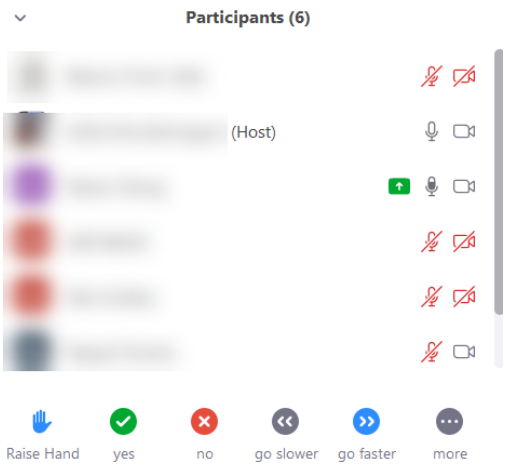
APNIC

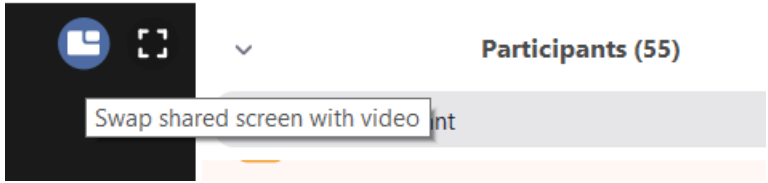
Packet Analysis for Network Security

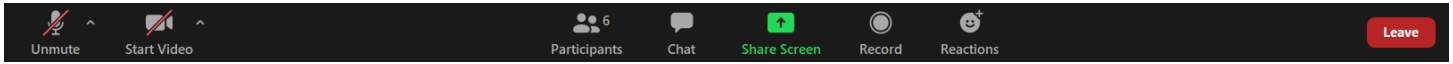
Using Zoom for this webinar

- Keep chat settings to “All Panelists and Attendees”
- Use chat to share text, information, URLs amongst all attendees
- If you wish to ask a question to the presenters:
  - Click the Q&A button
  - Type your question
  - The presenters will then answer your questions at an appropriate time
  - Note: Only the presenters will see your question, not other attendees
  - Please don’t use chat to ask questions of the presenters, we might not see it

