IR Team

Vulnerability Assessment

****

Contents

[Executive Summary 5](#_Toc510881111)

[1. Introduction 6](#_Toc510881112)

[1.1 Purpose 6](#_Toc510881113)

[1.2. Scope of this risk assessment 6](#_Toc510881114)

[2. Risk Assessment Approach 6](#_Toc510881115)

[2.1 Participants 6](#_Toc510881116)

[2.2 Techniques Used 7](#_Toc510881117)

[2.3 Risk Model 7](#_Toc510881118)

[3. System Characterization 7](#_Toc510881119)

[3.1 Technology components 8](#_Toc510881120)

[3.2 Users 8](#_Toc510881121)

[3.3 Network Diagram 9](#_Toc510881122)

[9](#_Toc510881123)

[4. Vulnerability List 10](#_Toc510881124)

[5. Conclusion 12](#_Toc510881125)

[6. Risk Assessment Results 13](#_Toc510881126)

**VULNERABILITY ASSESSMENT**

## Executive Summary

(UNIT) performed a vulnerability assessment on x.x.x.0/24 and x.x.x.0/24 network on (DATE). During the assessment, the (UNIT) applied advanced tools, a comprehensive application security knowledge base, and security vulnerability assessment methodologies for the detection of security issues and exposures within the network. The assessment results show that the server on the network as well as the machines on the network are vulnerable for many types of attacks. This vulnerability assessment is an independent review that assesses the network design, enumeration of systems and security vulnerabilities of the systems. The end result of this assessment is a comprehensive easy-to-read actionable report. The following are a summarized scope and results of the risk assessments.

* Server x.x.x.x Concerns
  + No Firewall on server
  + FTP ports opens
  + Server is missing patches
* Domain Controller users and computers Concerns
  + Users on the Domain Controller are not supposed to be there
  + Password need to be more complex
  + Computers can be added by everyone
* Network Concerns
  + Devices on the network that are not supposed to be there
  + Additional network discovered on ###.###.x.x
* Monitoring
  + With approval, Team 3 installed and deployed the Security Onion tool to monitor the network

**DETAILED ASSESSMENT**

# 1. Introduction

## Purpose

The state has activated (UNIT) to assess the situation of the network over threats from a hacktivist group Synonymous.

## 1.2. Scope of this risk assessment

Vulnerability assessment over the x.x.x.0/24 network. This included any systems on that network including Servers, computers and printers.

# 2. Risk Assessment Approach

## 2.1 Participants

|  |  |
| --- | --- |
| **Role** | **Participant** |
| Team Chief | (SM Name) |
| Assistant TC | (SM Name) |
| System Analyst | (SM Name) |
|  | (SM Name) |
| System Administrator | (SM Name) |
|  | (SM Name) |
| Incident Response | (SM Name) |
|  | (SM Name) |
|  | (SM Name) |
| Intel NCO | (SM Name) |
| Forensics | (SM Name) |
|  | (SM Name) |

## 2.2 Techniques Used

|  |  |
| --- | --- |
| **Technique** | **Description** |
| Nmap | Scanned the network and found # systems on the x.x.x.0/24 network |
| Zmap | Displays a network diagram |
| Remote Desktop | Log into other terminals |

## 2.3 Risk Model

(UNIT) used NIST publication SP-800-30 to identify risk, assess the risk and provide recommendations to reduce the risk.

# 

# 3. System Characterization

## 3.1 Technology components

|  |  |
| --- | --- |
| **Component** | **Description** |
| Server | One server x.x.x.x running multiple services |
| Databases |  |
| Operating Systems | Windows and Linux |
| Networks | x.x.x.0/24  x.x.x.0/24  x.x.x.0/24 |
| Interconnections |  |
| Protocols |  |

## 3.2 Users

See Appendix A.

## 3.3 Network Diagram

## 

See Appendix B for detailed discoveries through enumeration methodologies.

