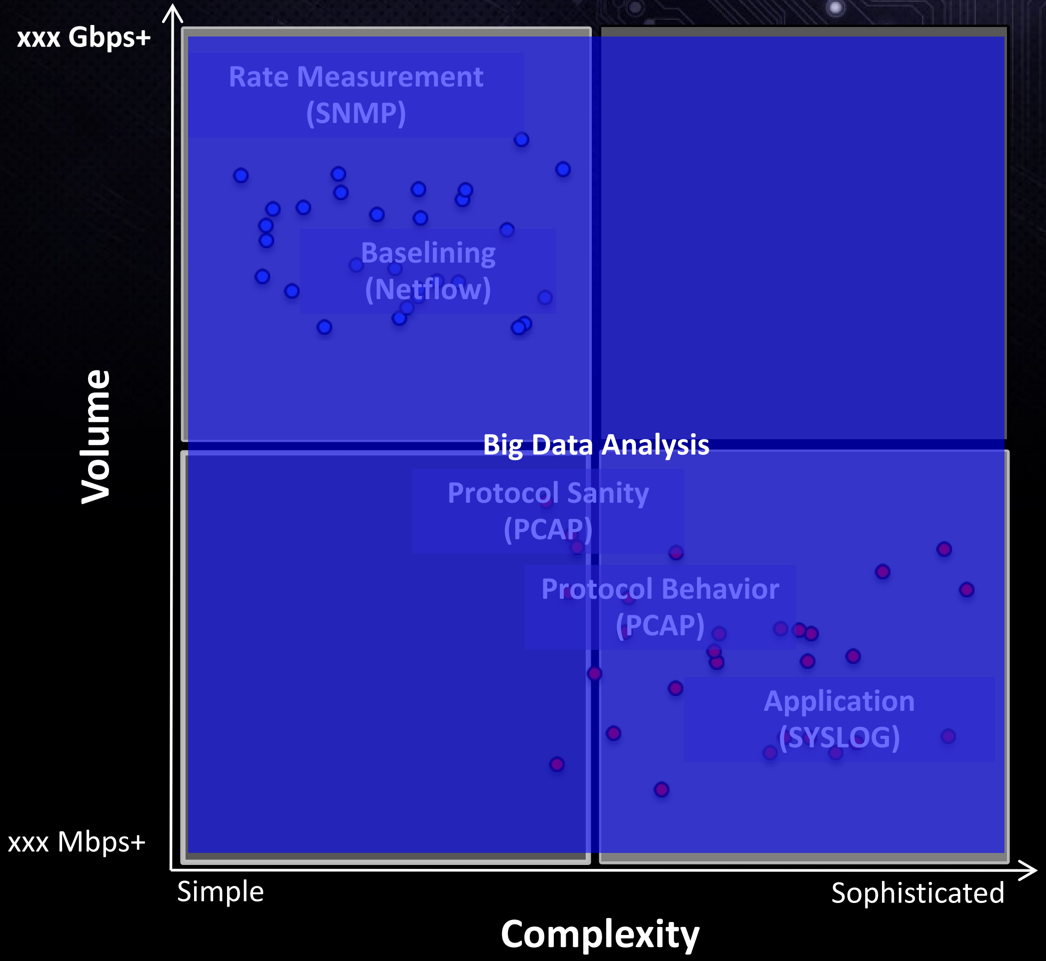
3: return

1: request

4: bypass distribution, attack backend!

End User

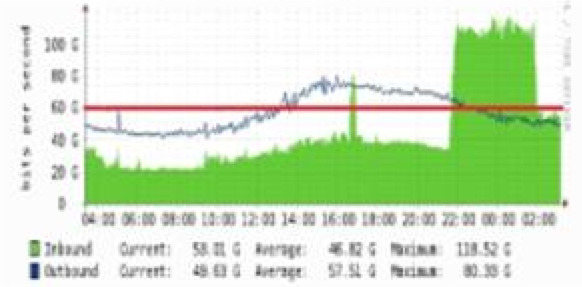
DDoS Detection



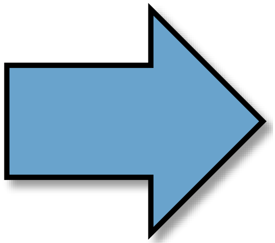
Rate- / Flow-Based Countermeasures

Detection

Rate Measurment



Baseline Enforcement



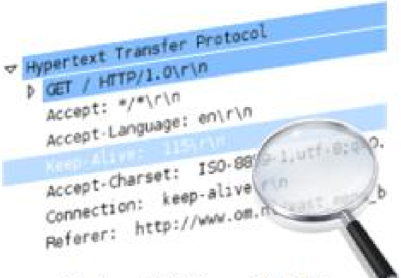
Mitigation

Protocol-Based Countermeasures

Detection

Protocol Sanity Checking

Protocol Behavior Checking



```
▽ Hypertext Transfer Protocol
  ▷ GET / HTTP/1.0\r\n
    Accept: */*\r\n
    Accept-Language: en\r\n
    Keep-Alive: 115\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.
    Connection: keep-alive\r\n
    Referer: http://www.om.n
```

Protocol Pattern Matching

Mitigation

Blanket Countermeasures

Detection

Traffic Statistics and Behavior
Big Data Analysis

Malicious Source Intelligence

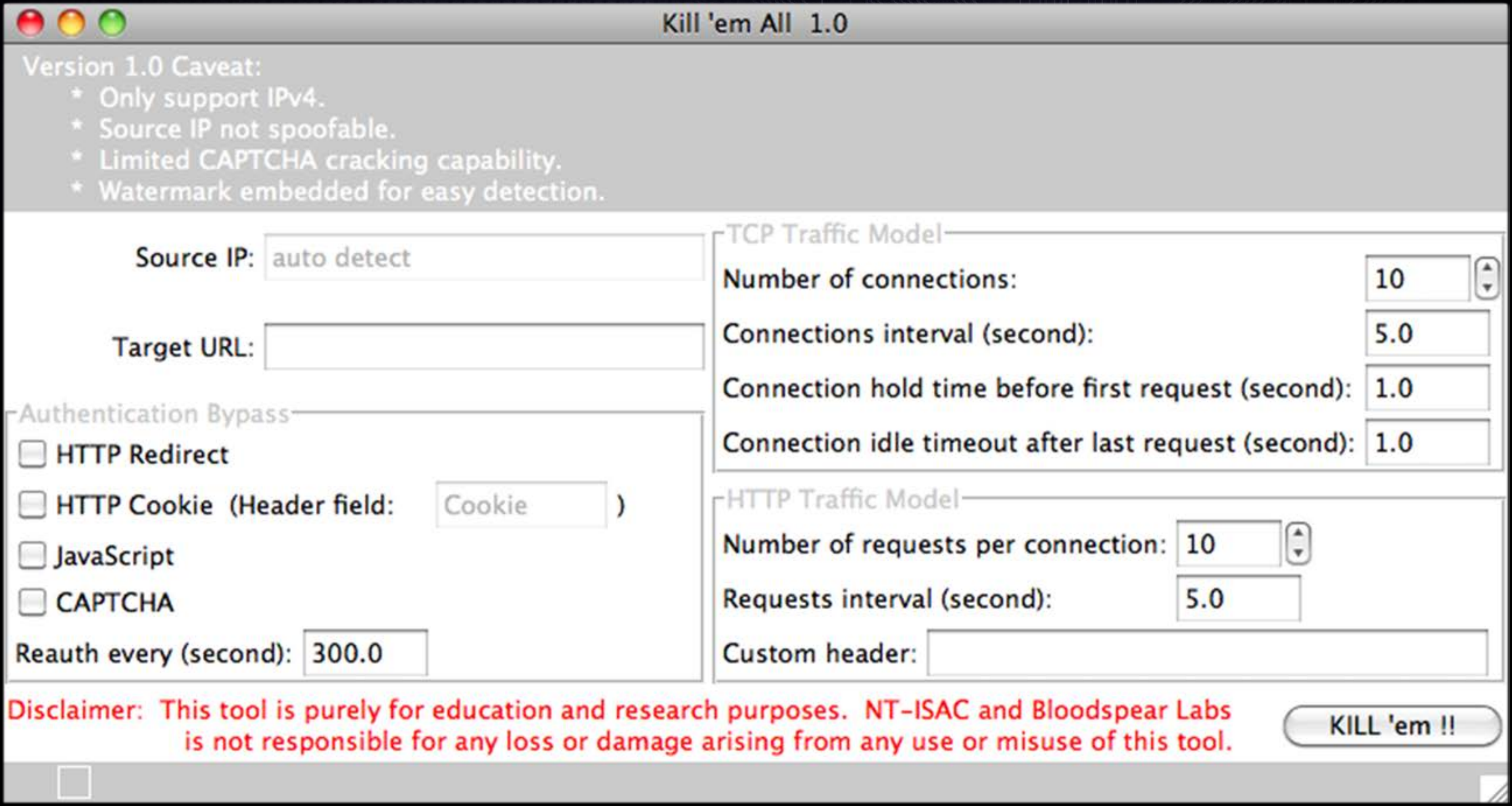
Source Host Verification

Mitigation

Source Host Verification

Verifies	TCP SYN	HTTP Redirect	HTTP Cookie	JavaScript	CAPTCHA
Non-Spoofed Source IP	✓	✓	✓	✓	✓
HTTP Compliant Application		✓	✓	✓	✓
Real Browser				✓	✓
Real Human					✓

PoC Tool



Kill 'em All 1.0

Version 1.0 Caveat:
- Only support IPv4.
- Source IP not spoofable.
- Limited CAPTCHA cracking capability.
- Watermark embedded for easy detection.

