Packet Analysis for Network Security

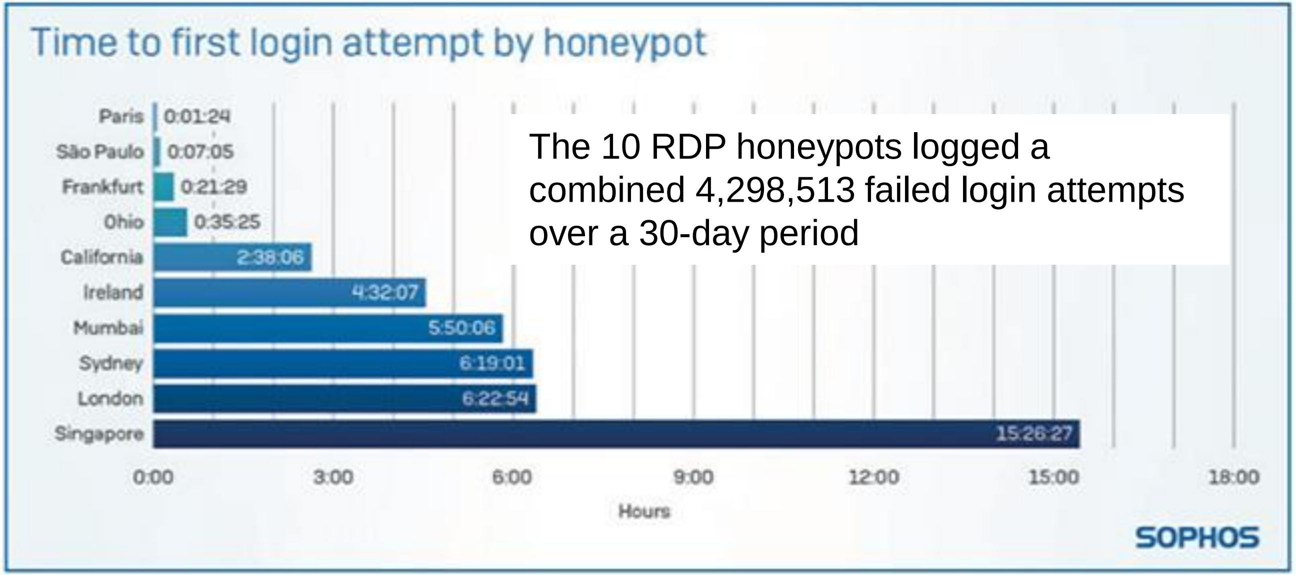
Agenda

- Why Network Security?
- Attack Frameworks
- Detection analysis techniques
- List of Free Open Source Software (F.O.S.S)
- Overview of Security Onion
- Demo Time

Amount of attacks – SSH attack

- APNIC 46 Network security workshop, deployed 7 honeypots to a cloud service
- 21,077 attacks in 24 hours
- Top 5 sensors
  - training06 (8,431 attacks)
  - training01 (5,268 attacks)
  - training04 (2,208 attacks)
  - training07 (2,025 attacks)
  - training03 (1,850 attacks)

Time of attack – RDP attack



The 10 RDP honeypots logged a combined 4,298,513 failed login attempts over a 30-day period

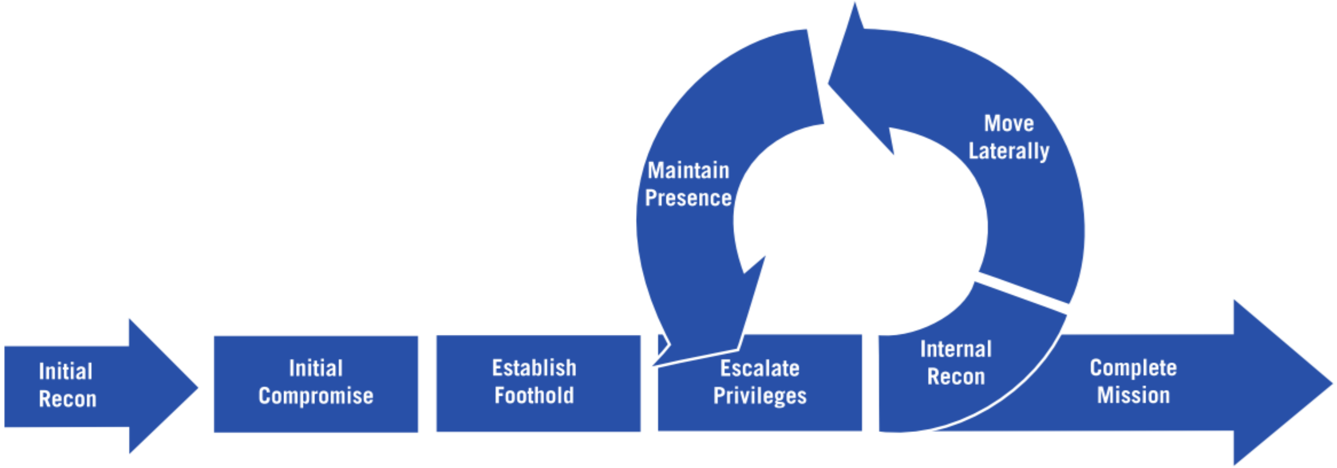
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-rdp-exposed-the-threats-thats-already-at-your-door-wp.pdf last accessed 24/07/2019

