Deployment of Commodity Network Probes at LBNL

Jim Mellander

Incident Response Manager
Computer Protection Program
Lawrence Berkeley National Laboratory

jmellander@lbl.gov
Agenda

- Linksys in Berkeley?
- Internal Monitoring Opportunities
- "Arp"
- Please Don’t Pass the Hash
- Conclusion
- Questions
Small but Mighty
Linksys Information

- Linksys commodity Routers run Linux off the shelf
  - Processor 200 Mhz MIPS – slow by modern standards, yet no slouch.
    - No floating point hardware, so we can’t cluster these and go into competition with Gary…
  - Open-source distribution from openwrt.org includes development tools and full access to Hardware.
    - Essentially can be viewed as a cheap (~ $50) network-enabled compute engine.
      - Wireless + 5 fast ethernet ports – we turn off the wireless port.
      - Performance tests indicated that it can handle a moderate amount of traffic
- Can be used for many monitoring needs
  - Fully monitor light-to-moderately-used 100 MB links, via tap – Bro has been run on it.
  - Stand-Alone network probe for detecting broadcast traffic patterns.
Linksys and its Master

- Linksys Routers set up to be autoconfiguring
  - Acquire address via DHCP.
  - Reports all traffic seen back to central collector
    - (Except for the reporting tunnel itself)
  - Turns on “happy” light pattern when successfully communicating
  - Regularly polls master for software updates.
- Master Linux box receives traffic
  - Inbound traffic pushed onto virtual interface via custom software.
  - Bro looking at virtual interface, running ARP scan detection script.
Monitoring opportunities on LBNL’s Internal Network

Linksys

Netflow

Hosts

Subnet switches

Internal routers

Core switch

Tap

Border router

ISP router

Internet

BRO
Scan Detection

• Detecting and acting upon scanning activity is a major defensive measure of ours.
  —Scanning activity is a fairly good indicator of hostile intent.

• Several scan detection methods
  —Easy – you access N different hosts, and you’ll be investigated.
  —Harder – Is the activity consistent with normal behavior?
    • How do we characterize that?
    • Stay tuned...
Our Friend for Intrasubnet Scan Detection - ARP

• ARP monitoring
  — Address Resolution Protocol is broadcast to all hosts on a subnet
    • To communicate with other hosts on a subnet, a host needs the Hardware Address of the target host, so that it can direct packets to it.
    • When a host receives an ARP request for the IP it is using, it replies with its IP address to the requestor.
  — Since ARP requests are broadcast, having one system on a subnet will allow seeing all ARP requests, which allows detection of hosts scanning within the subnet.
  — The Linksys boxes are used for this purpose, reporting back to a central collector.
Threshold Random Walk Scan Detection

• TRW – Threshold Random Walk
  — Based on the “Drunken Walk” principle
    1. A drunk who randomly staggers about will, in general, not get too far from their starting point.
    2. However, if there is “intentionality” to a walk, you will end up at a destination, although perhaps with detours.
  — Similarly, we attempt to determine “intentionality” of a person using a host, by looking at traffic patterns
    • If a system hits mostly “live” hosts, that indicates that it most likely has an intention to communicate with them.
    • If a system hits mostly “dead” hosts, this more than likely indicates that it is scanning for hosts to target.
  — Define “mostly”? 
    • Warning, MATH ahead....
TRW Formulas

- The ratio is calculated as:
  \[ \Lambda(Y) \equiv \frac{Pr[Y|H_1]}{Pr[Y|H_0]} = \prod_{i=1}^{n} \frac{Pr[Y_i|H_1]}{Pr[Y_i|H_0]} \]

- Where the probabilities are:
  \[ Pr[Y_i = 0|H_0] = \theta_0, \quad Pr[Y_i = 1|H_0] = 1 - \theta_0 \]
  \[ Pr[Y_i = 0|H_1] = \theta_1, \quad Pr[Y_i = 1|H_1] = 1 - \theta_1 \]