Source IP: auto detect

Target URL:

Authentication Bypass

□ HTTP Redirect

□ HTTP Cookie (Header field: Cookie)

□ JavaScript

□ CAPTCHA

Reauth every (second): 300.0

TCP Traffic Model

Number of connections: 10

Connections interval (second): 5.0

Connection hold time before first request (second): 1.0

Connection idle timeout after last request (second): 1.0

HTTP Traffic Model

Number of requests per connection: 10

Requests interval (second): 5.0

Custom header:

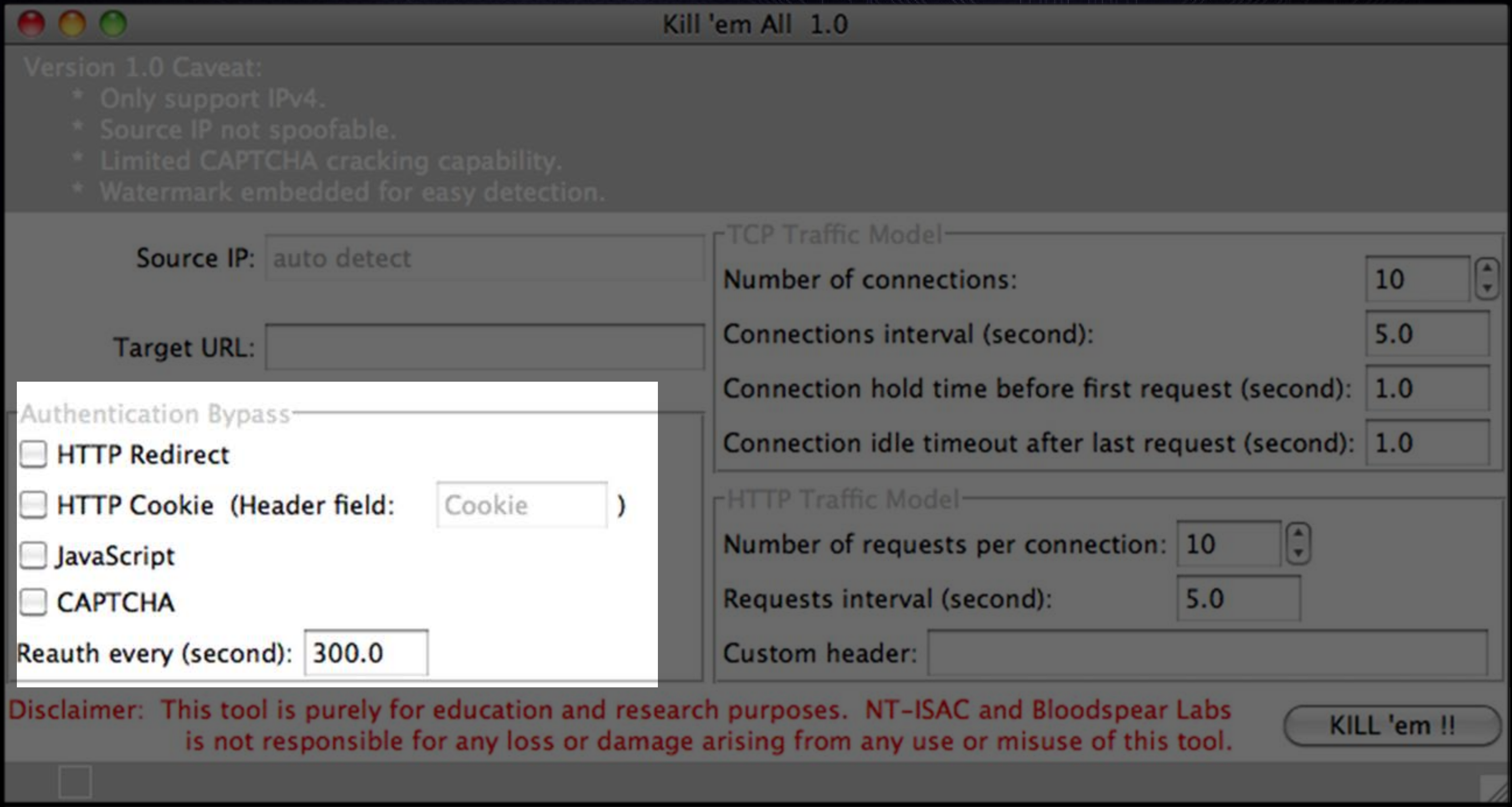
Disclaimer: This tool is purely for education and research purposes. NT-ISAC and Bloodspear Labs is not responsible for any loss or damage arising from any use or misuse of this tool.

PoC Tool Strengths

- True TCP/IP behavior (RST, resend, etc.)
- Believable HTTP headers (User-Agent strings, etc.)
- Embedded JavaScript engine
- CAPTCHA solving capability
- Randomized payload
- Tunable post-authentication traffic model

INDISTINGUISHABLE FROM HUMAN!!

PoC Tool: Authentication Bypass



Kill 'em All 1.0

Version 1.0 Caveat:
- Only support IPv4.
- Source IP not spoofable.
- Limited CAPTCHA cracking capability.
- Watermark embedded for easy detection.

Source IP: auto detect

Target URL:

Authentication Bypass

□ HTTP Redirect

□ HTTP Cookie (Header field: Cookie)

□ JavaScript

□ CAPTCHA

Reauth every (second): 300.0

TCP Traffic Model

Number of connections: 10

Connections interval (second): 5.0

Connection hold time before first request (second): 1.0

Connection idle timeout after last request (second): 1.0

HTTP Traffic Model

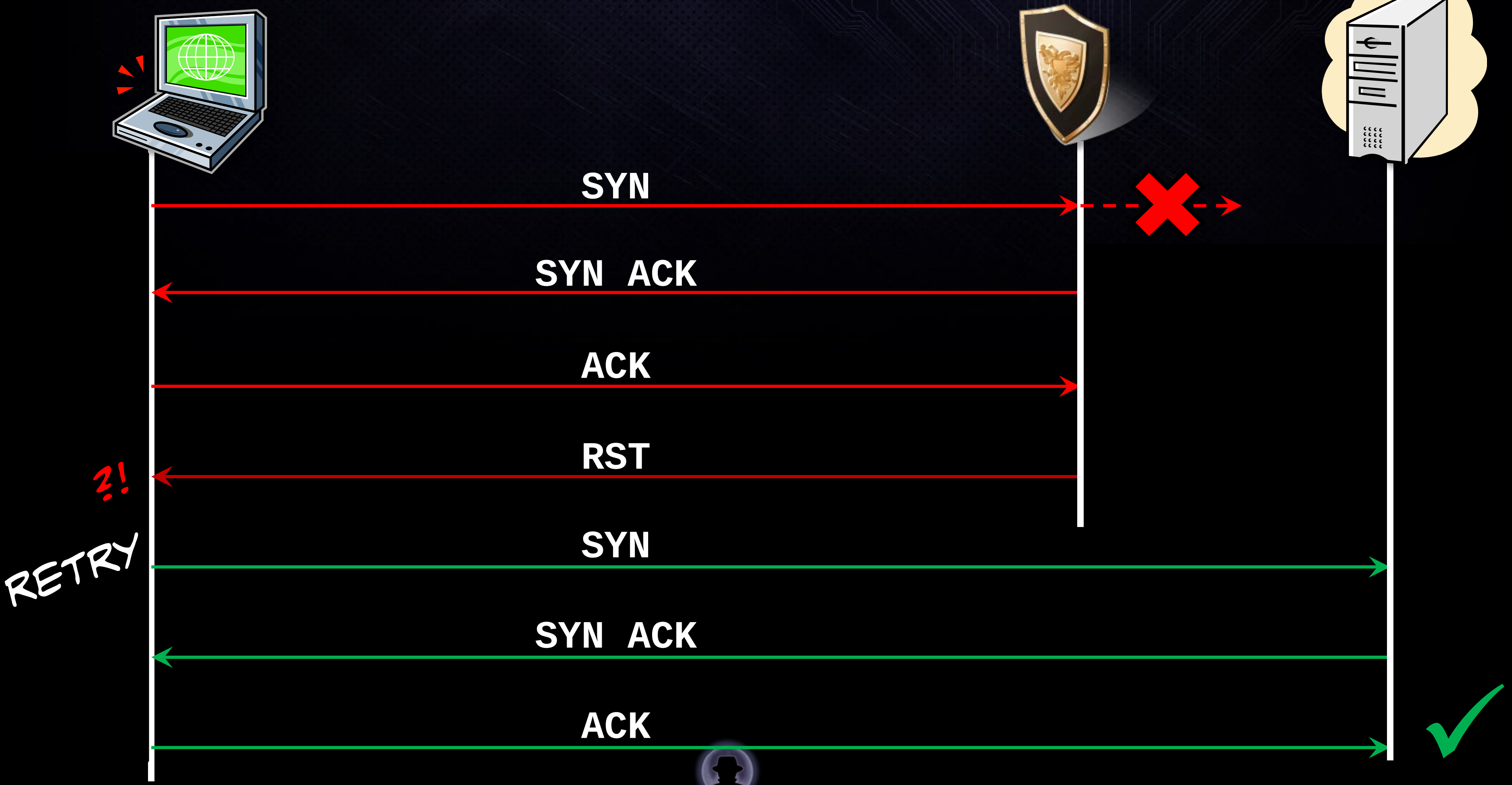
Number of requests per connection: 10

Requests interval (second): 5.0

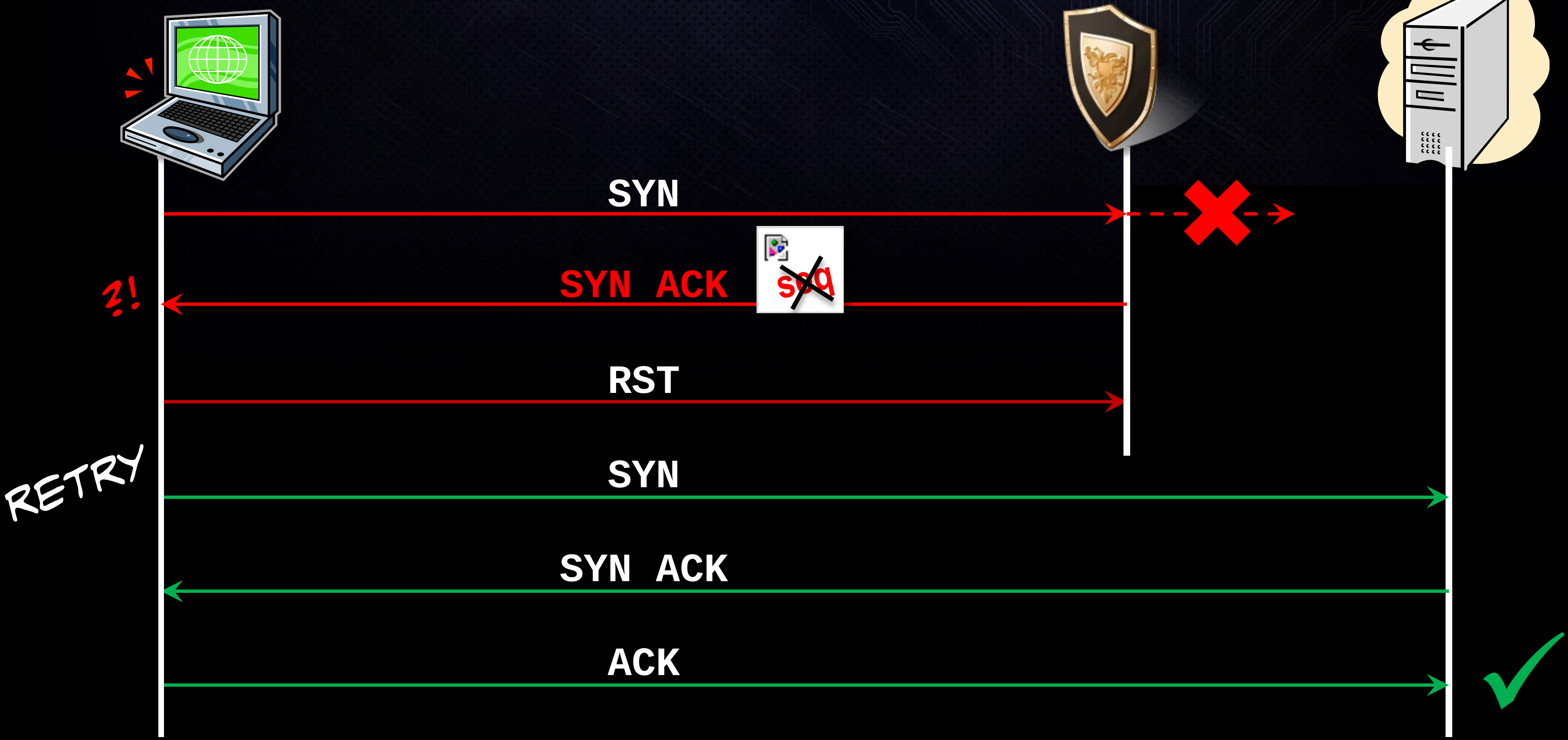
Custom header:

Disclaimer: This tool is purely for education and research purposes. NT-ISAC and Bloodspear Labs is not responsible for any loss or damage arising from any use or misuse of this tool.