Legislative requirements

- Government intervention and regulation
  - **Europe**, GDPR (General Data Protection Regulation)
  - **Australia**, Notifiable Data Breaches (NDB) scheme
  - **United States**, various State data breach notification Statutes
  - **India**, Personal Data Protection Bill (Early 2020)
  - **China**, Cybersecurity Law & draft Data Security Administrative Measures

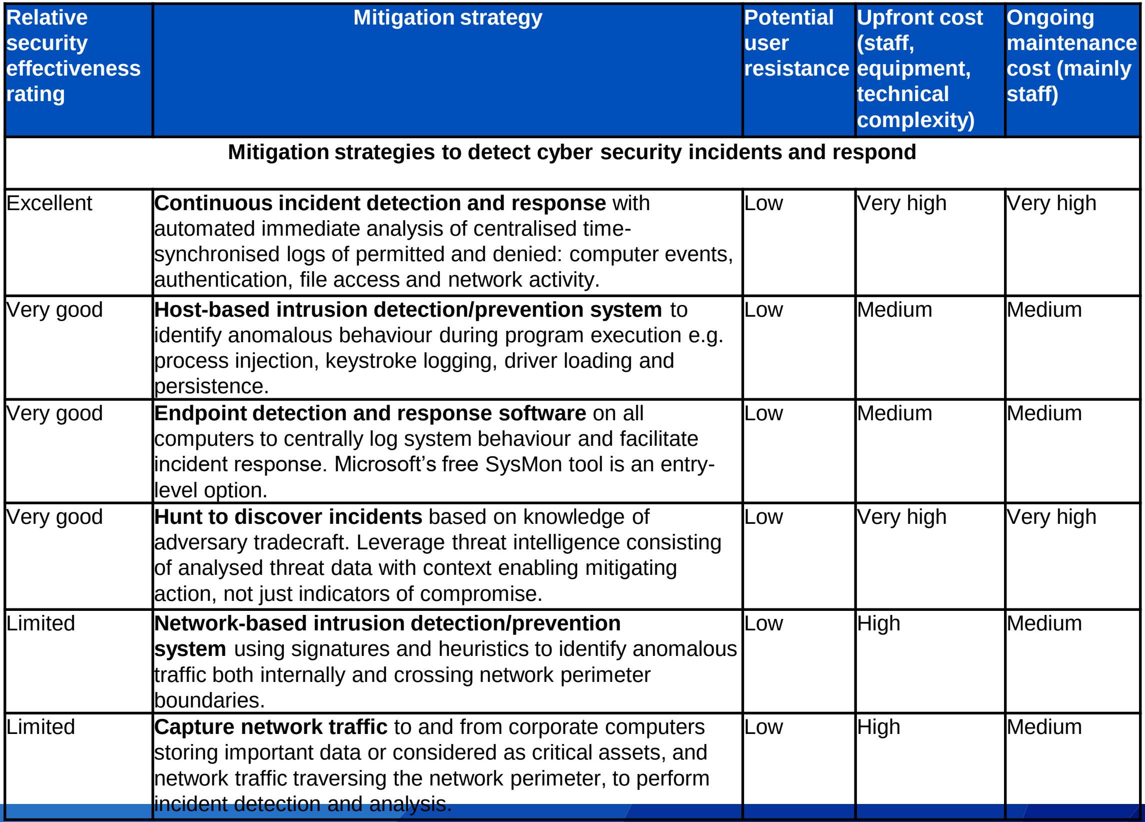
- Data protection laws of the world
  - https://www.dlapiperdataprotection.com

