Honeypots and Knowledge Discovery in Teaching Network Defense

Ping Wang, PhD, CISSP
University Professor
CAE POC
Robert Morris University
Email: wangp@rmu.edu

Overview

- **Focus**
  Role of honeypots for knowledge discovery in teaching network defense
- **Significance**
  - Major attacks on enterprise networks: DoS & system intrusions (Verizon, 2021)
  - Lack of knowledge for readiness & response (e.g. zero-day & ransomware)
  - Need for more talent with better knowledge for network defense against rising threats and attacks
- **Goal**
  To explore and illustrate the role of honeypot concept and strategy on knowledge dynamics from the *Art of War* in network defense

- **Disclaimer**
  Not a goal: Glorify or belittle any personality/book/culture.
  - Trojan horse malware ≠ Glorify/denigrate Homer/*Oddessy*/Greek culture
  - Salami attack ≠ advertise or demonize any deli shop

Theoretical Background

- ❑ Knowledge/intelligence – critical strategic factor to the outcome of warfare
  - ▪ Bacon (1561-1626): “Knowledge is power”
  - ▪ Modern KM: Individual K – Group K – Competition – Innovation
- ❑ Sun Tzu’s *The Art of War* (*AoW); 5th C. B.C.*
  AoW: 3 categories of knowing and not knowing vulnerability & strengths
  - ▪ If you know the enemy and know yourself, you need not fear the result of a hundred battles.
  - ▪ If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.
  - ▪ If you know neither the enemy nor yourself, you will succumb in every battle.
- ❑ K dynamics: K and ignorance are relative to each other
  - ▪ One’s power of knowledge grows if the opponent’s ignorance/arrogance grows
  - ▪ Pretend to be weak and the opponent may grow arrogant/ignorant (*AoW)*

Knowledge Discovery Matrix

	Knowledge	Goals
Yourself	• Know your own vulnerabilities • Know how to mitigate your own vulnerabilities • Know how to hide your assets and vulnerabilities from your opponent • Know how to set up fake vulnerabilities	• To minimize your vulnerabilities • To assess and manage your vulnerabilities and risks • Minimize your opponent's knowledge of your vulnerabilities • To mislead, misinform, distract, and deceive your opponent
Opponent	• Know your opponent's strengths • Know your opponent's assets and vulnerabilities • Know how to discover your opponent's vulnerabilities	• To be aware of threats and avoid striking the strong spots of your opponent • To exploit opponent's vulnerabilities • To maximize your knowledge of your opponent

