# KILL 'EM ALL

DDoS Protecion Total Annihilation!! ☠

Network Threats
Information Sharing
and Analysis Center

BLOODSPEAR
LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

# TO SERVE AND TO PROTECT

Network Threats
Information Sharing
and Analysis Center

BLOODSPEAR
LABORATORIES

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

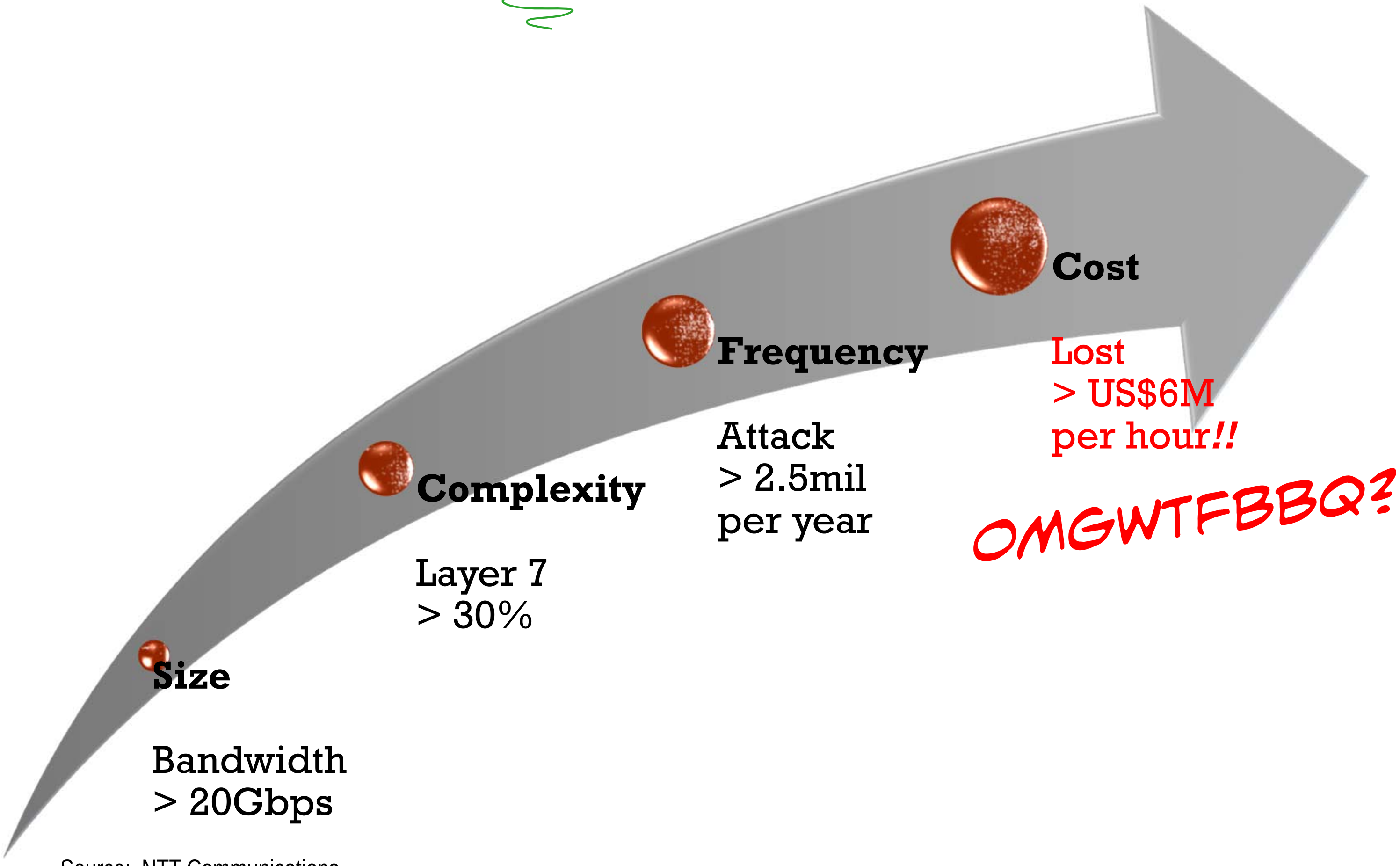
NEXUSGUARD
DDoS Mitigation Lab

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

# AGENDA

- DDoS Relevance, Attack Categories, Detection & Mitigation
- Source Host Verification: Authentication Methods
  - TCP SYN Auth
  - HTTP Redirect Auth
  - HTTP Cookie Auth
  - JavaScript Auth
  - CAPTCHA Auth
- PoC Tool
  - TCP Traffic Model
  - HTTP Traffic Model

# SHOW ME THE



**Size**

Bandwidth
> 20Gbps

**Complexity**

Layer 7
> 30%

**Frequency**

Attack
> 2.5mil
per year

**Cost**

Lost
> US$6M
per hour!!

OMGWTFBBQ?!