Attack Life Cycle



http://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/

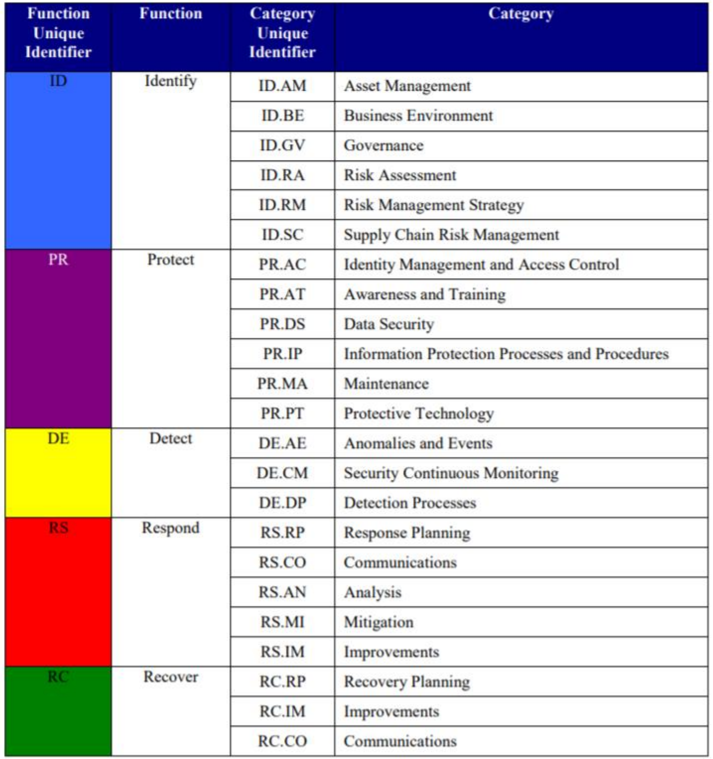
Mitigate Cyber Security incidents



Relative security effectiveness rating	Mitigation strategy	Potential user resistance	Upfront cost (staff, equipment, technical complexity)	Ongoing maintenance cost (mainly staff)
Mitigation strategies to detect cyber security incidents and respond				
Excellent	**Continuous incident detection and response** with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access and network activity.	Low	Very high	Very high
Very good	**Host-based intrusion detection/prevention system** to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence.	Low	Medium	Medium
Very good	**Endpoint detection and response software** on all computers to centrally log system behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry-level option.	Low	Medium	Medium
Very good	**Hunt to discover incidents** based on knowledge of adversary tradecraft. Leverage threat intelligence consisting of analysed threat data with context enabling mitigating action, not just indicators of compromise.	Low	Very high	Very high
Limited	**Network-based intrusion detection/prevention system** using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.	Low	High	Medium
Limited	**Capture network traffic** to and from corporate computers storing important data or considered as critical assets, and network traffic traversing the network perimeter, to perform incident detection and analysis.	Low	High	Medium

https://www.cyber.gov.au/sites/default/files/2019-03/Mitigation_Strategies_2017.pdf

NIST Cybersecurity Framework



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST Cybersecurity Framework

- Anomalies and Events (AE) in the Detect (DE) functional area, there are five subcategories:
  - **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed
  - **DE.AE-2:** Detected events are analyzed to understand attack targets and methods
  - **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors
  - **DE.AE-4:** Impact of events is determined
  - **DE.AE-5:** Incident alert thresholds are established

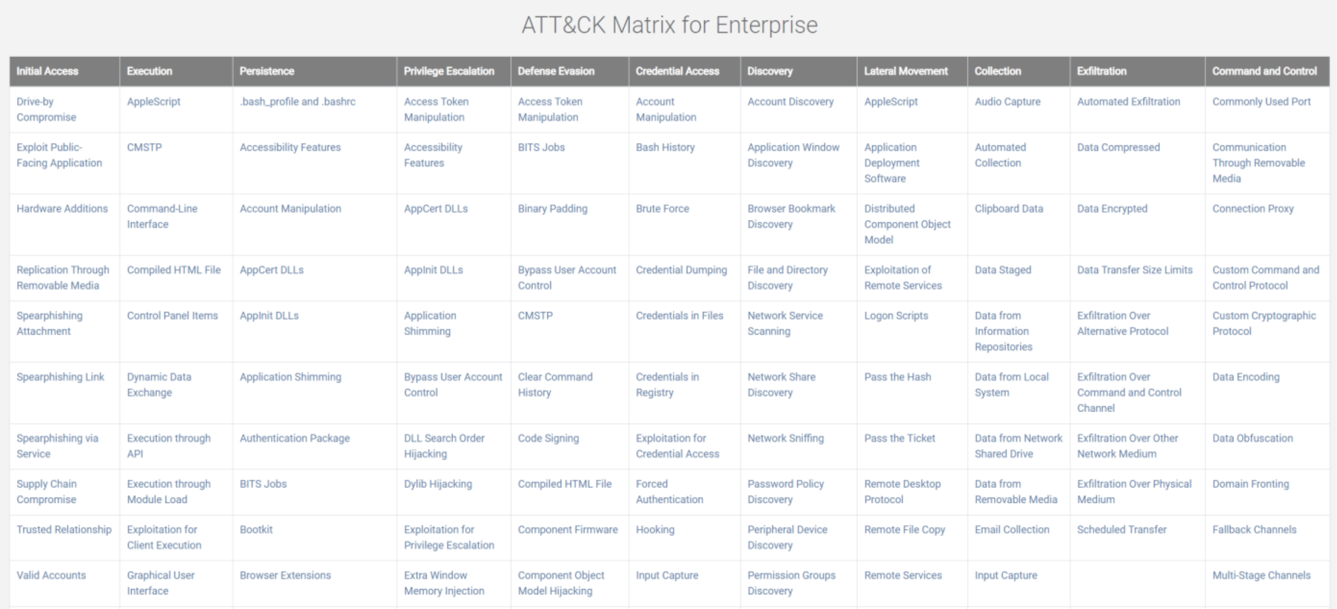
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST Cybersecurity Framework