  - Y = success (0) or failed (1) connection attempt
  - H0 = benign hypothesis
  - H1 = scanner hypothesis
  - \( \Theta_0 \) = probability that the source is benign, for a successful connection attempt
  - \( \Theta_1 \) = probability that the source is scanner for a successful connection attempt

- The thresholds are calculated based on
  - desired true positive (\( \beta = 0.99 \))
  - desired false positive (\( \alpha = 0.01 \))

  \[ \eta_1 \leftarrow \frac{\beta}{\alpha}, \quad \eta_0 \leftarrow \frac{1 - \beta}{1 - \alpha} \]
TRW In action

Scanner

Baseline

Non-Scanner

T I M E

Host exists

Host doesn’t exist
An ARP Scanner

Dec 15 16:54:52 198.128.26.24 -> ff:ff:ff:ff:ff:ff who-has 198.128.24.254
Dec 15 16:54:52 198.128.26.24 -> ff:ff:ff:ff:ff:ff who-has 198.128.24.255
Dec 15 16:54:52 198.128.26.24 -> ff:ff:ff:ff:ff:ff who-has 198.128.25.0
Dec 15 16:54:53 198.128.26.24 -> ff:ff:ff:ff:ff:ff who-has 198.128.24.251
Dec 15 16:54:53 198.128.26.24 -> ff:ff:ff:ff:ff:ff who-has 198.128.24.252
Dec 15 16:54:53 198.128.26.24 -> ff:ff:ff:ff:ff:ff who-has 198.128.24.253
Dec 15 16:54:53 198.128.26.24 -> ff:ff:ff:ff:ff:ff who-has 198.128.24.254
Dec 15 16:54:53 198.128.26.24 -> ff:ff:ff:ff:ff:ff who-has 198.128.24.255
Dec 15 16:54:53 198.128.26.24 -> ff:ff:ff:ff:ff:ff who-has 198.128.25.0
Dec 15 16:54:56 198.128.26.24 -> ff:ff:ff:ff:ff:ff who-has 198.128.25.1
Dec 15 16:54:57 198.128.26.24 -> ff:ff:ff:ff:ff:ff who-has 198.128.25.2
Dec 15 16:54:57 198.128.26.24 -> ff:ff:ff:ff:ff:ff who-has 198.128.25.3
Dec 15 16:54:57 198.128.26.24 -> ff:ff:ff:ff:ff:ff who-has 198.128.25.4
Dec 15 16:54:57 198.128.26.24 -> ff:ff:ff:ff:ff:ff who-has 198.128.25.5
Dec 15 16:54:57 198.128.26.24 -> ff:ff:ff:ff:ff:ff who-has 198.128.25.6

Dec 15 16:54:57 198.128.26.24 Status change Unknown -> Scanner
score=2050.176 entries=200
Please Don’t Pass the Hash

• A Microsoft “feature” now being exploited
The advent of NT domains in the mid-90’s

- You authenticate your laptop to a domain controller at work.
- What happens when you take it home, or on travel?
  - You can no longer authenticate to domain controller.
  - How are you going to be log in with credentials?
- Solution – keep track, on the system, of the last N different authentications (N=10 by default)
  - This way Windows can compare against the previous authentications that you made, when you were part of the domain.
- Keeping track of the actual password that was entered would be stupid, right?
  - Lets keep track of the password “hash”
Password Hashes

• A good idea...
  — Transform the entered password via a one-way (aka trapdoor) function.
    • Trapdoor functions make it easy to transform from a password to a hash, but ...
    • transforming back takes a much greater amount of work.
  — Compare the transformed password (aka hash) with the generated hash computed when the password was originally set.
    • If they match, the system knows that you entered the correct password, even without knowing the password, or transmitting it over the wire.
    • This is a good thing.
Passing the Hash, the Microsoft way