Using Zoom for this webinar







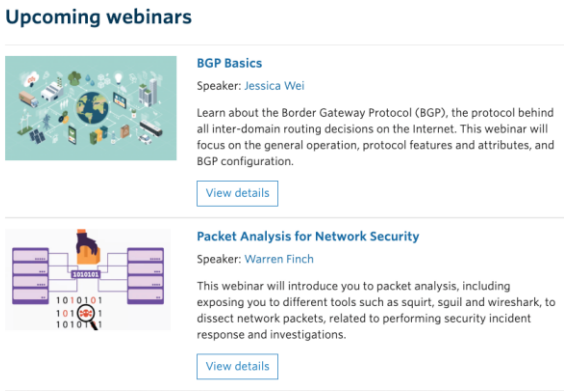
APNIC Academy – Free to the Public

APNIC ACADEMY

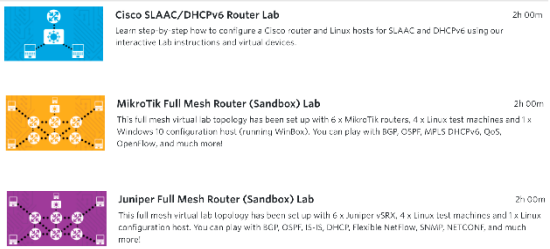
https://academy.apnic.net

ONLINE COURSES

LIVE WEBINARS



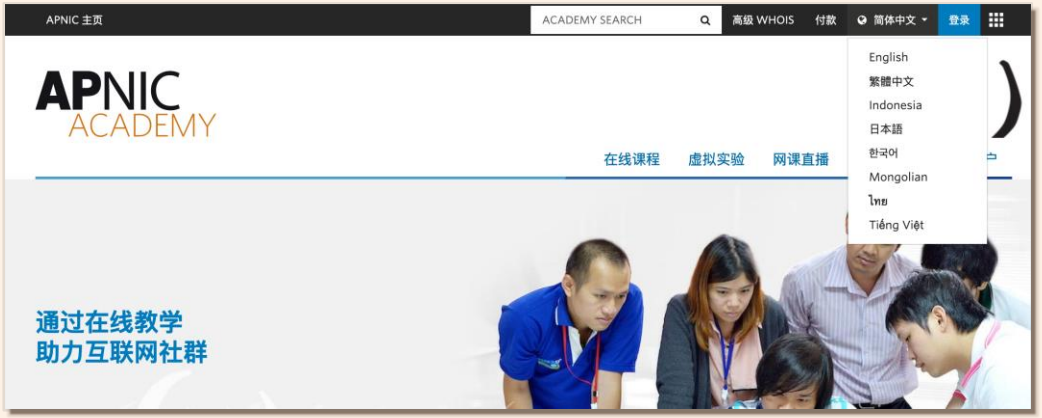
VIRTUAL LABS

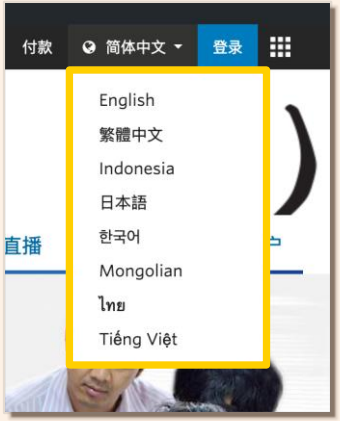


Sign up for training updates at:
https://info.apnic.net/l/229772/2017-11-01/shgx

APNIC Academy – Free to the Public

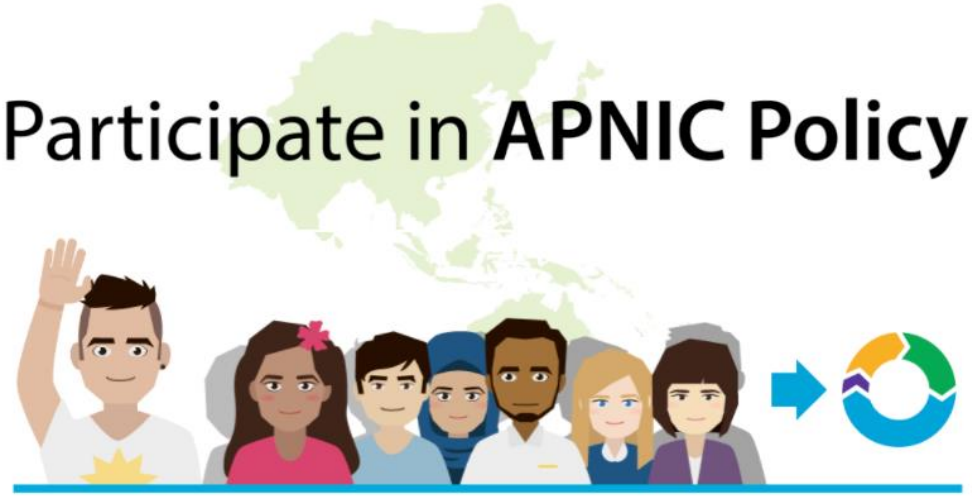
MULTILINGUAL SUPPORT x 8 LANGUAGES





NEW IPv6 FUNDAMENTALS COURSE

APNIC Policy Development Process



www.apnic.net/community/policy/participate

Networking from Home – NEW!

