Pentest Accountability By Analyzing Network Traffic & Network Traffic Metadata

RP1 Presentation By Henk van Doorn & Marko Spithoff

Relevance

Security Audits

- Company Detects (Attempted) Breach
- Accountability Of Actions

Research Questions

- Is it feasible to log all network traffic live during the execution of a pentest given specific storage, CPU and throughput constraints?
- When performing a live capture of network metadata during the execution of a pentest,
  - What information can be extracted from the metadata?
  - Can accountability of actions be provided based on metadata from the captured network traffic?
  - Based on the metadata from the captured network traffic could the captured traffic be categorized into attack vectors of the Intrusion Kill Chain?

Research Questions Continued

- Is it feasible to log network metadata live during the execution of a pentest given specific storage, CPU and throughput constraints?
- What legal aspects come into consideration when storing the collected (meta)data based on current European legislation?

Research Questions

- *Is it feasible to log network traffic live during the execution of a pentest given specific storage, CPU and throughput constraints?*

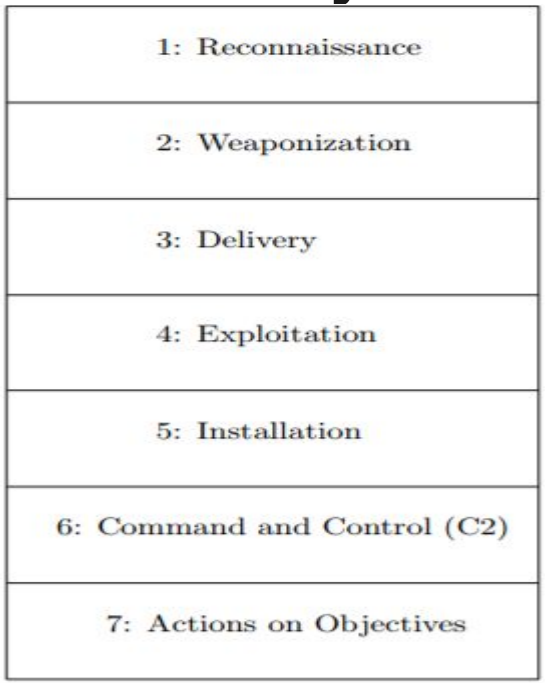
❏ Full Capture

❏ Metadata

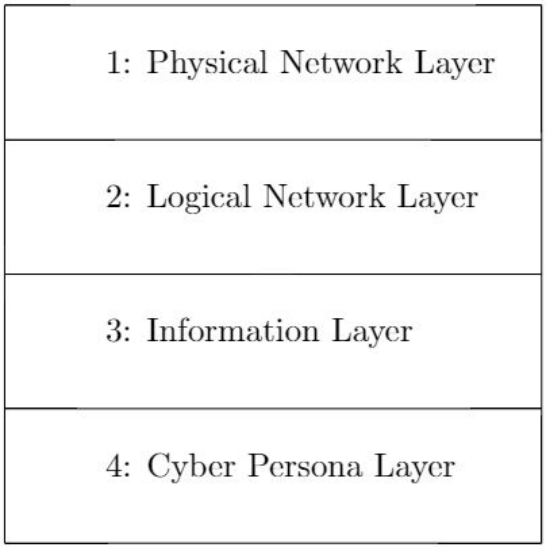
Related Work

- What Is Pentesting (Bishop)
- Cyber Kill Chain (Hutchins et al.)
- Using Metadata For Security Analysis (Feamster)
- Fast Portscan Detection (Jung et al.)
- Metadata Based Intrusion Detection (Yasinsac And Leckie)
- Toward Scalable Internet Traffic Measurement and Analysis with Hadoop(Lee and Lee)