- **DE.AE-2:** Detected events are analyzed to understand attack targets and methods
  - **CIS CSC** 3, 6, 13, 15
  - **COBIT** 5 DSS05.07
  - **ISA** 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
  - **ISA** 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2
  - **ISO/IEC** 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4
  - **NIST SP** 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
    - AU-6 - Audit Review, Analysis, and Reporting;
    - CA-7 – Continious Monitoring;
    - IR-4 – Incident Hadling;
    - SI-4 – Information System monitoring eg IDS, Automated tools, Alerts.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

ATT&CK Matrix for Enterprise

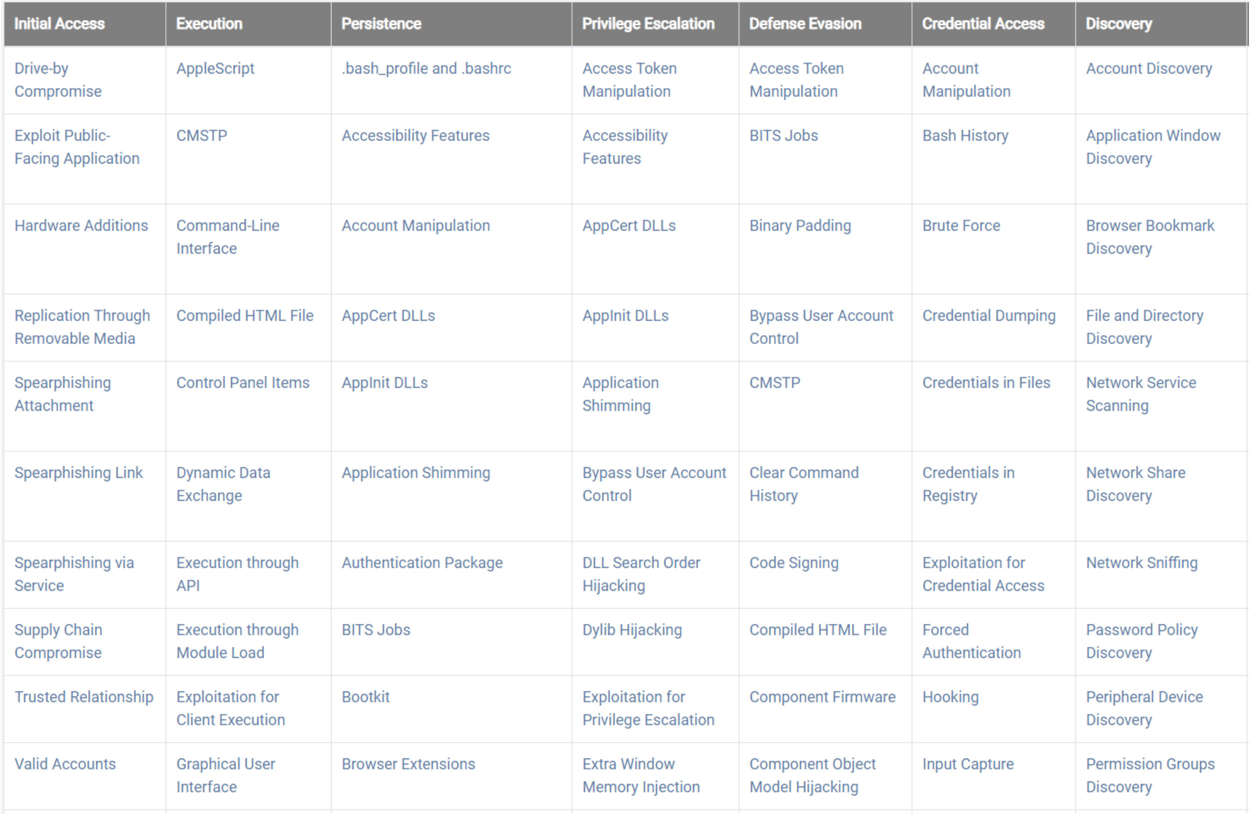


ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels

https://attack.mitre.org – accessed 12th Nov 2018

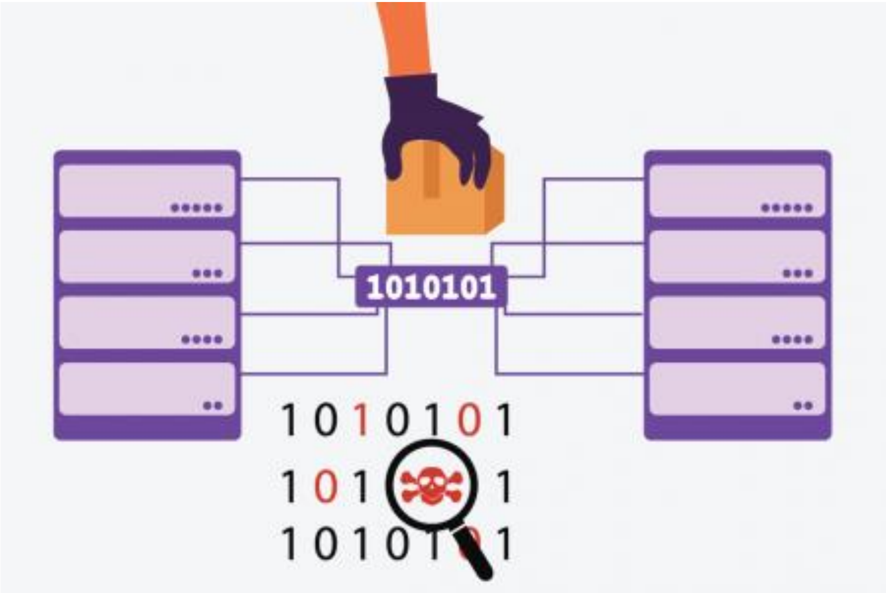
ATT&CK Matrix for Enterprise



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery

https://attack.mitre.org – accessed 12th Nov 2018