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

BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

# ATTACK CATEGORIES

Volumetric

Semantic

Blended

# MITIGATIONS

Traffic Policing

Proactive House Keeping

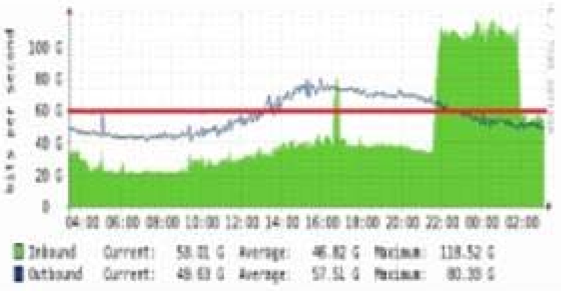
CDN / Clean Pipe

Black- / Whitelisting

Traceback

# DETECTIONS

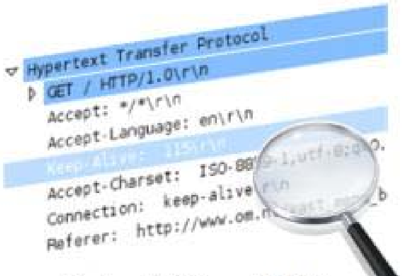
Rate Measurment



Baseline Enforcement

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

Big Data Analysis

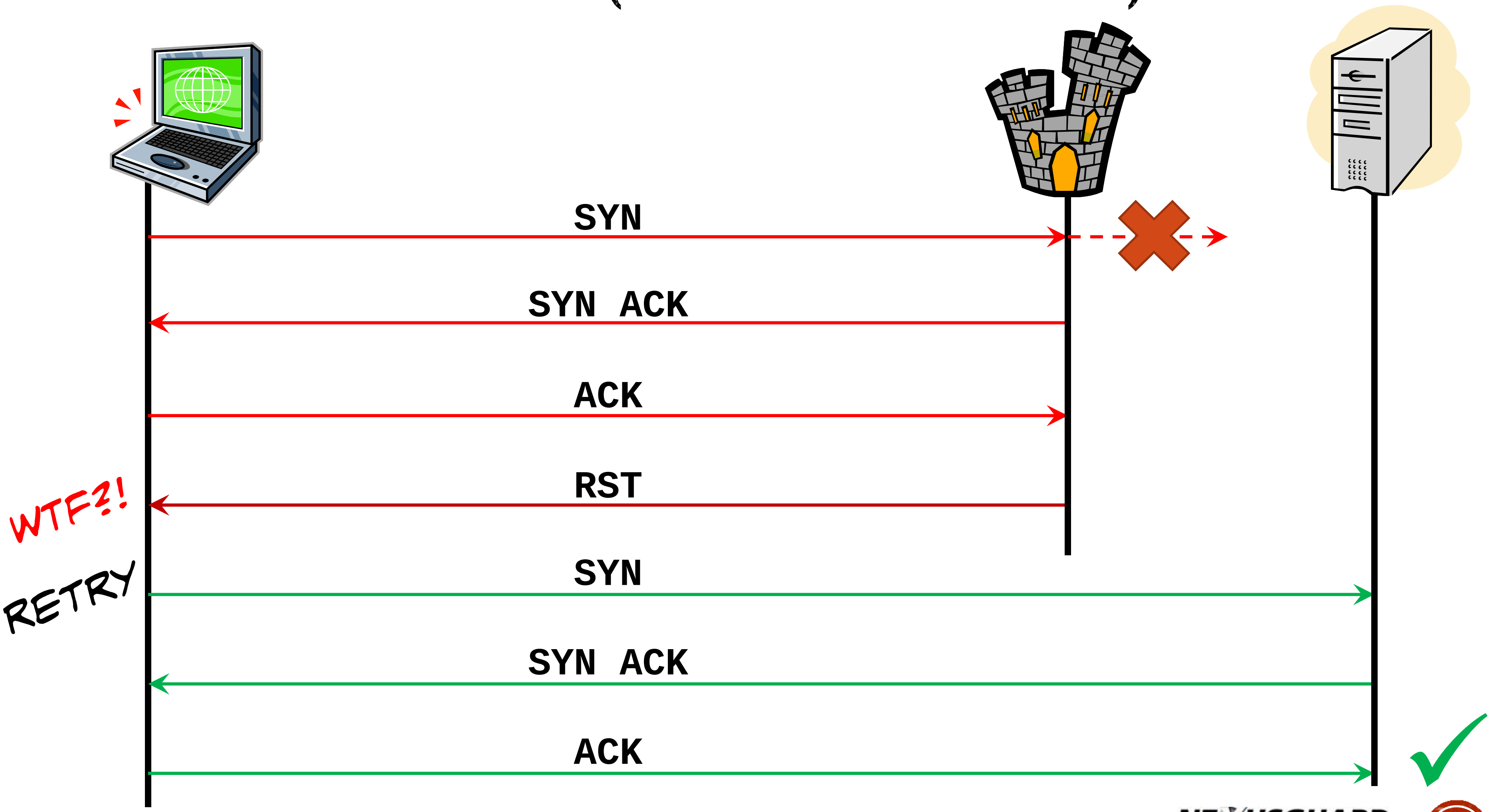
Malicious Source Intelligence

Source Host Authentication

BLOODSPEAR LABORATORIES

NEXUSGUARD DDoS Mitigation Lab

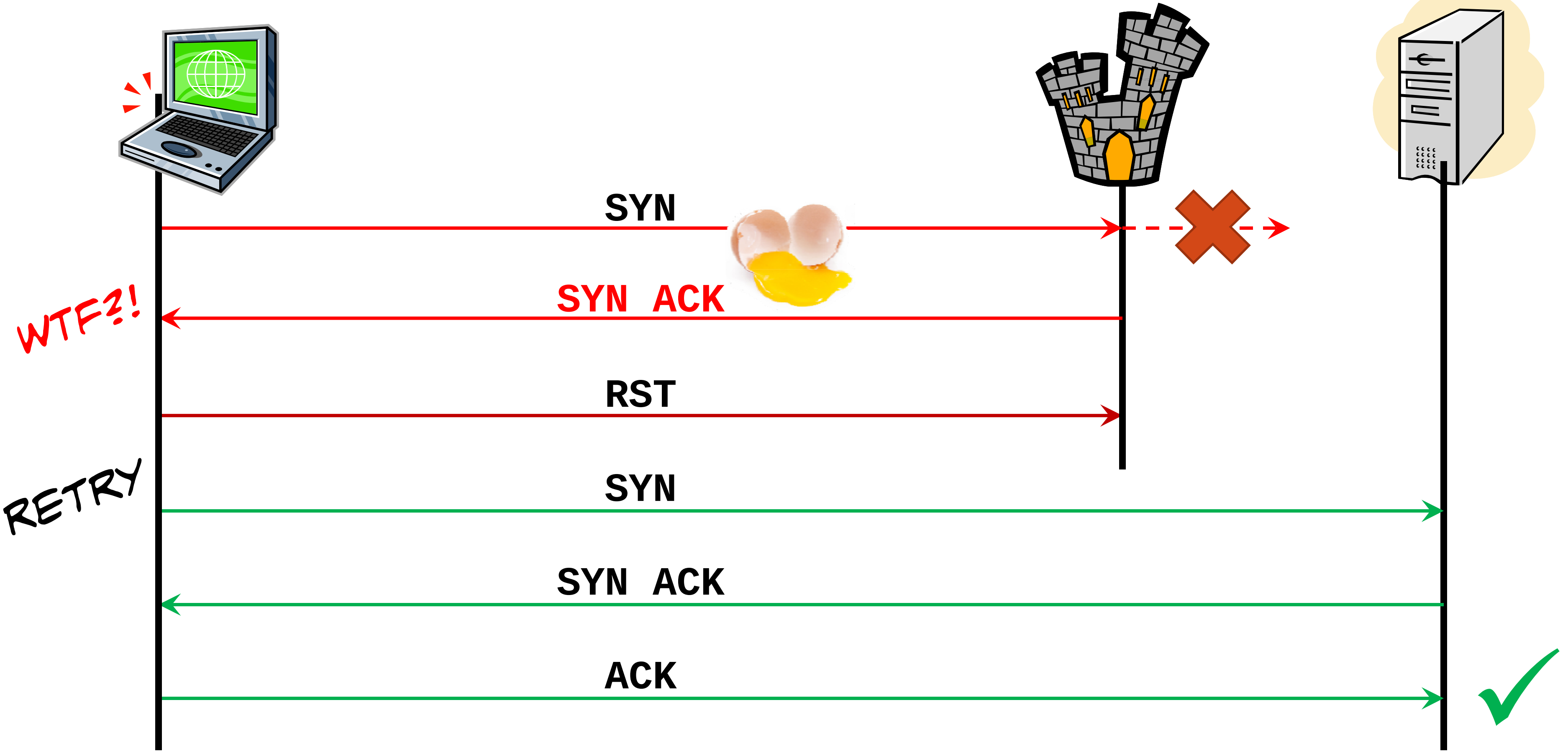
# TCP SYN AUTH (FORCEFUL RESET)



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

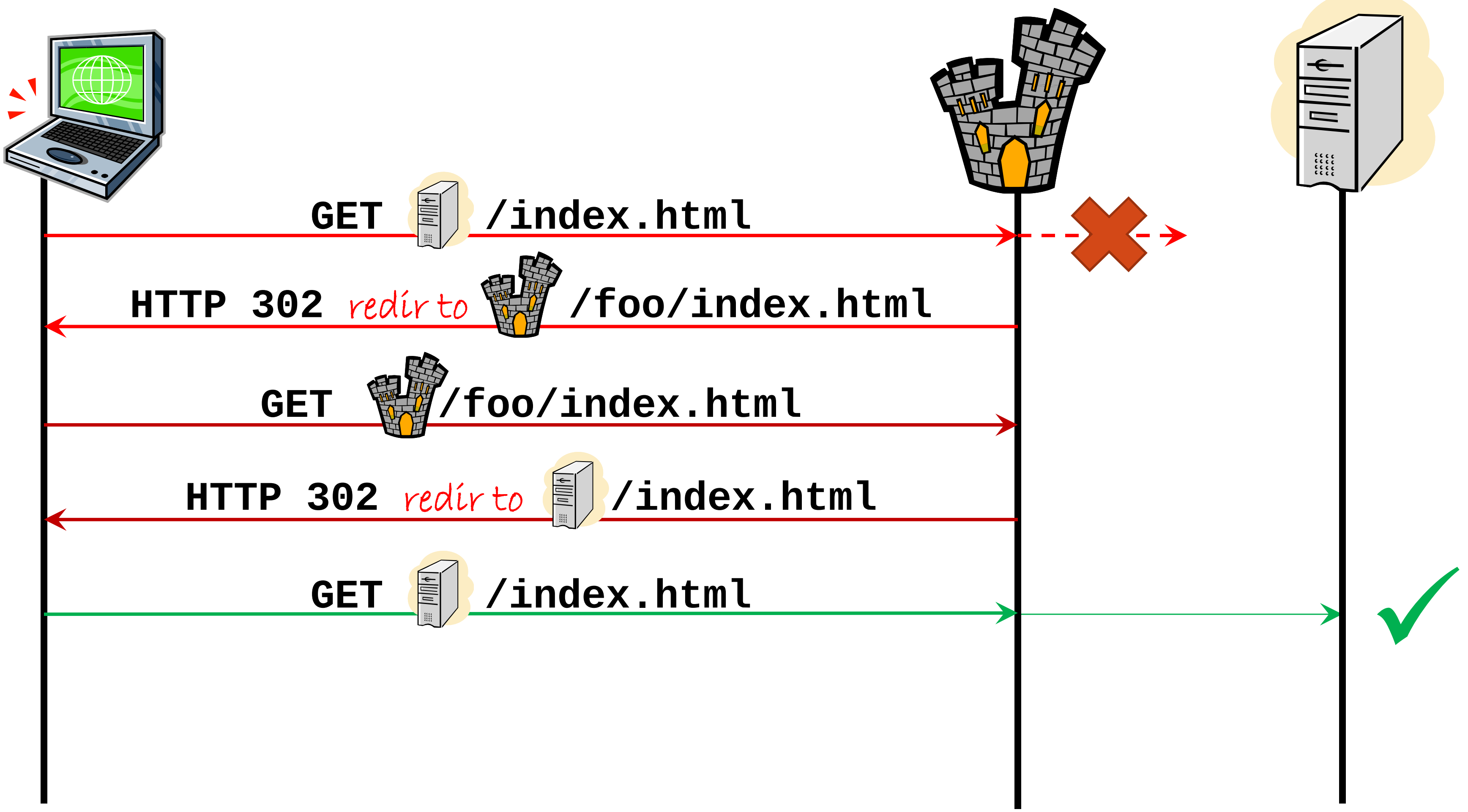
# TCP SYN AUTH (OUT-SEQ REPLY)



