Network Access Control

A newsletter for IT Professionals

Issue 9

I. Background of Network Access Control (NAC)

What is NAC?

Network Access Control ("NAC") enforces security of a network by restricting the availability of network resources to the endpoint devices based on a defined security policy.

The NAC Process

A common NAC solution firstly detects an endpoint device connected to the network. Once the device is detected, NAC server will initiate the authentication and security assessment process. This can be performed either directly by a software agent installed on the endpoint device, or indirectly by testing the responses of the endpoint device by an external network-based scanning engine. If the endpoint device satisfies the defined security policy of the protected network, access would be granted to the endpoint device according to its role or identity. Insecure endpoint devices will be isolated in a quarantined area until it is reintroduced to the network and assessed to meet the security requirements. Remediation may be suggested by the NAC solution to the endpoint device, depending on the risk of malicious attempt to access the network.

Depending on the network environment in need**,** there are two types of NAC solutions, agent-based and agent-less models, for the implementation of network access control.

Agent-based NAC Model

Agent-based NAC solution deploys NAC agent on the endpoint device. The NAC agent performs security checking and authentication on the endpoint device directly, and provides information and assessment results to the NAC server for authentication.

An example of agent-based NAC is by the 802.1X protocol. It is an IEEE defined protocol to prevent elements from connecting to the network before it is assigned an IP address. All endpoint devices, networking devices and legacy equipments must be configured to use 802.1X.

Reference:

http://www.enterasys.com/company/literature/nac-wp.pdf
http://www.juniper.net/us/en/local/pdf/whitepapers/2000216-en.pdf

I. Background of NAC (cont'd)

An 802.1X network requires the following three components to operate:

1. **NAC Agent** – acts as the client side. It is loaded onto the user's device and is used to request network access.
2. **NAC Network Device** – network infrastructure used to perform authentication, such as network switches or wireless access points.
3. **NAC Server** – receives Remote Authentication Dial In User Service (RADIUS) messages and uses it to verify the authentication credentials against a backend authentication database.

An NAC agent on the endpoint device presents the network credential to the NAC-compatible network device. The network device would pass it to the NAC server, and the server would check and validate the network credential. Once validated, a network port on the NAC-compatible network device would be opened and made available for the user to access the network.

Agent-less NAC Model

The other type of NAC solution does not require a permanent software agent to be installed on the endpoint device. Information about the endpoint device is gathered by vulnerability assessment from the network or temporary software installed on the endpoint device.

- **Network-based NAC**
  By leveraging vulnerability assessment tool such as Nessus vulnerability scanner, assessments on the endpoint device can be performed by gathering information such as the responses of the endpoint device. This model applies to traditional PC-type end systems, but is especially helpful in supporting the more diverse end system environments where nonuser-based end systems and end systems with non-traditional operating systems are present.

- **Applet-based / Dissolvable Agent-based NAC**
  This type of NAC is similar to the agent-based NAC solutions. Instead of a permanent software agent to be installed on the endpoint device, a Java applet, an ActiveX control or a dissolvable software agent is downloaded to a user endpoint device when accessing a web page from the protected network. Local assessment is performed by the temporary agent on the endpoint device.

Do Universities need NAC?

The education sector has been a huge customer of the existing NAC solutions in the market across the globe, together with government, health care and financial institutions.

Some vendors considered that the reason would be the large number of unmanaged devices in colleges and universities. They are mainly student computers which need some way to check they have fundamental protection.

Reference:
http://www.juniper.net/us/en/local/pdf/whitepapers/2000216-en.pdf
http://www.networkworld.com/newsletters/2007/0716nac2.html
http://www.enterasys.com/company/literature/nac-wp.pdf

I. Background of NAC (cont'd)

The following is a real industry story of Central Michigan University ("CMU") faced security threats and decided to implement NAC to resolve the vulnerabilities in their networks.