NETWORKING FROM HOME

Call for papers open now for first event on 2 June

https://nfh.apnic.net

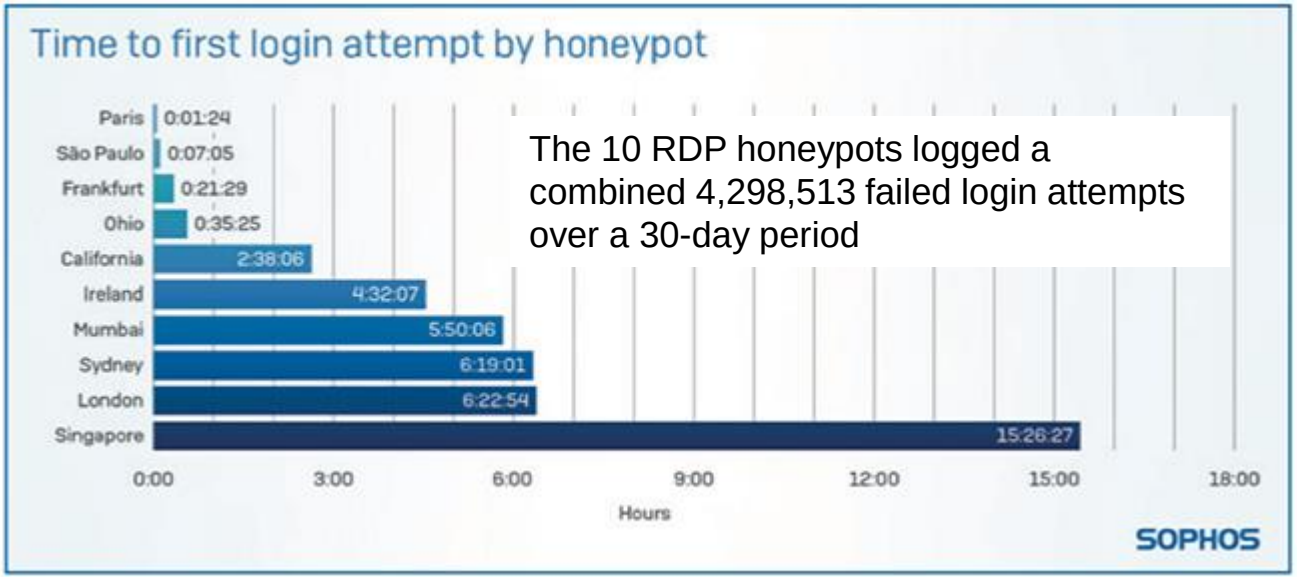
Agenda

- 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

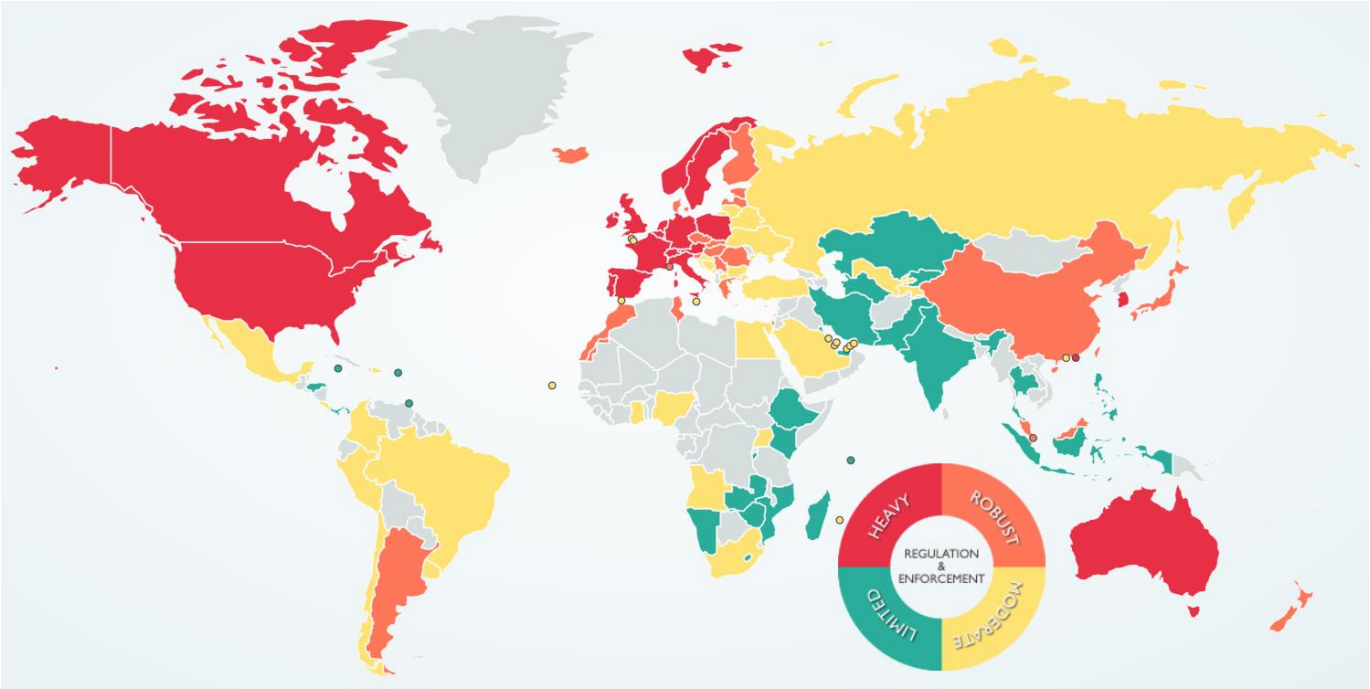
https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-rdp-exposed-the-threats-thats-already-at-your-door-wp.pdf last accessed 24/07/2019