Taxonomy Of A Pentest

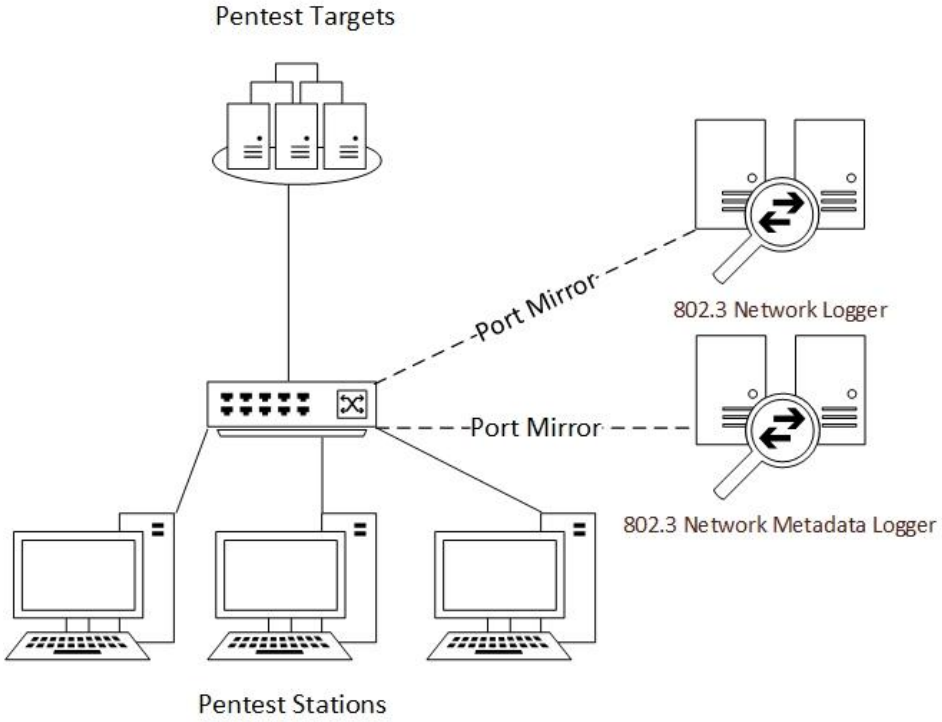


Hutchins et al.