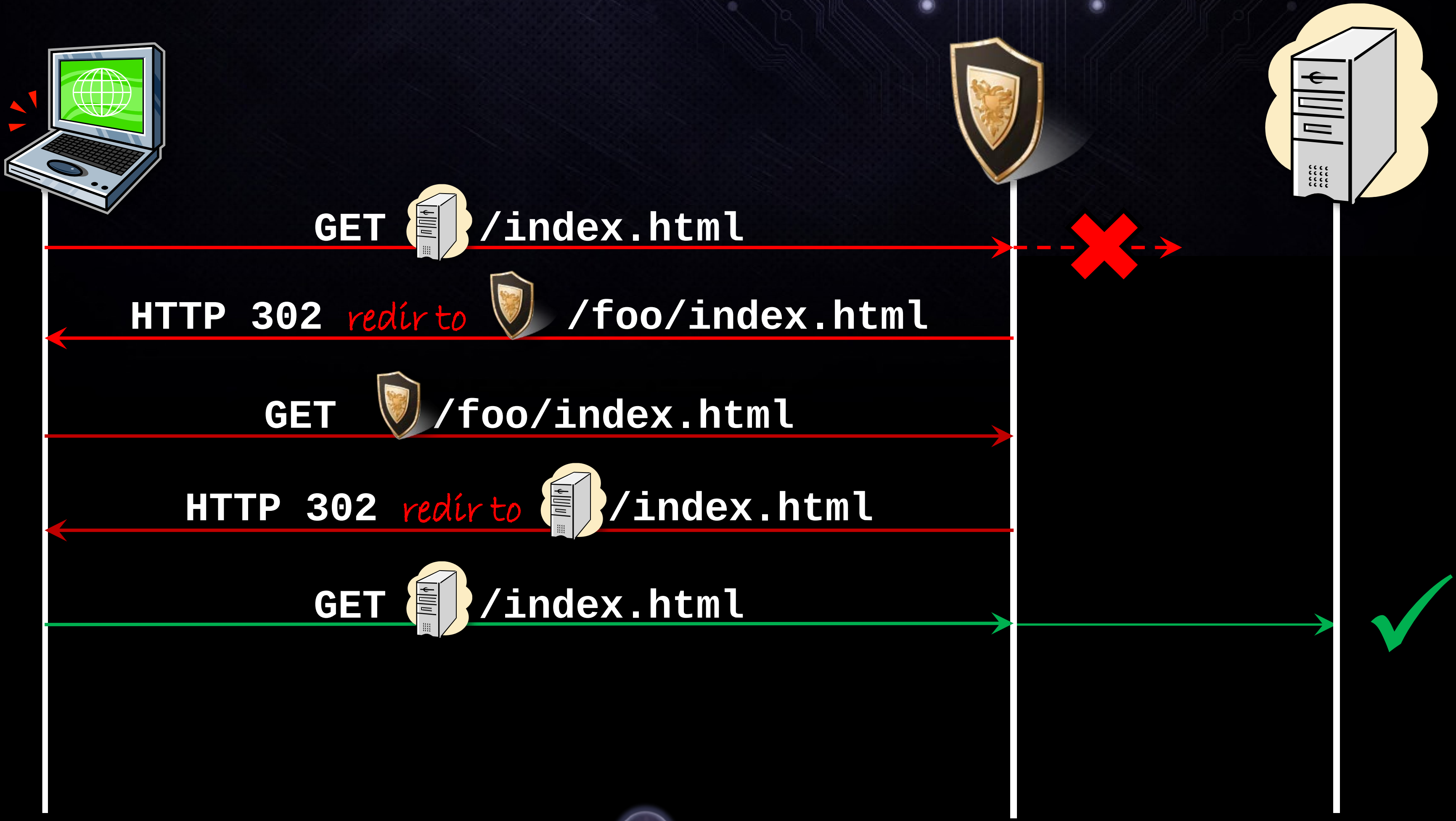
TCP SYN Auth (TCP Reset)



TCP SYN Auth (TCP Out-of-Sequence)