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

# HTTP REDIRECT AUTH



GET /index.html

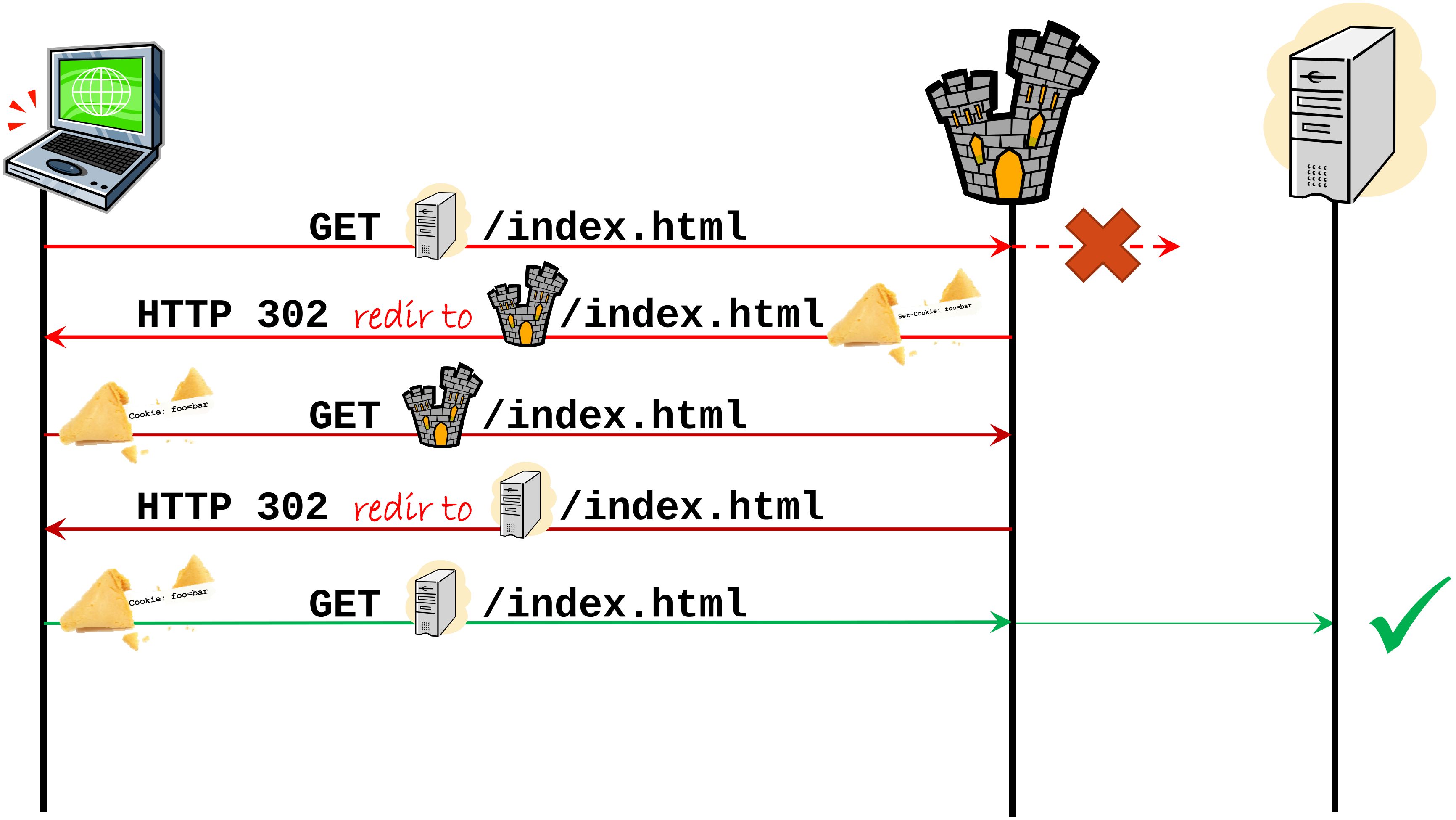
HTTP 302 redir to /foo/index.html

GET /foo/index.html

HTTP 302 redir to /index.html

GET /index.html

# HTTP COOKIE AUTH



GET /index.html

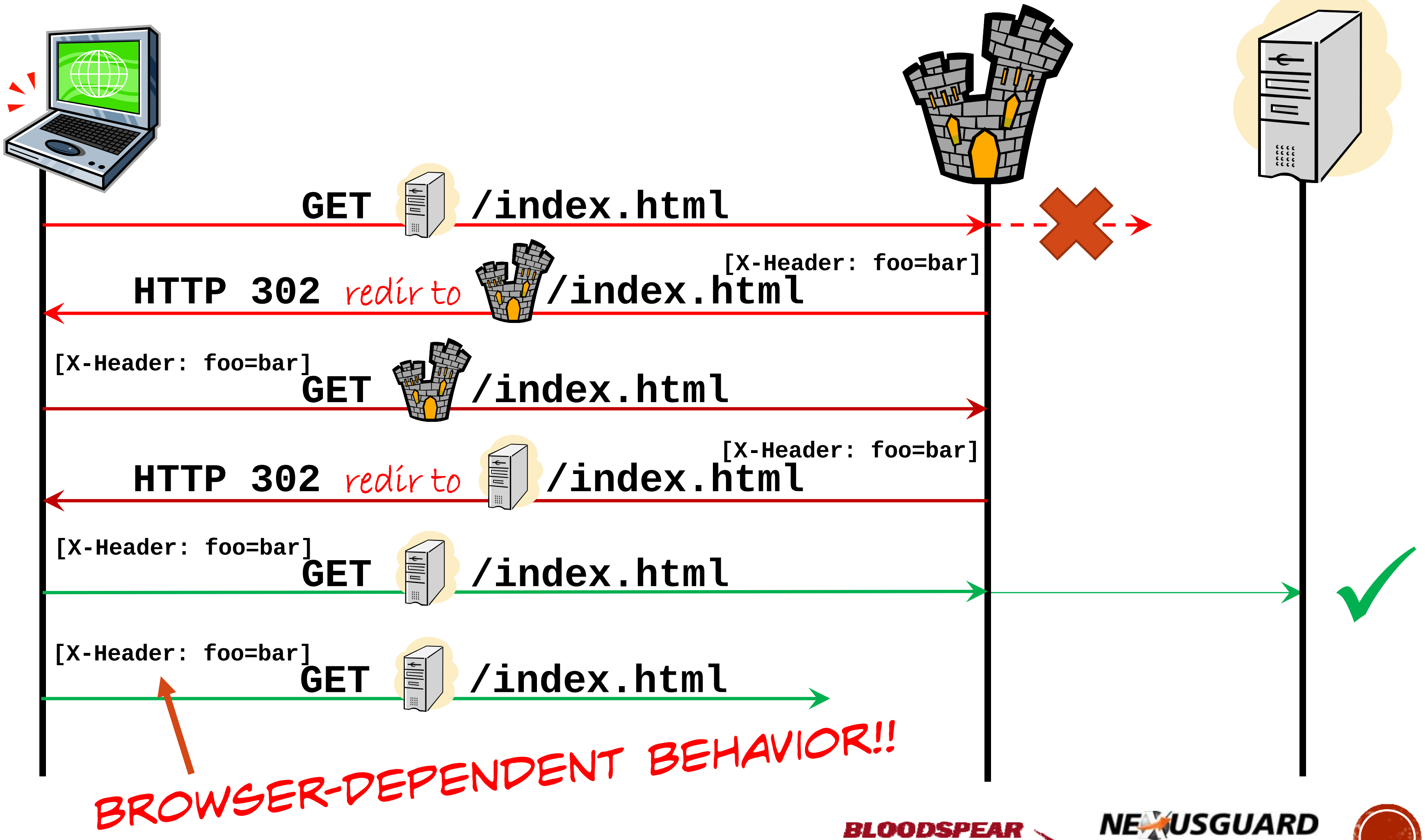
HTTP 302 redir to /index.html

GET /index.html