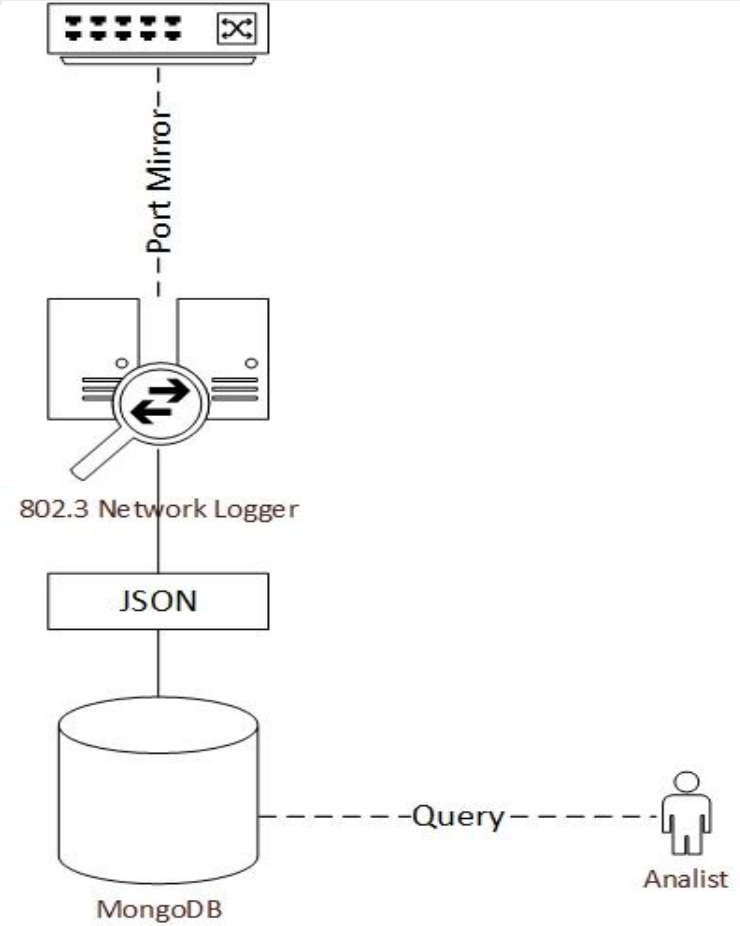


US DOD, Clark

Experiment Setup

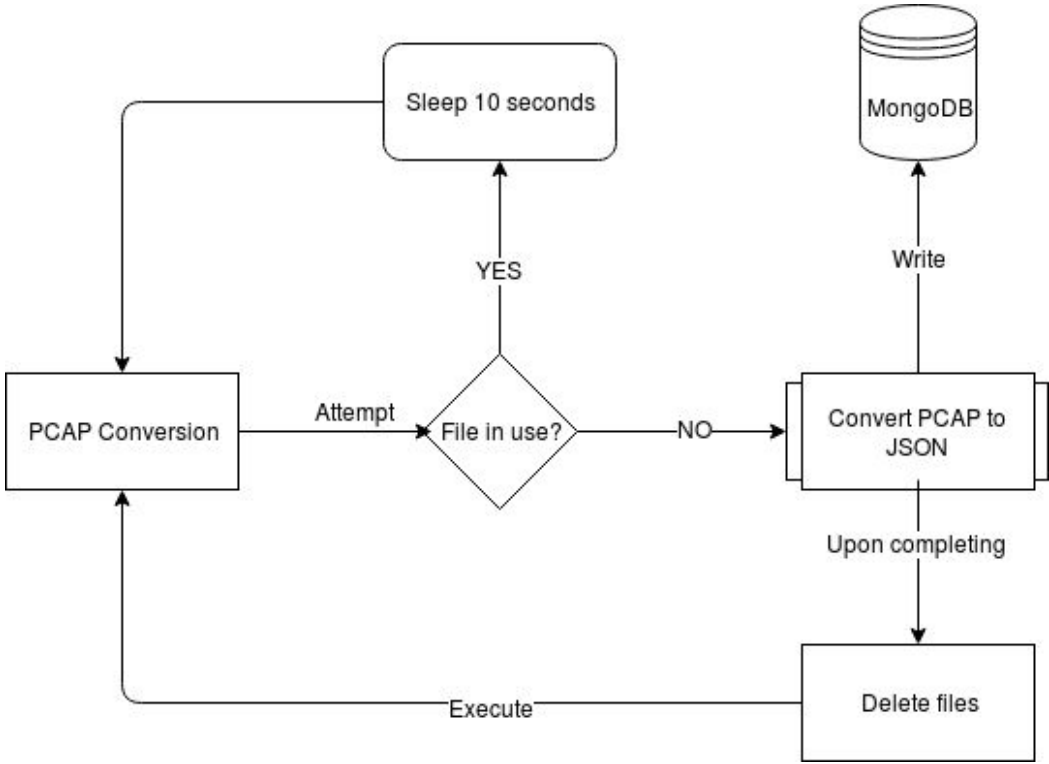


Full Data Capture



Flowchart
PCAP conversion

- Prevent file conflicts
- Convert to JSON
- Import into MongoDB
- Remove old files

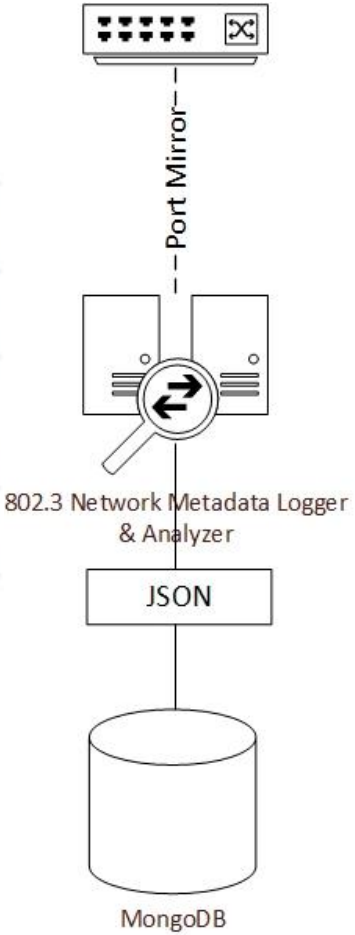


Results:Full Data Capture Verification

```
  % sudo ping -f -c 1000000 192.168.1.107

1000000 packets transmitted, 1000000 received, 0% packet loss, time
151825ms

MongoDB Enterprise > db.ICMP.count({      "layers.icmp" : {"$exists" :
true}});

2000000
```

