SWINBURNE UNIVERSITY OF TECHNOLOGY

IPv4 and IPv6 Greynets

Warren Harrop

Fred Baker, Warren Harrop, Grenville Armitage,
"IPv4 and IPv6 Greynets", RFC6018

Outline

- Greynets (review)
  - Darknets
  - Greynets
    - Implementing greynets
      - "greynetd"
- RFC6018
  - Router assisted greynets
- Future work

What is a greynet?

- Part of an IDS (Intrusion Detection System)
  - **Not** a *user installed, unauthorised application on a network host*
- A greynet [1,2] is a sparse enterprise (or campus) based darknet...
- Ok, what's a darknet?
  - Let's go back a step...

SWINBURNE UNIVERSITY OF TECHNOLOGY

[1] W.Harrop, G.Armitage "Defining and Evaluating Greynets (Sparse Darknets)," IEEE 30th Conference on Local Computer Networks (LCN 2005) Sydney, Australia, 15-17 November, 2005.
[2] W. Harrop, G. Armitage, "Greynets: A Definition and Evaluation of Sparsely Populated Darknets," (short paper) SIGCOMM 2005 - Workshop on Mining network data (MineNet-05), Philadelphia, Pennsylvania, USA. August, 2005.

Darknets

- Also called:
  - Network telescopes, Internet motion sensors
- Essentially:
  - A large contiguous set of IP addresses (/24 or greater)
    - Routed
    - Passively listened to
- Why?...

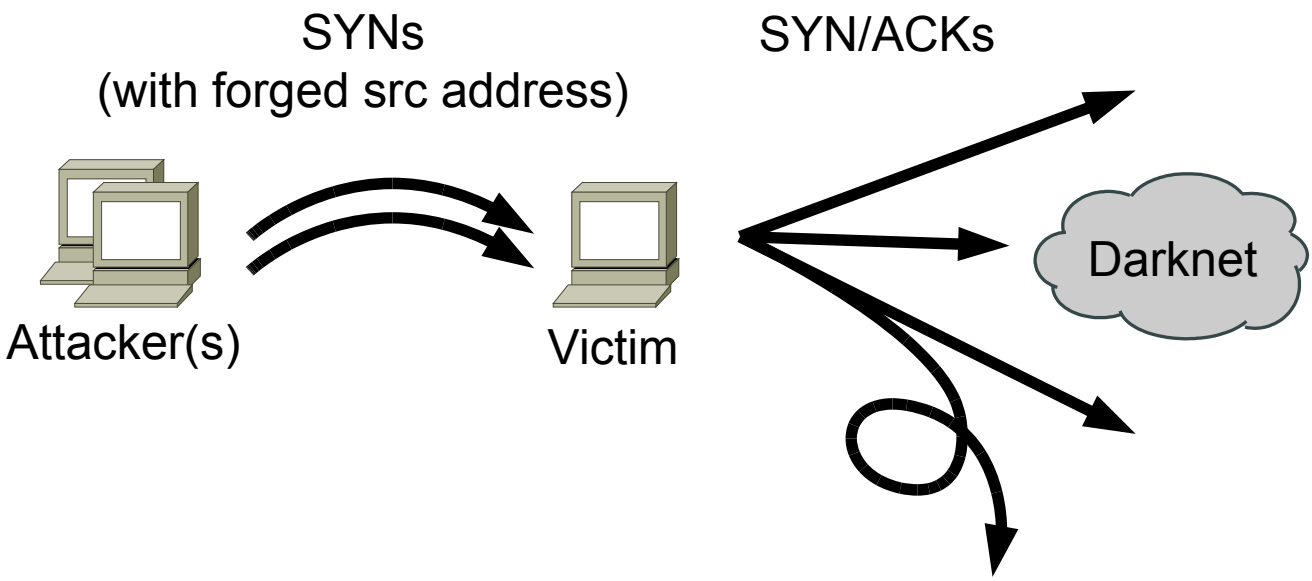
SWINBURNE UNIVERSITY OF TECHNOLOGY

Darknets (2)

