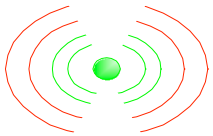
VPNSCAN: Extending the Audit and Compliance Perimeter



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

Business Issue

Most companies have a policy or policies governing Remote Access. In almost all cases, they have wording similar to or encompassing:

> •All VPN or Dialup connections to the Corporate Network will be made from Corporately owned hardware
>
> •Any Internet connection made from a non-Corporate location will use a properly configured (or Corporate owned and configured) hardware firewall
>
> •All Corporate owned laptops will have a Corporate approved, properly configured personal firewall installed.

In many cases, a list of corporate approved hardware / software firewalls are included in or referred by the policy. In a some companies, the IT group owns and administers all home-based firewalls (that they know about).

However, I have yet to work with a company that has a mechanism for enforcing this policy wording.

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

VPNSCAN is simply a collection of free-for-download available tools, “glued together” with some shell scripting and configuration files.

Because it is so modular, it is simple to change out one tool for another if required.

Configuration changes are made by updating configuration files rather than code.

Also, it is a simple matter to change script actions to match differing policy requirements for different environments.

VPNSCAN Components

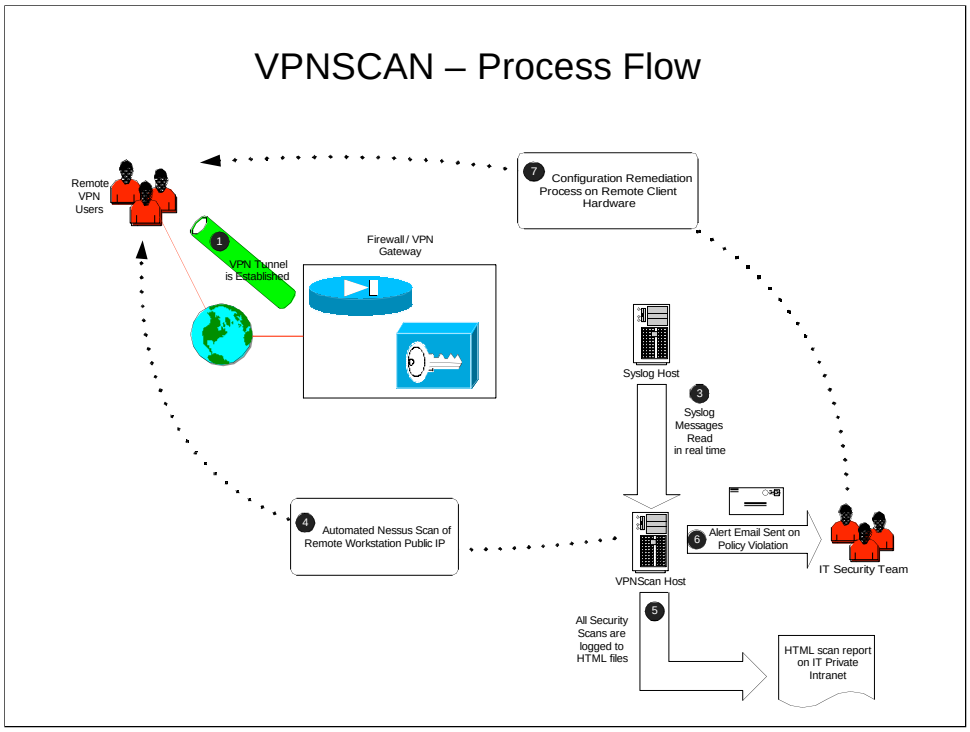
- **SWATCH** – monitors VPN gateway logs for successful connections
- A **Shell script** parses swatch output, then uses this to call another module to assess the remote node's public address
- **Nessus** is used to assess the remote station for policy compliance
- The Nessus scan is then interpreted 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 Components

SWATCH – An open source tool (http://sourceforge.net/projects/swatch/) that monitors logfiles in real-time. When an "event of interest" occurs, swatch will initiate the action configured for that event. In our case, we are "swatching" a syslog log from a cisco firewall or other VPN gateway, the "event of interest" is a successful VPN authentication, and the "action" is to call a script, which in turn calls another application to assess the remote station (Nessus).

Nessus – A closed source but freely available (http://www.nessus.org/) vulnerability scanner. Nessus is used to assess the remote station that is VPNing in. Nessus results are written to an HTML report file.