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

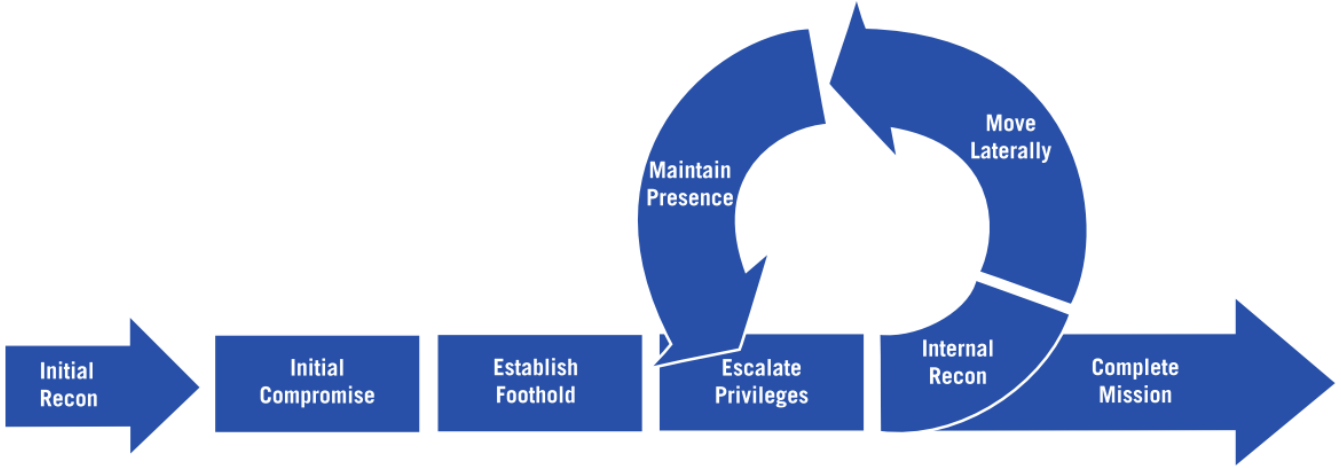
- Data protection laws of the world
  - https://www.dlapiperdataprotection.com

Legislative requirements



https://www.dlapiperdataprotection.com/index.html

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

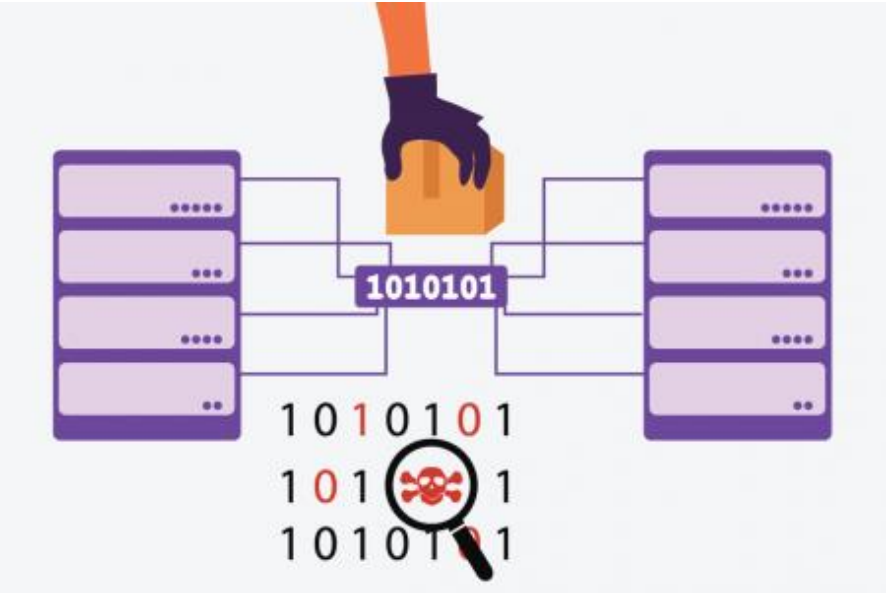
https://attack.mitre.org – accessed 12th Nov 2018