- Seems like a silly idea...but...
- No *legitimate* packets should be seen
- But yet...Two types of packet come in
  - Direct connection attempts
    - Automated malware (and the people who act like malware) will still send packets into this space in the search for hosts to defile
  - Backscatter from network attacks …

Backscatter

DDoS (Distributed Denial of Service Attack:



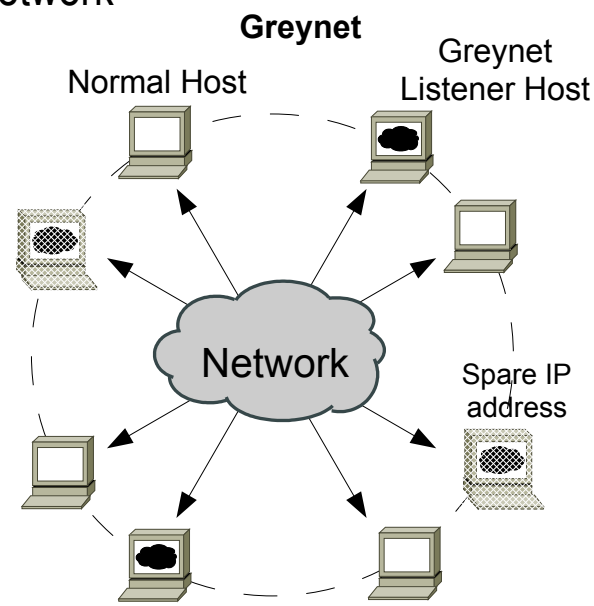
- Imaging if you darknet'ed 1.1.1.0/24, et al.
  - But that's another story...

Darknets (3)

- Darknets give a view of wider Internet activity
  - Good for research
- Can it be applied to the campus/enterprise for local security?
  - Problems:
    - Requires large contiguous blocks of addresses
      - Not always feasible
    - Large contiguous space can be avoided
      - Scans see no hosts – scans stop (or greatly reduce)

Greynet

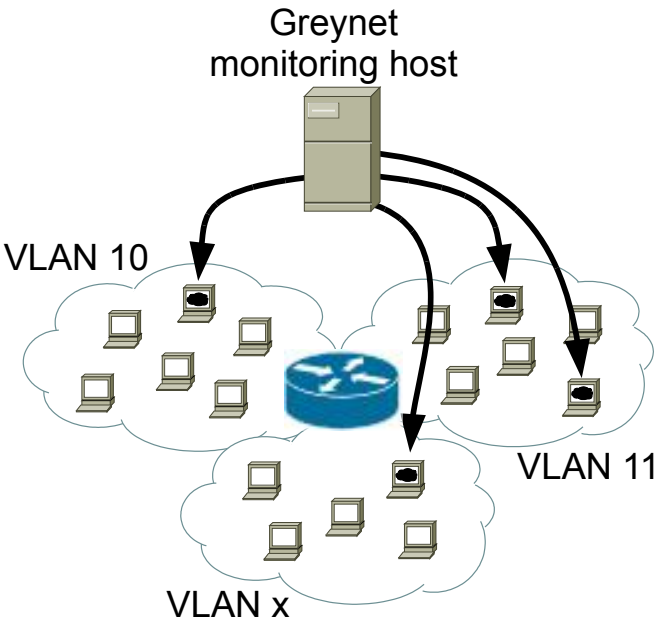
- "Distributed edge-network darknet"
- Make the darknet look 'inwards'
  - Place the darknet inside your network
- Not many can afford an entire /24 for a darknet so ...
  - Put darknet hosts among 'regular' 'lit' network hosts
- Network scans find a greynet hard to avoid