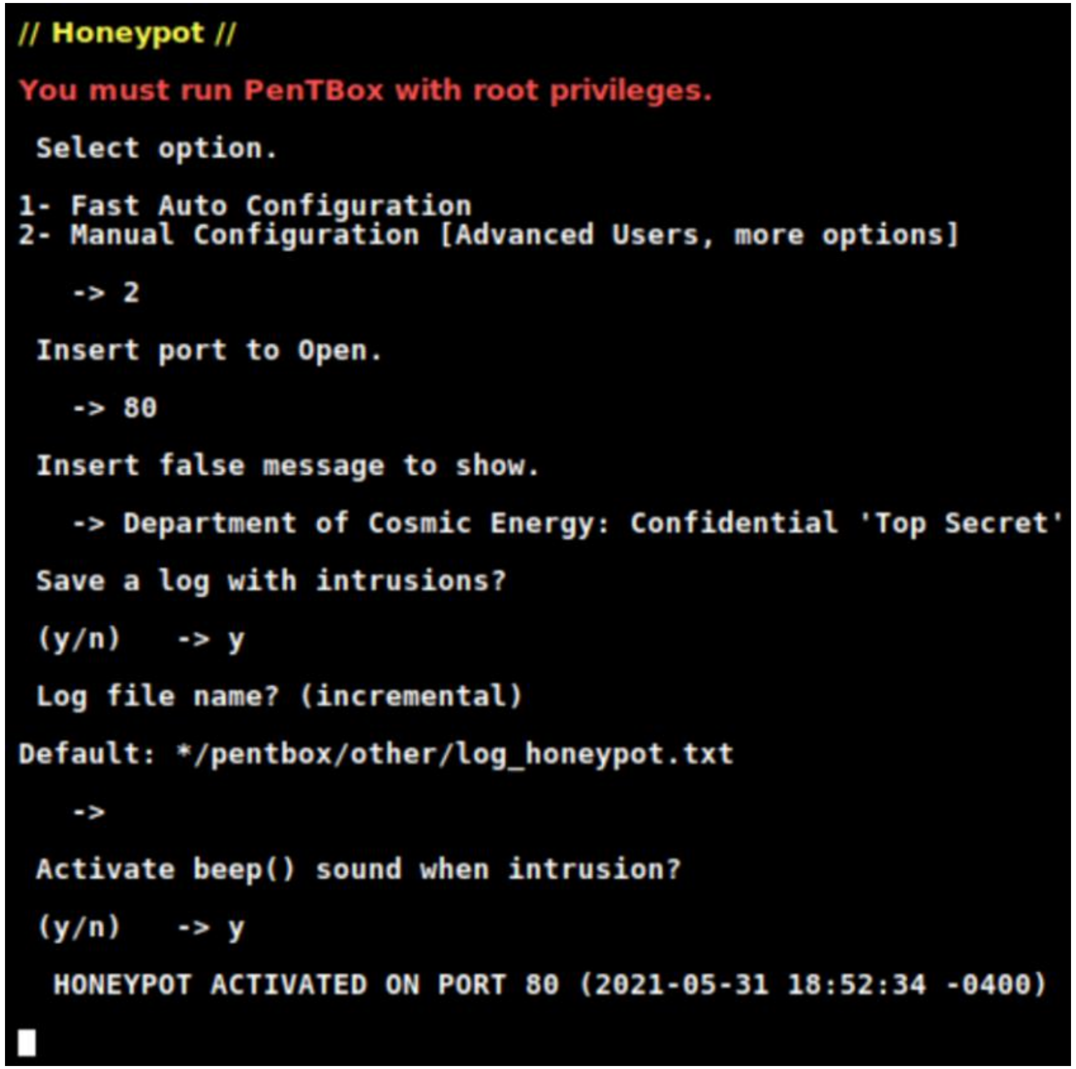
Honeypots & Knowledge Dynamics

- *AoW* Deception Concept
  - All warfare is based on deception.
  - Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near.
  - Hold out baits to entice the enemy. Feign disorder and crush him.
  - … Pretend to be weak, that he may grow arrogant.
- Honeypots
  - Intentional deception in cyber defense
  - To lure, mislead, trap, and monitor intruders using a bait
  - Increase your knowledge of intruders/opponents
  - Minimize knowledge or increase ignorance of intruders/opponents