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.

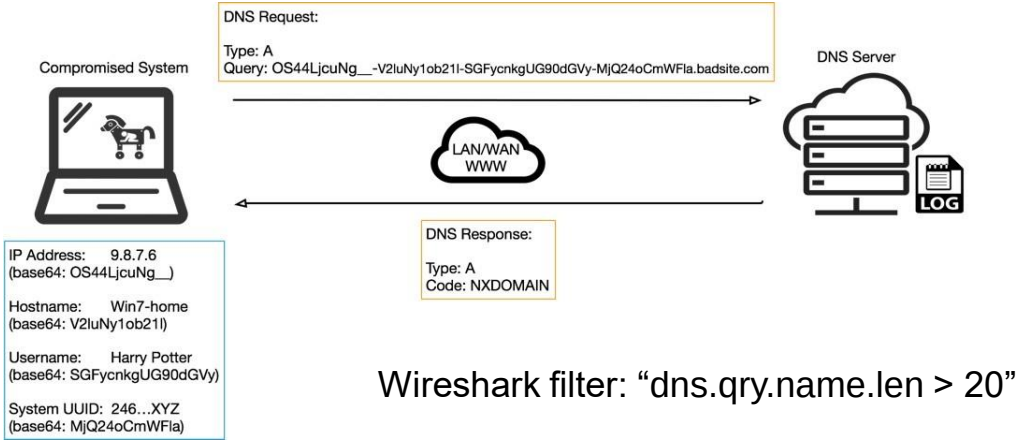
```
alert tcp $EXTERNAL_NET any -> any any (msg:"Nmap User-Agent
Observed"; flow:to_server,established; content:"User-Agent|3a|";
http_header; content:"|20|Nmap";  sid:1000001; rev:3;)
```

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.



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.

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.

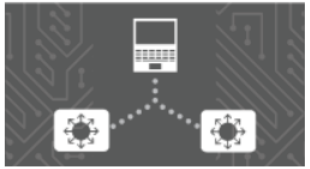
Packet capture

- 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.