# 4. Vulnerability List

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Risk** | **Mitigation** |
| Additional network identified | Vulnerable outbound or inbound network access | Install TACACS+ server to only allow specific users and devices on the network. |
| No firewall running | Vulnerable outbound or inbound network access | Install host based firewall and external proxy/firewall services |
| No updates installed per Windows Update | Attacker may be able to get past known exploits | Run Windows Update |
| Windows Update not configured to get updates | Attacker may be able to get past known exploits | Turn Windows Update on |
| Antivirus is not running | User may download files that can get jeopardize security in the operating system | Install and configure anti-virus |
| Microsoft FTP service is running | Provides another avenue of entry into the domain controller | Disable FTP service |
| DHCP Client Service is running | Domain controllers normally have static IPs | Check if the DHCP service is used and then disable |
| Account is named admin | Frequently used names for administrator accounts are attacked first | Rename admin accounts so they are not so easy to guess |
| Account is named Administrator | Frequently used names for administrator accounts are attacked first | Rename admin accounts so they are not so easy to guess |
| World Wide Web Publishing service is enabled | Provides another avenue of entry into the domain controller. | Disable World Wide Web Publishing Service |
| Minimum password length 7 characters | Passwords are too easy to guess due to a low password length | Change the password length to 14 characters |
| Password must meet complexity requirements - disabled | Passwords are too easy to guess due to not including other characters | Enable this setting |
| Store passwords using reversible encryption | Passwords are not stored one way which means it is easy for an attacker to obtain unencrypted passwords | Disable this setting |
| Count lockout duration - 5 min | This makes it much easier for an attacker to brute force guess passwords at login prompts or other prompts for passwords | Change this to an hour or greater, or set so that somebody else has to unlock the account |
| Account lockout threshold - 5 invalid logins | This makes it much easier for an attacker to brute force guess passwords at login prompts or other prompts for passwords | Change this to 3 |
| Reset account lockout counter - 5 min | This makes it much easier for an attacker to brute force guess passwords at login prompts or other prompts for passwords | Change this to an hour or greater, or set so that somebody else has to unlock the account |

# 5. Conclusion

In conclusion, (UNIT) performed a vulnerability assessment on x.x.x.0/24 and x.x.x.0/24 network on (DATE). (UNIT) vulnerability report shows that there are a number of ways to penetrate the network. (UNIT) believes remediation needs to be done immediately to secure the network from threats such as Synonymous. The risk assessment that follows outlines the (UNIT) recommendation of the highest threats and remediation prioritization.

# 6. Risk Assessment Results

Below are the vulnerabilities we recommend are mitigated with the highest priority.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Vulnerability** | **Risk** | **Possible Impact** | **Likelihood** | **Impact Level** | **Risk Level** |
| 1 | No firewall running | Vulnerable outbound or inbound network access | Allows any computer to try to connect to server. Multiple attacks and people from around the world could gain access to the server | H | H | H |
| 2 | Access this computer from the network - Everyone | The "Everyone" group includes users that are not on the domain | Hacker can gain access to a computer on the domain. From this computer they will be able to access the server and do damage. | H | H | H |
| 3 | Unknown user accounts | Someone has administrator access that shouldn’t. | Administrator has access to do anything on network. Delete users, add malicious code on systems, add back doors, ect. | H | H | H |
| 4 | Unknown Network devices | Devices may be able to launch internal attacks to the network. | Able to log into the Server. Server allows any network device to log remote into the server | H | H | H |
| 5 | Patches are not up to date | Known techniques are available to exploit old patches on both systems and Server | Server may be exploited by a known issue with windows. If attacks happen to Server, could lose access to domain. | M | M | M |
| 6 | Add workstations to domain - Authenticated Users | Normally all authenticated users are not allowed to add computers to the domain. This is so that rogue systems are less likely to be added to the network | If a rogue system is added to the domain, then it will be able to access the server. | M | M | M |
| 7 | Password must meet complexity requirements - disabled | Passwords are too easy to guess due to not including other characters | Hacker can use simple password cracking tools to gain password of administrators. With administrator password, they will be able to do anything they want on the domain. | M | M | M |