A set of **Shell Scripts** "glues" the components together. The script parses the SWATCH output to feed Nessus the proper parameters, parses out the Nessus output to validate if a policy infraction has occurred or not, and finally takes any action that is configured (in most cases the script sends an email to IT Security personnel).

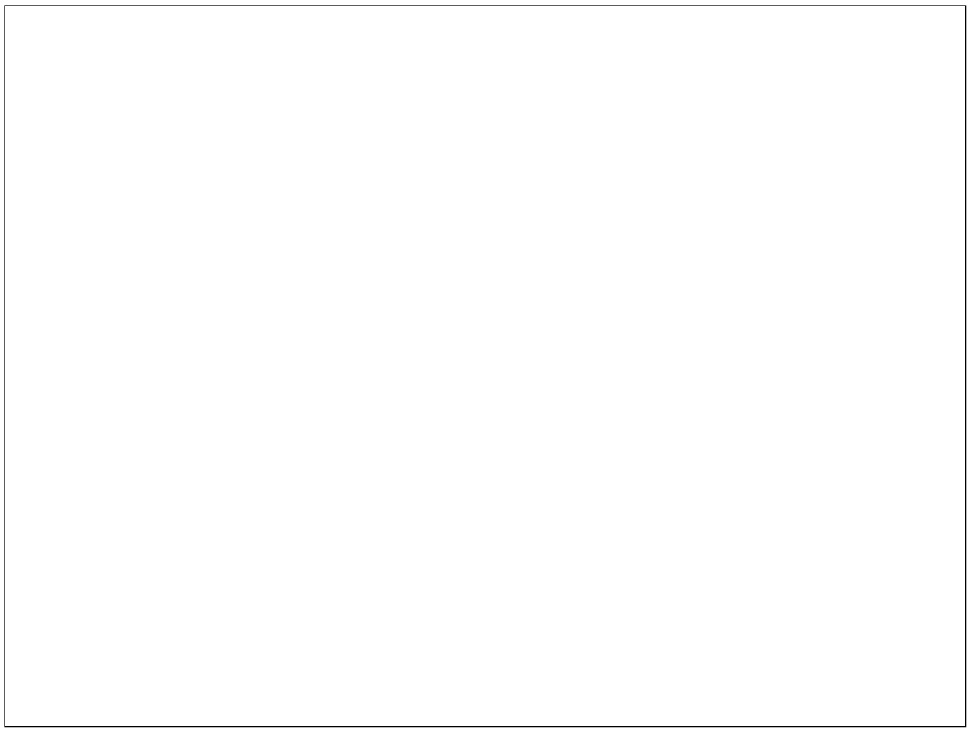


VPNSCAN – Process Flow

1. Client connects - This can be an IPSEC or SSL vpn connection but could just as easily be a Citrix or RDP connection (either CAG or native ICA), or a connection to an HTTP website (perhaps an internet facing corporate portal). The diagram shows a VPN connection to a “traditional” Firewall / VPN Gateway.
2. Log file entry is written - The key thing is that the event log needs to indicate the USERID that is connecting, as well as the public ip address of the connecting station. In some cases additional scripting may be required to get this information – for instance for a Citrix ICA or RDP session, you may need to update the login script to capture this information.
3. Swatch reads the log entry as it is written, and the “event of interest” is captured. In the case of a cisco VPN connection, swatch looks for the string “109005” in a syslog message, which indicates a successful connection message of the format:

   2006-09-06 21:35:11 Local4.Info 172.16.1.2 Sep 06 2006 21:35:11: %PIX-6-109005: Authentication succeeded for user username from 111.222.33.44/0 to 99.88.77.66/0 on interface outside

   Swatch calls the shell script with this message as input, which parses required information (userid and public ip address), then calls Nessus using these values.
4. Nessus scans the public ip (ports 1-65535), then ...
5. Nessus writes the scan results to an HTML file, typically in an http-browseable “IT Intranet” location.



VPNSCAN – Process Flow (continued)

6. Control then is passed back to the shell script, which evaluates the HTML output for any strings indicating a policy infraction. These strings are maintained in a config file. If a policy violation occurs, the script executes an “action”. In all installations to date, the “action” is an email sent to IT security personnel. However, this action could also include such items as:
   - suspending VPN privileges for the affected account
   - suspending the affected account entirely
   - modifying firewall rules to “shun” the public IP address of the remote station.
7. Remediation of the security infraction is normally a manual process, typically the IT security person will contact the affected client the next day via telephone, and arrange either a laptop reconfiguration (personal firewall configuration or installation), or else a reconfiguration or installation of an approved hardware firewall at the remote location.