Packet analysis



Signature analysis

- Distinctive marks of known bad traffic used to generate alerts.
  - virus detection,
  - malicious website or
  - malware files.
- Distinctive marks include:
  - IP addresses
  - Hostnames
  - Offsets – for example, memory related exploit
  - Debug information
  - "Ego" strings (strings left in the code)
  - Header information

Signature analysis

- An example could be detecting a nmap scan of a network by looking at the User-Agent string.

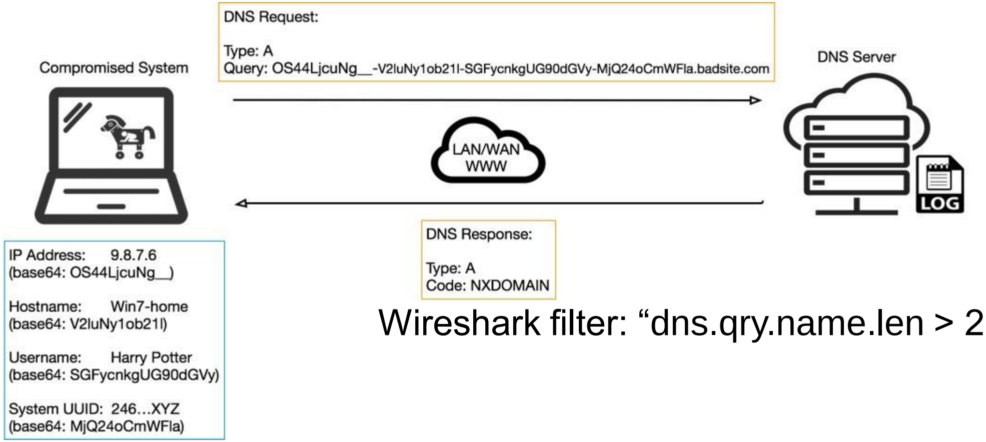
```
alert tcp $EXTERNAL_NET any -> any any (msg:"Nmap User-Agent
Observed"; flow:to_server,established; content:"User-Agent|3a|";
http_header; content:"|20|Nmap";  sid:1000001; rev:3;)
```

Session analysis

- Utilises the session metadata to determine what is happening during a session.
  - which devices causing the traffic
  - the type of traffic or
  - what data is being transferred.
- Looks at the behaviour of the sessions and looks for behaviour that is not normal.