HTTP 302 redir to /index.html

GET /index.html

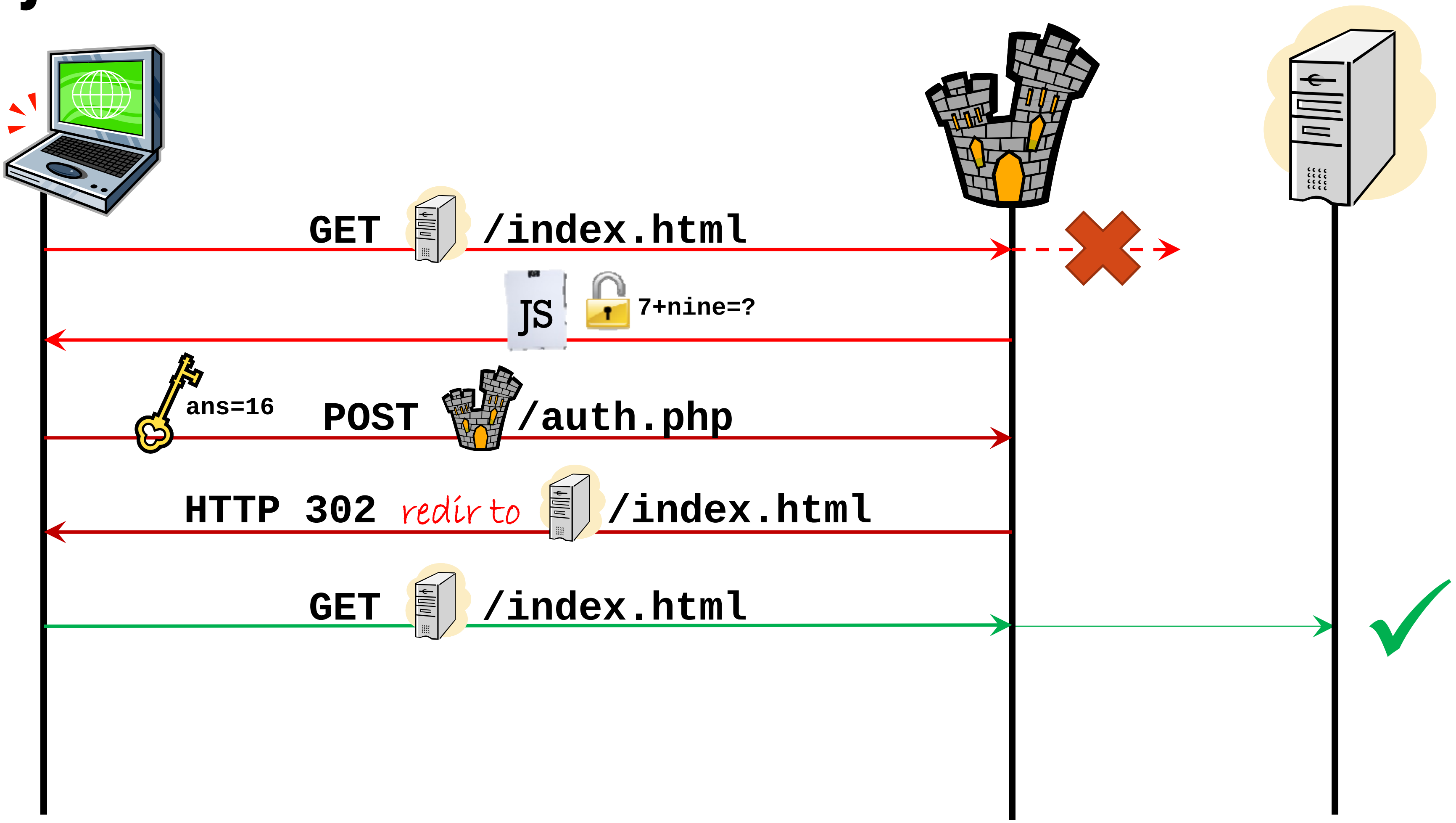
# HTTP COOKIE AUTH (HEADER TOKEN)



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

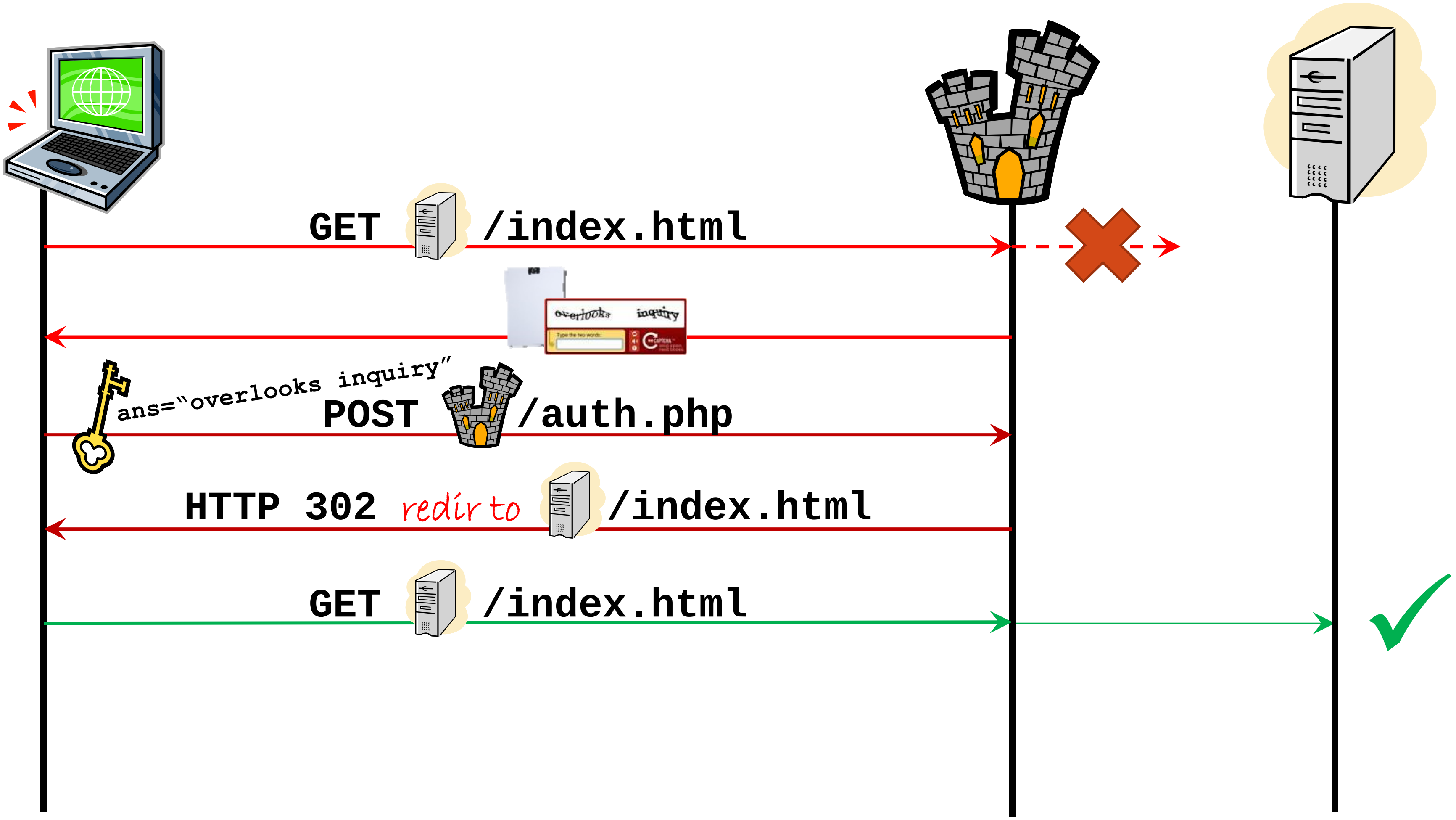
# JAVASCRIPT AUTH



BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

# CAPTCHA AUTH



GET /index.html

ans="overlooks inquiry"