HTTP Redirect Auth



GET /index.html

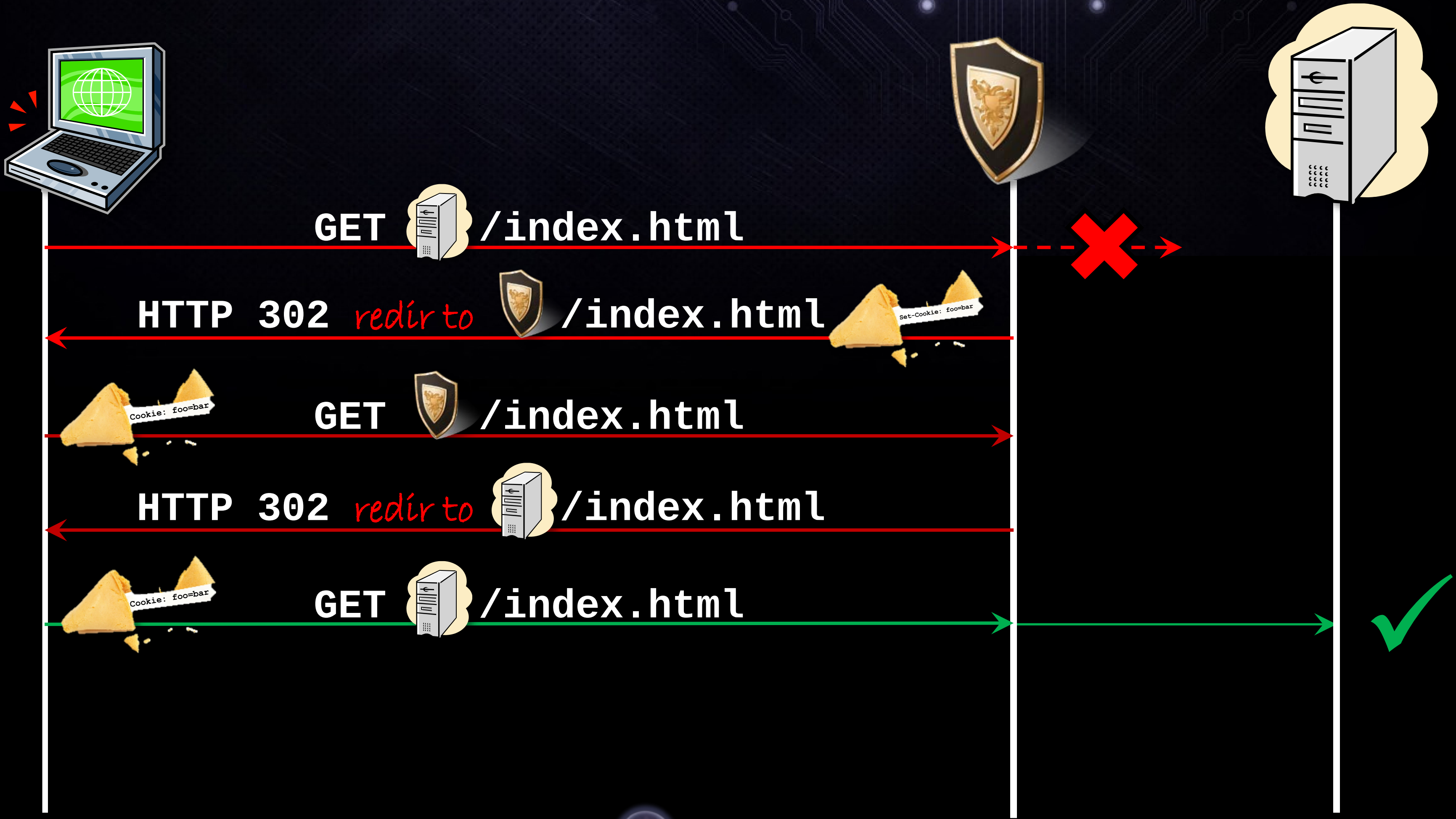
HTTP 302 redir to /foo/index.html

GET /foo/index.html

HTTP 302 redir to /index.html

GET /index.html

HTTP Cookie Auth



GET /index.html

HTTP 302 redir to /index.html

Set-Cookie: foo=bar

Cookie: foo=bar

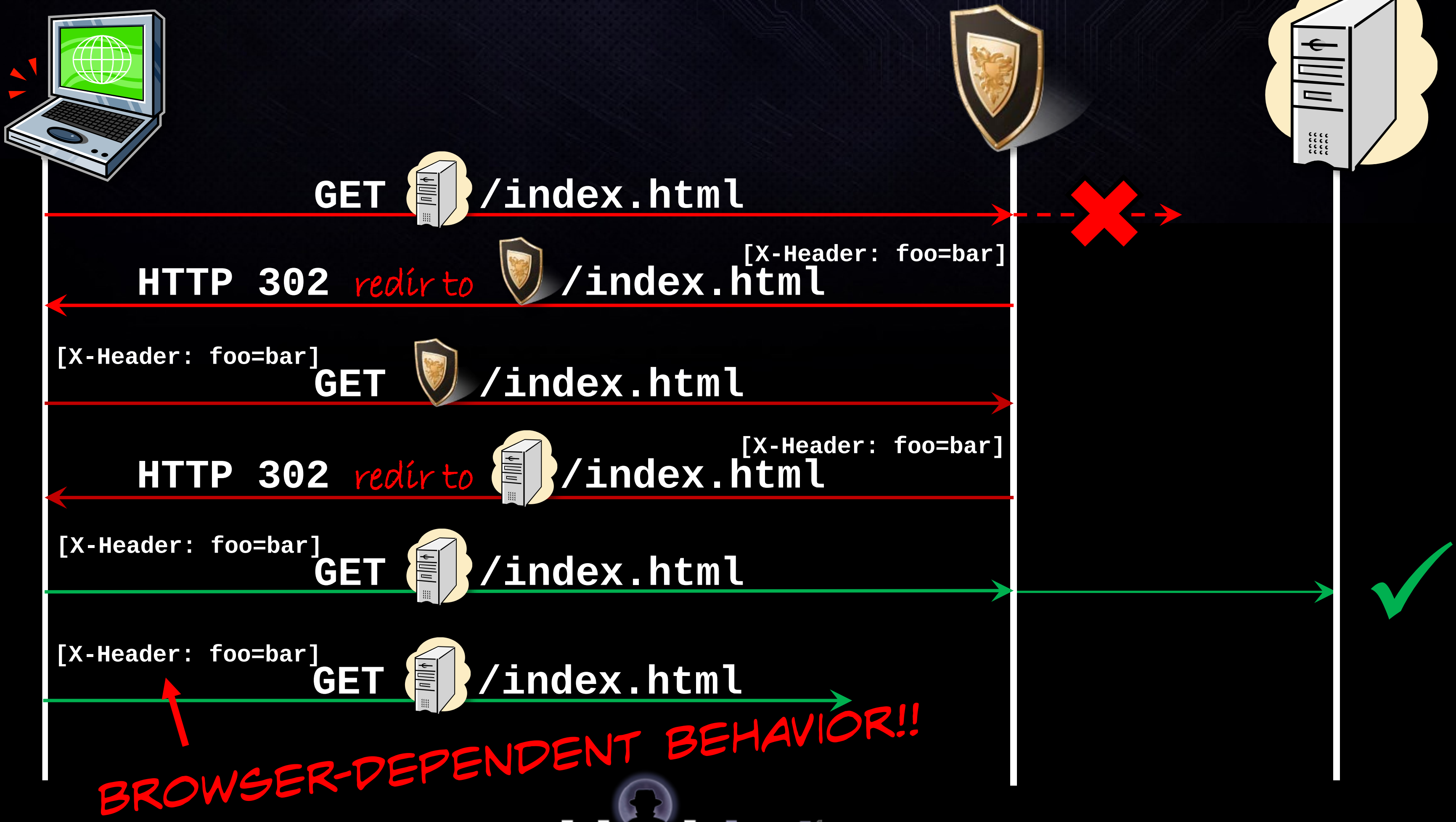
GET /index.html

HTTP 302 redir to /index.html

Cookie: foo=bar

GET /index.html

HTTP Cookie Auth (Header Token)



GET /index.html

[X-Header: foo=bar]

HTTP 302 redir to /index.html

[X-Header: foo=bar] GET /index.html

[X-Header: foo=bar]

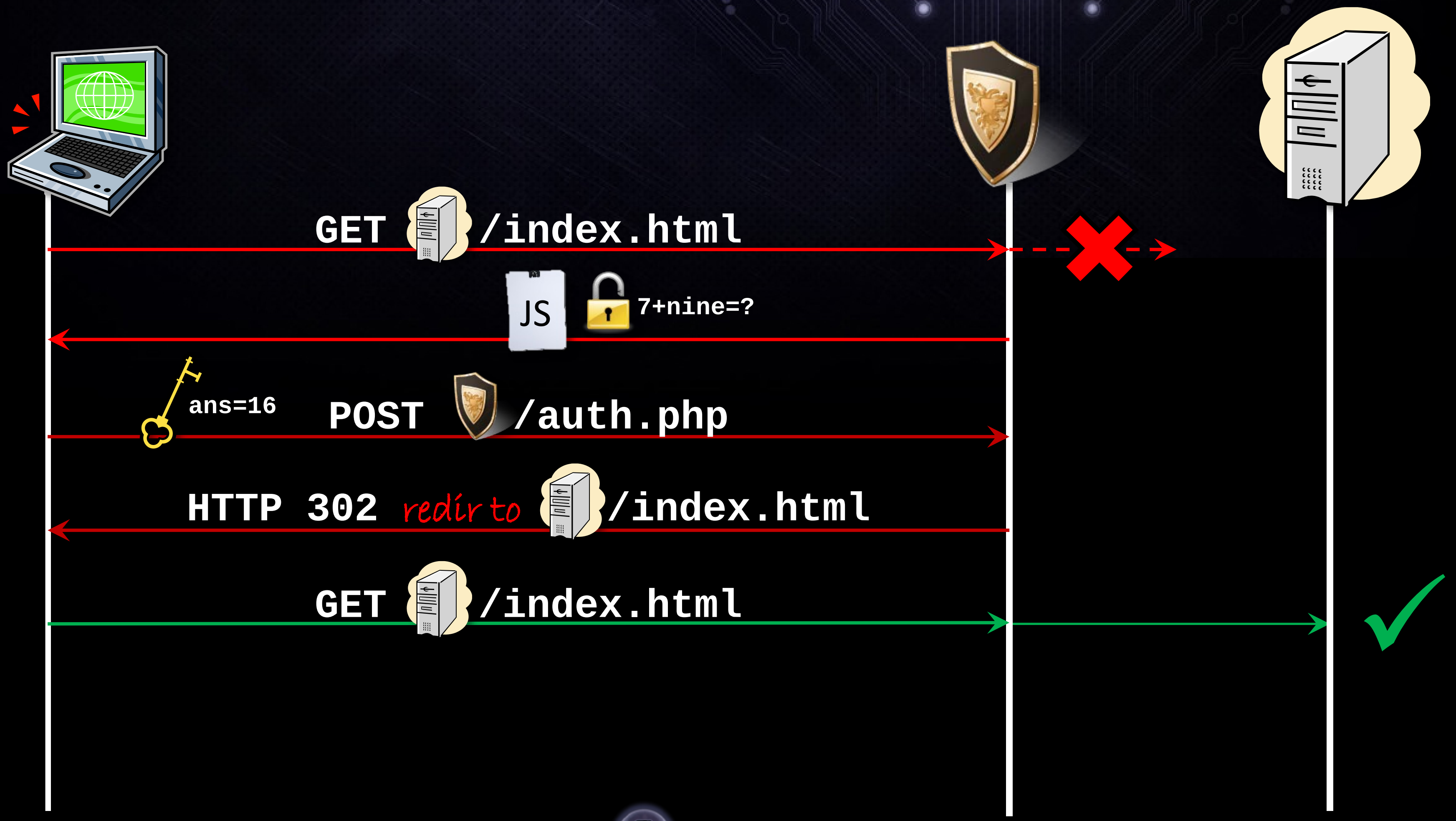
HTTP 302 redir to /index.html

[X-Header: foo=bar] GET /index.html

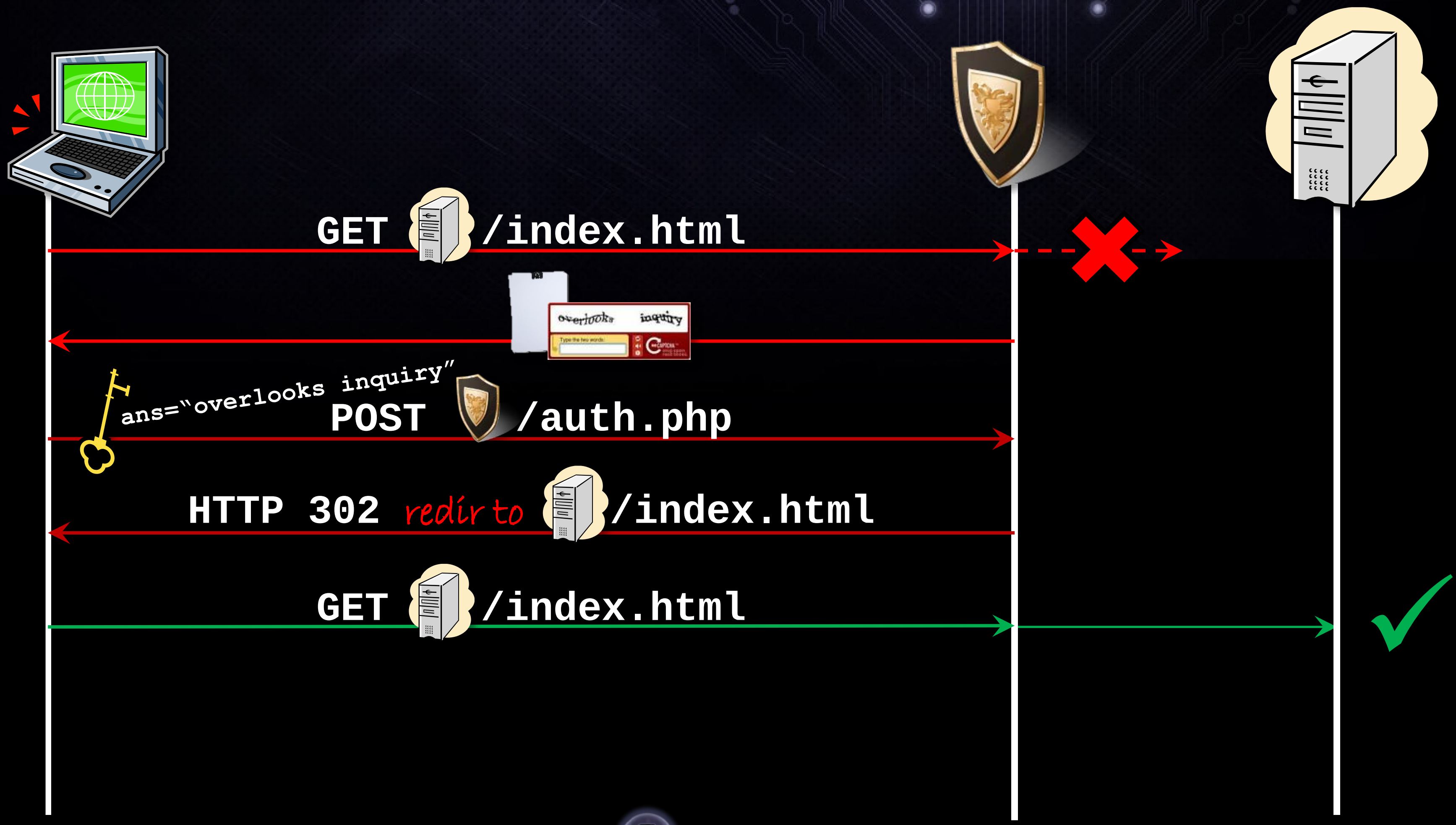
[X-Header: foo=bar] GET /index.html

BROWSER-DEPENDENT BEHAVIOR!!