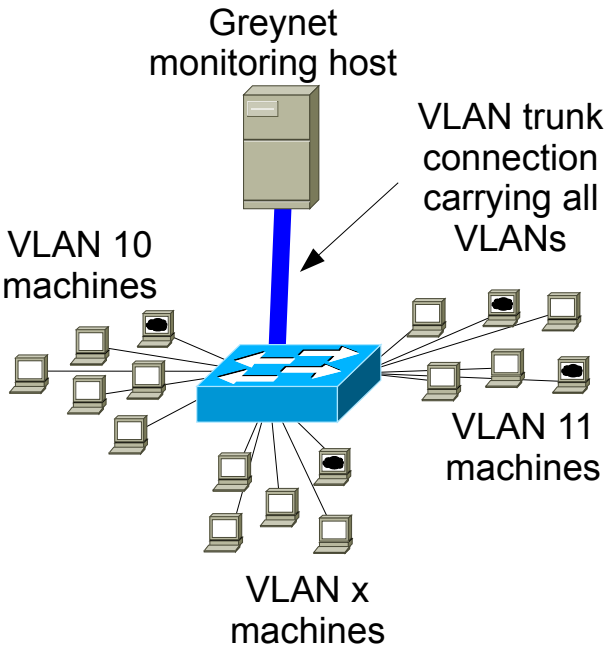


Greynet (2)

- From the packets that come to the greynet you now know:
  - Who's doing scanning inside my network?
    - Who's infected with malware?
      - What type of malware might be inferred from ports used and the scanning pattern

Greynet implementation

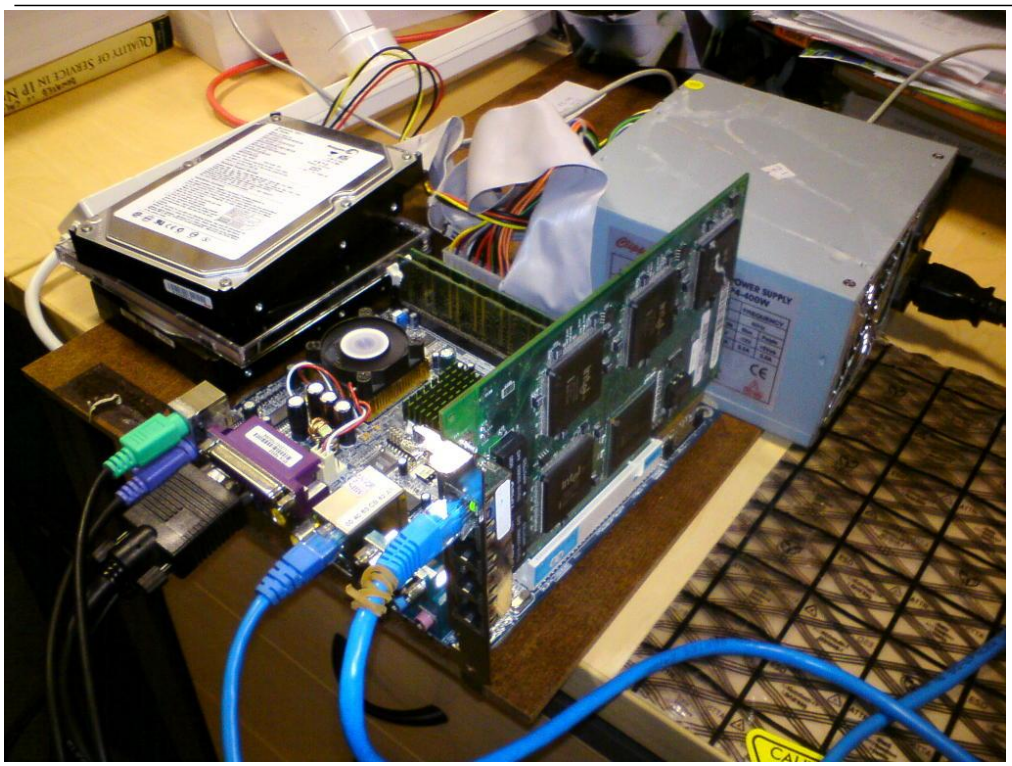




"greynetd"

- FreeBSD package
- Ease greynet implementation & deployment
- Stir together a FreeBSD machine & VLAN trunk –
  - DHCP integration
  - SNMP monitoring interface
  - Web interface for setup and control
- http://caia.swin.edu.au/greynets/

Demo



RFC6018

- Discusses greynets
  - The continuing importance of greynets in a IPv6 world
- Introduces a new method for implementation
  - Where routers lend a hand...