POST /auth.php

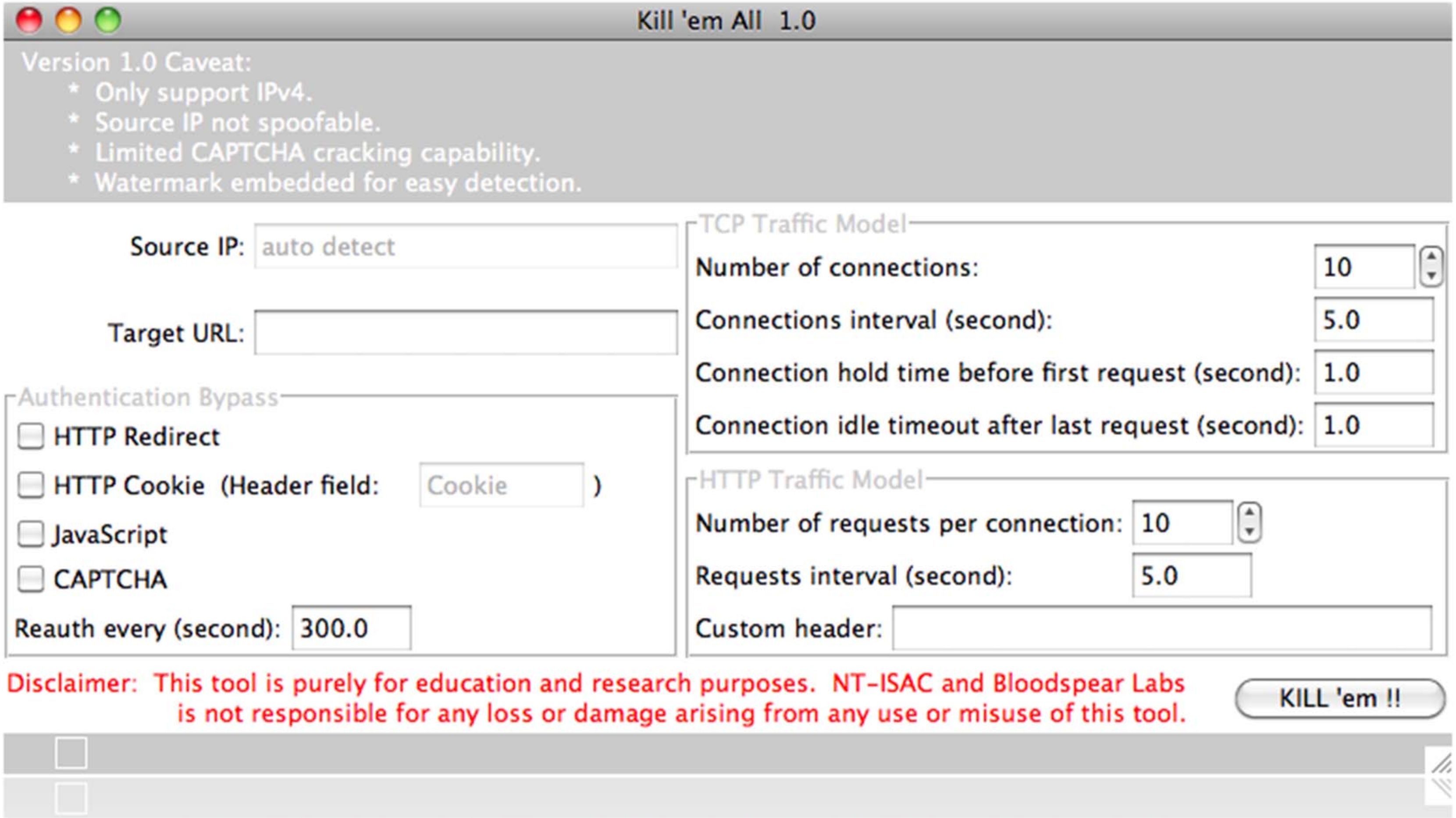
HTTP 302 redir to /index.html

GET /index.html

BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

# POC



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

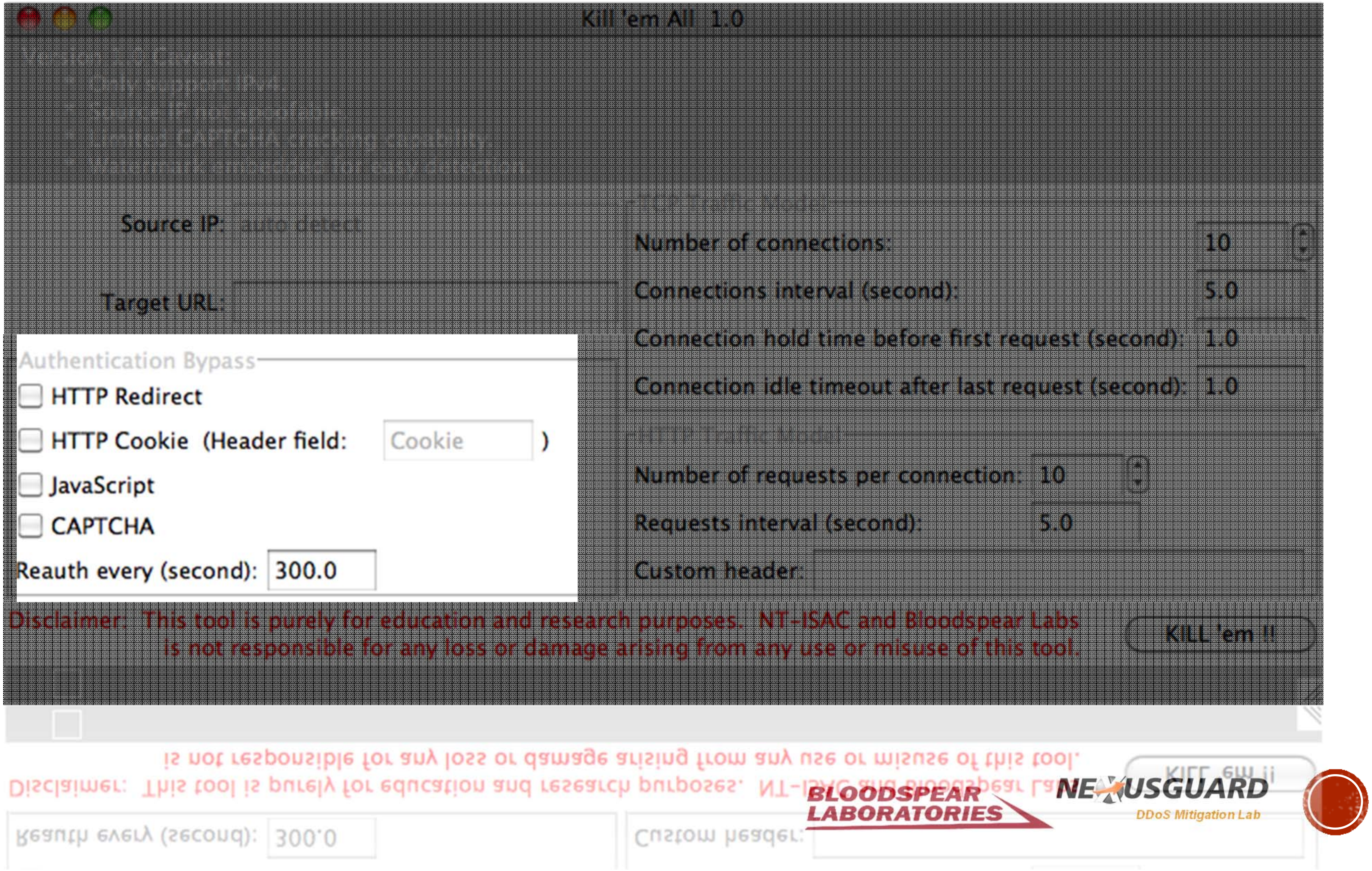
Custom header:

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.