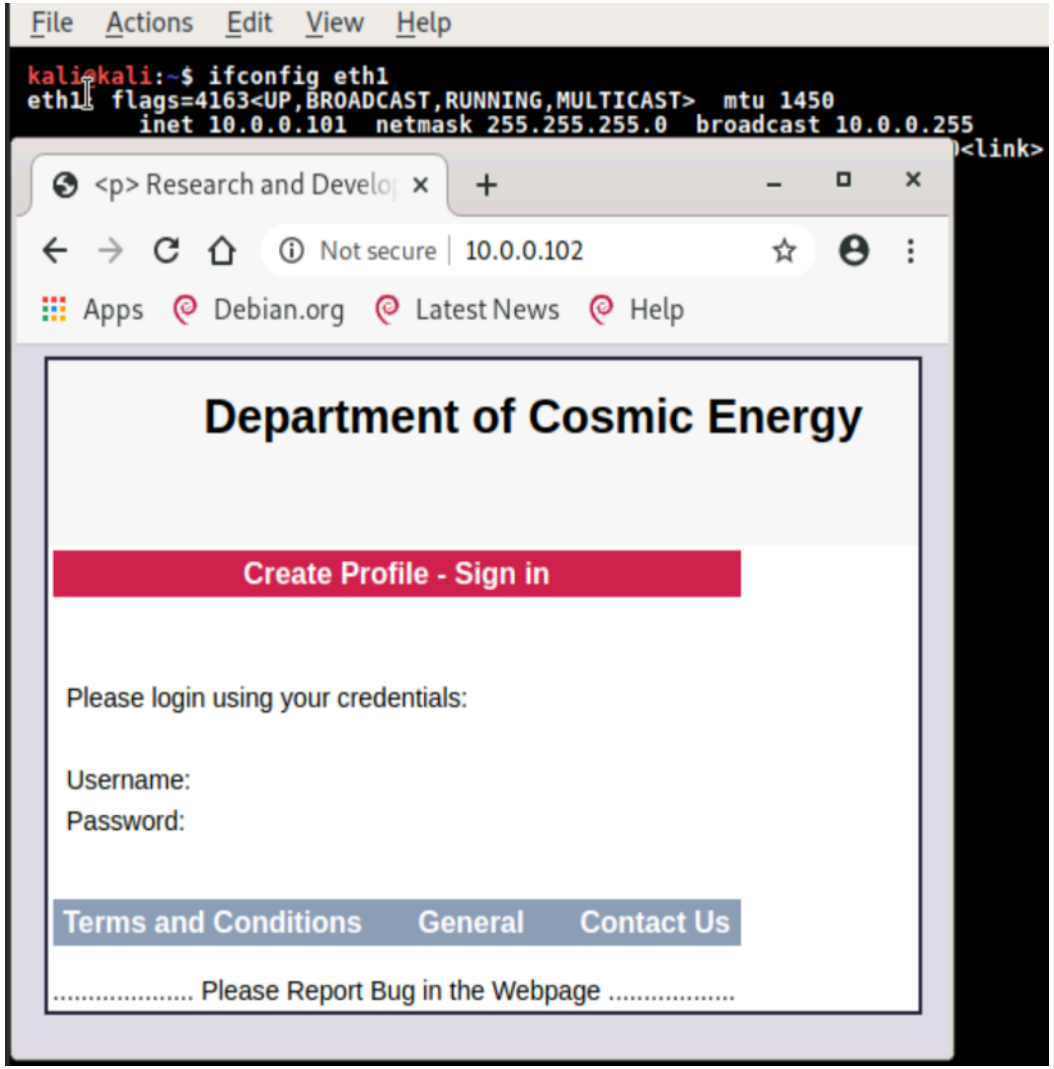
Simulation Methodology

- Virtual network simulation of intrusion detection with a honeypot
- 3 VMs: 2 Kali Linux VMs and Win10 VM on VirtualBox
- Target: Kali VM at 10.0.0.102
  - o Apache web server (bait) with a luring ‘Top Secret’ message label
  - o Firewall GUFW (Graphical Uncomplicated Firewall) set to Allow to be attractive
  - o PenTBox honeypot to listen for connections & monitor intruder activities
  - o Wireshark for traffic capture and analysis
- Tester: Kali VM at 10.0.0.101
  - Test web server
  - Lure intruders
- Attacker: Win10 VM at 10.0.0.103
  - o Launch intrusions and simulated DDoS flooding attacks
  - o Low Orbit Cannon (LOIC): Multiple simultaneous TCP/UDP requests to flood target
  - o Previous effective attacks on MITRE’s CVE

PenTBox Honeypot & Web Server Bait



```
// Honeypot //

You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   -> 2

 Insert port to Open.

   -> 80

 Insert false message to show.

   -> Department of Cosmic Energy: Confidential 'Top Secret'

 Save a log with intrusions?

 (y/n)   -> y

 Log file name? (incremental)

Default: */pentbox/other/log_honeypot.txt

   ->

 Activate beep() sound when intrusion?

 (y/n)   -> y

  HONEYPOT ACTIVATED ON PORT 80 (2021-05-31 18:52:34 -0400)

█
```



```
kali@kali:~$ ifconfig eth1
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1450
        inet 10.0.0.101  netmask 255.255.255.0  broadcast 10.0.0.255
                                                                )<link>
```

Department of Cosmic Energy

Create Profile - Sign in

Please login using your credentials:

