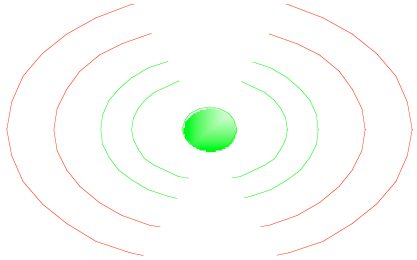
VPNSCAN: Extending the Audit and Compliance Perimeter



Rob VandenBrink

rvandenbrink@metafore.ca

Business Issue

- Most clients have a remote access or other governing policy that has one or more common restrictions on VPN connections:
  - VPN connections will use Corporate-owned hardware only.
  - VPN enabled stations will use a Corporate-Approved hardware or software firewall
  - In some cases IT will administer any home firewalls (or at least, the ones they know about)
- However, most companies to not have mechanisms to audit or enforce these policy statements

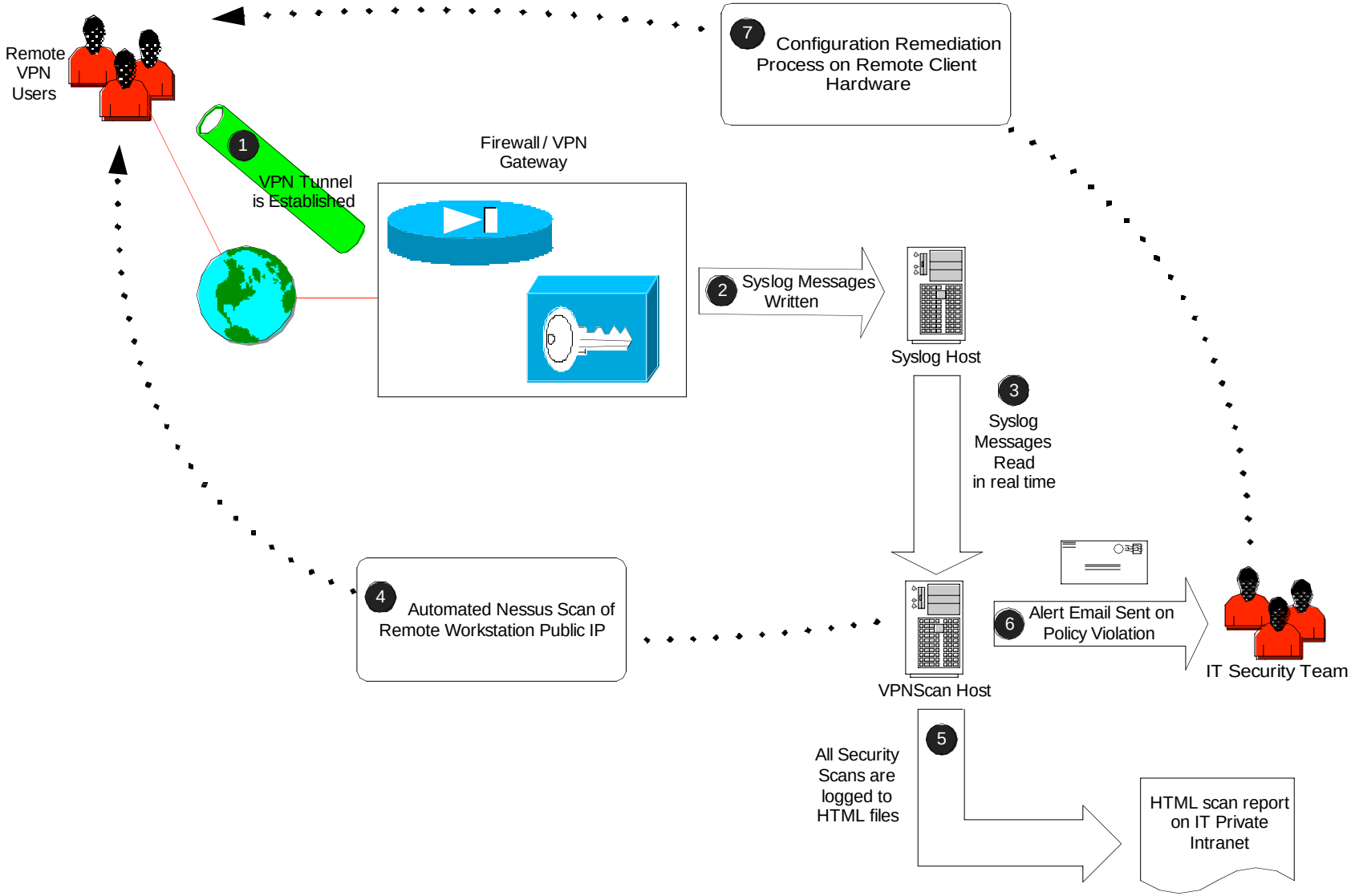
VPNSCAN

- VPNSCAN can be used to detect violation of these policy Statements
- VPNSCAN is a collection of freely available or open source tools.
- Tools are “glued together” using shell scripts
- Because of this modularity, updates to VPNSCAN are easily implemented as business or technical requirements change

VPNSCAN Components

- **SWATCH** – monitors VPN gateway logs for successful connections
- A **Shell script** parses swatch output, then uses this to call another module to assess the remote node's public address
- **Nessus** is used to assess the remote station for policy compliance
- The Nessus scan is then interpreted by the **shell script**, to verify compliance.
- Finally, the **shell script** takes action on a policy violation. Typically this is an email to the IT Security group.