BLOODSPEAR LABORATORIES

NEXUSGUARD DDoS Mitigation Lab

# POC



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

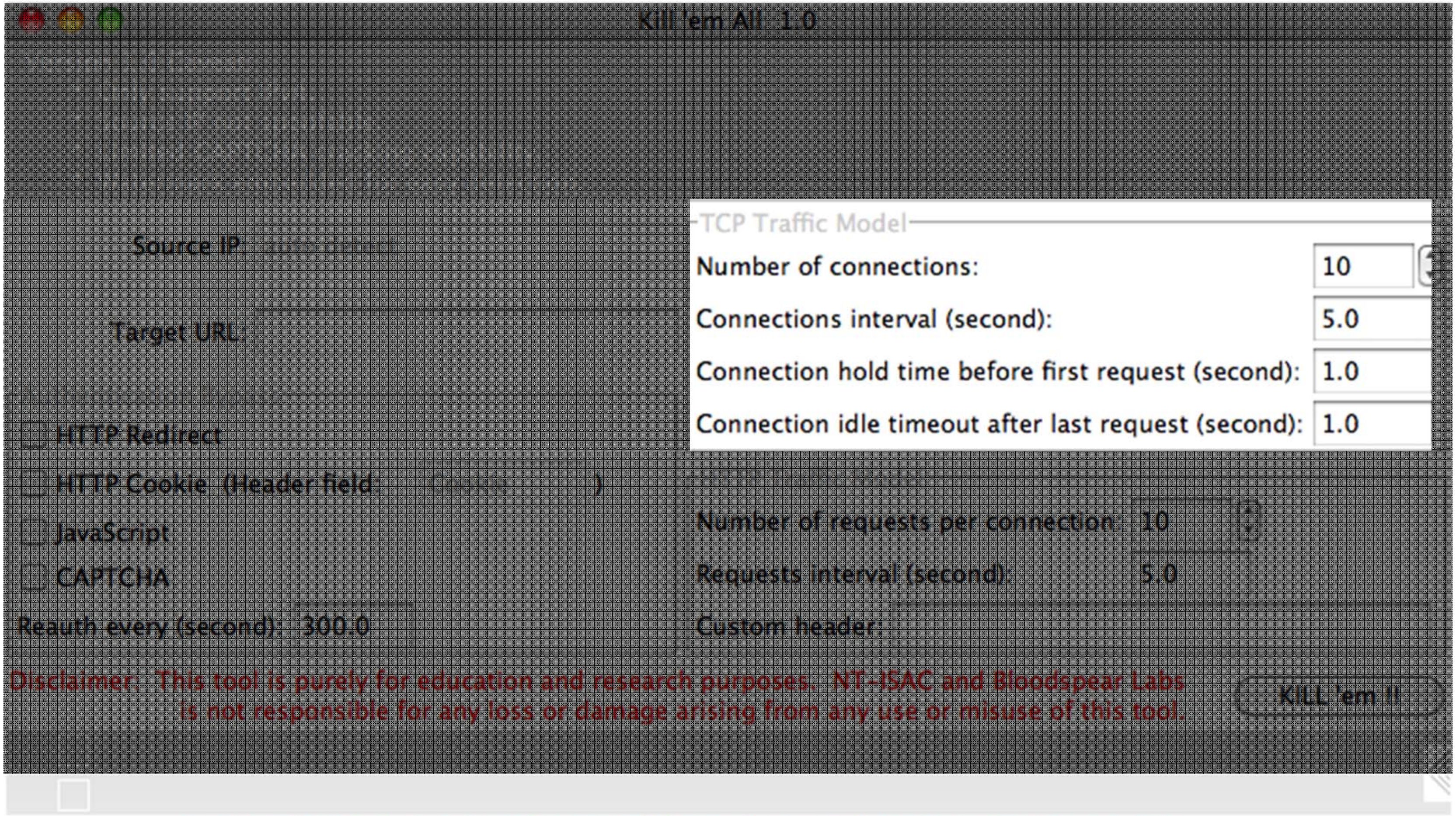
Custom header:

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.

BLOODSPEAR LABORATORIES

NEXUSGUARD DDoS Mitigation Lab

# POC



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

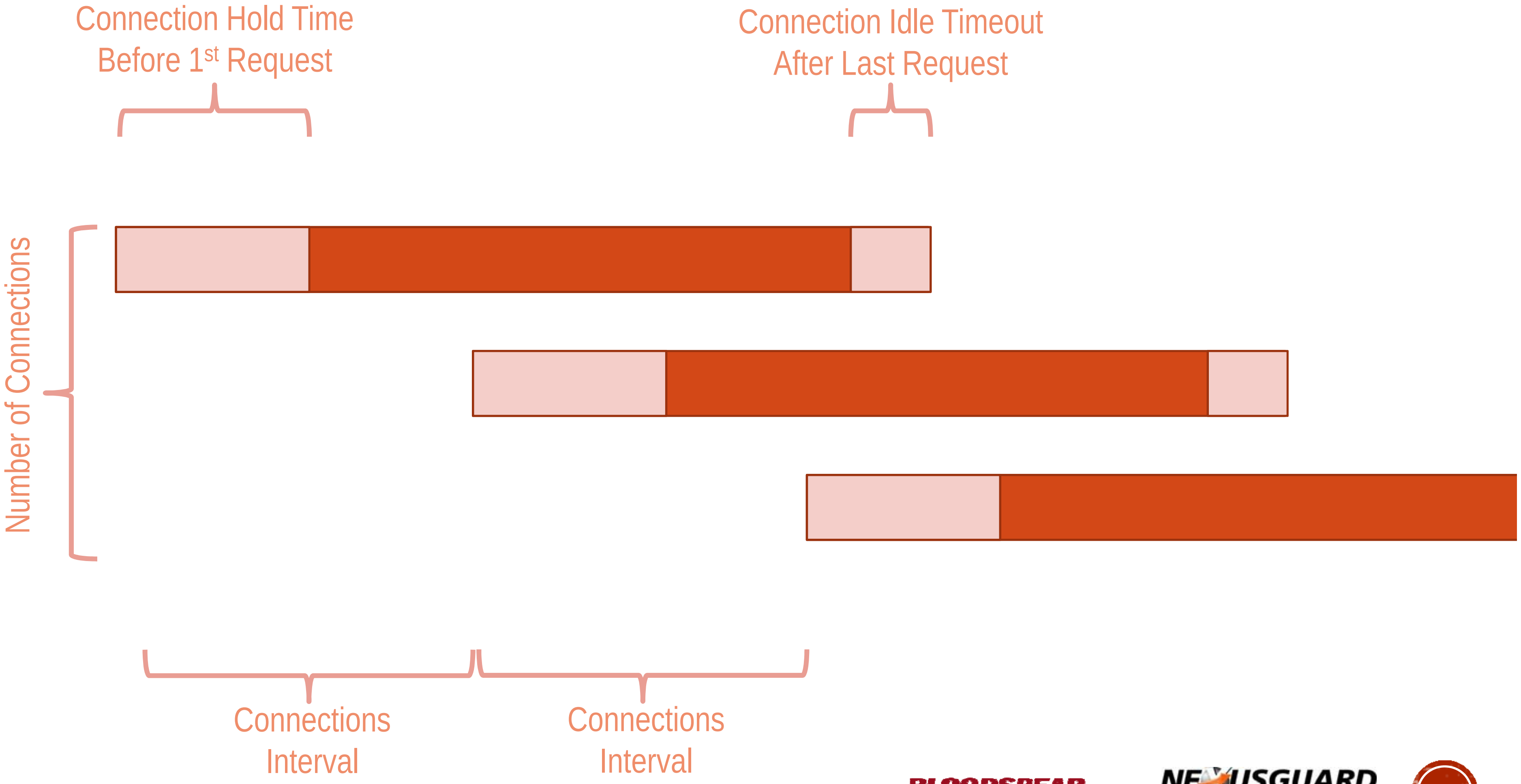
Custom header:

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.