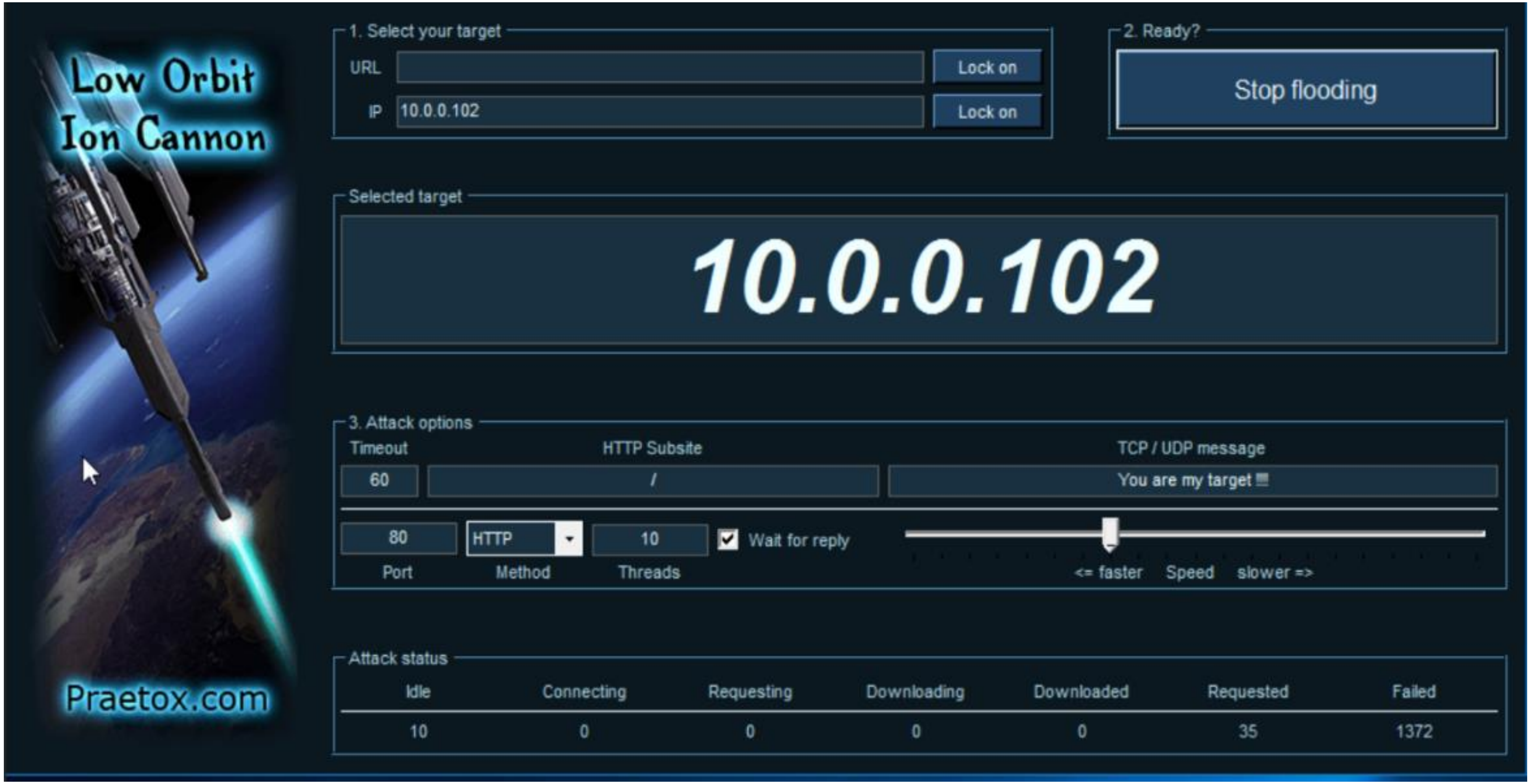
Username:

Password:

Terms and Conditions | General | Contact Us

.... Please Report Bug in the Webpage ....

LOIC DDoS Launched from Attacker VM



1. Select your target

URL:

IP: 10.0.0.102

2. Ready?

Selected target: 10.0.0.102

3. Attack options

Timeout: 60

HTTP Subsite: /

TCP / UDP message: You are my target !!!