IPv6 scanning

- IPv4 networks have host sparsity but that's nothing...
- IPv6 - even a very large switched LAN is likely to use a small fraction of the available addresses
  - $2^{64} \approx 1.8 \times 10\text{^}19 \approx$ 18 trillion ≈ A metric crap-load
- So will IPv6 scanning not be a problem in the future?
  - Too much space, so not worth attempting?
  - Will everyone use “privacy extensions” (RFC4941)?

IPv6 scanning (2)

- The field can be narrowed [1] [2]:
  - Potential for manual addressing such as: x::1, x::2, etc.
  - A company buys a certain kind of NIC - addresses are limited to a much smaller range
  - Observe DNS, SMTP envelopes, XMPP messages, FTP, HTTP, etc, that carry IP addresses in other ways
- No known attacks in the wild as of now, but the belief is that they will happen

SWINBURNE UNIVERSITY OF TECHNOLOGY

[1] Chown, T., "IPv6 Implications for Network Scanning", RFC 5157, March 2008.
[2] Bellovin, S., et al, "Worm Propagation Strategies in an IPv6 Internet", ;login:, February 2006

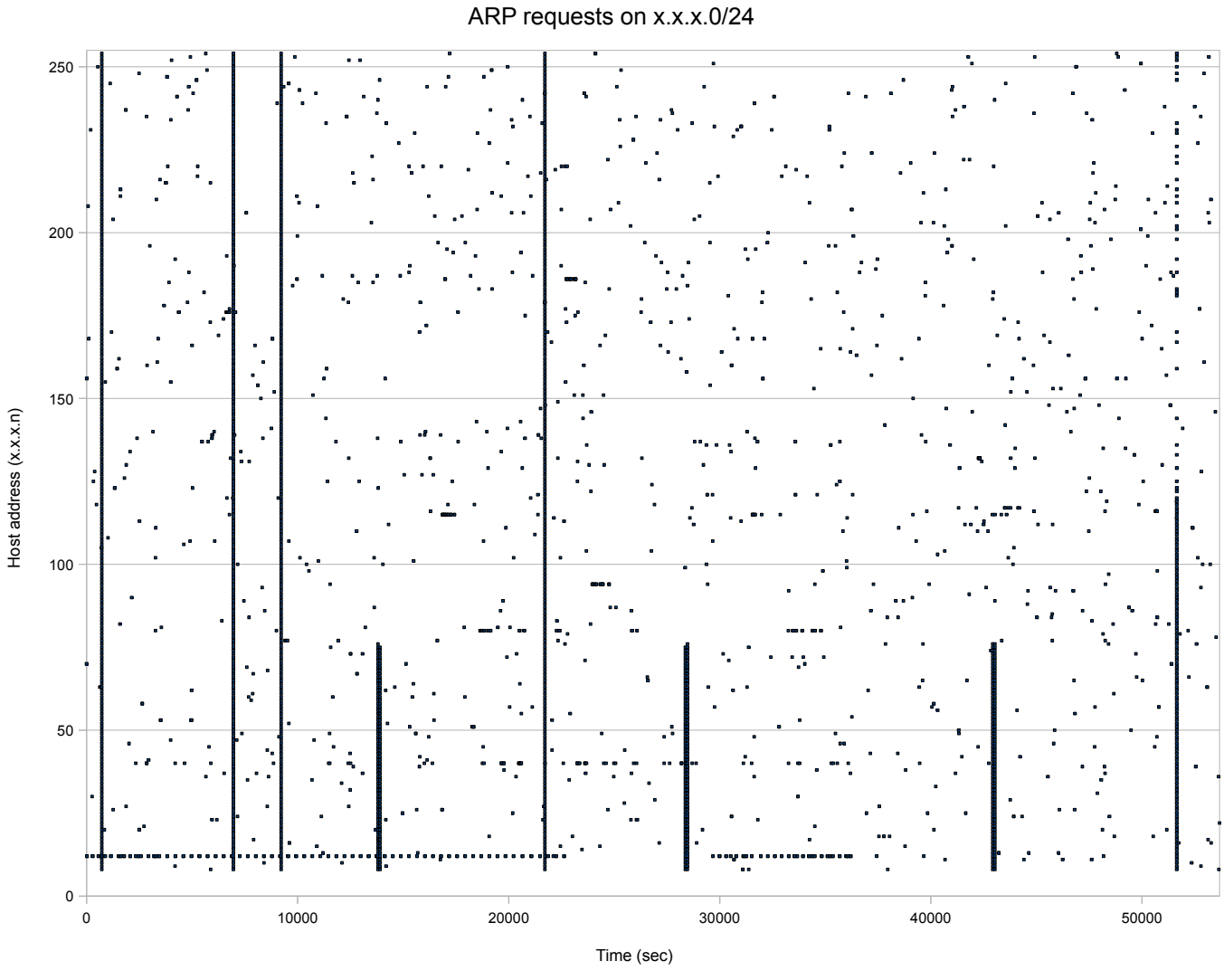
Router behaviour (reminder)

