Brian Cullinan
Michael Brooks
12/8/2010

Project 5

Organization Selection:

We have chosen to analyze the IT department in the College of Engineering. This will give us the unique opportunity to discover devices on the NAU network as well as provide valuable feedback to it's administrators.

Security Risk Assessment

Each of the following vulnerabilities has a risk value assigned to it, as well as a plan to fix the vulnerability. This is a very quick assessment, we believe that there are more issues like these that exist in NAU's infrastructure.

SQL Injection

Risk: HIGH
Description: A SQL Injection vulnerability was found on the cefns NAU website using the Sitewatch(https://sitewat.ch) service. This particular vulnerability can allow different levels of access to the system. An attacker will be able to read any data stored in the database or pollute all output from the query, and execute malicious javascript code on clients viewing the page. In some cases it is also be possible for an attacker to plant an executable PHP script in the webroot.
PoC:
This proof of concept will take more than 10 seconds to load, it appears that that sleep(10) is being called multiple times:
http://cefns.nau.edu/Academic/Biology/biograd.php?mode=showus&id="or sleep(10) or 1="
To confirm we set the time to zero, and the page loads quickly:
http://cefns.nau.edu/Academic/Biology/biograd.php?mode=showus&id="or sleep(0) or 1="
Solution: Properly escaping the SQL query will solve this, in php: mysql_escape_string() should be used. Precautions can be taken to limit the impact of this attack, such as putting the SQL server on a different machine, making sure the MySQL user account doesn't have `FILE` privileges and limiting web access to the database. For the future it is vital that all web applications are regally scanned for vulnerabilities. Sitewatch (https://sitewat.ch) is a free service which will make sure that NAU's web application are safe. You can contact mike@sitewat.ch for more information.

Password Protection

Risk: HIGH
Description: Printers and other network assets are lacking an administrative password. This sort of access can be used to collect valuable information such as passwords to other network resources. This sort of vulnerability also puts the network at risk at the mercy of the manufacturers security policy. If there is a vulnerability in the software from the manufacturer, all of the clients are subject to the vulnerability.
Location: http://hp2605-69-322p.cefns.nau.edu
Solution: Set a password for all network devices, or disallow the device to be accessed through public channels. For example only allowing connections to be made from the spooling server.

Subsequent Tasks

The most important tasks have been outlined above. These are additional tasks that should be addressed in order to improve general computer security.

Physical Security

Risk: Medium
Description: The network is very vulnerable to physical security. The wireless connection is encryption free and open to traffic sniffing and man in the middle attacks. The storage closet for all network communications in and out of the building is vulnerable to lock picking, which also makes it vulnerable to man in the middle attacks.
Solution: Upgrade your locking mechanism for the networking closet. Enforce encryption to be used on top of the open wireless connection, even for port 80 and 443!

Workstation Security

Risk: Medium
Description: Workstations use AD for user authentication, however, many workstations are still vulnerable to malware and virus infection. This could provide a gateway for an internal and distributed attacks on the NAU network. Additionally, all of the workstations share the same root password, which makes brute-forcing even easier, since the failed login attempt period won't matter when there are so many computer to work with.
Solutions: Use a password algorithm for each workstations administrator account, or change security policy so that an administrator in AD can be used to manage the machine. Use a 2 factor security policy such as a key fob and administrative password. Do not allow anyone else to have administrative privileges that would allow them to contract malware or viruses. Use a persistent disk to reset a computers configuration every time the computer reboots, and cycle the computers every night.

Security Policy

Risk: HIGH
Description: A full code analysis should be done on all scripts running on the CEFNS website. This analysis should implement a security model such as OWASP, COBIT, or proprietary

models such as SDL from Microsoft. The NAU security policy is not compatible with policies that address application, software, network, or any modern technologies.
Location: http://www5.nau.edu/its/security/formspolicies.aspx
Solution: Define a security policy that is compatible with and enforcing of a more encapsulating security policy such as COBIT.

User Authentication and Access Controls

Risk: Low
Description: Uses active directory for authentication. May have vulnerabilities in default Windows client or Centrify-AD. The enforced passwords require at least 1 capital letter and 1 number, but they are still guessable. The system gives the user only 5 login attempts then 30 minute break.
Solution: Keep software on all servers and clients up to date, and make sure any transactions done over LDAP or AD are over a secure tunnel.

Server Security

Risk: Medium
Description: There are many services running on many different servers. All of these services may be vulnerable, so it is important to keep all software up to date. We have chosen one server in particular to analyze, the server hosting the engineering website. This server is particularly valuable because it will affect many users if it is corrupted. This server may contain a few interesting vulnerabilities. For example, it contains all web data, including configurations files and possibly password files to databases that run in conjunction with scripts. According to the scan, the only tcp ports open on this server 80, 199, and 443, which is good. However there are 5 MySQL servers available to the public. Its possible that these servers could be compromised remotely via a vulnerability in MySQL or by a Brute Force attack.

Network Perimeter Security

Internal NMAP Scan:
https://bjcullinan.com/Share/Documents/College/Computer%20Science/CS%20499%20CS/log.scan
External NMAP Scan:
https://bjcullinan.com/Share/Documents/College/Computer%20Science/CS%20499%20CS/log%20%282%29.scan

By looking at the difference between an NMAP scan done on the local network vs one done over the open Internet we can get an idea of what the firewall rulesets are protecting the perimeter. The firewall rule sets are mostly permissive. However, a remote attacker will not be able to find tcp ports 135, 139 or 445 open. This is likely to be very intentional due to the history of MS-RPC being extremely vulnerable to attack.
Local:
Interesting ports on ator.cefns.nau.edu (134.114.64.32):

Not shown: 1709 filtered ports
PORT STATE SERVICE
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-term-serv
Remote:
Interesting ports on ator.cefns.nau.edu (134.114.64.32):
Not shown: 996 filtered ports
PORT STATE SERVICE
80/tcp open http
3389/tcp open ms-term-serv
49153/tcp open unknown
49154/tcp open unknown

Software Security

There is a SQL Injection vulnerability in http://cefns.nau.edu/. This is unacceptable, because it puts all of NAU at risk. To make sure that this never happens again regular testing of NAU's servers can be done for free using Sitewatch(https://sitewat.ch).

Conclusion

Overall, the survey of the network was very successful. We have discovered many devices, many of which offer intrusion in to the internal network. This sort of intrusion bypasses the top level firewall, and although that firewall is not very restrictive, it can give an attacker unwanted access to more areas of the network.
We have discovered many devices that do not have strong password security, or lacking passwords completely.