VPNSCAN – Process Flow



Policy Violation Detection

- Policy violation is detected by the presence of specific strings in the Nessus Scan. These generally include:

String Detected	Indicates the presence of
445/tcp	Microsoft-DS
23/tcp	telnet
161/udp	SNMP
5631/tcp	PC/Anywhere
135/tcp	DCE Endpoint Resolution
139/tcp	Netbios Session Service
DCE/RPC	DCE or RPC Services
137/udp	WINS Name Service
138/udp	Netbios Datagram Service
135/udp	DCE Endpoint Resolution
3389/tcp	RDP
5900/tcp	VNC
5901/tcp	VNC
6000/tcp	X-Windows
6001/tcp	X-Windows
6002/tcp	X-Windows
6003/tcp	X-Windows
389/tcp	LDAP
2049/tcp	NFS
2049/udp	NFS
2967/tcp	Norton Antivirus Corporate Client
Security Hole Found	Nessus Key String indicating a serious vulnerability

Remediation can take many Forms

Active countermeasures often have an associated risk or security exposure

Possible Action taken by Script	Security Exposure
Modify the firewall rules to deny all access from that address	Admin exposure on firewall
Modify the firewall rules to deny VPN access from that ip address	Admin exposure on firewall
Disable the VPN authentication for that account	Admin exposure on AD
Disable that account entirely	Admin exposure on AD
Send an email detailing the violation to IT Security group for manual remediation	Standard SMTP email concerns (packet capture)

Risks / Decisions in Remediation

- Explicit denies of any type will almost certainly be viewed as a denial of service by the client community.
- Maximizing service delivery and “pain avoidance” is almost always a significant motivator for IT groups.
- Management is often more inclined to “take the hit” on a few major incidents, as opposed to continued client pressure regarding perceived service issues.
- After hours coverage and premiums are also often a consideration
- To date, all VPNSCAN implementations have opted for email notification with manual remediation, typically during business hours the next day.

Design Decisions - Components

- CENTOS was used to host this service - freely available, binary compatibility with a “Corporate OS” for future upgrades (Redhat)
- SWATCH was chosen to detect “events of interest” – it is easily extended to support other VPN Gateways
- Nessus was chosen as the scanner to detect policy violations – an industry standard “free” scanner.
- VPNSCAN is ideally deployed as a Virtual Machine – it has low memory, cpu and disk requirements.

Design Decisions – Build / Deploy

Build:

- Use config files instead of hard-coding run values (vpnscan.cf)
- Use config files instead of hard-coding policy violations (services.deny)
- Entire solution is built in /opt for portability and easy separation of application from OS

Deploy:

- Use existing syslog repositories when possible (watch directory ACLs)
- Use existing intranet to publish results when possible (again, watch ACLs)

Configuration File - VPNSCAN.CF

```
#
# These Variables are typically ok as-is
#
#This is where the app is installed
BASEDIR=/opt/vpnscan

# The Nessus Server - typically this is localhost
NESSUSSERVER=127.0.0.1
# Credentials for accessing Nessus
NESSUSUSR=vpnscan
NESSUSPWD=Passw0rd123

# Where should we deposit the Nessus Reports
REPORTDIR=/opt/vpnscan/mnt/vpnscans
# Where should we look for our syslog file
SYSLOGDIR=/opt/vpnscan/mnt/syslog
#

# These variables are site-specific and should be tailored
#
#

# The Corporate mail server, spam filter or other valid smtp host
SMTPSRV=172.16.1.22
# Which user or group should receive alerts
ALERTUSR=itservices@metafore.ca
```

Typical Client Results

After VPNSCAN is installed, clients often learn some surprising things:

- Often as many as 15% of VPN users connect directly to the internet, without protection, as instructed by their ISP.
- Corporate Remote control clients are often left on by default (RDP, PC/Anywhere, CarbonCopy Dameware).
- Personal Firewall Software are often misconfigured (ports left open for MS Networking).

Typical Client Results

Continued ...

- Errors in IT deployed Group Policy will often be found (control of Windows Firewall for instance).
- “Technical” users will often improperly configure firewalls, or will connect wireless firewalls backwards.
- Even if all the rules are followed, “travelers” connecting from a hotel are often “forced” to violate policy.

Future Development

- Windows version - based on KIWI syslog, Nessus for Windows and cmd/vbscript scripting.
- Support for additional platforms (Checkpoint, Citrix CSG, HTTP authentication etc).
- Extensions to detect unprotected users behind NAT Firewalls at Hotels etc.

Summary

- VPNSCAN fills a policy requirement for many Corporations
- VPNSCAN is:
  - simple to build
  - Built on free toolset
  - Extensible for various VPN Platforms
  - Easily modified for various remediation methods
- Did I mention free?

Acknowledgements

- SANS (http://www.sans.org) and the SANS Technology Institute (http://www.sans.edu) for the motivation and opportunity to develop, publish and present this idea
- Alan Paller for assistance and direction in proofing this presentation
- Jim Purcell for his assistance as advisor for the original GSEC Paper (http://www.sans.org/reading_room/whitepapers/auditing/1711.php)

Product and documentation References:

- CENTOS http://www.centos.org
- Swatch http://sourceforge.net/projects/swatch/
- Nessus http://www.nessus.org
- Cisco Documentation http://www.cisco.com/univercd
- VMWare http://www.vmware.com
- KIWI Syslog http://www.kiwisyslog.com/syslog-info.ph