Vernier NETWORKS

Ensuring Network Compliance

Beyond NAC: What's your next step?

Mark "Simple Nomad" Loveless

November 15, 2007

USENIX LISA '07 – Dallas, TX

Agenda

- Basic Info
- Issues After NAC
- Next Steps
- Q&A

Basic Info

Why You Should Care

- NAC is maturing
  - Vernier alone has 1000+ customers, plus we have dozens of competitors
- Most corporations are either evaluating or considering NAC in the future
- <Insert chart with colors and arrows moving in a circle here> and say things like “synergy”, “paradigm shift”, and “at the end of the day…”
  - Your Cxx is being bombarded with material about NAC, arm yourself with knowledge

What NAC Is (and Isn't)

- It is a way of regulating and controlling access to your network
- It is a method of enforcing policy on endpoints before joining the network
- It is not a security solution, but it is an enhancement
- It is not a policy solution, again it is an enhancement

- The security and policy implications of NAC may not seem obvious

Where (or What) NAC Should Be

- The “VP at the airport” scenario
  - NAC should not be black and white, access or no access
- You should be inline, you should be FAST
  - IDS/IPS should be in there as well (great for post auth)
- If you are doing IDS/IPS, it should be state of the art and not an add-on
- It should work for the “you can’t look at our data” departments
  - Legal, Accounting, HR
- Deployment should be seamless and scalable
  - No changes to existing infrastructure

Who Owns NAC?

- Sys Admins?
- Network Technicians?
- Internal Auditing?

Issues After NAC Deployment

Adaptation by “Attackers”

- Expect attacker tactics to increasingly consider NAC
  - Already researchers are looking for ways to bypass NAC solutions
- All items that are “allowed by default” will be exploited

Adaptation to New Technology

- Everyone is on Windows and everything is great (or at least functional)
  - What happens after a merger when the new company is on Windows, Linux, and Macs? Has NetWare? Uses LDAP?
- A new policy directive states there will be no “IT department accounts” on end user systems
  - Can you just use dissolvable agents?
  - Will the dissolvable agent run on Linux? A Mac?

Policy Compliance

- Enforcing policy during network authentication is one thing, enforcing it post-authentication is another

Alternate Paths In

- The mobile workforce still poses major challenges
  - Wireless, dial-in (yes it still exists), VPN
- Contractors/Guests
  - Your policy should address this category
  - Bear in mind your contractor/guests' employer's policy may suck
- The perimeter technology is still required
  - Firewalls, mail server anti-virus, etc

Next Steps

NAC Vendors Don't Tell You…

- Post authentication, the user could be doing bad things
  - It is possible to "lie" to the code that checks your system for compliance
  - I authenticate as a Windows user (via a virtual instance of XP) and use my authenticated IP address from my Linux box
- To be effective, you must be inline, in the core, the perimeter, and everywhere in between
  - Basically you have to be between any user and every resource they might try to access
- NAC controls access to network resources like servers
  - It does not control access to applications or data independent of servers

NAC Vendors Don't Tell You… pt.2

- Tunneling protocols bypasses virtually all vendors
  - Variations on wifi auth bypassing work against NAC
- If the goods are in data, ACLs mean nothing
  - Bob has legitimate access to the Data Warehouse, can you tell if Bob is collecting data snippets to do some insider trading or identity theft?
  - Alice in Accounting and Bob in Accounting have the same profile, can you tell which one is looking at data they shouldn't be looking at?

Where Things Are Headed

- Identify more than users
  - Identify the applications they use
  - Identify the data they access
- Limit access to network resources based upon *layered* profiles
  - Access limited based upon user identity
  - Access limited based upon application usage
  - Access limited based upon data
- Correlation of events
- Automation of reactions to events
- This is not NAC, but something bigger

Vernier NETWORKS

Ensuring Network Compliance

Q&A

Fin

- mloveless@verniernetworks.com
- thegnome@nmrc.org

- http://www.nmrc.org/~thegnome/beyond-nac-07.ppt