Session analysis

- An example is once a network has been compromised, Domain Name Services (DNS) may be used to exfiltrate data.



DNS Request:

Type: A
Query: OS44LjcuNg__-V2luNy1ob21l-SGFycnkgUG90dGVy-MjQ24oCmWFla.badsite.com

DNS Response:

Type: A
Code: NXDOMAIN

IP Address: 9.8.7.6
(base64: OS44LjcuNg__)

Hostname: Win7-home
(base64: V2luNy1ob21l)

Username: Harry Potter
(base64: SGFycnkgUG90dGVy)

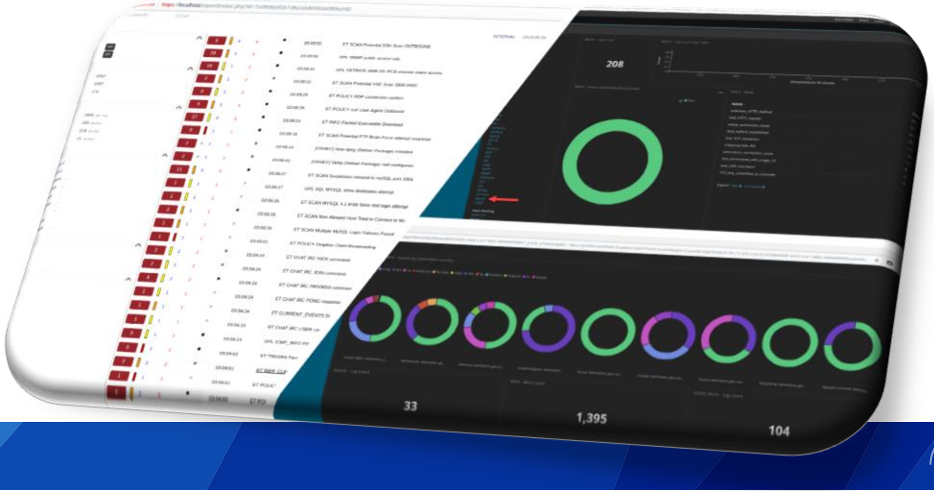
System UUID: 246…XYZ
(base64: MjQ24oCmWFla)

Wireshark filter: “dns.qry.name.len > 20”

https://unit42.paloaltonetworks.com/dns-tunneling-how-dns-can-be-abused-by-malicious-actors/

Which technique?

- Signature analysis
  - can be used to create the alert; then
- Session analysis
  - can help investigate the alert further.



```
ET SCAN Potential SSH Scan OUTBOUND
GPL SNMP public access udp
GPL NETBIOS SMB-DS IPC$ unicode share access
ET SCAN Potential VNC Scan 5800-5820
ET POLICY RDP connection confirm
ET POLICY curl User-Agent Outbound
ET INFO Packed Executable Download
ET SCAN Potential FTP Brute-Force attempt response
[OSSEC] New dpkg (Debian Package) installed
[OSSEC] Dpkg (Debian Package) half configured
ET SCAN Suspicious inbound to mySQL port 3306
GPL SQL MYSQL show databases attempt
ET SCAN MYSQL 4.1 brute force root login attempt
ET SCAN Non-Allowed Host Tried to Connect to My
ET SCAN Multiple MySQL Login Failures Possib
ET POLICY Dropbox Client Broadcasting
ET CHAT IRC NICK command
ET CHAT IRC JOIN command
ET CHAT IRC PRIVMSG comman
ET CHAT IRC PONG response
ET CURRENT_EVENTS Si
ET CHAT IRC USER cw
GPL ICMP_INFO PIN
ET TROJAN Fam
ET WEB_CLIE
ET POLIC
ET PO
```

FOSS Tools

- Open source network monitoring and log management tools:
  - Elasticsearch
  - Logstash
  - Kibana
  - Snort
  - Suricata
  - Zeek (formerly Bro)
  - Sguil
  - Squert
  - Tcpdump

* FOSS - Free Open Source Software

Log Management

- Logstash
  - used to gather data from multiple sources and transform it for storage.
- Elasticsearch
  - distributed, RESTful search and analytics engine.
- Kibana
  - Visualisation tool for Elasticsearch and other data sets

https://www.elastic.co/products/

Intrusion Detection tools

- Snort
  - Intrusion detection system (IDS).
- Suricata
  - Intrusion detection system (IDS).

