

Bypassing Network Access Control Systems





Ofir Arkin, CTO Blackhat USA 2006

ofir.arkin@insightix.com http://www.insightix.com

What this talk is about?

- Introduction to NAC
- The components of a NAC solution
 - _ Pre-Admission
 - Element Detection
 - · Risk Profiling
 - · Quarantine Methods
 - · Managed Vs. Unmanaged Elements
 - Enforcement at L2 Vs. L3
 - _ Post-Admission
 - · Behavior related
- How to bypass NAC solutions
 - Software
 - Hardware

Ofir Arkin

- CTO and Co-Founder, Insightix http://www.insightix.com
- Founder, The Sys-Security Group http://www.sys-security.com
- Computer Security Researcher
 - Infrastructure Discovery
 - ICMP Usage in Scanning
 - Xprobe2 (The Active OS Fingerprinting Tool)
 - VoIP Security
 - Information Warfare
- Member
 - VoIPSA (Board member, Chair security research committee)

insighti

NAC An Introduction

4

NAC - An Introduction

Introduction

- The threat of viruses, worms, information theft and the lack of control of the IT infrastructure lead companies to implement security solutions to control the access to their internal IT networks
- A new breed of software and hardware solutions from a variety of vendors has emerged recently
- All are tasked with one goal controlling the access to a network using different methods and solutions

NAC - An Introduction

Introduction

- Network Access Control (NAC) is a set of technologies and defined processes, which its aim is to control access to the network
- A common criterion for NAC does not exist and therefore the definition of what does a NAC solution should contain varies from one vendor to another
 - Cisco Network Admission Control
 - Microsoft NAP
 - Trusted Computing Group (TCG) Trusted Network Connect (TNC)
 - Other

NAC Capabilities



NAC Capabilities

The Basic Capabilities

- The most essential capabilities any NAC solution must have are the ability to detect a new element connecting to the network, and the ability to verify whether or not it complies with a defined security policy
- If the element does not comply with the defined security policy, the NAC solution must restrict the element's access to the network



NAC Functions

- The following is a list of functions that may, or may not, be included with a vendor's NAC offering:
 - Element detection (must) The ability to detect new elements as they are introduced to the network
 - Authentication The ability to authenticate each user accessing the network no matter where they are authenticating from and/or which device they are using

NAC Capabilities

NAC Functions

- End point security assessment The ability to assess whether a newly introduced network element complies with the security policy. These checks may include the ability to gather knowledge regarding an element's operating system, the presence of an anti virus software, the list of installed patches, etc.
- Remediation The process of quarantine an element not complying with the defined security policy until the issues causing it to be non-compliant are fixed. When quarantined the element is able to access a defined set of remediation servers allowing the user fixing the non-compliant issues
- Enforcement (must) If the element does not comply with the defined security policy, the NAC solution must restrict the element's access to the network.

NAC Capabilities

NAC Functions

- Authorization The ability to verify access by users to network resources complies with an authorization scheme defined in an existing authorization system (such as Active Directory, RADIUS servers, etc.) allowing enforcing identitybased policies
- Post-Admission Protection Is the process of continuously monitoring users, elements and their sessions for suspicious activity (i.e. worms, viruses, malware, etc.). If detected the action taken by a NAC system may vary from isolating the offending system to dropping the session. Post admission protection functions similar to Intrusion Prevention Systems (IPS), and may be used as a means



A List of Methods

Element Detection

Software

- DHCP Proxy
- DHCP Extensions
- Broadcast Listeners
- Switch Integration
- 802.1x
- Hardware
 - In-Line devices
 - Out-of-Band devices

insighti

Element Detection



INS



- Strengths
 - Most organizations use DHCP
 - Easy to deploy

- Weaknesses
 - Must use agent software
 - Agent software is usually restricted to Windows-based operating systems
 - Detection at L3 hence enforcement at L3
 - Elements can infect and/or penetrate other elements on their subnet, and cannot be stopped
 - No actual knowledge regarding the enterprise network
 - No knowledge of what is on the network
 - No knowledge on actual network topology lead existence of other, uncovered venues to access the network
 - Exceptions needs to be manually inputted (if at all)
 - Not a complete solution (does not detect everything)
 - Cannot be extended to include remote users

- Bypass
 - Assigning a static IP Address
 - Elements can infect and/or penetrate other elements on their subnet, and cannot be stopped
 - NAT (Not able to detect masquerading elements behind an allowed elements)
 - Mimicking exceptions

INSI

Element Detection

DHCP Extensions



DHCP Extensions

- Strengths
 - Does not need to replace the existing DHCP supporting infrastructure
- Weaknesses
 - Client-based software must support DHCP extensions (or use specialized client software)

INSI



Broadcast Listeners

Weaknesses

- Must be deployed on each and every subnet
- A lot of moving parts
- Knowledge regarding the enterprise network must be obtained prior to deployment (i.e. which are the different subnets, where are the locations to be deployed, etc.)
- Exceptions are hard to configure (i.e. the only information available is a MAC address and an IP address)
- No knowledge on actual network topology lead existence of other, uncovered venues to access the network
- Cannot be extended to include remote users

