Out of Band Monitoring Scenarios

Doug White, PhD, CISSP, CCE, PI(RI)

Director, Center for Forensics, Applied Networking, and Security

Roger Williams University

The Sad Tale of Jing An

- The idea of DMZ!
  - DMZ should contain ONLY compromised assets
  - This idea has become compromised and is often misunderstood!
  - Only outward facing, expendables should be placed here

The Sad Tale of Jing An

- So what did Jing An do wrong?
  - Placing backup device in DMZ
  - Pull backups from the outward facing device
  - Both approaches compromise the backup if the server is compromised

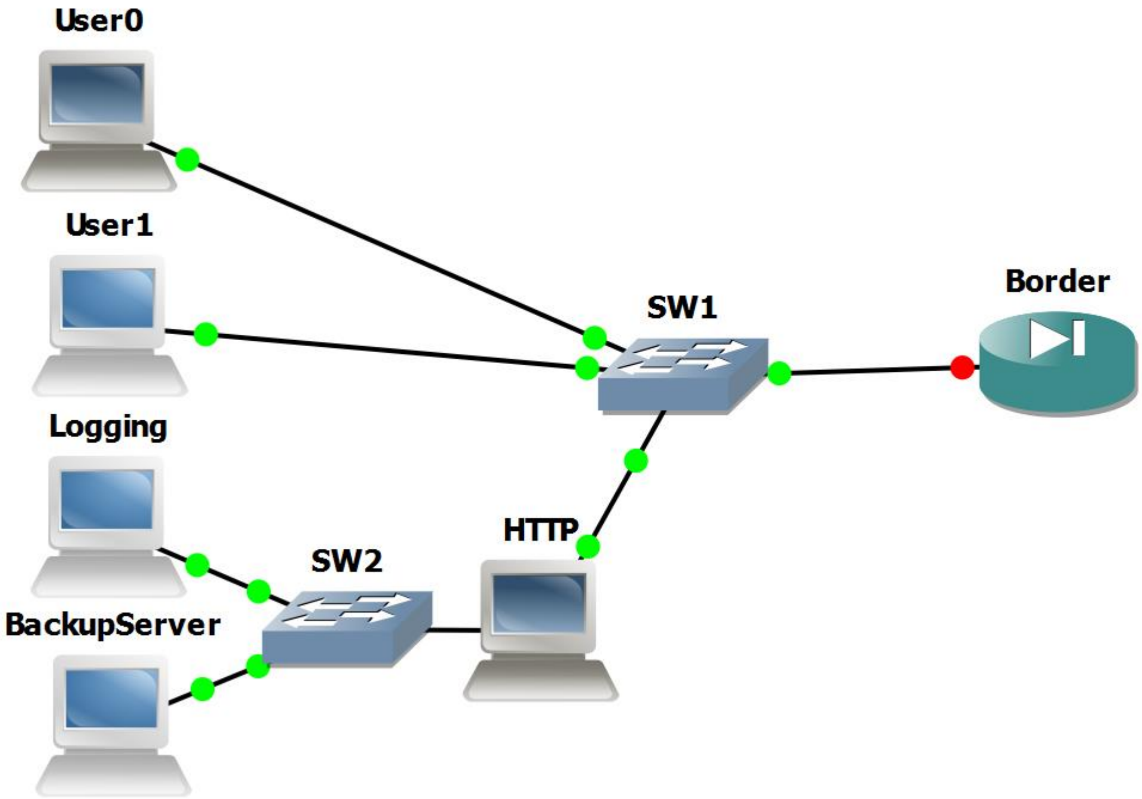
The Sad Tale of Jing Cha

- An undercover operation which reviews websites of illegal activity
  - Dump all desktops into the same subnet
  - Add all monitoring to the same subnet
  - Treat this as a DMZ!
  - Guess what happens.

Again

- Compromise of one machine in the global subnet
  - All machines compromised
  - Logging server (if it had existed) compromised
  - All other resources compromised