- To determine the MAC address of a neighbour to which a datagram needs to be sent:
  - ARP or Neighbour Discovery
    - Enqueue the datagram
    - Emit a Neighbour Solicitation or ARP Request
    - Await a Neighbour Advertisement or ARP Response
    - On receipt, dequeue and forward the datagram
  - Host's MAC address is kept in the router's tables

SWINBURNE UNIVERSITY OF TECHNOLOGY

Augment behaviour to enable greynets

- When a datagram triggers an ARP Request or Neighbour Solicitation...
- The router forwards a copy of this datagram over a link to the Greynet's analytic equipment
  - "Link": A different physical interface, a circuit, VLAN, tunnel, UDP or other encapsulation...
    - (Or we could send the data in IPFIX format [RFC5101][RFC5610])



Router assisted greynet

- Analytic equipment receives two types of datagrams
  - Those destined for 'dark' IP addresses - interesting
  - Datagram for a legitimate local neighbour who has (temporarily), no MAC address in the router's tables – less interesting
  - Further datagrams arriving before ARP reply or Neighbour Advertisement might also be sent to the analytical equipment
    - Or might not...

What traffic to forward?

- What subset of traffic is interesting and economical to forward?
  - Intentionally left open in the RFC6018
  - Questions
    - What can be learned from a given sample?
    - What the impact on the router and other equipment in is there?

What traffic to forward? (2)

- Possibilities:
  - All datagrams triggering an ARP Request or Neighbour Solicit
  - The subset of those that are not responded to within some stated interval and are therefore likely dark
  - All such datagrams up to some rate
  - All such datagrams matching (or not matching) a specified filter rule
  - etc.

Extensions

- Optionally respond to datagrams
  - Dynamic Honeypot
  - Honeypot “lite” - reply with a SYN/ACK
- Other filters to trigger a send to the greynet
  - Eg. Datagrams failing a unicast reverse forwarding path (uRPF) check [RFC2827]

Security

- Holding and forwarding traffic
  - Load on network and router
    - Attack potential
- But, for an attack that results in excessive ARPs
  - Listening hosts must intelligently discard anyway
  - Consumes greynet network bandwidth that is presumably set aside specifically for that purpose

Future Work

- Outline deployment scenarios
  - Pros and cons of each
- Implementation on FreeBSD
- Test
- It would be cool to see a big router vender implement the functionality...

Conclusion

- Greynets
- Instantiation
  - A machine connected to a VLAN trunk
    - greynetd
  - Assistance from a router
    - RFC6018
- Future work
- End.

SWINBURNE UNIVERSITY OF TECHNOLOGY