Packet Analysis for Network Security

Lab exercise: TCP dump

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

```
# 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

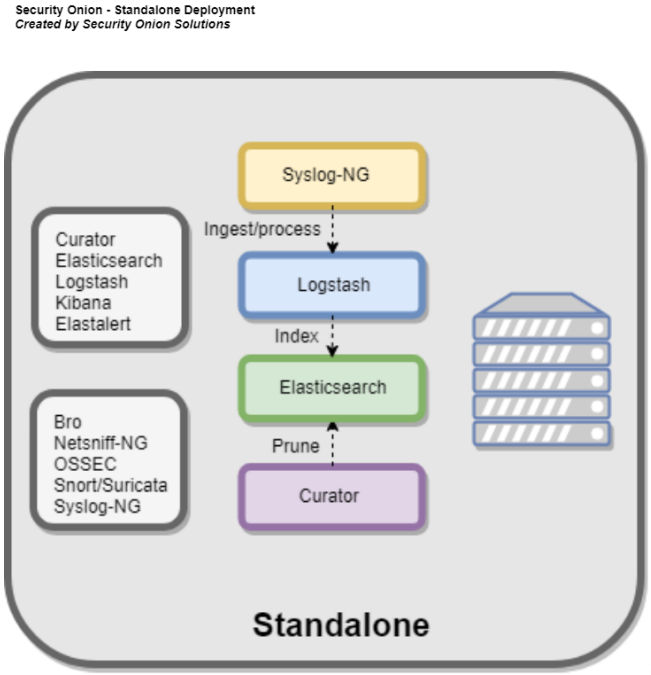
-A = include ascii strings from the capture

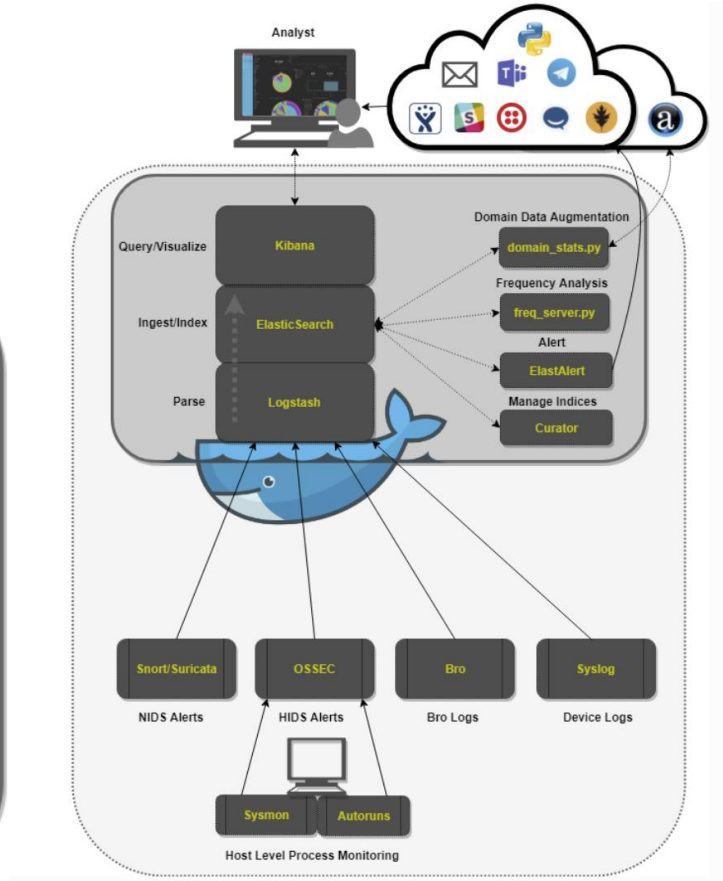
Security Onion

- 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





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

How to Install

- Straight forward, if experience installing Ubuntu 16.04
  - Download
    - https://github.com/Security-Onion-Solutions/security-onion/blob/master/Verify_ISO.md
  - Base install is similar to Ubuntu installation
  - Once Ubuntu is installed double-click on the setup icon on the desktop.
  - Select the evaluation mode, as this will install all the tools on the one machine (standalone).

Security Onion - commands

Command	Description
sudo soup	Update Security Onion (and Ubuntu)
sudo so-status	Check service status
sudo sostat	Generate Security Onion statistics
sudo so-start sudo so-stop sudo so-restart	Start all services Stop all services Restart all services
sudo so-user-add	Add user for Sguil/Squert/Kibana
sudo rule-update	Update rules after modifying file
sudo so-allow sudo so-allow-view	Open ports for ufw View current firewall rules

https://securityonion.readthedocs.io/en/latest/cheat-sheet.html

Security Onion - files

Folder / Files	Description
/etc/nsm/	Location of configuration files
/etc/nsm/securityonion.conf	Security Onion general settings
/opt/bro /nsm/bro/logs	Location of Bro files Location of Bro log files
/etc/elasticsearch	Location of ElasticSearch files
/etc/logstash	Location of LogStash files
/etc/kibana	Location of Kibana files
/var/log	Location of log files