JavaScript Auth



CAPTCHA Auth



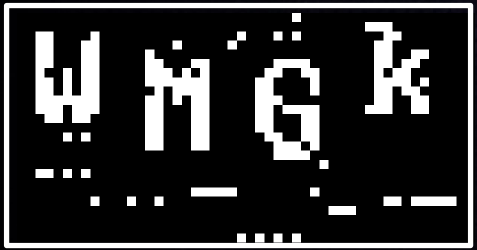
GET /index.html

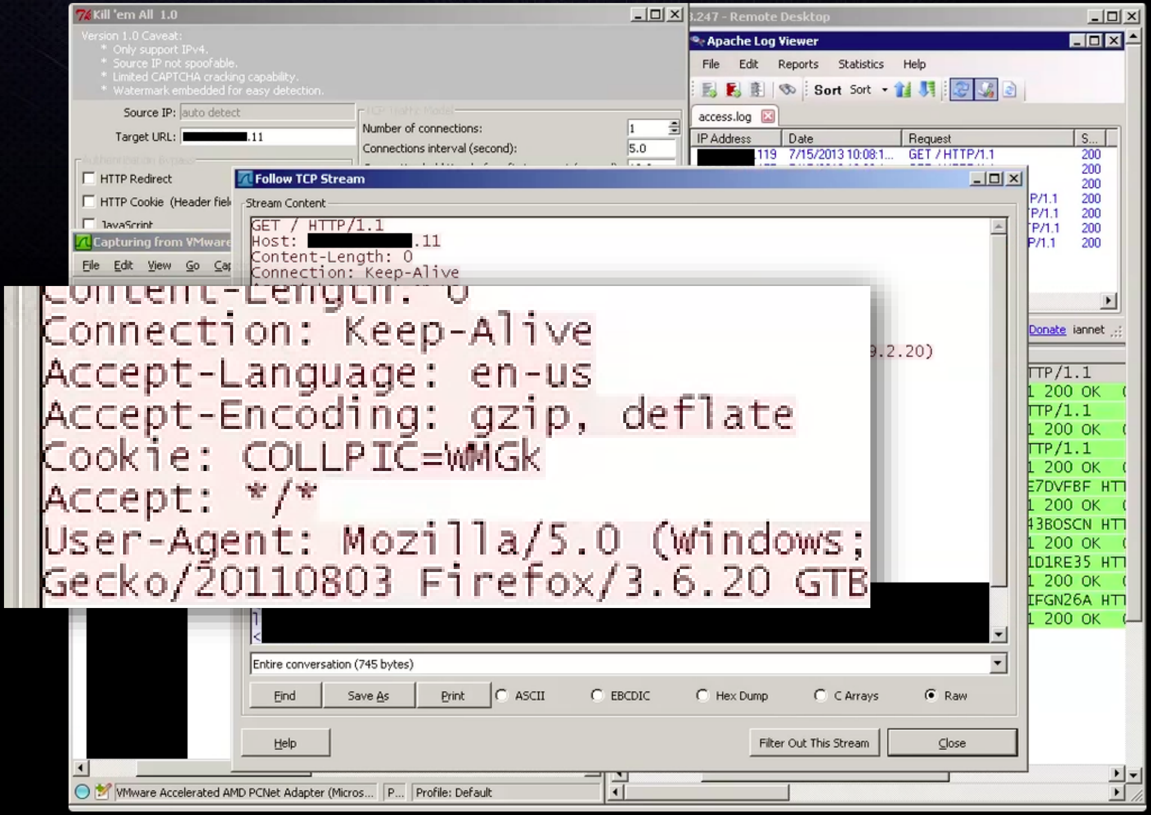
ans="overlooks inquiry"
POST /auth.php

HTTP 302 redir to /index.html

GET /index.html

CAPTCHA Pwnage





Version 1.0 Caveat:
- Only support IPv4.
- Source IP not spoofable.
- Limited CAPTCHA cracking capability.
- Watermark embedded for easy detection.

Source IP: auto detect

Target URL: [redacted].11

Number of connections: 1

Connections interval (second): 5.0

□ HTTP Redirect

□ HTTP Cookie (Header fiel

□ JavaScript

IP Address	Date	Request	S...
[redacted].119	7/15/2013 10:08:1...	GET / HTTP/1.1	200
			200
			200
		P/1.1	200
		P/1.1	200
		P/1.1	200
		P/1.1	200

Stream Content

```
GET / HTTP/1.1
Host: [redacted].11
Content-Length: 0
Connection: Keep-Alive
```

```
Content-Length: 0
Connection: Keep-Alive
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Cookie: COLLPIC=WMGk
Accept: */*
User-Agent: Mozilla/5.0 (Windows;
Gecko/20110803 Firefox/3.6.20 GTB
```

```
9.2.20)
```

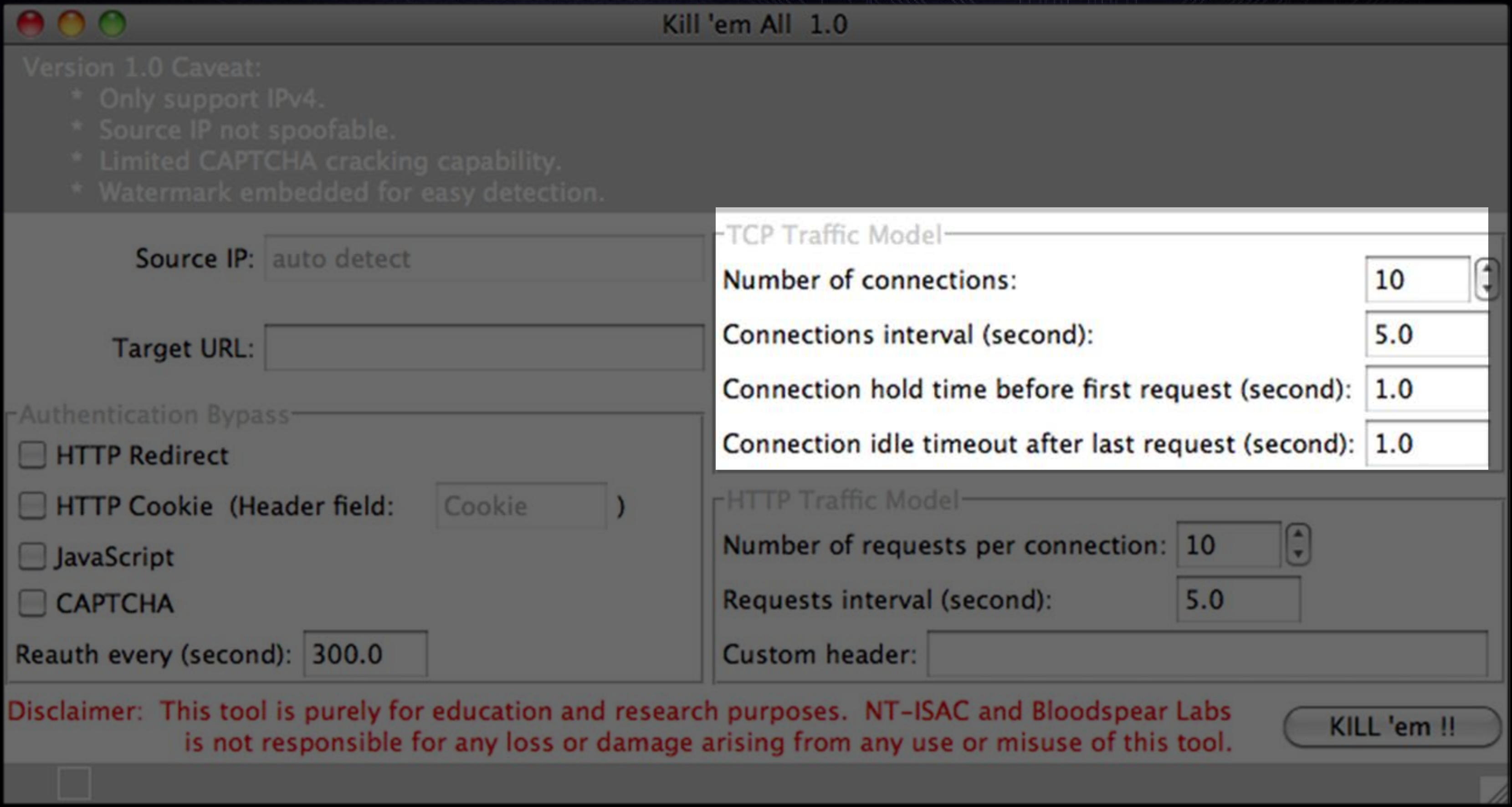
```
TTP/1.1
1 200 OK
TTP/1.1
1 200 OK
TTP/1.1
1 200 OK
E7DVFBF HTT
1 200 OK
43BOSCN HTT
1 200 OK
1D1RE35 HTT
1 200 OK
IFGN26A HTT
1 200 OK
```

Entire conversation (745 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

VMware Accelerated AMD PCNet Adapter (Micros... P... Profile: Default

PoC Tool: TCP Traffic Model



Kill 'em All 1.0

Version 1.0 Caveat:

- Only support IPv4.
- Source IP not spoofable.
- Limited CAPTCHA cracking capability.
- Watermark embedded for easy detection.

