**RIS 420 - Research Assignment #1**

Members Names: Thomas Reid Zuk, Cyril V, Mike Nguyen

Date of submission: March 6th, 2016

**Table of Contents**

**NetBios: 137-139**

**Description:**

NetBios stands for network basic input/output system. NetBios is an API that operates on the Session layer of the OSI model to provide a communication interface between an application and a network. It provides name resolution, datagram and session services across 3 ports; 137, 138 and 139 respectively. Netbios packets can be transported over many different Network layer protocols such as TCP/IP, UDP and IPX. Data using protocol 139, the session service, utilizes TCP, while ports 138 and 137 services utilize UDP. NetBios allows for old systems and applications to operate on a TCP/IP network. It was primarily used for file sharing services.

**Vulnerabilities:**

If not properly mitigated NetBios over TCP/IP can provide large amounts of information on a network such as hosts, services running and network layout. The Session service provided by the NetBios over TCP/IP allows two devices to establish a connection, having this exposed could allow someone to intercept and manipulate these services.

Using a tool called NBSTAT NetBios services on port 139 can reveal large amounts of information about a host. Computer name, remote name, IP Address, list of local NetBios names, contents of the session table and destination session IP addresses.

**Risks and Risk Mitigation:**

An attacker gaining such detailed information about a network and system they could use it to find other vulnerabilities within a network or a host.

To help mitigate the risks the following steps should be taken. Disable null sessions, have strong administration passwords, have strong passwords for file shares if they are in place, disable the Guest account, do not allow root access remotely, do not share system folders such as Windows folders.

**Wireshark Analysis:**

**Microsoft-DS: 445**

**Description:**

Microsoft-ds port 445 stands for Microsoft Directory Services. It is a Microsoft Active Directory service that is required for Active Directory access and authentication. (msdn site) It has been implemented for use since the launch of Windows 2000. Port 445 and Microsoft-ds replaced the usage of port 139 in Netbios service for file sharing and transfer. Port 445 is known as "SMB over IP".

**Vulnerabilities:**

Leaving port 445 open will leave you vulnerable to some worms, such as W32.Deloader and IraqiWorm (aka Iraq\_oil.exe ), [W32.HLLW.Moega](http://www.sarc.com/avcenter/venc/data/w32.hllw.moega.html), [W32.Sasser.Worm](http://www.sarc.com/avcenter/venc/data/w32.sasser.worm.html),[W32.Korgo.AB](http://www.sarc.com/avcenter/venc/data/w32.korgo.ab.html) (09.24.2004), [Backdoor.Rtkit.B](http://www.sarc.com/avcenter/venc/data/backdoor.rtkit.b.html) (10.01.2004), [Trojan.Netdepix.B](http://securityresponse.symantec.com/avcenter/venc/data/trojan.netdepix.b.html) (01.16.2005), as well as the [Windows Null Session Exploit](http://www.brown.edu/Facilities/CIS/CIRT/help/netbiosnull.html).

NetBios worms using port 445 have used the PsExec tool and other tools to replicate by continually scanning networks and the internet for other machines with port 445 open and replicating themselves. A trojan called Lioten is associated with port 445 vulnerabilties.

**Risks and Risk Mitigation:**

Remote control of a Windows machine with port 445is possible. If port 445 is open on a host that host is highly susceptible to an attack and can even have a worm uploaded to the system.

Many ISP have taken risk mitigation of port 445 vulnerabilities into their own hands by blocking any traffic using port 445. Although many ISP's help to prevent attacks associated with port 445 it is not a good idea to leave it solely in their hands. On a router blocking port 445 traffic will help to ensure no traffic uses port 445.

**Wireshark Analysis:**

**DNS: 53**

**Description:**

DNS stands for Domain Name System and is a vital backbone for the functionality of the internet. DNS resolves domain names such as google.com and facebook.com into IP Addresses. All internet devices has a IP address, so DNS is a critical service for all users of the internet, especially non-technical users. Ports above 49152 can be used to receive local DNS and Remote DNS queries and responses to a local or remote DNS server.

All websites, businesses, charities and personal websites alike all user DNS servers in some way or another. Large businesses like Google.com have their own DNS server that both the public and internal operations can use. Most websites use an external DNS provider when they purchase a domain name for their website to manage domain name to IP resolution services. Consumers looking to make personal websites may use a site such as GoDaddy.com to buy a domain, who in turn manages DNS services. Within an organizations network an internal DNS may be used to resolve names of local servers to make services easier to use such file servers.

**Vulnerabilities:**

Due to the nature of how many users browse the internet, through domain names, exploiting DNS services is a large target for attackers. DNS spoofing and DNS cache poisoning are two methods of exploiting DNS services that expose users to many attacks.