Industry Story

The CMU had a localised security incident for its campus of more than 27,000 students because of worm infection. Internet access was shut down for all the residence halls, and an army of students were gathered to patch student systems one at a time, by hand. There were 26 residence halls and apartments in CMU. To head off infection, networking, help desk and residence hall staff members burned more than 1,600 CDs with the latest Windows patches and the university's licensed antivirus package. In less than three days, roughly 6,000 users with unpatched systems and out-of-date antivirus programs showed up, along with additional 800 virus-related incidents came to light. IT shut down the entire dorm rooms because it had no idea whose system was infected, which has fomented mass resentment in CMU.

To prevent the same disaster from happening again, the university wanted an automated process that could authenticate students' devices before they connected to the CMU network and kick them off if they became contaminated. They found an "out-of-band" NAC solution which can be quickly deployed because it analyse the network passively. It is suitable for their requirements and implemented it at last. The NAC manages, secures and controls approximately 17,000 devices accessing the CMU network when the university is in session, enforcing the network authentication and registration policies. This includes quickly identifying, locating and tracking network clients, and isolating at-risk users and devices in a quarantine area.

See the article: (http://www.bradfordnetworks.com/3368)

Key Benefits Achieved Through NAC

1. **Zero-day Attack Mitigation**
   NAC solutions is able to prevent the access of endpoint device that lack antivirus, patches, or host intrusion prevention software to the network and lower the risk of cross-contamination of computer worms with other devices in the network.

2. **Policy Enforcement**
   NAC solutions allow network operators to define and enforce policies, including security requirements to be met by the endpoint device or the types of computers or roles of users allowed, in the protected network.

3. **Access Management**
   NAC controls or restrict access by endpoint device to the network based on their health. Vulnerable endpoint devices are allowed to communicate on the protected network since they could pose a security risk to critical processes and services.

Reference:
http://www.enterasys.com/company/literature/nac-wp.pdf
http://en.wikipedia.org/wiki/Network_Access_Control

II. Risks of NAC in Universities

If an NAC solution is deployed in the university, it is possible to meet undesired situations affecting the effectiveness of NAC and the overall network environment.

- **Incompatibility**

  Many NAC products require all devices in the NAC-protected network to use the same protocol, e.g. 802.1X, or to be based on certain operating systems. It is common that some of the network devices in the network either have been implemented for a long period or operate on different protocol / operating systems, which may not be compatible with the NAC solution. This would affect the functionality of the NAC solution and brings ineffectiveness in protecting the network access.

- **Inaccurate Authentication**

  Depending on the type of NAC solutions implemented, the authentication by the NAC software may subject to the risk of spoofing by hackers' machines, such as MAC spoofing, which causes incorrect authentication of the hacker and result in unauthorised access to the protected network.

- **Temporary Access before Authentication**

  Some NAC allows temporary access for endpoint devices being remediated, which opened a window for malicious parties to access protected network without being authenticated by NAC.

- **Quarantined Area**

  Instead of attempting to directly bypass the NAC controls to attack the protected network, there is a risk that an attacker intentionally places its endpoint device into the quarantined network. There are more insecure endpoint devices in the isolated network, and it is more possible to exploit and compromise the other endpoint devices which may be reintroduced into the protected network.

- **Hardware or Software Failure**

  NAC software or hardware is subject to accidental malfunction, or deliberate exploitation. The lack of system upgrades and maintenance can lead to hardware or software failure. Without proper monitoring of overall operation status by the IT operations team, such failures may go undetected for a prolonged time period and create great exposures to both external and internal threats that harm universities' information security.

Reference:
http://www.enterasys.com/company/literature/nac-wp.pdf
http://www.blackhat.com/presentations/bh-dc-07/Arkin/Paper/bh-dc-07-Arkin-WP.pdf

III. Exploitations on NAC

Vulnerabilities of NAC can cause malfunctioning of the NAC system or even security breaches of the whole NAC-protected network. Here are some common exploitation examples of NAC solutions in the industry.

