Corporate Security: A Hacker Perspective

Mark “Simple Nomad” Loveless

LISA’06 – Washington, DC

08Dec2006

About Myself

- Senior Security Researcher, Vernier Networks Inc
  - NAC/IPS
- Founder, NMRC
  - Hacker collective

Agenda

- Attacker world
- Attack trends
- Attack techniques
- Mitigation

Vernier NETWORKS

Random Thought #1

- Seeing :wq in a /var/log/* file is a Bad Thing
- Bad because you see it, but real bad because you've been 0wn3d by someone who is so lame they can't edit logfiles

Attacker World

Vernier NETWORKS

Attacker Goals and Dreams

- 0day – the attacker goal
- Remote root access – the attacker dream
- Remote root 0day – the holy grail
- The nature of the 0day forms the nature of the attack
- 0days are worth more now than they've ever been

Vernier NETWORKS

What is 0day?

- Number of days a commercial piece of software has been on the market
  - Having a cracked copy of a new game before it even shipped was wicked cool
- Security flaw, usually remote (and preferably root access), vendor and sys admins do not know about the flaw
  - As soon as vendor/admin community is aware, no longer 0day
- Currently 0day seems to be:
  - An unpatched flaw that the vendor and sys admins know about
  - Non-public working exploit for a patched flaw

The Disclosure Cycle

- Researcher finds a flaw
- Researcher reports flaw to vendor
- Vendor develops fix
- Vendor releases patch
- Researcher releases advisory
  - A responsible researcher releases technical details after a suitable patch period, assuming that is possible

The “Other” Disclosure Cycle

- Blackhat finds a flaw
- Blackhat shares flaw with very few friends
- Usage of flaw is done to minimize vendor notification
- Blackhat tries to find yet another flaw before first flaw is discovered
- Once discovered or blackhat bored, blackhat may sell the exploit
- The object may be to sell the exploit anyway

Vernier NETWORKS

When Disclosure Cycles Meet

- Vendor releases patch
- Researcher releases advisory
- Unpatched and patched versions of “fix” files are reverse engineered
  - Bindiff w/IDA, OllyDbg, advisory clues etc
- Exploit code is developed based upon flaw
  - Whitehats use this to develop IDS/IPS signatures
  - Blackhats use this to develop attack code
  - Both hats look for “silent” patches

Targeted Penetration

- Still around, but by proportions not growing
- The “Hacking Exposed” generation
  - Statistically most targeted penetrations are successful by any skilled attacker
  - Tactics have changed substantially, most focus on defeating perimeter security

Random Thought #2

- What is the difference between someone being bad and a Bad Thing?
- An inbound connection to port 4444 is someone being bad
- Before each MetaSploit exploit module runs, it tries to connect on the assigned port in case it is already open
  - Port 4444 connection failed followed by a few packets then port 4444 connection succeeded is a Bad Thing

Attack Techniques

Various Attack Techniques

- "Click on this"
  - Also applies to "preview this"
- Inject and input manipulation
- Buffer overflows
- Heap overflows
- Format strings

New Recon Techniques

- Repeated attacks from throw-away hosts
- Single packet/connection OS detection
  - E.g. Windows PPTP gives up major build version
  - Port 0 scanning
- Attackers using dark IP space

IDS/IPS mapping

- Compromise DNS server, create subzone
  - Map out related dark IP space
  - Launch attacks from subzone
  - Note DNS queries to subzone
- Trigger simple and well known attacks from throw-away hosts
  - Did we get a response or a “response”?
  - Work on mapping IDS/IPS vendor based upon what is caught/not caught is underway

One 0day per Target

- Prudent usage of 0day
  - Only used for a foothold, usually just past the perimeter
- Normal non-0day usage for remainder of the attack (this is usually all that is needed once inside)

Random Thought #3

- Apparently working for Microsoft is evil but working for spammers is not….

Attack Trends

A Professional Blackhat

- Works for a single spammer/spyware/id theft organization
  - Many are extremely organized
- Doesn't worry (too much) about IDS/IPS/Anti-virus
- Goal is to hit fast and hit hard
- Pay is decent, around $200k per year for decent quality work
- Foreign governments/nation states/organized cybercrime willing to pay $40k-$120k for remote root 0day

Vernier NETWORKS

Freelance Professional Blackhat

- Works for spammer organizations
- Works for information brokers
- Involved with identity theft rings
- More concerned with keeping 0days 0day
- Extremely proficient at reverse engineering
- At the high end, mad wicked skills == mad wicked money

Vernier NETWORKS

Finding Flaws

- Fuzzing still works
- Checking for silent patches via BinDiff
- Checking for similar flaws in different parts of the code
- Checking for lousy fixes

What's Hot!

- Anything WiFi/Bluetooth
- Client flaws are big
  - No firewall needed
- Targeted malware
  - No more Code Red, it incites patching, awareness, and remediation
- Expect more buzz with handhelds (e.g. Blackberry)
- My botnet is bigger than your botnet
  - Six figure-sized botnets are not unheard of
  - Leasing and timesharing

What's Not

- Cross side scripting
  - Big with spammers, not with hacker types
- Individual compromises
  - As stated, proportionately not growing
  - Everything is done en masse

Current Hotspots

- Anything WiFi
- Client-side flaws
- Problems during protocol exchanges
- Microsoft big, Apple even bigger
- The caring and feeding of botnets

Random Thought #4

- On the plane home, fire up your laptop around midflight
- Note how many laptops are advertising a peer-to-peer network
- You can connect to these, and if unpatched, attack them

Mitigation

Lock It Down

- Patch
  - Mean time to exploit from patch is getting smaller
  - Many large banks have adopted a “patch and fix” policy
- Harden
  - Limit access to only what is needed
  - Locking down ACLs can save your bacon with regards to 0day

Looking Forward

- Understand your porous perimeter
  - Perimeter security is dead
- Consider new technologies to mitigate attacks
  - Network access management (yes, shameless plug)
  - Intelligent IPS solutions

Bad News, Good News

- Thousands of computers are being compromised every day
- The good news is that we are probably closer to the “every vulnerable box is compromised” end of the scale, so eventually the level of compromised systems will roughly stablize

A Note on Pen Tests

- Don’t have the pen tester only test for known bugs, or with public exploits
- There is no reason why a pen tester is the only type of person with a private collection of non-public exploit code for publicly known flaws
  - Blackhats do the exact same thing
- While using HE techniques catches low-hanging fruit, a real pen tester will use these advanced techniques to get in

Random Thought #5

- On that flight home, if you get that First Class upgrade, and if you identify a WinCE device via bluetooth, do not connect to it
- It is a Boeing plane that did not get the upgrade to turn off the “default on” for Bluetooth on the WinCE system running the navigation display system
- Don’t point this out midflight, nice people with handscuff will help you off the plane
- Have a great flight home!

Q&A

- Contact me:
  - mloveless@verniernetworks.com
  - thegnome@nmrc.org
- Web:
  - http://www.verniernetworks.com/