Port: 80

Method: HTTP

Threads: 10

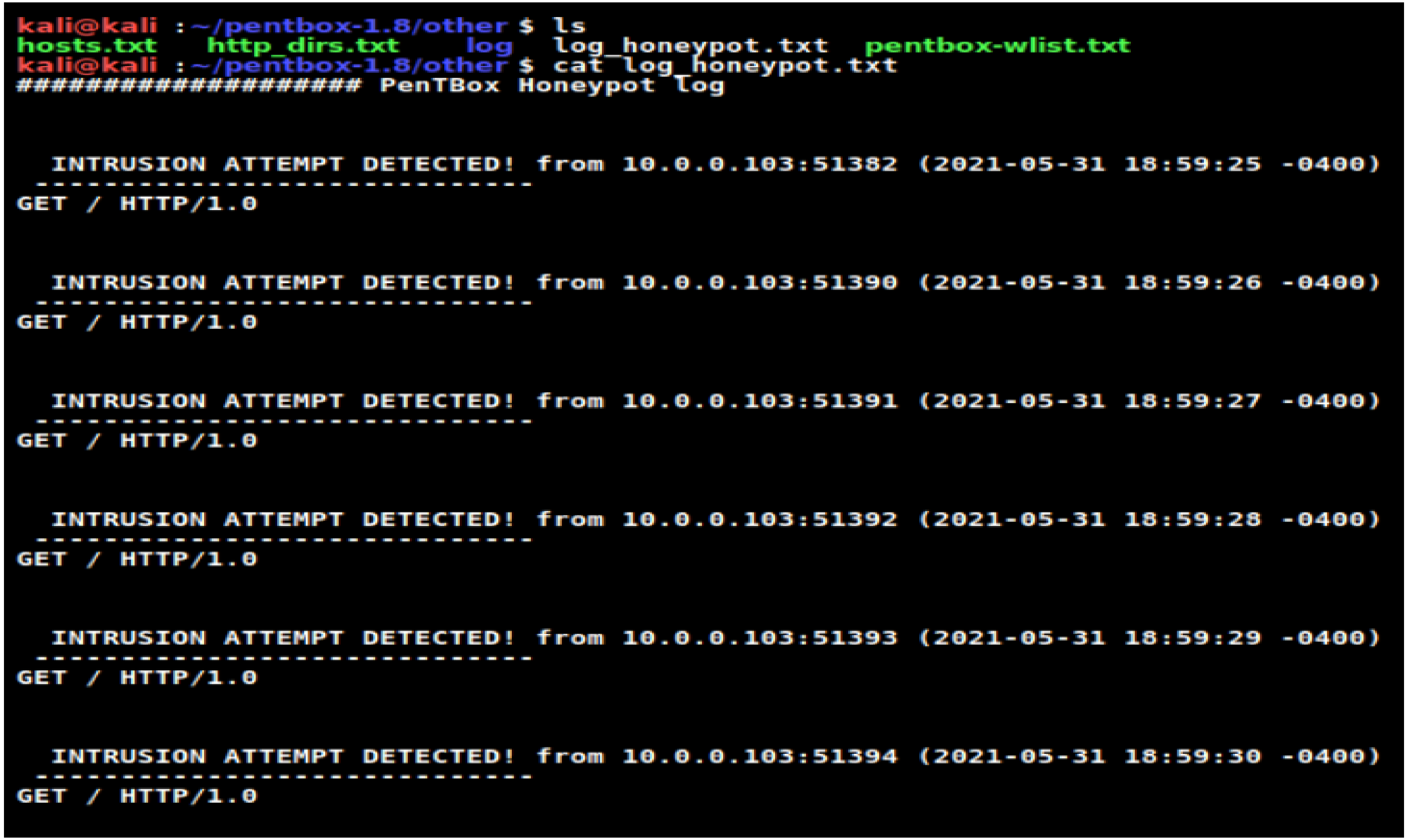
☑ Wait for reply

<= faster Speed slower =>