Network Monitoring

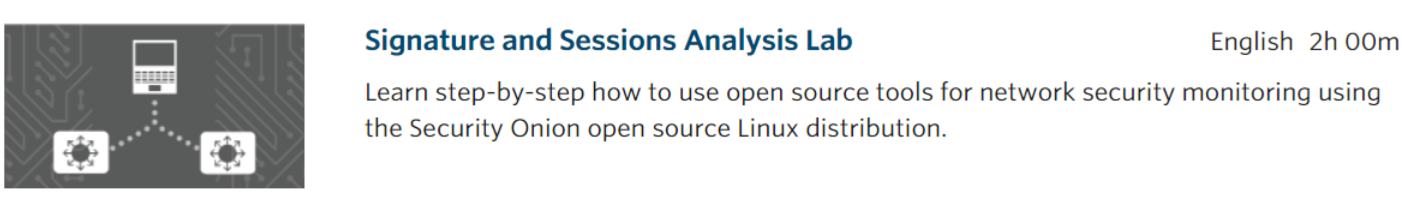
- Zeek (formerly Bro)
  - Network traffic analysis tool
- Sguil
  - collection of free software components for Network Security Monitoring (NSM) and event driven analysis of IDS alerts
- Squert
  - web application that is used to query and view event data stored in a Sguil database.

Packet capture

- TCPdump
  - command line utility used to capture and analyse packets on network interfaces.
- Wireshark
  - utility used to capture and analyse packets on network interfaces.
- Cloudshark
  - web-based utility used to analyse packet captures.

Lab Exercise

https://academy.apnic.net/en/virtual-labs/



Signature and Sessions Analysis Lab English 2h 00m

Learn step-by-step how to use open source tools for network security monitoring using the Security Onion open source Linux distribution.

TCPdump command example

```
# cd /opt/samples

# tcpdump -nn -r fake_av.pcap | wc -l

# tcpdump -nn -r fake_av.pcap | head

# tcpdump -nn -r fake_av.pcap | cut -f 3 -d " " | head

# tcpdump -nn -r fake_av.pcap 'tcp or udp' | cut -f 3 -d " " | cut -f 1-4 -d "." | head
```

Display top 10 destinations

```
# tcpdump -nn -r fake_av.pcap 'tcp or udp' | cut -f 5 -d " " | cut -f 1-4 -d "." | sort |
uniq -c | sort -nr | head
```

-nn = don’t use DNS to resolve IPs and display port no
-r = replay pcap file
-f = field to select
-d = delimiter to use

TCPdump command example

```
# tcpdump -nn -r fake_av.pcap 'port 53' | head -5

# tcpdump -nn -r fake_av.pcap 'port 53' | grep -Ev '(com|net|org|gov|mil|arpa)'
| cut -f 9 -d " " | head

# tcpdump -nn -r fake_av.pcap 'port 53' | grep -Ev '(com|net|org|gov|mil|arpa)'
| cut -f 8 -d " " | grep -E '[a-z]’
```

If a suspicious domain name is found, use https://www.virustotal.com/gui/home/url

To check if malicious

TCPdump command example

TCPdump command example

```
# cd /opt/samples/mta
```

```
# for capfile  in $(ls *.pcap); do tcpdump -nn -r $capfile 'port 53' | grep -Ev
'(com|net|org|gov|mil|arpa)' | cut -f 8 -d " " | grep -E '[a-z]'; done;
```

Check for plain text passwords in pcap files

```
# for capfile  in $(ls *.pcap); do tcpdump -nn -r $capfile  port http or port
ftp or port smtp or port imap or port pop3 or port telnet -lA | egrep -i -B5
'pass=|pwd=|log=|login=|user=|username=|pw=|passw=|passwd=
|password=|pass:|user:|username:|password:|login:|pass |user '; done;
```