/opt/samples	Example packet capture files

https://securityonion.readthedocs.io/en/latest/cheat-sheet.html

Security Onion - rules

Folder / Files	Description
/etc/nsm/rules/downloaded.rules	Downloaded IDS rules
/etc/nsm/rules/local.rules	Custom IDS rules
/etc/nsm/rules/threshold.conf	Rule thresholds
/etc/nsm/pulledpork/disabledsid.conf	Disabled rules by SID
/etc/nsm/pulledpork/modifysid.conf	Modified rules
/etc/nsm/pulledpork/pulledpork.conf	Pulled Pork Configuration
/etc/elastalert/rules	Elastalert rules

https://securityonion.readthedocs.io/en/latest/cheat-sheet.html

Import packet captures

Command	Description
sudo tcpreplay -i ens34 -M10 fake_av.pcap	Import the packet capture as new traffic with the current date and time, using interface ens34, limiting to 10MB throughput
sudo so-replay	Import all the sample packet captures as new traffic with the current date and time.
sudo so-import-pcap fake_av.pcap	Import the traffic, whilst keeping the timestamp the same as the original packet capture date and times.

https://securityonion.readthedocs.io/en/latest/pcaps.html
https://securityonion.readthedocs.io/en/latest/so-import-pcap.html

Import packet captures

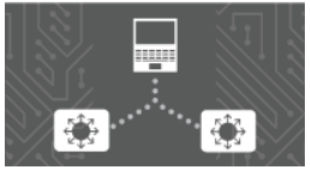
Command	Description
capinfos {pcap file}	Display statistics about the packet capture file
tshark -F pcap -r {pcapng file} -w {pcap file}	Convert packet capture Next Gen file to earlier packet capture format

https://securityonion.readthedocs.io/en/latest/so-import-pcap.html

Packet Analysis for Network Security

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.

Exercise

- Import the sample captured (pcap) files /opt/samples/markofu/jackcr-challenge.pcap

/opt/samples/markofu/outbound.pcap