Source IP: auto detect

Target URL:

Authentication Bypass

□ HTTP Redirect

□ HTTP Cookie (Header field: Cookie)

□ JavaScript

□ CAPTCHA

Reauth every (second): 300.0

TCP Traffic Model

Number of connections: 10

Connections interval (second): 5.0

Connection hold time before first request (second): 1.0

Connection idle timeout after last request (second): 1.0

HTTP Traffic Model

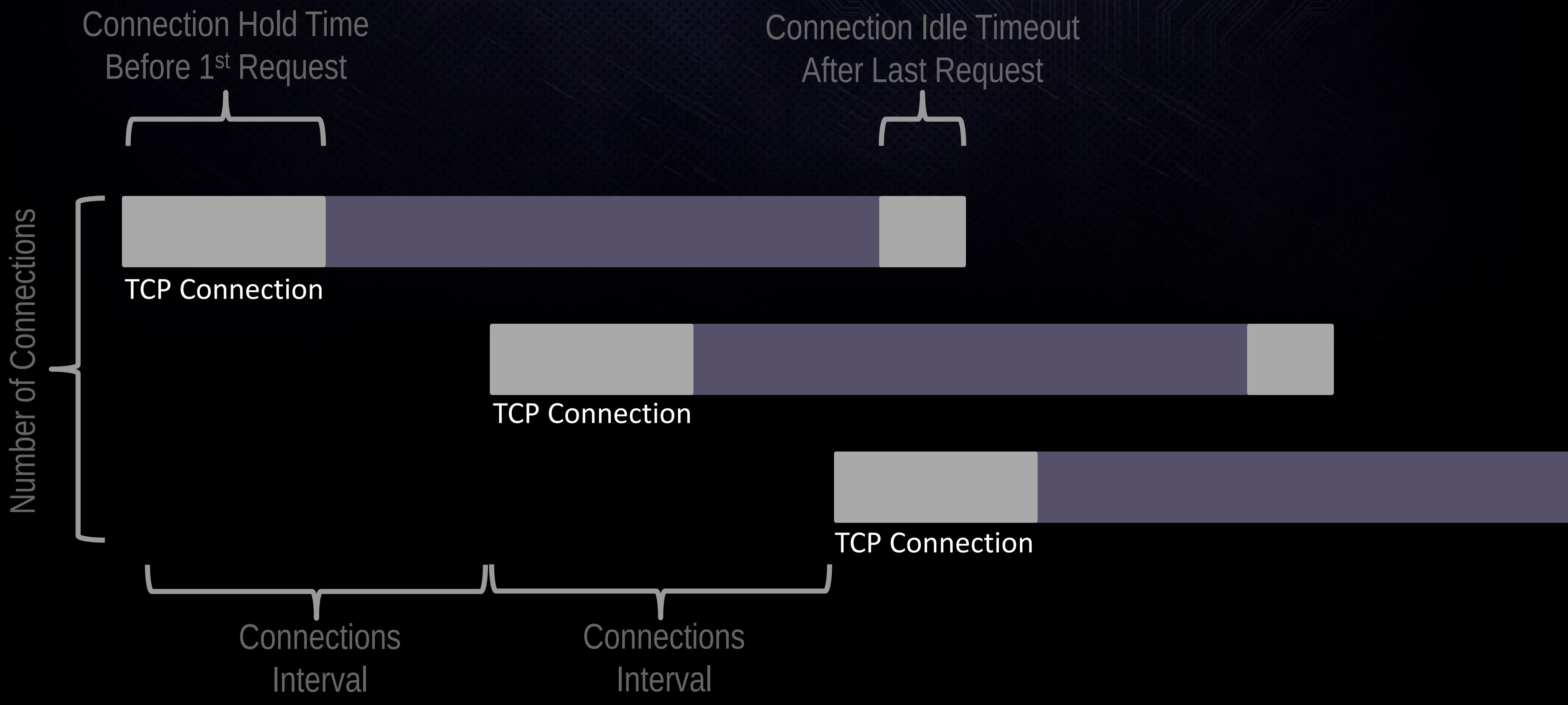
Number of requests per connection: 10

Requests interval (second): 5.0

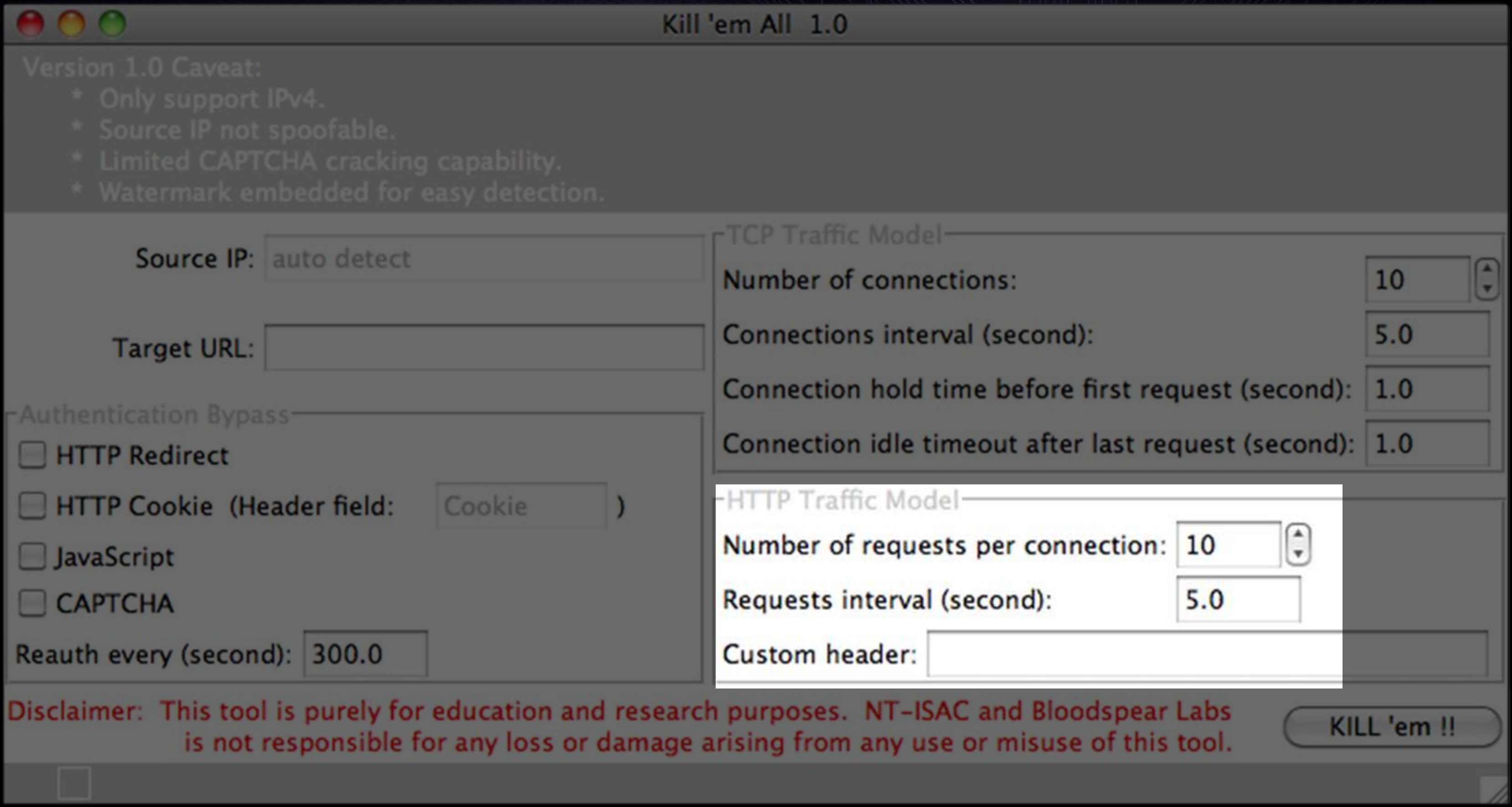
Custom header:

Disclaimer: This tool is purely for education and research purposes. NT-ISAC and Bloodspear Labs is not responsible for any loss or damage arising from any use or misuse of this tool.

TCP Traffic Model



PoC Tool: HTTP Traffic Model



Kill 'em All 1.0

Version 1.0 Caveat:
- Only support IPv4.
- Source IP not spoofable.
- Limited CAPTCHA cracking capability.
- Watermark embedded for easy detection.

Source IP: auto detect

Target URL:

Authentication Bypass

□ HTTP Redirect

□ HTTP Cookie (Header field: Cookie)

□ JavaScript

□ CAPTCHA

Reauth every (second): 300.0

TCP Traffic Model

Number of connections: 10

Connections interval (second): 5.0

Connection hold time before first request (second): 1.0

Connection idle timeout after last request (second): 1.0

HTTP Traffic Model

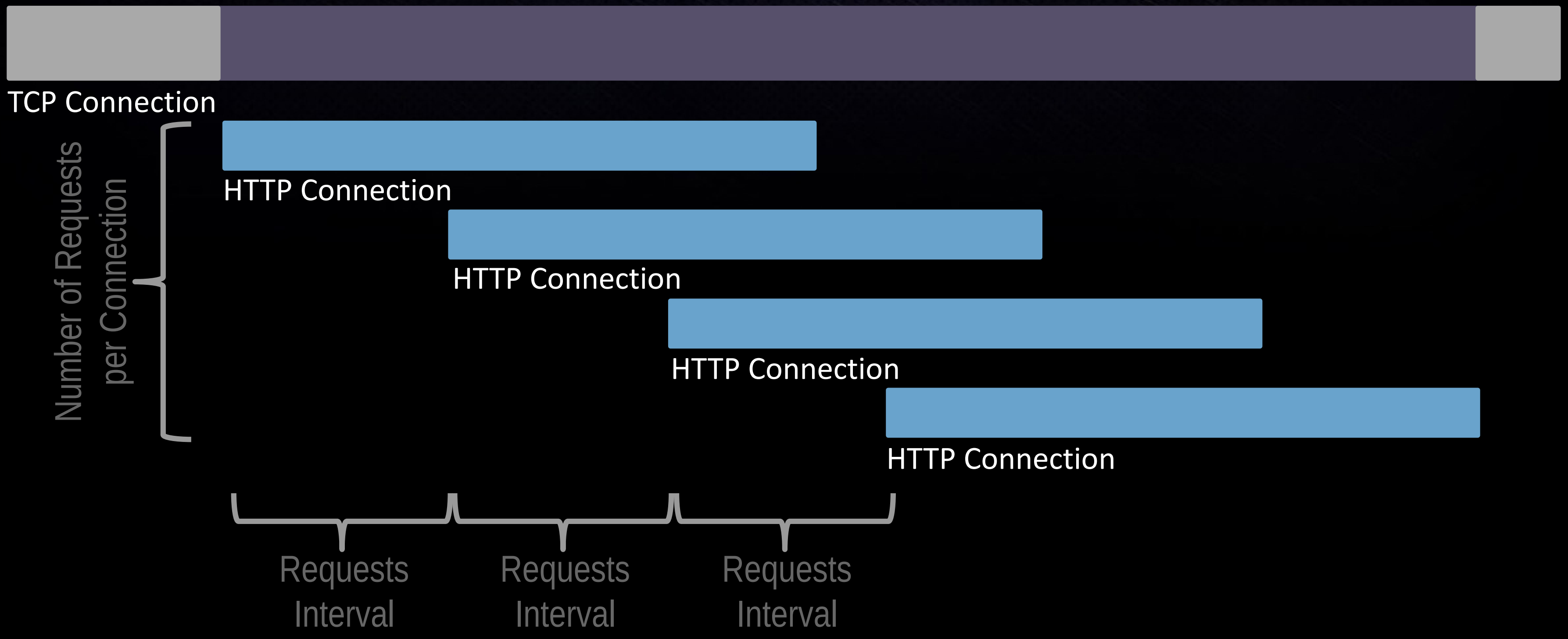
Number of requests per connection: 10

Requests interval (second): 5.0

Custom header:

Disclaimer: This tool is purely for education and research purposes. NT-ISAC and Bloodspear Labs is not responsible for any loss or damage arising from any use or misuse of this tool.