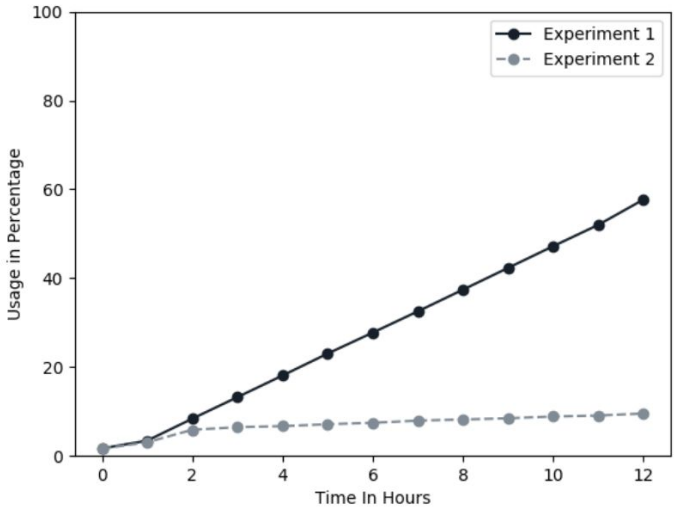
Metadata Capture

Destination Mac Address, Source Mac Address	Data Link Layer
IP Version, Destination IP Address, Source IP Address	Network Layer
TCP Source Port, TCP Destination Port, TCP Sequence Number, TCP Flags, TCP Window Size	Transport Layer
UDP Source Port, UDP Destination Port	Transport Layer



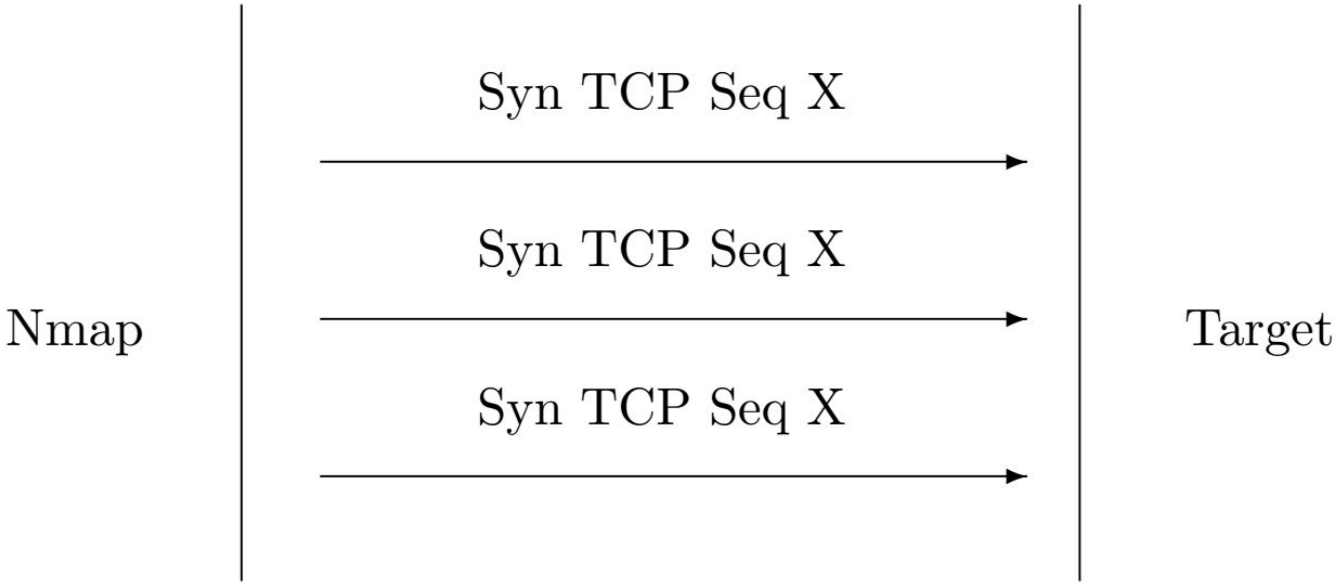
Results: Metadata Capture

- Software Limitations
  - Scapy vs Sockets
  - Python vs C
- Hardware Constraints
  - Storage
  - CPU
  - Network
  - Memory
  - Disk IO