BLOODSPEAR LABORATORIES

NEXUSGUARD DDoS Mitigation Lab

# TCP TRAFFIC MODEL



Connection Hold Time Before 1st Request

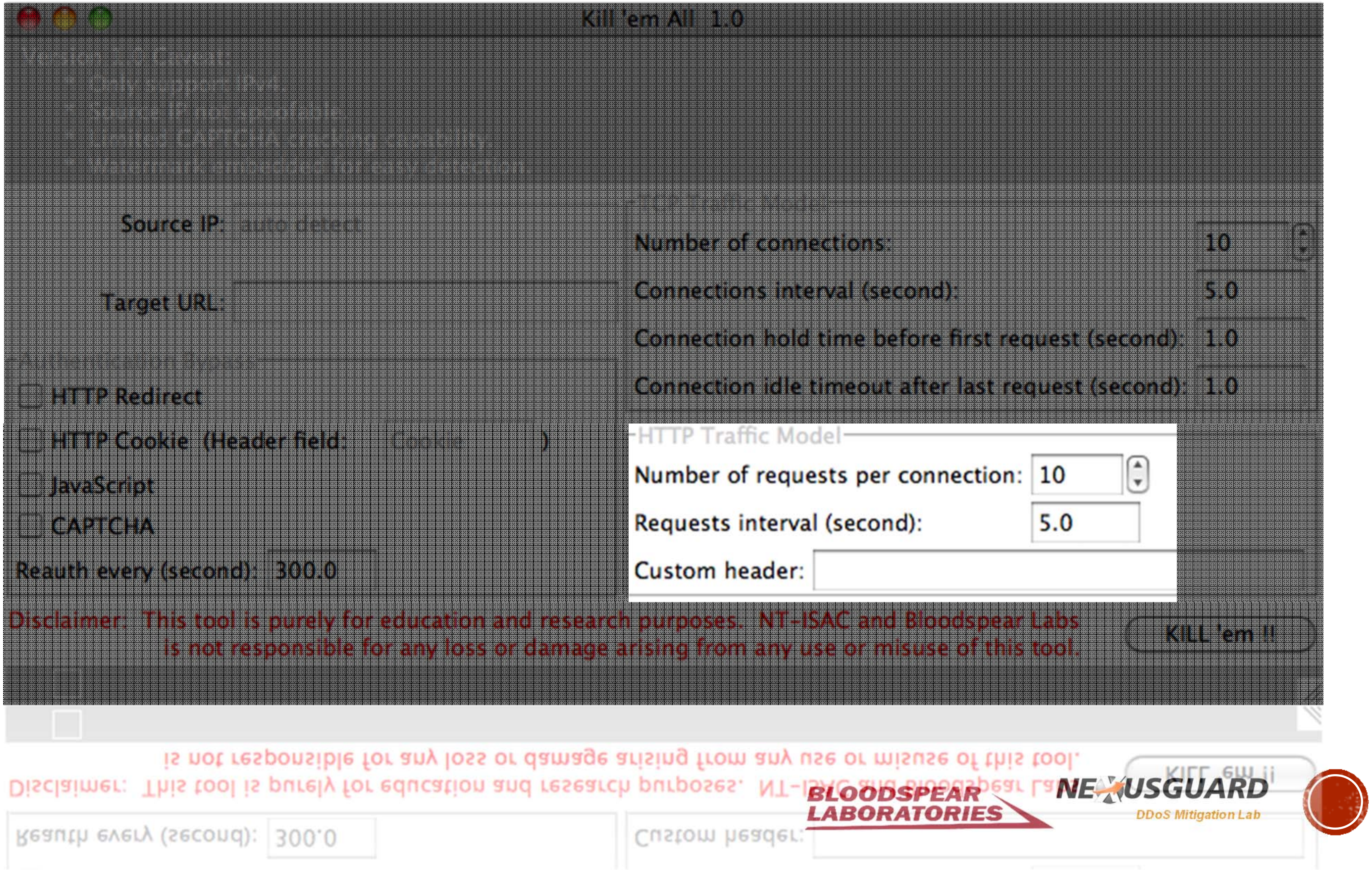
Connection Idle Timeout After Last Request