The stupidest configuration ever



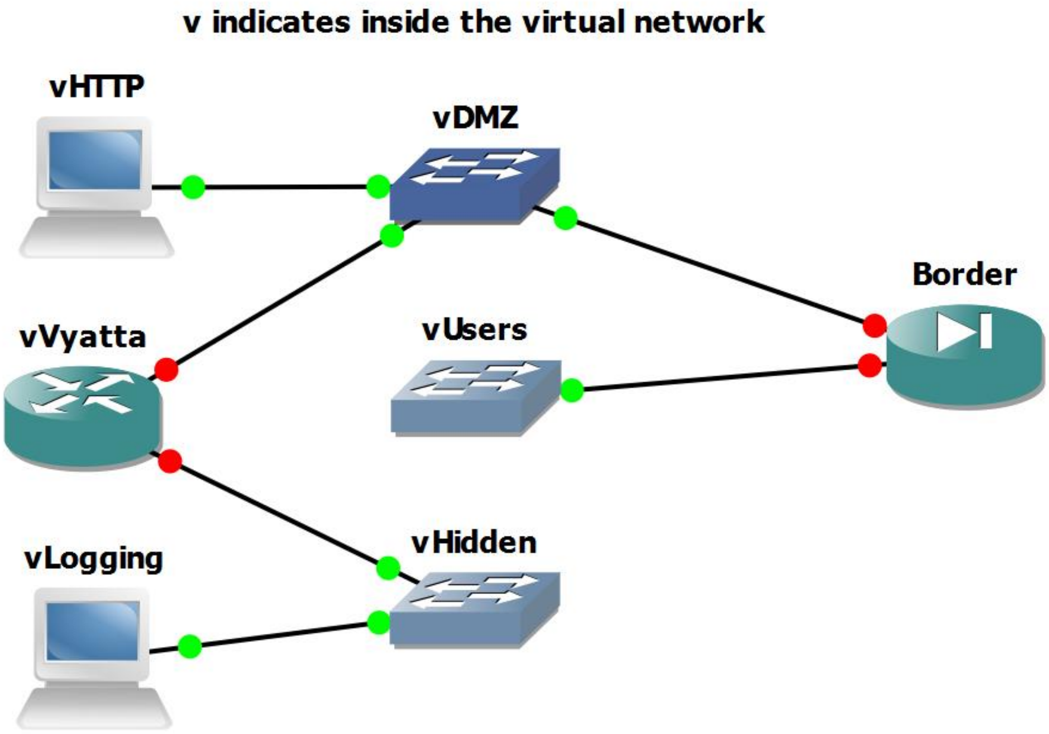
Tools

- So how do we fix this mess
  - SNORT – an open source IDS system (snort.org)
    - Can run with a variety of gui front ends
    - Low overhead so is supported on low end hardware
    - Even better is to run it on VMWARE
  - Logging servers with syslog
    - This is simple listening daemon that can again be run on vmware

Living the Virtual Life

- So if we virtualize these networks
  - We can migrate all features into a single hardware box and separate the networks using vswitches
- NOTE: we can do all this physically as well but it is more resource intensive