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

Policy Violation Detection

The violation of policy is detected by parsing the Nessus output for the presence of specific strings. These strings are kept in a text file, /opt/vpnscan/etc/services.deny.

Note the last string in the file “Security Hole Found”. This line is one of the primary reasons for using Nessus instead of a lighter weight tool such as NMAP (which would detect all of the other criteria).

This could be extended further to evaluate more stringent criteria – for example, scans could be further assessed by their total aggregate risk, as indicated by exceeding an agreed upon Common Vulnerability Scoring System (CVSS) score (see http://www.first.org/cvss/). A total CVSS score for a given Nessus Scan can be computed in a shell script in a single line:

```
cat scanresults.html | grep CVSS | cut -f2 -d":" | awk -v COLUMN=1 '{ sum += $COLUMN } END { print sum}‘
```

Note however that Nessus does not maintain a CVSS value for 100% of the items that it may log to a report. For this reason, reliance on a total CVSS “score” as a single measure of security posture is not encouraged.

Remediation can take many Forms

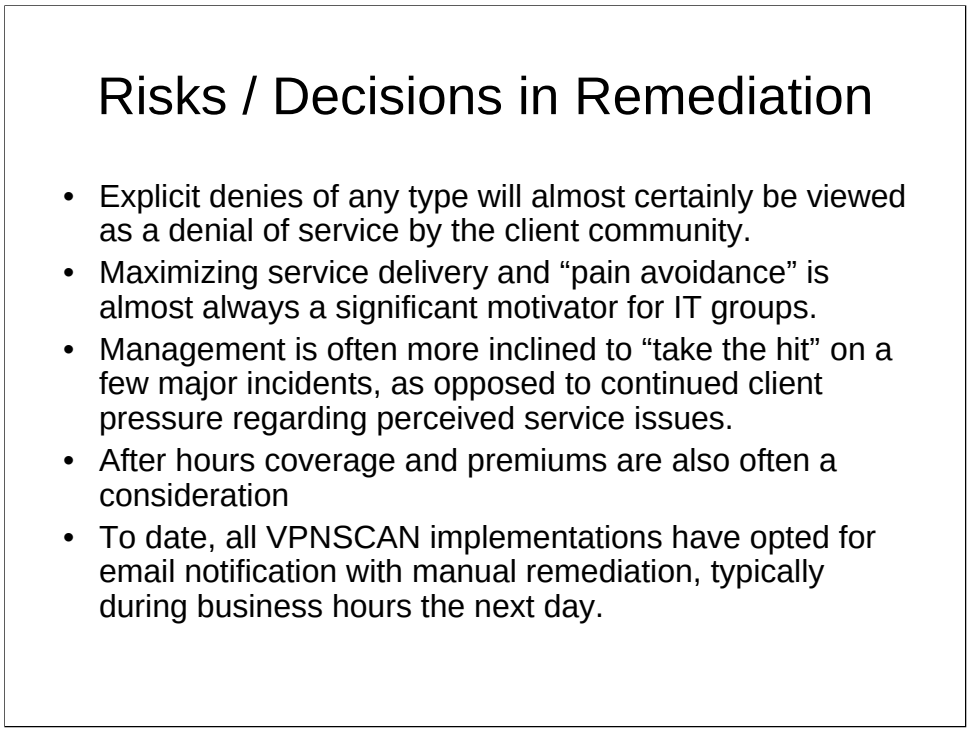
Active countermeasures often have an associated risk or security exposure

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)

Remediation can take many Forms

As discussed, a scan indicating a policy infraction results in an automated response. The response can fall anywhere within a continuum of options, which could include such items as:

1. Modifying firewall rules to “shun” the public IP address of the remote station. This requires a manual action to remove, either by the script or by security personnel. A significant risk in automating this action is that the script needs administrative-level access to the firewall to code or uncode these restrictions. Compromising the VPNSCAN station could then easily lead to a compromise of the firewall (!!)
2. Modify firewall rules to only deny VPN access from that IP address. Exactly as in the “shun” option, manual action is required to un-code this restriction, and the script requires an administrative access.
3. Suspending VPN privileges for the affected account. This is typically a change to the client’s Active Directory account. Similar to the above changes, the script will require domain administrator privileges to make this change
4. Suspending the affected account entirely – again, domain administrative privileges are required.
5. Send an email to IT Security personnel. This option requires no elevation of privileges, but as always with sensitive information, care should be taken that the email cannot be “captured” in transit.