Number of Connections

Connections Interval

Connections Interval

# POC



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

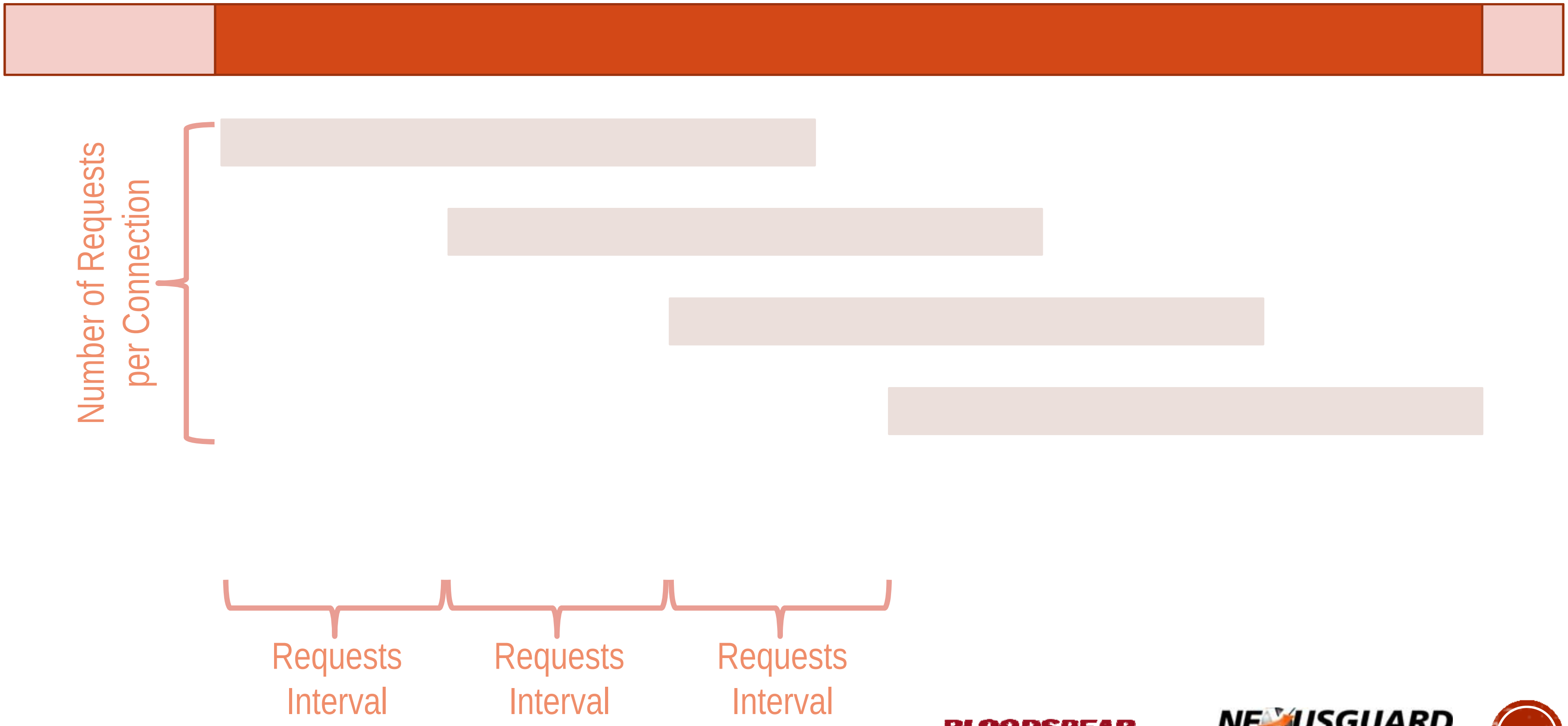
Number of requests per connection: 10

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



# AUTHENTICATION BYPASS

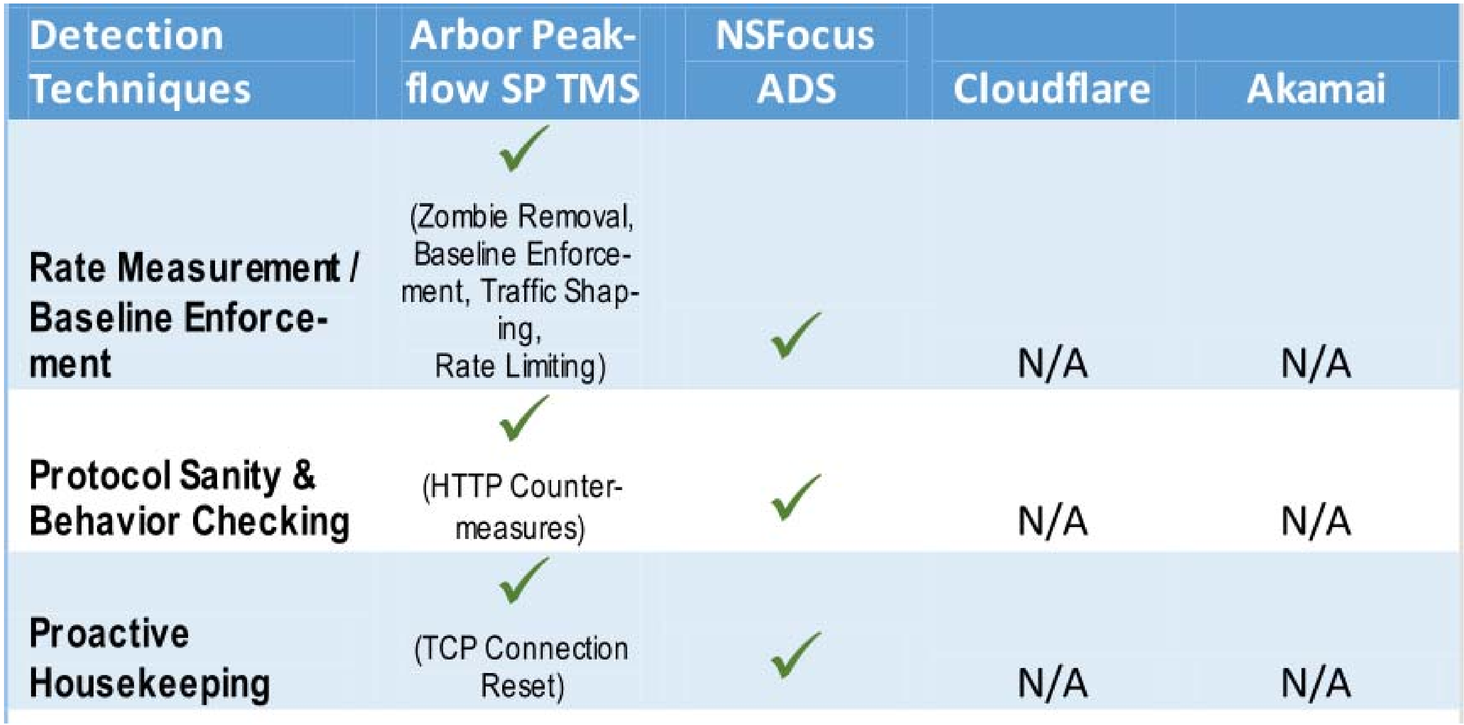
| Detection Techniques | Arbor Peak-flow SP TMS | NSFocus ADS | Cloudflare | Akamai |
|---|---|---|---|---|
| **Source Host Verification** | | | | |
| TCP SYN Authentication | ✓ | ✓ | N/A | N/A |
| HTTP Redirect Authentication | ✓ | ✓ | ✓ | N/A |
| HTTP Cookie Authentication | ✓ | ✓ | ✓ | N/A |
| JavaScript Authentication | —<br>(Not implemented)<br>in TMS) | ✓ | ✓ | N/A |
| CAPTCHA Authentication | —<br>(Not implemented<br>in TMS) | ✓ | ✗ | N/A |

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

BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

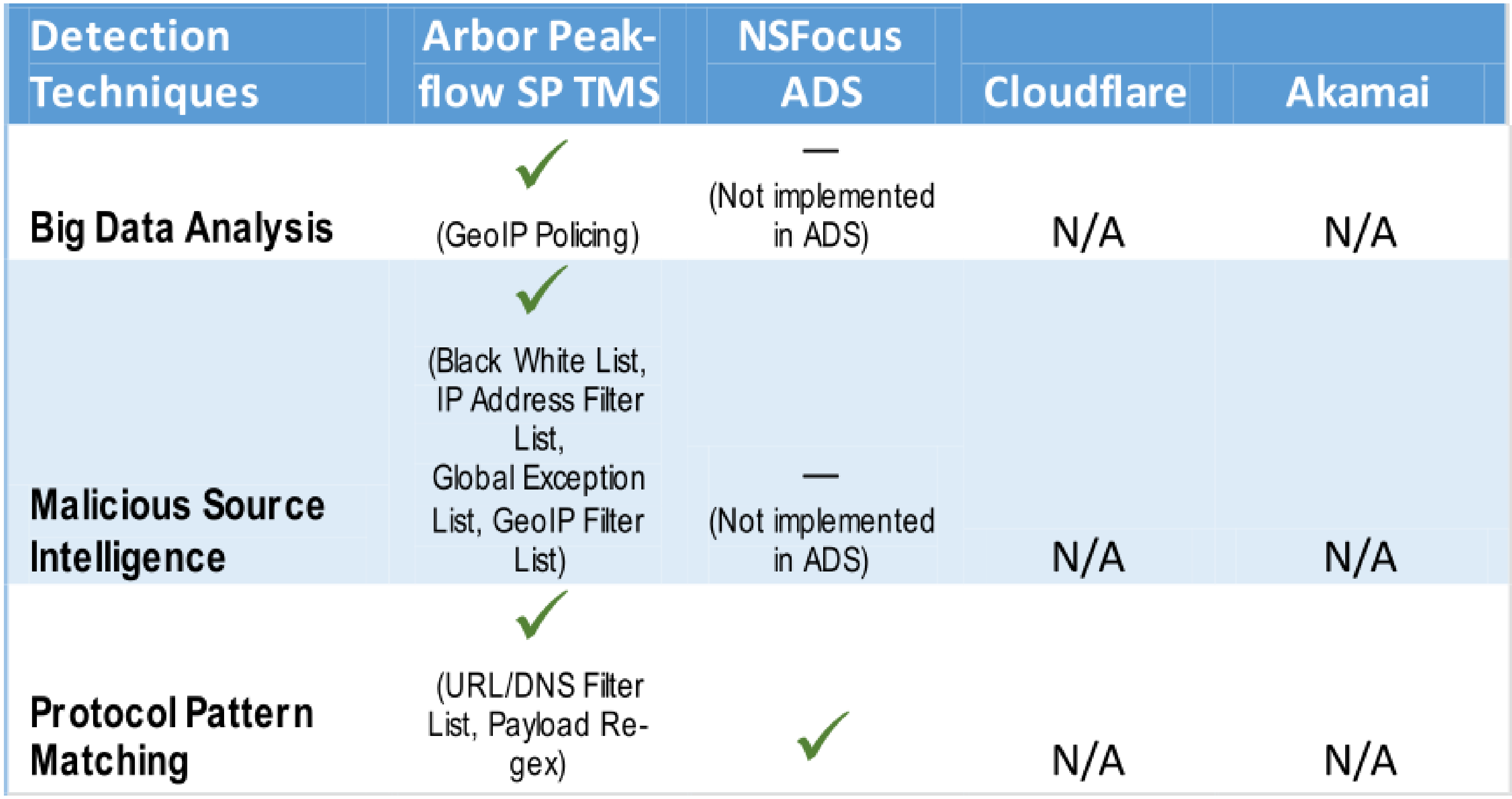
# POST-AUTHENTICATION ATTACK



| Detection Techniques | Arbor Peakflow SP TMS | NSFocus ADS | Cloudflare | Akamai |
|---|---|---|---|---|
| Rate Measurement / Baseline Enforcement | ✓<br>(Zombie Removal, Baseline Enforcement, Traffic Shaping,<br>Rate Limiting) | ✓ | N/A | N/A |
| Protocol Sanity & Behavior Checking | ✓<br>(HTTP Countermeasures) | ✓ | N/A | N/A |
| Proactive Housekeeping | ✓<br>(TCP Connection Reset) | ✓ | N/A | N/A |

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

# POST-AUTHENTICATION ATTACK



| Detection Techniques | Arbor Peak-flow SP TMS | NSFocus ADS | Cloudflare | Akamai |
|---|---|---|---|---|
| Big Data Analysis | ✓<br>(GeoIP Policing) | —<br>(Not implemented in ADS) | N/A | N/A |
| Malicious Source Intelligence | ✓<br>(Black White List, IP Address Filter List, Global Exception List, GeoIP Filter List) | —<br>(Not implemented in ADS) | N/A | N/A |
| Protocol Pattern Matching | ✓<br>(URL/DNS Filter List, Payload Re-gex) | ✓ | N/A | N/A |

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

BLOODSPEAR LABORATORIES

NEXUSGUARD
DDoS Mitigation Lab

# NEXT-GEN MITIGATION

# THANK YOU!

tony.miu@nexusguard.com

waileng.lee@bloodspear.org