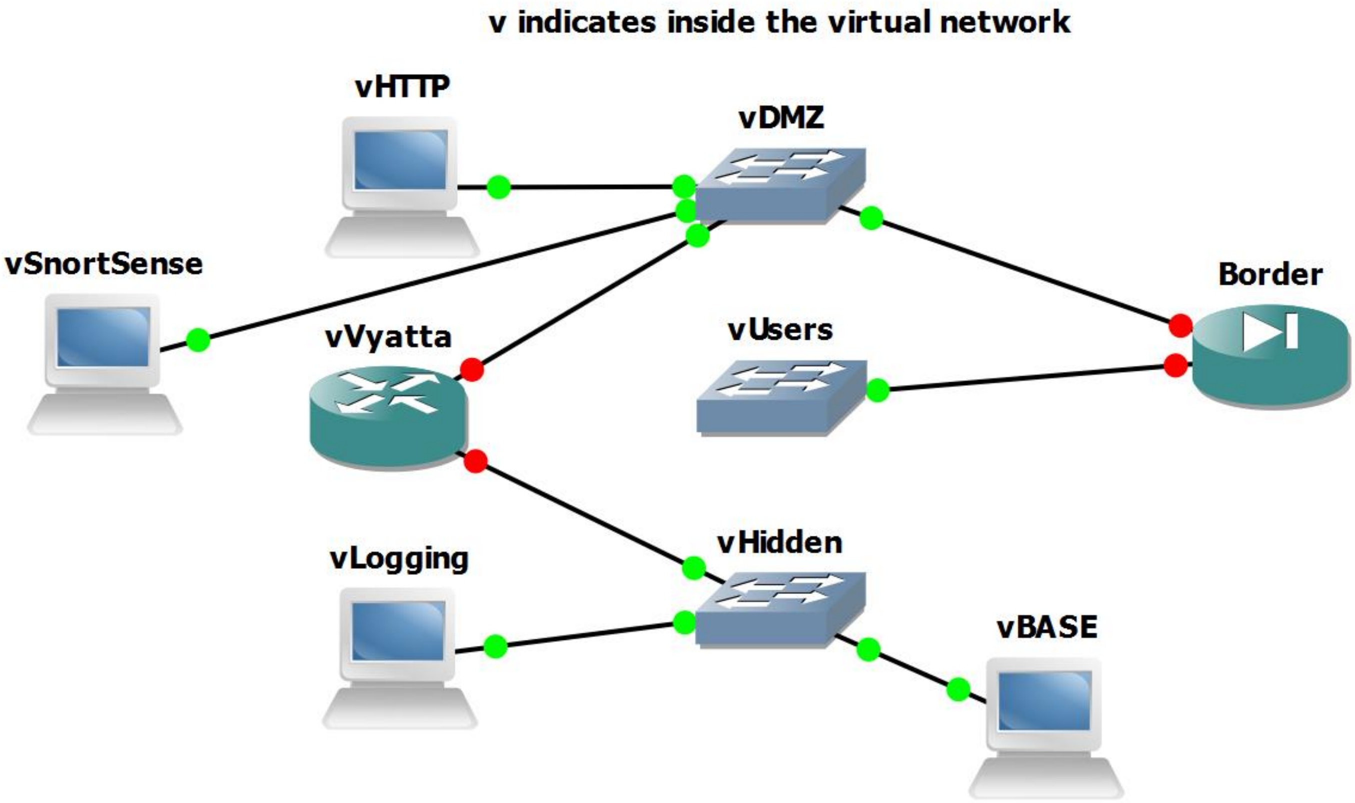
The Virtual Out of Band Logging



Things to Note

- Vyatta is an open source router/firewall
  - This could be done with any virtualized firewall or firewall/router combo to bridge between
  - Only UDP/514 is allowed through the vyatta. All other ports are blocked (we used UDP/51400)
- VLogging
  - Hardened, using splunk or other logging tool system

Snort Sensor

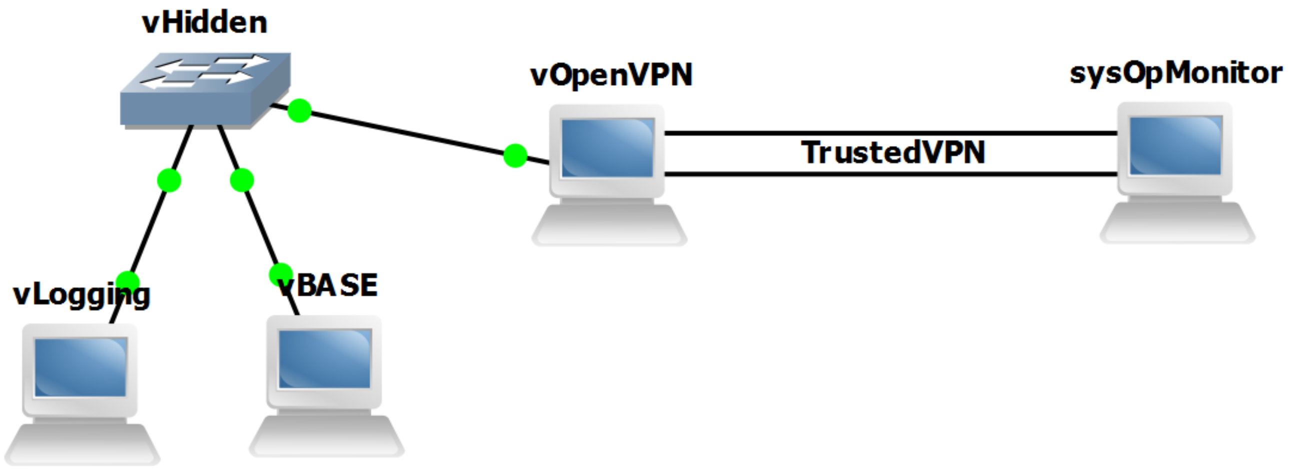


Things to Note

- The Snort sensor was simply a vm running snort with a standard ruleset.
  - Rules which monitor traffic on syslog should be implemented but it's a good idea to exclude normal traffic patterns to avoid sensory overload
  - Our trigger was any sort of probe of the vVyatta or the vLogging or vBase ip addresses since this would imply compromise of the vHTTP.

Trusted Path

v indicates inside the virtual network



OpenVPN

- Open Source Encrypted Tunnel which can extend a subnet
- sysOpMonitor can be
  - Vmware via vSwitch
  - External, out of band, location
  - Etc.

Threat Vectors

- vHTTP is primary point of entry
  - Compromise server and attempt to push syslog attacks into the vHidden area
    - Likely outcomes
      - Probes from vHTTP should trigger SNORT alerts to vBase well in advance of compromise
- Physical compromise of sysOpMonitor
  - As with all things, physical compromise is the greatest threat
  - Ensure SOM is well protected and hardened

Secondary Threats

- Lack of monitoring
  - Skills
  - Complacency
- Operator Compromise

Non-Virtualized

- VPN tunnel should be used for Logging, BASE, and SOM
- SOM should be isolated from Logging and Base with separate key set
- Logging and Base subnet is vpn point to point
  - But could be end to end
- SOM is end to point hybrid vpn

Total Cost

- Zero.
- NOTE: since we were using our own snort rules and only focused on the specific triggers, we did not subscribe to the snort ruleset. If you are using SNORT as a full IDS, you need the rule subscription.

Internet Resources

- www.snort.org/docs -- snort setups
- Base.secureideas.net – base setups
- Openvpn.net/howto.html
- Splunk.com
- Vyatta.org

Reference

- White, Doug, and A. Rea. 2003. “The Jing An Telescope Factory (JATF): A Network Security Case Study,” *Journal of Information Systems Education*. Vol 14:3. pp. 307-318.

Contact Information

- dwhite@rwu.edu
- (646)-485-5502