Risks / Decisions in Remediation

IT departments are typically “Risk Adverse”. However, this often takes a back seat when faced with client complaints.

Any active response to a security event that might affect access to resources is always viewed as a service interruption by clients.

While security personnel may prefer an active response, helpdesk personnel and upper management prefer a passive approach, permitting the security exposure to continue to allow the client continued access. As a department, most IT groups are motivated more by avoiding the pain of continual client complaints resulting from an active response strategy, as opposed to facing 1 or 2 major system outages per year due to security events that they might face with a more passive approach. Hopefully, the fact that we are seeing more security incidents that have to do with data theft and negative publicity than outages will have an impact on this stance.

Finally, in many environments security personnel are viewed as senior staff, and work a standard 8 hour day. In many cases even the helpdesk only covers an 8 or 12 hour window. In environments such as this, shortening the response window on security events involves unpopular corporate decisions involving rotating shifts, rotating pager(s), or some other method of covering “after hours” windows of operation.

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 – Components

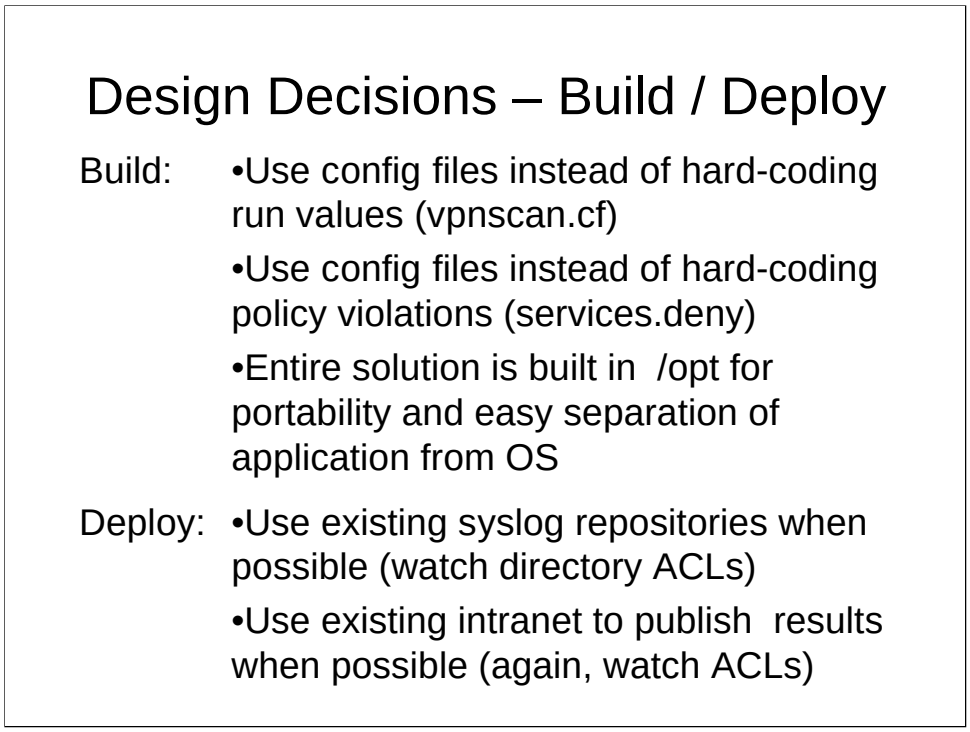
CENTOS was chosen as the host operating system for VPNSCAN. CENTOS has a unique market niche, in that it has binary compatibility with the Redhat enterprise versions of Linux. This gives it two advantages for delivering key system functions:

- System stability is valued over a “bleeding edge” feature set
- There is an easy migration path to a “Corporate” version of Linux (ie Redhat).

SWATCH was used to detect “events of interest” as it monitors standard text logs of any kind, and can easily support any VPN gateway as well as other access methods such as HTTP, RDP or Citrix ICA.

Nessus was chosen as the scanner for VPNSCAN because it is free, and can be configured to detect many security configuration errors. If only a port scan was required, NMAP would certainly do the job. An importante Nessus feature is the catch-all phrase “Security Hole Found”, attached to anything Nessus detects that is of significance in a VPNSCAN deploy.

VPNSCAN has low requirements for memory, cpu and disk resources. This makes it an ideal candidate for deployment as a virtual machine. This also tremendously simplifies tasks such as backup, restore, and transport to different environments.



Design Decisions – Build / Deploy

All configurations for "run" values of VPNSCAN, such as SMTP server addresses, email alert destinations etc, are in a configuration file (/opt/vpnscan/etc/vpnscan.cf).