HTTP Traffic Model

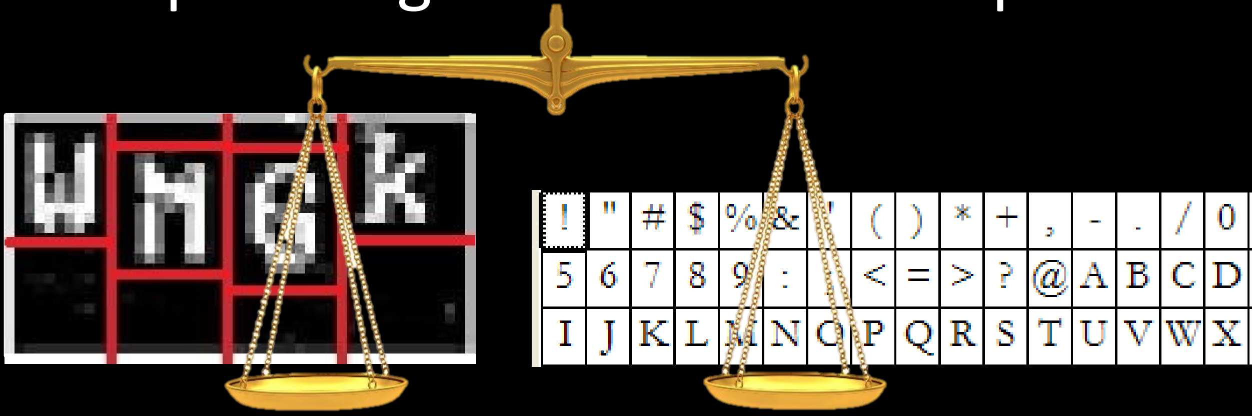


PoC Tool Design

- 3 tries per authentication attempt (in practice more likely to success)
- True TCP/IP behavior thru use of OS TCP/IP stack
- Auth cookies persist during subsequent dialogues
- JavaScript execution using embedded JS engine (lack of complete DOM an obstacle to full emulation)

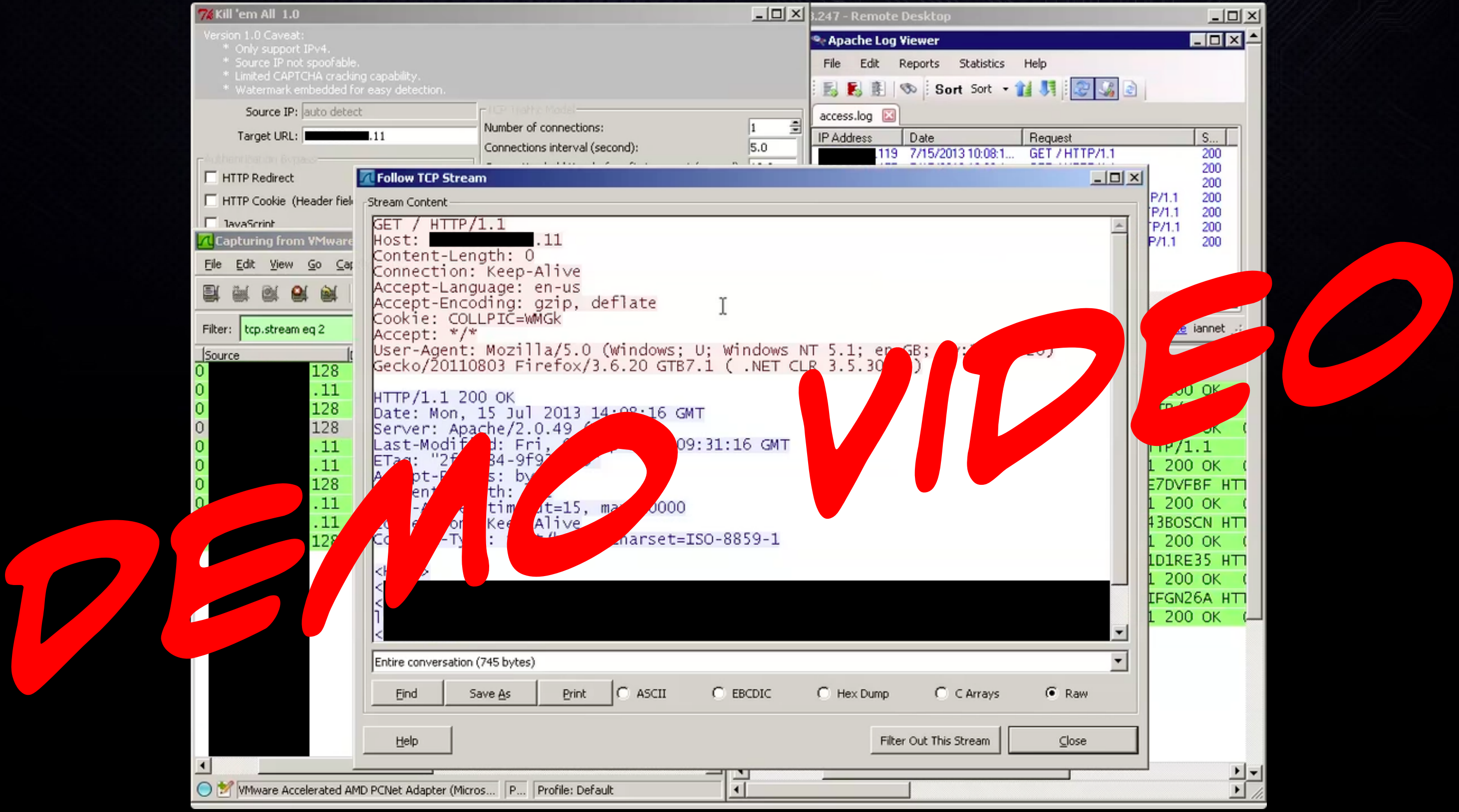
CAPTCHA Bypass Design

1. Converted to black-and-white for max contrast
2. 3x3 median filter applied for denoising
3. Word segmentation
4. Boundary recognition
5. Pixel difference computed against character map



!	"	#	$	%	&	'	(	)	*	+	,	-	.	/	0
5	6	7	8	9	:	;	<	=	>	?	@	A	B	C	D
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X

PoC Tool in Action



Version 1.0 Caveat:
- Only support IPv4.
- Source IP not spoofable.
- Limited CAPTCHA cracking capability.
- Watermark embedded for easy detection.

Source IP: auto detect

Target URL: [redacted].11

Number of connections: 1

Connections interval (second): 5.0

□ HTTP Redirect
□ HTTP Cookie (Header fiel
□ JavaScript

Filter: tcp.stream eq 2

IP Address	Date	Request	S...
[redacted].119	7/15/2013 10:08:1...	GET / HTTP/1.1	200

```
GET / HTTP/1.1
Host: [redacted].11
Content-Length: 0
Connection: Keep-Alive
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Cookie: COLLPIC=WMGk
Accept: */*
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB;
Gecko/20110803 Firefox/3.6.20 GTB7.1 ( .NET CLR 3.5.30

HTTP/1.1 200 OK
Date: Mon, 15 Jul 2013 14:08:16 GMT
Server: Apache/2.0.49
Last-Modified: Fri,                09:31:16 GMT
ETag: "2f   84-9f9
                   charset=ISO-8859-1

[redacted]
```

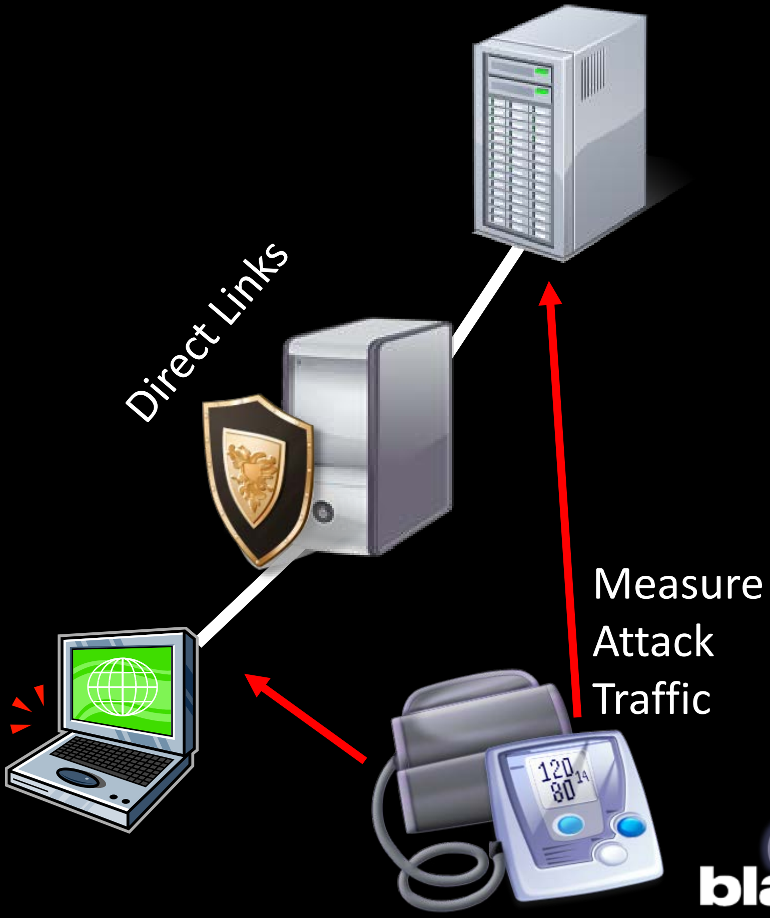
Entire conversation (745 bytes)