```
sudo tcpreplay -i ens33 -M10 /opt/samples/markofu/jackcr-challenge.pcap

sudo tcpreplay -i ens33 -M10 /opt/samples/markofu/outbound.pcap
```

Exercise 1: Squert

- Q1
  - What type of malicious traffic is suspected?

- Q2: What is the top source IP and destination IP
  - Source _____, Destination _____ .

- Q3: What is the other IP address communicating with the top source IP?

Exercise 1: Squert

EVENTS | SUMMARY | VIEWS

Filter

INTERVAL: 2019-05-04 00:00:00 -> 2019-05-04 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY:

TOP SIGNATURES (2362 events) viewing 10 of 172 results

COUNT	%TOTAL	#SRC	#DST	SIGNATURE	ID
321	13.59%	1	1	ET TROJAN Gh0st Remote Access Trojan Encrypted Session To CnC Server	2013214
298	12.62%	1	1	ET TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 102	2021716
297	12.57%	1	1	ET TROJAN Backdoor family PCRat/Gh0st CnC traffic	2016922
166	7.03%	11	10	ET POLICY PE EXE or DLL Windows file download HTTP	2018959
139	5.88%	3	2	ET CURRENT_EVENTS DRIVEBY Nuclear EK Payload	2019873
72	3.05%	2	3	ET INFO EXE - Served Inline HTTP	2014519
39	1.65%	3	3	GPL SNMP public access udp	2101411
37	1.57%	3	2	ET CURRENT_EVENTS Nuclear EK Landing Jan 14 2014	2020180
37	1.57%	3	3	ET INFO Packed Executable Download	2014819
37	1.57%	3	2	ET CURRENT_EVENTS Nuclear EK Landing Jan 06 2014	2020103

TOP SOURCE IPS viewing 10 of 84 results

COUNT	%TOTAL	#SIG	#DST	IP	COUNTRY
918	38.87%	5	2	172.16.150.20	RFC1918 (.lo)
129	5.46%	9	1	128.199.52.211	UNITED KINGDOM (.gb)
124	5.25%	8	1	178.62.255.107	EUROPE (.eu)
98	4.15%	25	17	192.168.204.137	RFC1918 (.lo)
93	3.94%	5	1	59.53.91.102	CHINA (.cn)
75	3.18%	7	1	95.85.23.178	EUROPE (.eu)
72	3.05%	2	2	192.168.56.52	RFC1918 (.lo)
65	2.75%	8	1	92.63.88.61	LATVIA (.lv)
52	2.20%	4	1	65.99.252.112	UNITED STATES (.us)
50	2.12%	5	5	10.6.8.101	RFC1918 (.lo)

TOP DESTINATION IPS viewing 10 of 122 results

COUNT	%TOTAL	#SIG	#SRC	IP	COUNTRY
916	38.78%	3	1	58.64.132.141	HONG KONG (.hk)
473	20.03%	41	12	192.168.204.137	RFC1918 (.lo)
93	3.94%	5	1	192.168.23.129	RFC1918 (.lo)
75	3.18%	7	1	192.168.204.139	RFC1918 (.lo)
72	3.05%	3	2	192.168.3.35	RFC1918 (.lo)
53	2.24%	5	2	10.7.9.101	RFC1918 (.lo)
45	1.91%	2	1	10.0.4.15	RFC1918 (.lo)
36	1.52%	2	1	192.168.3.65	RFC1918 (.lo)
35	1.48%	3	6	192.168.10.101	RFC1918 (.lo)
30	1.27%	1	1	172.31.19.73	- (-)

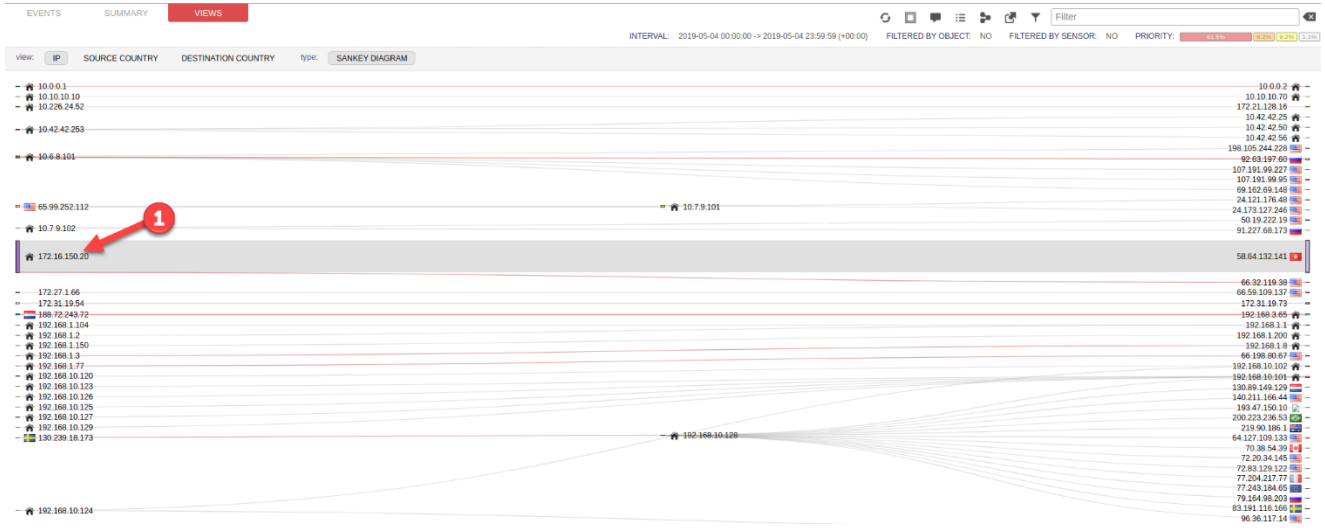
TOP SOURCE COUNTRIES viewing 10 of 18 results

COUNT	%TOTAL	#SIG	#DST	COUNTRY	#IP
199	22.28%	8	2	EUROPE (.eu)	2
129	14.45%	9	1	UNITED KINGDOM (.gb)	1
126	14.11%	17	6	UNITED STATES (.us)	9

TOP DESTINATION COUNTRIES viewing 10 of 23 results

COUNT	%TOTAL	#SIG	#SRC	COUNTRY	#IP
918	76.69%	5	2	HONG KONG (.hk)	2
124	10.36%	38	17	UNITED STATES (.us)	32
38	3.17%	6	4	RUSSIAN FEDERATION (.ru)	4

Exercise 1: Squert



Exercise 2: Sguil

- Question: What was the rule that generated the original alert?

Exercise 3: Sguil

- Question: What is the filename of the downloaded suspicious file?

Exercise 4: Wireshark/Netminer

- Question: Can the downloaded suspicious file be extracted?

Exercise 5: Malicious file

- Q1: What is the md5 hash value of the downloaded file?

- Q2: When the hash value is submitted to Virus Total, is it found to be malicious?


Questions

Thank You!