Nmap TCP Detection

- Mean Completion Time: 13.302947s



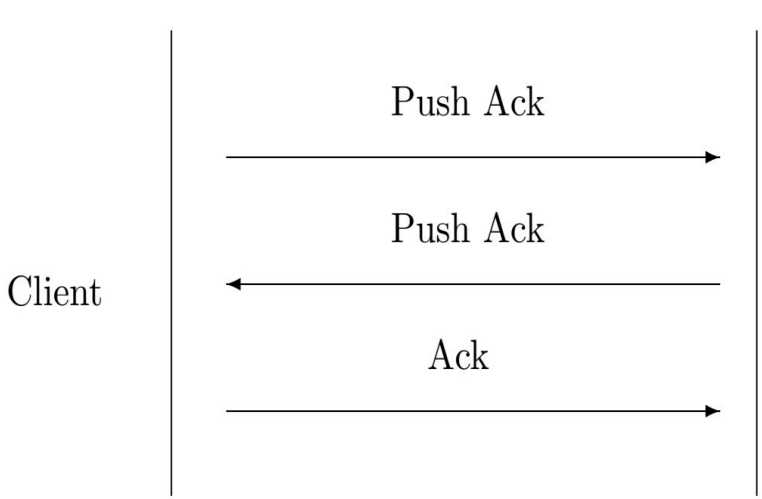
Results: Nmap TCP Detection

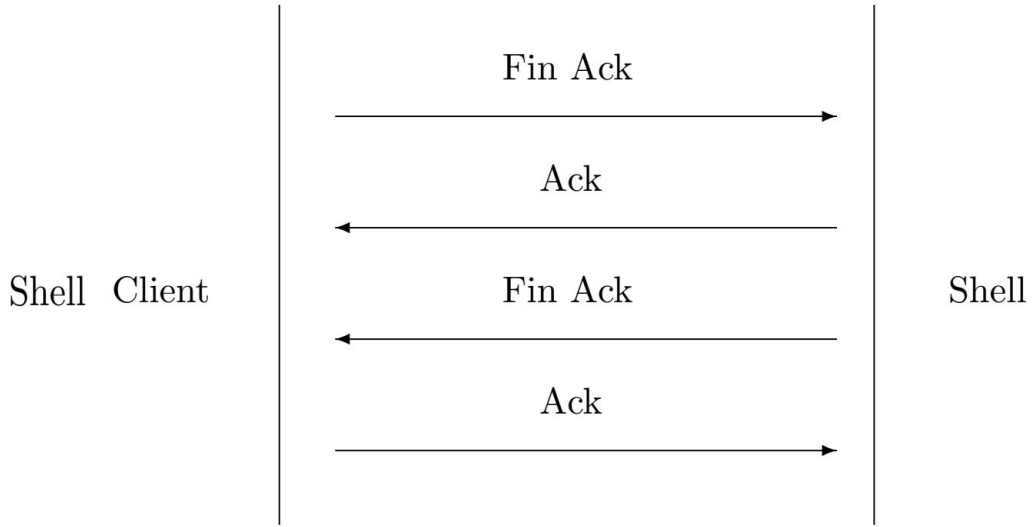
- 100 Nmaps Performed From Virtual Host
- 100 Nmap Scans Detected
  - Port Scan Detected On: 2018-01-31 11:30:43,993446, From IP: 192.168.1.109, To IP:192.168.1.108, TCP Sequence:2393481580
  - Port Scan Stopped On: 2018-01-31 11:30:47,907038, Number Of Ports Scanned 615, TCP Sequence:2393481580
- Accountability: Plausible

Tcp Shell Detection

- Character At A time Mode
- "almost all requests to web servers have their TCP PUSH and ACK flags set" (Roesch et al.)
    - Could This Be Applied To TCP Shells?

TCP Shell Detection Continued





Results:TCP Shell Detection

- 100 Reverse TCP Shell Connections Build & Destroyed
- 100 Reverse TCP Shells Detected
  - Connection Detected On: 2018-01-29 14:50:58,419131, IP: 192.168.1.108:8080, Connects To IP: 192.168.1.107:39294
  - Connection Stopped On: 2018-01-29 14:51:08.424046, From IP: 192.168.1.108:8080, To IP: 192.168.1.107:39294
- Accountability: Plausible

Results

- Storing All Network Traffic Seems Plausible With Enterprise Solutions
  - 12 Hour Total 5,5 GiB
- Storing All Network Metadata Seems Plausible With Small Business Solutions
  - 12 Hour Total 261 MiB
- Achieving Accountability Seems Plausible Using Metadata
- Hardware Performance Differences
- Further Research Needed For Proposed Methods
- Scapy Makes Inefficient Use Of System Resources
- Python Is Not Fast Enough To Log Traffic Realtime

Discussion

- Legal Aspects Of Storing All Data

Future Work

- Research Into Proposed Methods
  - Other TCP Protocols
  - Detection Methods Known Or New?
- Rewriting The Methods Into C
- Rewrite Methods For UDP Thresholds
- Effect Of VPN’s On Proposed Methods
- Multithreading on pcap(ng)

Questions?