-l = force line buffered mode

-A = include ascii strings from the capture

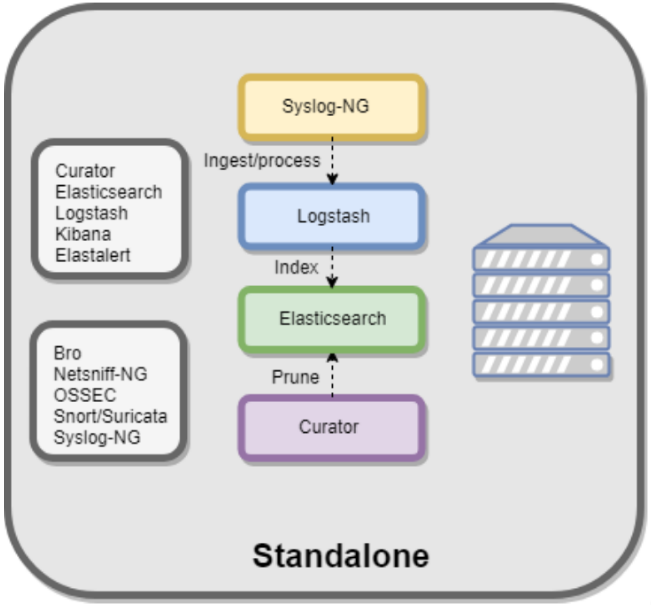
Security Onion

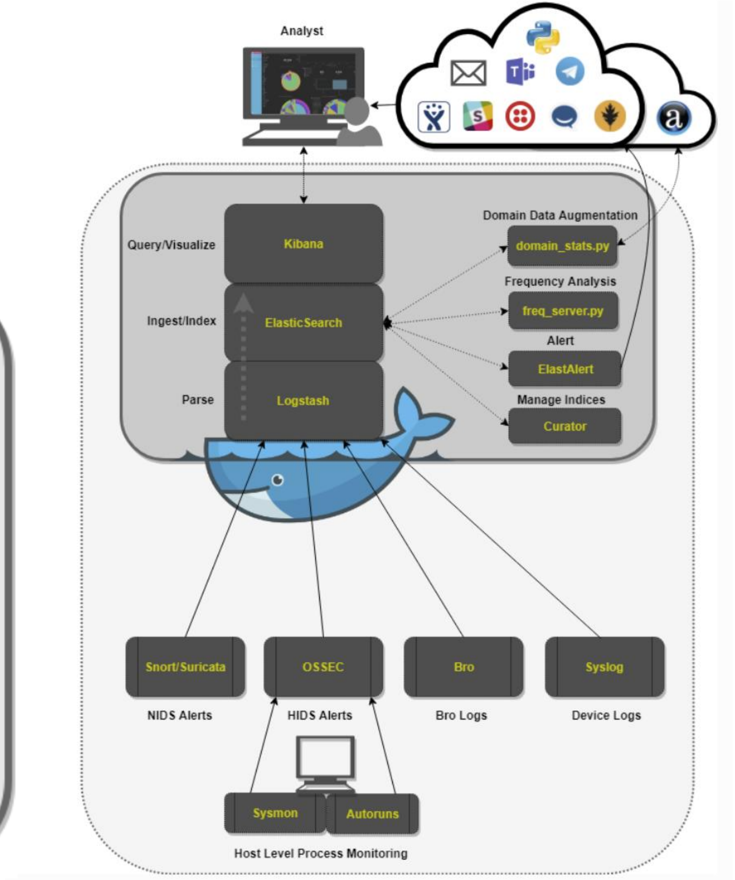
- Linux-based open source network monitoring and log management toolkit.
- Can be installed as a Virtual Machine (VM) or on a physical machine.
- Best practice is to use two network interfaces:
  1. Management Network
  2. Monitored Network

https://securityonion.net

Security Onion

Security Onion - Standalone Deployment
Created by Security Onion Solutions

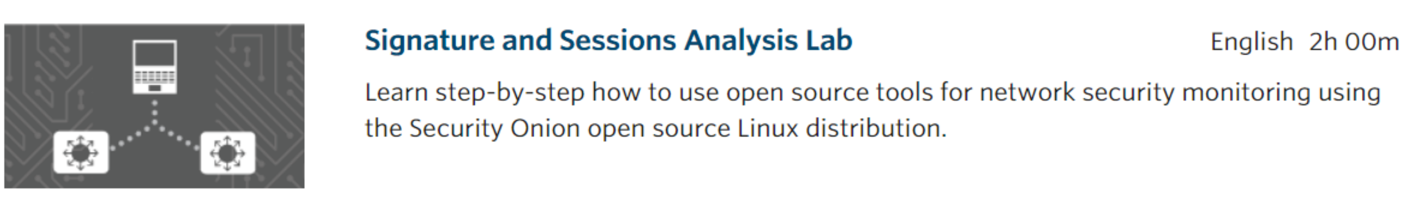




https://securityonion.readthedocs.io/en/latest/architecture.html

Lab Exercise

https://academy.apnic.net/en/virtual-labs/



Signature and Sessions Analysis Lab English 2h 00m

Learn step-by-step how to use open source tools for network security monitoring using the Security Onion open source Linux distribution.

Any questions?