**Control Name:**

AC-17 REMOTE ACCESS

<https://nvd.nist.gov/800-53/Rev4/control/AC-17>

**Control Description:**

Remote access to a system needs to be authenticated before given access to said system. Remote access must be managed through restrictions and configurations set upon the systems handling the method of connection. Any form of remote connection should have security requirements set in place before the connector can access internal systems. Remote access connections need to be monitored and encrypted. Remote access connections need to go through managed network access points and should not circumvent security systems. Organizations using remote access need the capability to close and disable connections being made to internal systems.

**My Examples:**

* Monitoring VPN connections and passing its traffic through a managed access point before reaching its intended destination.
* Access controls for remote connections, only allow access to what is needed.
* Specific settings needed on a user’s system/software before connections are established.
* Multifactor authentication before establishing a remote connection.
* Limit access points and parse traffic through an IDS/IPS before arriving to its intended destination.
* The user connecting should protect the information he is accessing, physically and digitally, from being disclosed.

**Control Name:**

RA-5 VULNERABILITY SCANNING

<https://nvd.nist.gov/800-53/Rev4/control/RA-5>

**Control Description:**

Performing vulnerability scans on information systems and applications being used in the organization. A frequency schedule and comprehensive requirements must be set in place by the organization. New vulnerabilities that may affect a system or application should be identified and reported. Vulnerability scanning tools and techniques used by an organization should work together to automate the vulnerability management process. Vulnerability scanning tools should be capable of updating their vulnerability database and the organization must set a schedule for said updates. Vulnerability scanning tools and techniques should be able to follow the standards for:

* Enumerate platforms, software flaws, and improper configuration.
* Formatting checklists and test procedures.
* Measuring vulnerability impact.

Organizations must analyze the reports generated by tools and remediate legitimate vulnerabilities found within an allotted amount of time. This time frame is set by the organization in accordance to the risk each finding possesses. The findings should be shared to authorized personnel that oversee similar systems affected by the same vulnerability. Organizations determine what information is publicly available and need to have a plan of action for taking down information if needed. Organizations should be aware of a scans access into sensitive areas and should have procedures for dealing with privileged access. An organization should also make sure vulnerabilities found have not been exploited and should analyze trends found in reports.

**My Examples:**

* Using tools such as Nessus, Nmap, OpenVAS for vulnerability scanning and management.
* Having a daily or weekly signature/CVE update on the tools being used.
* Red team exercises being used to find vulnerabilities as well (Social Engineering).
* Assessments on each finding and finding anything related on online databases such as CVE, NVD, and CWE.
* Using the CVSS to help in the risk assessment for each vulnerability found.
* Remediating each vulnerability found through patching, fixing misconfigurations, and/or through other means.

**References**

Joint Task Force Transformation Initiative. (2013). Control-AC-17-REMOTE ACCESS (SP 800-53 Rev. 4). Retrieved from National Institute of Standards and Technology(NIST) website: https://nvd.nist.gov/800-53/Rev4/control/AC-17

Joint Task Force Transformation Initiative. (2013). Control-RA-5-VULNERABILITY SCANNING (SP 800-53 Rev. 4). Retrieved from National Institute of Standards and Technology(NIST) website: https://nvd.nist.gov/800-53/Rev4/control/RA-5