Strings that identify policy infractions are similarly coded in a text file (/opt/vpnscan/etc/services.deny).

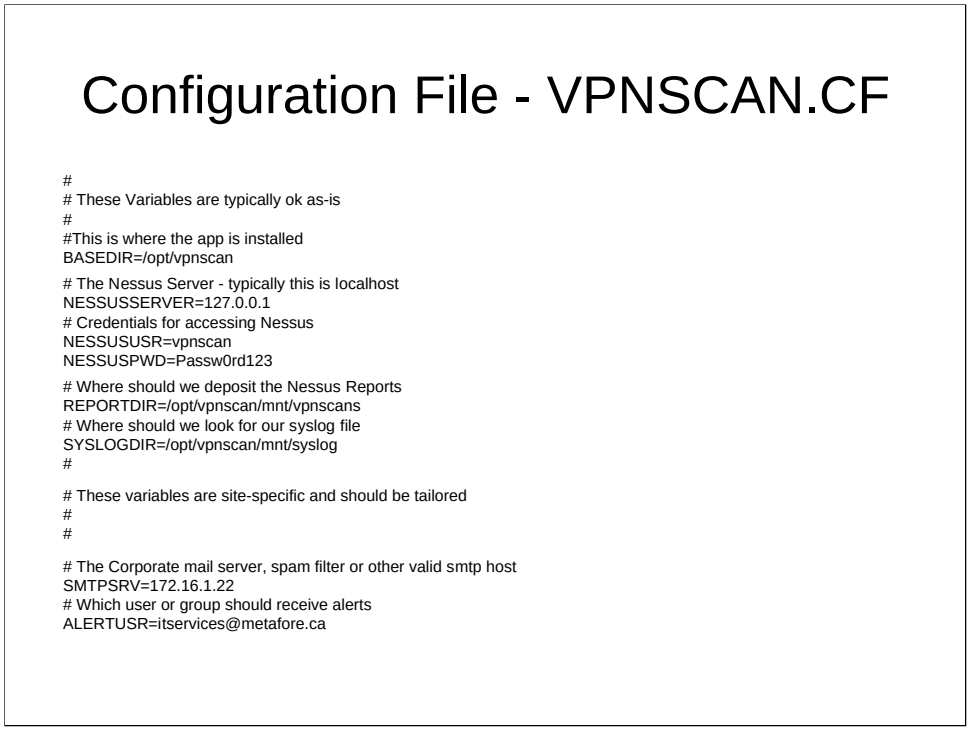
All components for VPNSCAN are located in the /opt/vpnscan directory for several reasons:

- To permit portability to other platforms
- Separates VPNSCAN components from other Operating System components
- If required, /opt or /opt/vpnscan can be a separate mountpoint, so that if for some reason vpnscan requires significant disk (for instance, if syslog is local), disk space required by the root filesystem is not at risk

If a corporation is already logging their firewall activity, existing log repositories should be used, rather than creating another separate log.

If an existing IT "Intranet" resource exists, that directory structure should be used to post any VPNSCAN results.

For both syslog and scan results directories, ensure that the directory ACLs are appropriate for the information stored – neither of these directories should be publicly accessible within your organization.



Configuration File – /opt/vpnscan/etc/vpnscan.cf

Vpnscan.cf holds several parameters:

BASEDIR is the directory that holds VPNSCAN – this is typically /opt/vpnscan

NESSUSSERVER is the server where the Nessus daemon runs. Typically this is the local host, but can be an existing server if Nessus is used for other purposes in an environment.