Client-side Exploitations

Some of the common exploitations of NAC are originated from the client-side processes, which avoid the element detection, agent installation and guest authentication processes.

- **Device Detection Bypass**

  Device detection is a key feature of a NAC solution to detect new endpoint devices as they are introduced to the network. This is usually achieved by sniffing network traffic at different TCP/IP layers.

  There are ways to bypass the device detection if the detection technique depends on a certain protocol to disclose the existence of an element on the network. The NAC solution is not able to detect the presence of the endpoint device if another protocol can be used.

  An example is bypassing a device detection using a broadcast listener by avoiding the generation of broadcast messages.

- **Agent Installation Bypass**

  Security checking and authentication is performed by the NAC agent on the endpoint device for agent-based NAC solutions.

  A known vulnerability of NAC is to bypass the mandatory installation of the NAC agent by changing the browser's user-agent string. A Windows endpoint device avoids NAC agent installation by masquerading to be a non-Windows machine, which is not compatible with the NAC solution.

  One of the ways to exploit this vulnerability is to change the default parameters of the Windows TCP/IP stack and use a custom HTTPS client, instead of a browser. The user can still connect to the network without running any host-based checks.

- **Guest Authentication Bypass**

  Guest authentication can be performed on an NAC server separated from the internal user NAC server. There is a known vulnerability of existing NAC solutions in the market targeted at guest authentication.

Reference:
http://www.blackhat.com/presentations/bh-dc-07/Arkin/Paper/bh-dc-07-Arkin-WP.pdf
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4430
http://www.securityfocus.com/bid/47092/discuss

III. Exploitations on NAC (cont'd)

Vulnerability exists in the configuration file of the RADIUS authentication software of a guest server system. This vulnerability could result in authentication bypass without requiring a valid username or password.

This misconfiguration may allow an unauthenticated guest user to access the protected network. Successful exploitation of the vulnerability could allow unauthorised users to access the protected network.

Exploitation on Management Traffic

An exploitation has been found targeting at the exchange of information between the NAC servers or network devices. Hackers have exploited vulnerabilities against the confidentiality of information exchanged between NAC management servers and controlled devices.

- **Shared Secret Compromised**

  The NAC management server is the administration server and database which centralises configuration and monitoring of all NAC controlled devices, users, and policies in an NAC solution deployment.

  NAC controlled devices are the gateways between an untrusted and trusted network. They manage the traffic between the untrusted and trusted networks according to the instruction from the NAC management server.

  A vulnerability exists in a popular NAC solution that can allow an attacker to obtain the shared secret that is used between a NAC controlled devices and the NAC management server from error logs that are transmitted over the network.

  Successful exploitation of such vulnerability could enable an attacker to gain complete control of the NAC controlled device remotely over the network.

Reference:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1155
http://secunia.com/advisories/29822

IV. Hardening Steps for NAC

To act upon the known exploitations and possible vulnerabilities of the NAC systems, the university should consider the following hardening steps to enforce a higher security.

Operating System Checks

Section III mentioned an exploitation regarding agent installation bypass. Users might attempt to bypass NAC agent installation by masquerading a Windows machine as a non-Windows machine (e.g., Linux, MacOSX, etc.).

To harden the NAC system against this exploitation, the administrator can define Network Scanning rules on the NAC management server and use network scans to perform additional OS-specific checks, which is able to detect users attempting to masquerade their Windows machines as non-Windows machines. Masqueraded Windows machines would be detected and the NAC agent installation would not be avoided.

Network-based Authentication

Apart from the client-based scans and remediation, some NAC solutions can perform network-based scans on systems and provide web-based remediation.

Network-based authentication can help prevent some of the exploitations originated from the client-side of the NAC solution. The network-based scans can be used for either non-Windows systems or Windows systems.

To use the network scanning with an NAC solution, the plug-ins for the open source vulnerability scanners should be installed and the configuration of the NAC solution should be enabled to work with the vulnerability scanner such as Nessus vulnerability scanner.