Attack status

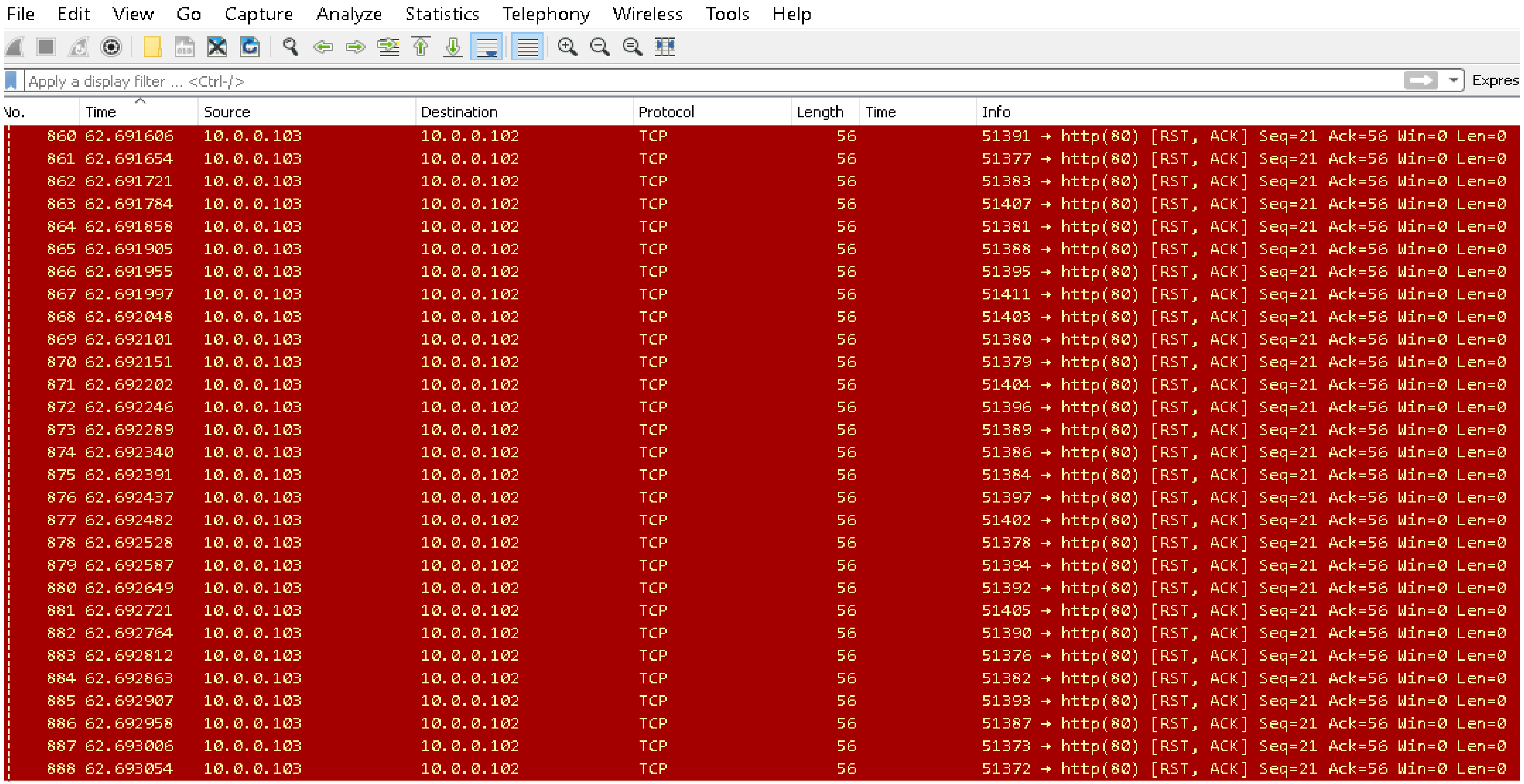
Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
10	0	0	0	0	35	1372