Broadcast Listeners

- Bypass
 - Static ARP entries
 - NAT
 - Mimicking exceptions

Switch Integration



Switch Integration

Weaknesses

- Must have prior knowledge regarding the entire list of switches it needs to integrate with (receive information from)
- Depends on the ability to query a switch using SNMP
- Depends on a switch to provide with information regarding a new element operating on the network (SNMP trap)
- Provides poor information regarding elements operating on the network (their MAC address and their IP address)
- Cannot be extended to include remote users

Switch Integration

- Bypass
 - Find and connect to an unmanaged switch
 - Connect two switches through a hub
 - Connect elements through a switch or a hub
 - NAT
 - Mimicking allowed elements ("No Port Security")
 - The same MAC address of an existing element and a different IP address
 - The same MAC address and IP address of an existing element



802.1x







802.1x

- Strengths
 - Can prevent elements to connect to the network even before assigned an IP address
- Weaknesses
 - Difficult manageability
 - All elements on the network must be configured to use 802.1x
 - Legacy networking elements must be upgraded to support 802.1x
 - Not all of the networking elements can support 802.1x
 - Not all of the elements residing on the network are 802.1x capable (can authenticate) (i.e. legacy equipment, AS-400, printers, etc.)
 - The cost for implementing a solution which is based on 802.1x is high (time, resources, infrastructure upgrade, etc.)
 - No knowledge on actual network topology lead existence of other, uncovered venues to access the network



- Bypass
 - Mimicking exceptions (i.e. a printer)
 - NAT





In-Line Devices

- Strengths
- Weaknesses
 - No knowledge on actual network topology lead existence of other, uncovered venues to access the network
 - Deployment must involve a network re-architecture
 - Deployment must be as close as possible to the access layer to be efficient and productive
 - A possible point of failure
 - Deployment is time consuming
 - Extremely Costly
 - Detection at L3 only
 - Infection of other elements on the same subnet and/or switch is possible
 - Some elements may only generate L2 traffic

In-Line Devices

- Bypass
 - Mimicking an element
 - NAT
 - Elements can infect and/or penetrate other elements on the same switch/subnet, and cannot be stopped



Out-of-Band Devices

- Strengths
 - Fast to implement
 - Less moving parts
 - Real-time
 - Detection at L2
- Weaknesses

End Point Security Assessment



Agent-based Solutions End Point Security Assessment

- Agent-based
 - Strengths
 - Provides a wealth of information regarding a host (OS, patches, A/V Signatures)
 - Can provide a full featured solution
 - Weaknesses
 - Usually available for Microsoft Windows operating systems only
 - Management can be a nightmare
 - No awareness of the entire network, not everything is covered

Agent-less Solutions End Point Security Assessment

- Agent-less
 - Strength
 - No need to install additional software
 - Deployment might be fast (depends on the tye of solution)
 - Weaknesses
 - Information regarding a certain element might not always be available (i.e. querying the host to receive a certain property of the host may not unveil the requiered information)

Risks

End Point Security Assessment

- It all breaks down to what is being checked, and does the information is helpful or not?
 - Patches
 - Security related patches (and other patches) are not enrolled into the enterprise as soon as they are available
 - It may take up to a year to enroll a major update of an operating system (i.e. Microsoft Windows XP SP2)
 - Zero day is not blocked
 - The checks performed may be useless. Zero day viruses, worms, and vulnerabilities do not have remediation
 - Understanding the real risk
 - The risk from an element does not only rely on the version of the A/V signature file it may be running (I.e. information theft, unauthorized access, etc.)



Quarantine Methods

Separate Subnet/VLAN

- Separate, non-routable, network address space
- Weaknesses
 - Creates a self infecting quarantine area of restricted elements
 - In the case of DHCP, it is easily bypassed by assigning an element a static IP address (and changing routes)

Quarantine Methods

Switch Integration

- Shutting down a switch port
 - Shutting down a switch port without knowing the topology of the network and without relating to who is connected to that particular switch
 - Creates situations in which legitimate elements may be disconnected from the network
 - Must have a prior knowledge on who are all of the switches which are available on the network
 - Must have SNMP R/W access to all of the switches
 - Unmanaged switches are a big issue
- ACLs
 - ACLs provides enforcement at L3 only. Not all routers are capable of using them. Creates an extra load on a router

Quarantine Methods

- ARP Poisoning
 - Strengths
 - Effective method
 - Performed at L2
 - Does not rely on switch integration
 - Weaknesses
 - · Must be deployed and/or connected to each subnet

Other Problematic Issues



Other Problematic Issues

- Authentication as the only supervision means
 - No supervision on an element's action on the network once it is cleared to operate
- Authorization is not part of NAC
- Enforcement at L2 Vs. at L3
- Managed Vs. Unmanaged Elements
- No knowledge regarding the 'big picture'

Example



Microsoft NAP

Microsoft NAP Components



INS

Microsoft NAP Components Interaction



Microsoft NAP

- Strengths
- Weaknesses



The Required



Questions?

Resources

Microsoft NAP

http://www.microsoft.com/technet/itsolutions/network/nap/default.mspx

Cisco NAC

http://www.cisco.com/en/US/netsol/ns466/networking_solutions_packa ge.html

TCG

https://www.trustedcomputinggroup.org/home

Thank You