**Risks and Risk Mitigation:**

A device connected to a spoofed DNS could have any traffic querying a domain name redirected to a malicious site, traffic intercept (man in the middle) and traffic manipulated.

A good way to prevent a device from being exposed to a DNS spoofing attack is to manually configure the DNS settings of a device to use only approved and properly configured DNS servers such as Google DNS. For organizations with services that use internal domain names a local DNS is required. Configuring machines to use the internal DNS as the primary DNS and then using a trusted DNS for internet queries is a great way to reduce and eliminate DNS spoofing attacks.

**Wireshark Analysis:**

**IRC: 194**

**Description:**

IRC stands for Internet Relay Chat, it is used for exactly what the name implies, for text communication over the internet. There are many web application and client side IRC clients that are popular internet chat rooms for various use and well known for use by hacker groups such as LulzSec and Anonymous. Many IRC networks use alternative ports instead of 194, such as 6667, 6697, and 994. Some web site based IRC networks list they have used the follow ports 6665, 6666, 6667, 8000, 8001, 8002, 6697, 7000, 7070. Some ports are associated with SSL/encrypted traffic, others are associated with plain text IRC networks.

IRC is a text chat service, so any text sent using IRC services could be expose. This could include website links, personal information, stories, and general conversation information. The most common use for IRC by a business is running an IRC service for users. IRC is likely not used for internal business operations as it is unprofessional and very casual in natural. Most businesses would elect to use more secure and professional services like email.

Many browser based IRC services use SSL to encrypt their users traffic. Freenode, a popular IRC client uses 6697, 7000, 7070 ports for SSL traffic.

**Vulnerabilities:**

Some IRC services that are browser based inherit vulnerabilities such as cross site scripting, remote code execution, expose users IP's which have lead to DDOS and DOS attacks.

**Risks and Risk Mitigation:**

Before using and IRC client, both browser based or stand alone make sure it encrypts all traffic to prevent information from being exposed.

**Wireshark Analysis:**

**MySQL: 3306**

**Description:**

MySQL is a relational database system that was created by Oracle in 1995. MySQL has a registered port of 3306, meaning the Internet Assigned Numbers Authority (IANA) has assigned and the port for use with the MySQL port. No other ports are commonly associated with a MySQL data base because it is a registered port and service.

Being a database, MySQL could potentially expose any information stored in a database that uses MySQL. MySQL is one of the top relational database platforms and is used by organizations such as NASA, Verizon, and YouTube. MySQL may be used by any software, website, or web application for its relational database needs. Encrypting MySQL traffic, via a SSL certificate for a website, is highly recommended. Sending unencrypted database traffic exposes any connection to the database to interception of data. This could be anything from price of a product on a eCommerce platform, to credit card information, to usernames and passwords.

**Vulnerabilities:**

Databases are a large target for many attacks, user data ranging from pointless internet forum comments, to names, passwords, addresses and emails can be very valuable for attackers. MySQL has had its fair share of vulnerabilities in the past, and there are currently no known vulnerabilities. The past year, 2015, saw only 1 vulnerability published and fixed, in comparison to 2014 which saw 38 vulnerabilities. SQL injection is a infamous vulnerability with the SQL platform, MySQL has only had 4 known total SQL injection vulnerabilities, all of which have been patched.

**Risks and Risk Mitigation:**

Practices to help prevent any exploitation of MySQL services include never allow 'root' access remotely, never use the 'root' user account for executing queries from a service such as a website. Have strong passwords for all accounts, especially the root account. Keep MySQL services up to date to prevent against any known vulnerabilities that may be discovered.

**Wireshark Analysis:**

**Sources**

http://www.techrepublic.com/blog/it-security/the-problem-with-netbios/

http://www.pcmag.com/encyclopedia/term/47773/netbios

https://technet.microsoft.com/en-us/library/cc940063.aspx

https://wiki.wireshark.org/NetBIOS

https://isc.sans.edu/port.html?port=445

http://www.speedguide.net/port.php?port=445

https://msdn.microsoft.com/en-us/library/dd979226(v=crm.6).aspx

https://tools.ietf.org/html/rfc7194

http://www.speedguide.net/port.php?port=194

https://freenode.net/irc\_servers.shtml

https://technet.microsoft.com/en-us/library/dd197515(v=ws.10).aspx

https://developers.google.com/speed/public-dns/

https://ca.godaddy.com/help/what-is-dns-665

https://www.infoblox.com/sites/infobloxcom/files/resources/infoblox-whitepaper-cybercriminal-guide-exploiting-dns.pdf

http://dev.mysql.com/doc/refman/5.7/en/introduction.html

https://www.mysql.com/customers/