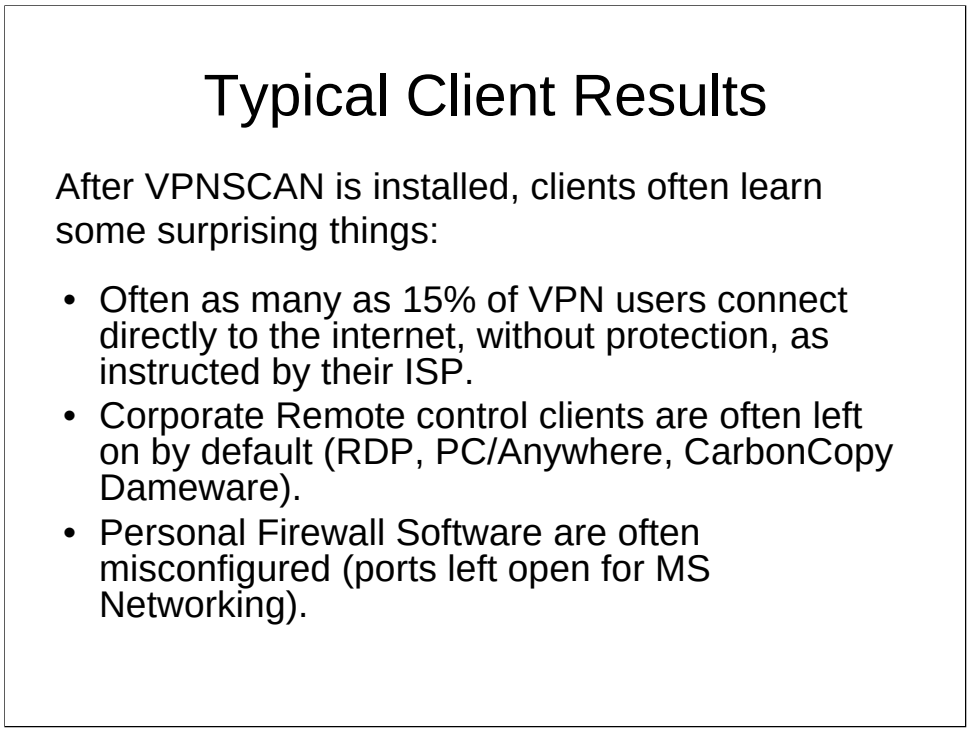
The **NESSUSUSR** and **NESSUSPWD** variables hold the credentials for the Nessus client. Ensure that these credentials are NOT used in other critical areas of the infrastructure. Also ensure that these credentials are NOT as trivial as shown. Remember that Nessus can crash remote hosts - these credentials can be dangerous !

REPORTDIR is the location for the Nessus report files. This is typically indicates a mountpoint to a remote directory which holds the IT “intranet”

SYSSLOGDIR is the location where the text logs for the VPN gateway are located. This is also typically a mountpoint to a remote syslog directory.

SMTPSRV is the address or FQDN of a server that will accept emails

ALERTUSR is the email address to send alerts to. In smaller environments it indicates a mail group for the entire IT group, in larger environments it will be a mail group for the IT Security or Infrastructure team.



Typical Client Results

After VPNSCAN is installed, the results are often surprising to IT managers.

In many cases, corporate users rely on their ISP for support in setting up their home Internet connections. Often this means that as many as 15% of the clients who use VPN services have their laptops connected directly to the cable or dsl modem.

Often, corporate users will “suspend” or “hibernate” their laptops when they leave work, and simply “resume” when they get home and VPN in. From their perspective, this has the advantage of maintaining drive maps and other connections (usually without the bother re-authenticating), as well as the convenience of a quicker startup. However, it also means that any corporate remote control /remote support tools will in most cases still be running.

Personal firewalls are also often configured incorrectly to permit file sharing or shared printing, which opens significant SMB vulnerabilities on the internet (starting at null shares and working up from there)

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.

Typical Client Results (continued)

Scanning stations that have not previously been monitored will often find errors made by IT, either in configuring personal firewalls or in Active Directory Group Policy implementations

It’s surprising how many “technical” users connect up their wireless firewalls backwards (with the WAN port unconnected).

After everyone is compliant, anyone who travels can easily be “forced” to violate corporate policy when connecting up through a hotel’s internet services. This often leads IT groups towards a more stringent deployment of corporate based personal firewalls, HIDS (host based intrusion detection) for laptops, or in some cases “portable” hardware firewalls.

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.

Future Development

A Windows based VPNSCAN has been deployed, using Kiwi syslog (http://www.kiwi-enterprises.com), Nessus for Windows (http://www.nessus.org), and .cmd files to replace the function of the linux shell scripts. This fills the same function as the linux based deployment, but sacrifices in a few areas – the OS and the tools are not free, and the flexibility in tool selection available for a linux platform is not there for Windows. So far, all production deployments of VPNSCAN have been on a linux platform.

Support for additional platforms has been introduced (Citrix ICA, Cisco ASA5500, Cisco VPN 3000), and is planned for other access methods (standard IIS based HTTP, Checkpoint).

Finally, an unprotected client on a shared network at a typical Hotel will normally pass a VPNSCAN / Nessus assessment. Work has started to properly assess stations on such shared networks – the challenge is to differentiate Hotel NAT firewalls from “sanctioned” home-office NAT firewalls.

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

Questions are welcome …