Intrusion Detections In Honeypot Logs



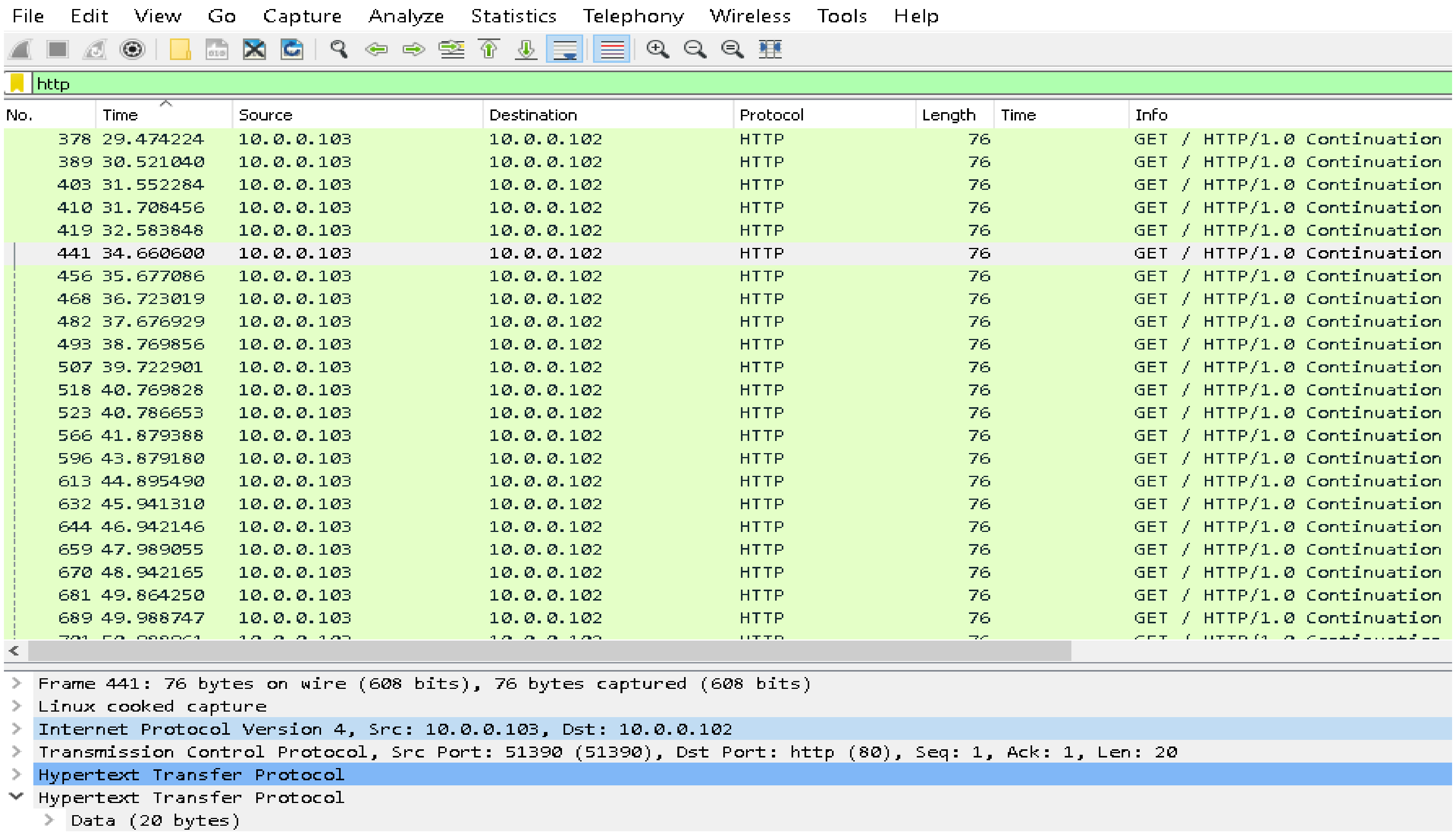
```
kali@kali :~/pentbox-1.8/other $ ls
hosts.txt   http_dirs.txt   log   log_honeypot.txt   pentbox-wlist.txt
kali@kali :~/pentbox-1.8/other $ cat log_honeypot.txt
#################### PenTBox Honeypot log


  INTRUSION ATTEMPT DETECTED! from 10.0.0.103:51382 (2021-05-31 18:59:25 -0400)
 -----------------------------
GET / HTTP/1.0


  INTRUSION ATTEMPT DETECTED! from 10.0.0.103:51390 (2021-05-31 18:59:26 -0400)
 -----------------------------
GET / HTTP/1.0


  INTRUSION ATTEMPT DETECTED! from 10.0.0.103:51391 (2021-05-31 18:59:27 -0400)
 -----------------------------
GET / HTTP/1.0


  INTRUSION ATTEMPT DETECTED! from 10.0.0.103:51392 (2021-05-31 18:59:28 -0400)
 -----------------------------
GET / HTTP/1.0


  INTRUSION ATTEMPT DETECTED! from 10.0.0.103:51393 (2021-05-31 18:59:29 -0400)
 -----------------------------
GET / HTTP/1.0


  INTRUSION ATTEMPT DETECTED! from 10.0.0.103:51394 (2021-05-31 18:59:30 -0400)
 -----------------------------
GET / HTTP/1.0
```