Plug-ins for port scanning, obtaining information from Windows systems and operating system identification are useful for preventing the exploitations from the client-side including device detection bypass and agent installation bypass.

Related Article

Detect Users Who Attempt to Bypass Agent Checks for Cisco Clean Access

- **Nessus Plug-ins for Operating System Identification (e.g. plug-in #11936)**
  There are plug-ins available for Nessus vulnerability scanner which is able to identify the operating system of the endpoint device. This can prevent agent installation bypass by identifying exceptions of a Windows machine masquerading as a non-Windows machine or vice versa.

Reference:
http://www.cisco.com/warp/public/707/cisco-sr-20060826-nac.shtml
http://www.cisco.com/warp/public/707/cisco-sa-20110330-nac.shtml

IV. Hardening Steps for NAC (cont'd)

- **Plug-ins for Port Scanning (e.g. nmap.nasl)**
  A list of open ports and listeners can be provided by the use of port-scanning plug-ins. These plug-ins also have the ability to detect which operating system is used on the endpoint device by TCP fingerprinting, which can help prevent device detection bypass and agent installation bypass.

- **Plug-ins to Obtain Information from Windows Systems (e.g. Server Message Block ("SMB")-related plug-ins and plug-in #10859)**
  SMB-related Nessus plug-ins, specifically plug-in #10859 (SMB get host SID), can be enabled to distinguish a Windows device and a non-Windows device. It is shown by only returning values for Windows systems. Hence, if it returns any information, it can be safely concluded that the system runs a Windows operating system.
  Plug-ins that recover information from Windows systems using NETBIOS can also serve the purpose. If a system returns NETBIOS information, it is likely to be a Windows system. Agent installation bypass can be prevented by these plug-ins.

See the article:
(http://www.cisco.com/en/US/products/ps6128/products_tech_note09186a0080545b62.shtml)

NAC Software Maintenance

In all cases, the IT staff should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release.

Vendors usually release free software updates for known vulnerabilities of high risk of exploitation. Before applying the software updates, the IT staff should contact the vendor's technical assistance centre or the contracted maintenance provider to check the software for feature set compatibility and known issues specific to their environment.

Vulnerabilities Awareness

There are both vendor advisories publications and independent organisation references which provide pools of information about latest vulnerabilities and exploitations.

The IT staff should pay attention to the newly discovered vulnerabilities and look for available updates from the vendor to harden the NAC system.

Reference:
http://www.cisco.com/en/US/products/products_security_advisories_listing.html
http://www.cisco.com/en/US/products/ps6128/products_tech_note09186a0080545b62.shtml

V. Summary

The deployment of NAC is more common in the educational sector around the globe. Undoubtedly, NAC is useful to protect the security of the internal network from the endpoint perspective.

Nonetheless, vulnerabilities have been found on different NAC products in the vendor market. Apart from resources spent on the launch of the NAC solution, the administrators and security officers should pay attention to the hardening of the NAC system itself, so as to bring the best outcome to protect the internal network.

The university should also keep updated with the IT security trends to make the best move before the hackers do any harm to the institutional system.

Copyright Statement
All material in this document is, unless otherwise stated, the property of the Joint Universities Computer Centre ("JUCC"). Copyright and other intellectual property laws protect these materials. Reproduction or retransmission of the materials, in whole or in part, in any manner, without the prior written consent of the copyright holder, is a violation of copyright law.

A single copy of the materials available through this document may be made, solely for personal, noncommercial use. Individuals must preserve any copyright or other notices contained in or associated with them. Users may not distribute such copies to others, whether or not in electronic form, whether or not for a charge or other consideration, without prior written consent of the copyright holder of the materials. Contact information for requests for permission to reproduce or distribute materials available through this document are listed below:

copyright@jucc.edu.hk
Joint Universities Computer Centre Limited (JUCC),
Room 223, Run Run Shaw Building,
c/o Computer Centre, The University of Hong Kong,
Pokfulam Road, Hong Kong