Hacking in Plain Site: Native Service Abuse

Agenda

1. Disclaimer
2. Purpose
3. Network Time Protocol
4. Network Time Protocol Safeguards
5. Address Resolution Protocol (ARP)
6. ARP Safeguards
7. Internet Control Message Protocol
8. ICMP Safeguards
9. Domain Name Service (DNS)
10. DNS Safeguards
11. Summary
12. Contact Us

Disclaimer

This slide deck is for informational and educational purposes only. Any content in this slide deck is intended to assist organizations understand one of many techniques that may be used to undermine the integrity of their information systems and network. The use of the information contained in this slide deck for any purpose other than stated above is prohibited. This slide deck may be redistributed without written consent in its original format without any alterations.

Purpose

Once on a network the abuse of native resources can assist any authorized or unauthorized entity to map the network and exfiltration of data without the installation of any malware. This presentation is designed to provide a basic view of some of the techniques that can be used to abuse native network services and resources. The techniques included in this slide deck only represent basic possibilities an actual techniques may be different or much more complex. Possible remediation to these abuses will be provided as well, but these recommendations are not all inclusive and only constitute one way to deal with these types of abuses.

Network Time Protocol

NTP is a critical resource for most organizations, but it is also a highly valuable tool for anyone that wants to map a network or covertly remove data from the network. Systems are designed to respond to various types of NTP packets. A simple script can be created to sent NTP packets to all of the potential internal IP addresses to determine not only which Ips are associated with active hosts, but which kind of hosts hold those IP addresses base on TTL (time to live) values. There are also a number of places within NTP packets themselves that lend themselves to the insertion of data to be exfiltrated.

Network Time Protocol Safeguards

The most valuable NTP asset to an intruder is the Stratum 1 server. If the Stratum 1 server is compromised NTP abuse can be performed nearly flawlessly and understandably. The highest security for the stratum 1 server would be to host it on its own VM and reset the server nightly using a write-once read-many media source that holds a snapshot of the current configuration settings. To detect NTP abuse from sources other than time servers, organizations should look for endpoints that are transmitting NTP packets to many IP addresses, or endpoints that are sending a sustained stream of NTP packets to a list of non-NTP server IP addresses.

Address Resolution Protocol

Address Resolution Protocol (ARP) is an invaluable resource for anyone that would like to map a network. A flat-file containing a list of non-routable IP addresses can be integrated into a script that will send ARP requests to all possible Ips on the network. The responses will provide a clear mapping of all of the Ips and routers on the network.

ARP Safeguards

Organizations may want to establish technical rules that alert when hosts are sending out arp requests for IP addresses that are not active on the network, arp requests to a large number of IP addresses from a single host, and hosts that have a large ratio of arp traffic compared to other traffic types.

Internet Control Message Protocol

Internet Control Message Protocol (ICMP) has many types that lend themselves to abuse. The most common types that are commonly known to be attacked are type 8 (Echo) and type 13 (Time Stamp). Often, organizations may block one, but not both of these ICMP traffic types. Manual techniques or simple scripts can be leveraged to abuse many types of ICMP traffic to map networks and possibly covertly transmit data. One example of such a covert channel is the LOKI ICMP type 8 covert channel.

ICMP Safeguards

Organizations may want to enable known ICMP abuse rules on security equipment. For organizations that do block ICMP type 8 or 13 at the firewall, other ICMP types should also be disabled when possible. Any hosts that are transmitting unusual ICMP types should be investigated. Any ICMP connections that exceed the standard number of packets or maintain prolonged connection time lengths are a sign of compromise.

Domain Name Service (DNS)

Very few networks can operate without the use of DNS; therefor, a compromise of the DNS server and/or abuse of the DNS protocol has become a foundational technique for intruders of all skill levels. Data can be hidden in domain names, malicious/fictitious DNS records can be created, and rogue DNS can be used to map the network and transport data.

DNS Safeguards

Organizations may want to ensure their DNS Servers are consistently free from compromise and recursive DNS is disabled. Organizations may want to ensure that no unauthorized DNS records exist in their DNS records and that no unauthorized DNS servers are present within the environment. Internal and External DNS servers may need to be logically and physically separated. Any hosts that have unusually long DNS connections, an unusually high number of DNS requests, or are sending DNS packets in incorrect connection order should be investigated. IPS signatures should be used after proper auditing and testing due to false positive potentials, (long DNS name query signatures can cause false positives with sites that stream media).

Summary

There are many ways to exploit native network services with the goal of mapping a network or moving data using manual techniques and simple scripts. Knowing some of the basics will permit security personnel to create simple rules for detecting potentially malicious traffic. Techniques used in the wild may be more complicated by using bounce hosts, spoofing, many origin hosts, or any other number of techniques. However, knowing the basic concepts can assist in the detection of the types of activity described in this slide deck. There are many more services that can be abused, and any packet that permits data padding can be used to move data covertly. To ultimate goal is to know your network, be able to distinguish normal traffic from abnormal, and realize that IPS identifiable malware is usually only used by scrip kiddies.

Connect With Us

1. **LinkedIn**
   https://www.linkedin.com/company/anthko-cyber-security
   (or search for “Anthko”)

2. **Our Website**
   AnthkoCyberSecurity.com