• ... gone horribly awry
  — What if someone got the hash from the local cache and sent that directly to be authenticated to another host?
    • Well, if the account and hash were acceptable to the other host, you would be authenticated.
  — Ever had problems with your system, and an administrator had to login with their credentials?
    • Yikes, those credentials would also be cached.
  — So, if I were an evil hacker who got onto your box, I could look in the hash cache, and try those credentials all over the lab....
Please don’t Pass the Hash

• That was NT, we’re in the Vista (and beyond) era, this must just be a historical oddity?
  —Way back in 1997, a Windows exploit named "NT Pass the Hash" was posted on Bugtraq.
  —In 2007, Core Security released the Pass-The-Hash Toolkit.
  —“It’s not a Bug, it’s a Feature” – Bill Gates, 10/23/95

• Current, and for the foreseeable future, Windows “feature”
  —How do we deal with this feature?
Pass the Hash Mitigations (or not)

• Mitigations
  —Reduce N (number of cached credentials)
    • Active Directory systems get policy pushed down which reduces N to 1.
    • Can also manually change settings.
  —If they can’t get access to the “Hash Cache” even if they get on the box, they can’t use them against us.
    • Most users have administrative rights.
    • Removing administrative rights breaks many things and makes users unhappy.
• OTP – One Time Passwords – that should help here, right?
  • Stored hashes are from after OTP authentication, so this doesn’t help. 😞
Pass the Hash Detection

- **Detection**
  - Increase Windows logging
    - In process of determining whether event logs can give insight into pass-the-hash attempts.

- **Honeypots**
  - What about deploying systems which are not normally logged into by anyone, but ....
  - ... are waiting for anyone to “pass-the-hash” to them,
  - ... and report all such attempts back to security staff?
  - Sprinkling such systems throughout the network would be time-consuming, and a maintenance nightmare, right?
  - Do we have existing infrastructure that can be leveraged to allow wide deployment of honeypots?
Linksys as honeypot

- Linksys running hacked version of Samba (An opensource implementation of the Microsoft authentication and filesharing protocol)
  - Anyone can attempt authentication, triggers email to security staff.
- Honeyd honeypot software also compiled for Linksys, in Beta test
  - Allows the Linksys to respond to several IP addresses
  - Allows system to look more like a Windows box, even to OS fingerprinting applications.
Sample email:

Subject: SMB login attempt from 131.243.64.201 to 128.3.3.109 Port 139
Tue Dec 16 13:42:58 PST 2008 131.243.64.201 logged in to 128.3.3.109 port 139
Couldn't find user administrator
Rejecting user 'administrator': authentication failed
Tue Dec 16 13:42:58 PST 2008 131.243.64.201 logged out of 128.3.3.109 port 139
Future Directions

• Automated blocking of internal scanners or honeypot attackers.
  —Obviously, false positive rate must be darn near zero before we can contemplate this.
• Active network actions - Current implementation is strictly passive, but …
  —Linksys could provide packet injection under direction from Master to isolate a host, even within its subnet, or…
  —Provide a framework for a host-registration infrastructure…
  —etc.
Conclusions

• Out of the box ideas can bear fruit with time:
  — Valuable solutions don’t have to cost much
    • Right-sizing solutions to problems
  — Once an infrastructure is in place, it can be used for purposes not originally anticipated.
    • There are many more interesting possibilities for this technology!
• We can now see scanning within subnets, which we were previously blind to.
• We have proven that honeypot technology is possible within our infrastructure.
  — Many improvements are likely in the future.
Questions

• Questions?
Additional Material
Maps between IP addresses and hardware addresses.

Every packet on the wire must have both source and destination hardware (MAC) addresses for delivery purposes.

Broadcast asks “who has a given IP address?”

Response from host with that IP address: “I do”

Only visible within a subnet
Password Hashes – the Microsoft Way

```
Seattle1

SEATTLE + 1*****

Constant

DE

Key

DE

Key

Concatenate

Constant

LM Hash
```