Wireshark Capture of Flooding Requests



```
No.   Time       Source      Destination  Protocol  Length  Time  Info
  860 62.691606  10.0.0.103  10.0.0.102   TCP           56        51391 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  861 62.691654  10.0.0.103  10.0.0.102   TCP           56        51377 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  862 62.691721  10.0.0.103  10.0.0.102   TCP           56        51383 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  863 62.691784  10.0.0.103  10.0.0.102   TCP           56        51407 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  864 62.691858  10.0.0.103  10.0.0.102   TCP           56        51381 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  865 62.691905  10.0.0.103  10.0.0.102   TCP           56        51388 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  866 62.691955  10.0.0.103  10.0.0.102   TCP           56        51395 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  867 62.691997  10.0.0.103  10.0.0.102   TCP           56        51411 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  868 62.692048  10.0.0.103  10.0.0.102   TCP           56        51403 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  869 62.692101  10.0.0.103  10.0.0.102   TCP           56        51380 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  870 62.692151  10.0.0.103  10.0.0.102   TCP           56        51379 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  871 62.692202  10.0.0.103  10.0.0.102   TCP           56        51404 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  872 62.692246  10.0.0.103  10.0.0.102   TCP           56        51396 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  873 62.692289  10.0.0.103  10.0.0.102   TCP           56        51389 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  874 62.692340  10.0.0.103  10.0.0.102   TCP           56        51386 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  875 62.692391  10.0.0.103  10.0.0.102   TCP           56        51384 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  876 62.692437  10.0.0.103  10.0.0.102   TCP           56        51397 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  877 62.692482  10.0.0.103  10.0.0.102   TCP           56        51402 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  878 62.692528  10.0.0.103  10.0.0.102   TCP           56        51378 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  879 62.692587  10.0.0.103  10.0.0.102   TCP           56        51394 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  880 62.692649  10.0.0.103  10.0.0.102   TCP           56        51392 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  881 62.692721  10.0.0.103  10.0.0.102   TCP           56        51405 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  882 62.692764  10.0.0.103  10.0.0.102   TCP           56        51390 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  883 62.692812  10.0.0.103  10.0.0.102   TCP           56        51376 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  884 62.692863  10.0.0.103  10.0.0.102   TCP           56        51382 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  885 62.692907  10.0.0.103  10.0.0.102   TCP           56        51393 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  886 62.692958  10.0.0.103  10.0.0.102   TCP           56        51387 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  887 62.693006  10.0.0.103  10.0.0.102   TCP           56        51373 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
  888 62.693054  10.0.0.103  10.0.0.102   TCP           56        51372 → http(80) [RST, ACK] Seq=21 Ack=56 Win=0 Len=0
```

HTTP GET Requests Captured



http

No.	Time	Source	Destination	Protocol	Length	Time	Info
378	29.474224	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
389	30.521040	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
403	31.552284	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
410	31.708456	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
419	32.583848	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
441	34.660600	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
456	35.677086	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
468	36.723019	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
482	37.676929	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
493	38.769856	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
507	39.722901	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
518	40.769828	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
523	40.786653	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
566	41.879388	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
596	43.879180	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
613	44.895490	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
632	45.941310	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
644	46.942146	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
659	47.989055	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
670	48.942165	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
681	49.864250	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation
689	49.988747	10.0.0.103	10.0.0.102	HTTP	76		GET / HTTP/1.0 Continuation

```
> Frame 441: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
> Linux cooked capture
> Internet Protocol Version 4, Src: 10.0.0.103, Dst: 10.0.0.102
> Transmission Control Protocol, Src Port: 51390 (51390), Dst Port: http (80), Seq: 1, Ack: 1, Len: 20
> Hypertext Transfer Protocol
v Hypertext Transfer Protocol
    > Data (20 bytes)
```

Conclusions

- Recap: Illustrate network K discovery with honeypot & DDoS attacks
- Limitation: Low interaction honeypot for educational use
- Educational Value
  - Lower Value: Hands-on experiential learning on pentesting tools
  - Higher Value: Stimulate students’ strategic/creative thinking on the dynamics of knowledge/intelligence in cyber defense
- Credits
  Based on IACIS Best Paper Award research (Wang & D’Cruze, 2021)
- Questions?
- Thank you!