DEMO VIDEO

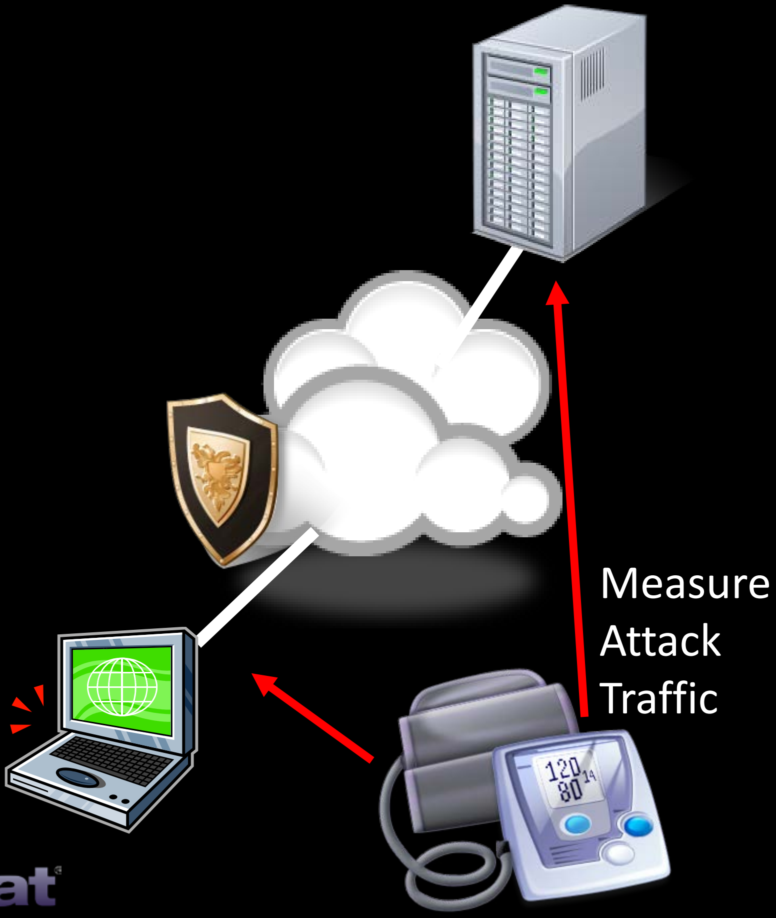
black hat
USA 2013

Testing Environment

Against Devices

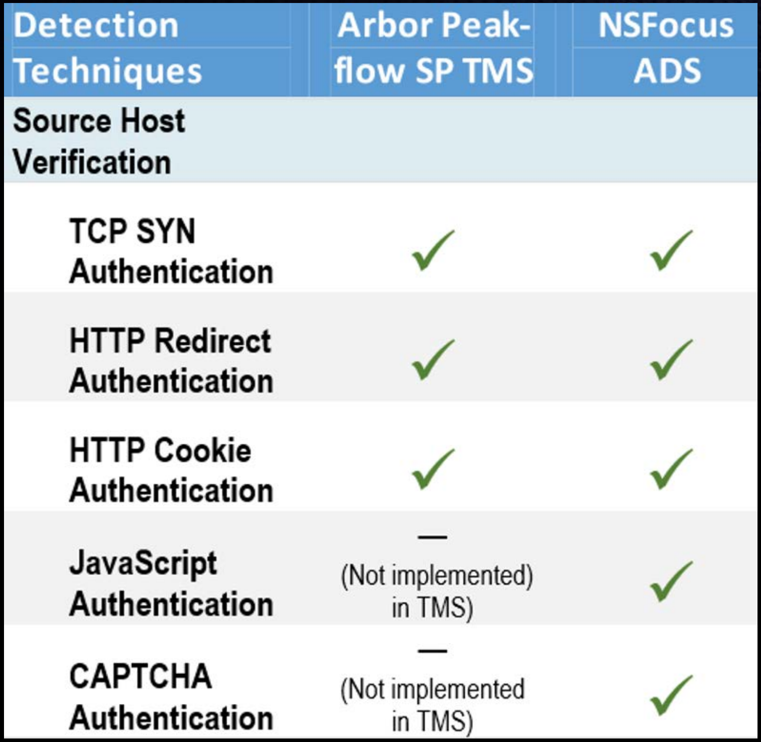


Against Services



Mitigation Bypass
(Protection Products)

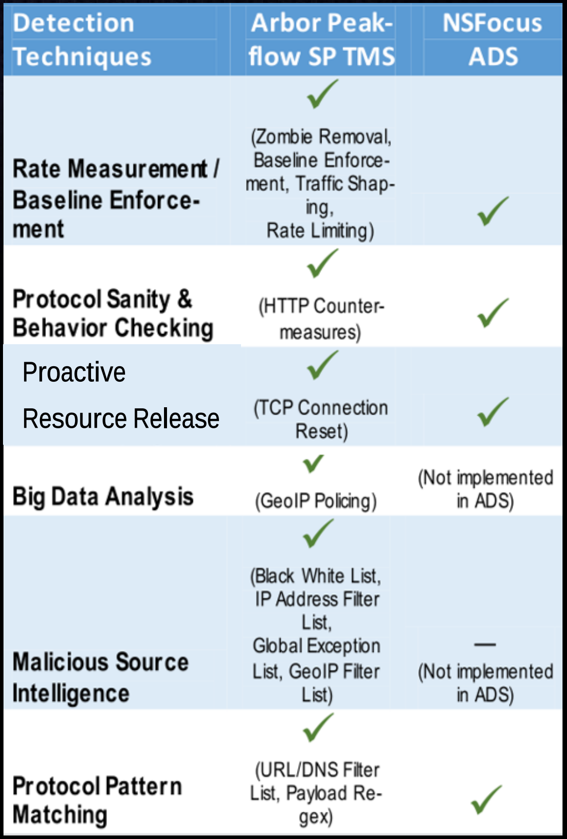
Auth Bypass



Detection Techniques	Arbor Peak-flow SP TMS	NSFocus ADS
Source Host Verification		
TCP SYN Authentication	✓	✓
HTTP Redirect Authentication	✓	✓
HTTP Cookie Authentication	✓	✓
JavaScript Authentication	— (Not implemented) in TMS)	✓
CAPTCHA Authentication	— (Not implemented in TMS)	✓

Testing results under specific conditions, valid as of Jul 13, 2013

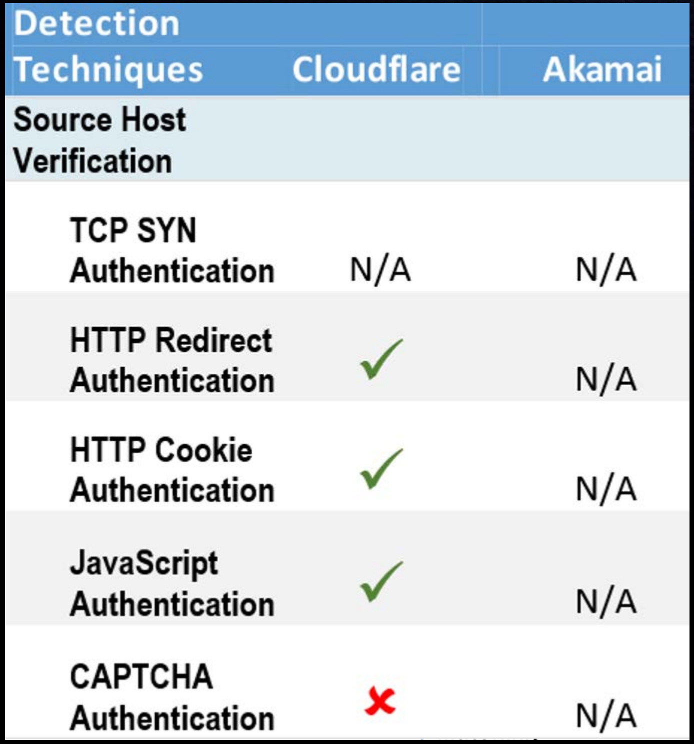
Post-Auth



Detection Techniques	Arbor Peak-flow SP TMS	NSFocus ADS
Rate Measurement / Baseline Enforcement	✓ (Zombie Removal, Baseline Enforcement, Traffic Shaping, Rate Limiting)	✓
Protocol Sanity & Behavior Checking	✓ (HTTP Countermeasures)	✓
Proactive Resource Release	✓ (TCP Connection Reset)	✓
Big Data Analysis	✓ (GeoIP Policing)	(Not implemented in ADS)
Malicious Source Intelligence	✓ (Black White List, IP Address Filter List, Global Exception List, GeoIP Filter List)	— (Not implemented in ADS)
Protocol Pattern Matching	✓ (URL/DNS Filter List, Payload Regex)	✓

Mitigation Bypass
(Protection Services)

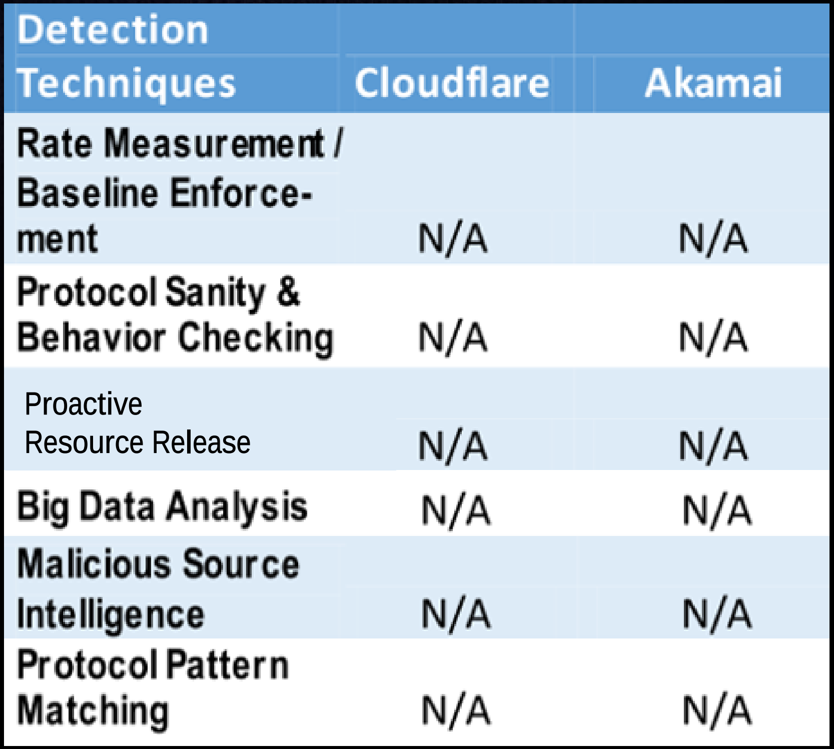
Auth Bypass



Detection Techniques	Cloudflare	Akamai
Source Host Verification		
TCP SYN Authentication	N/A	N/A
HTTP Redirect Authentication	✓	N/A
HTTP Cookie Authentication	✓	N/A
JavaScript Authentication	✓	N/A
CAPTCHA Authentication	✗	N/A

Testing results under specific conditions, valid as of Jul 13, 2013

Post-Auth



Detection Techniques	Cloudflare	Akamai
Rate Measurement / Baseline Enforcement	N/A	N/A
Protocol Sanity & Behavior Checking	N/A	N/A
Proactive Resource Release	N/A	N/A
Big Data Analysis	N/A	N/A
Malicious Source Intelligence	N/A	N/A
Protocol Pattern Matching	N/A	N/A

Next-Generation Mitigation

- Client Puzzle – add cost to individual zombies.

Conclusion

- DDoS is expensive to business
- Existing DDoS protection insufficient
- Next-Generation solution should make attack expensive

Thank You!

tony.miu@nexusguard.com

albert.hui@ntisac.org

waileng.lee@ntisac.org

http://www.ntisac.org