**Appendix A.**

|  |  |  |
| --- | --- | --- |
| **Name** | **Type** | **Description** |
| admin | User | CTED |
| Administrator | User | Built-in account for administering the computer/domain |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| Allowed RODC Password Replication Group | Security Group - Domain Local | Members in this group can have their passwords replicated to all read-only domain controllers in the domain |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| battletroll | User | SWW |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| Cert Publishers | Security Group - Domain Local | Members of this group are permitted to publish certificates to the directory |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| Cloneable Domain Controllers | Security Group - Global | Members of this group that are domain controllers may be cloned. |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| Denied RODC Password Replication Group | Security Group - Domain Local | Members in this group cannot have their passwords replicated to any read-only domain controllers in the domain |
| DnsAdmins | Security Group - Domain Local | DNS Administrators Group |
| DnsUpdateProxy | Security Group - Global | DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers). |
| Domain Admins | Security Group - Global | Designated administrators of the domain |
| Domain Computers | Security Group - Global | All workstations and servers joined to the domain |
| Domain Controllers | Security Group - Global | All domain controllers in the domain |
| Domain Guests | Security Group - Global | All domain guests |
| Domain Users | Security Group - Global | All domain users |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| Enterprise Admins | Security Group - Universal | Designated administrators of the enterprise |
| Enterprise Read-only Domain Controllers | Security Group - Universal | Members of this group are Read-Only Domain Controllers in the enterprise |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| Group Policy Creator Owners | Security Group - Global | Members in this group can modify group policy for the domain |
| Guest | User | Built-in account for guest access to the computer/domain |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| Protected Users | Security Group - Global | Members of this group are afforded additional protections against authentication security threats. |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| RAS and IAS Servers | Security Group - Domain Local | Servers in this group can access remote access properties of users |
| (Account Name) | User | User Account |
| Read-only Domain Controllers | Security Group - Global | Members of this group are Read-Only Domain Controllers in the domain |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| Schema Admins | Security Group - Universal | Designated administrators of the schema |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| team-admin | User | DCO Admin account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| (Account Name) | User | User Account |
| **Legend** | | |
| Users that are known and authorized by Network Provider | | |
| Administrator users and groups that need to be reviewed. Network Provider will need to make sure that these user accounts and users in the groups are authorized. | | |
| Users that are not known by Network Provider. Suggest deleting user accounts and finding out who created these accounts. | | |

**Appendix B.**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Match nMap with DNS** |  |  |  |  |  |  |  |  |
| **No match to nMap** |  |  |  |  |  |  |  |  |
| Type / Role | Name | OS | IP Address | DNS Host Name | Landing Host Public | Services | Ports Open |  |
|  | Router |  | x.x.x.x |  |  |  |  |  |
|  |  | Linux | x.x.x.x |  |  | ssh-rpcbind-https-nfs | 22-111-443-2049 |  |
| security onion |  | Linux | x.x.x.x |  |  | ssh | 22 |  |
| domain controller | ADSERVER | Windows | x.x.x.x | ADSERVER |  | ftp-nameserver-domain-http-kerberos-msrpc-netbios-ldap-microsoftds kpasswd5-httprpcepmap-ldapss-globalcat-mswbtserver-pharos-krb524-intermapper-unkown | 21-42-53-80-88-135-139-389-445-593-636-3268-3269-3389-4443-4444-8181-49152-49153-49154-61 |  |
| syslog | ip-x.x.x.x | Linux | x.x.x.x |  |  | ssh | 22 |  |
| kali | Kali | Linux | x.x.x.x |  |  | ssh | 22 |  |
|  |  |  | x.x.x.x | DESKTOP-J6GHTTL |  | ms-wbt-server | 22 |  |
| printer |  |  | x.x.x.x |  |  | ssh-jetdirect | 22-9100 |  |
|  | ip-x.x.x.x | Linux | x.x.x.x |  |  | ssh-telnet-rpcbind-xrdp | 22-23-111-3389 | Telnet should not be used. Passwords are sent in plain text. Passwords could be compromised |
|  | ip-x.x.x.x | Linux | x.x.x.x |  |  | ssh-telnet-rpcbind-xrdp | 22-23-111-3389 | Telnet should not be used. Passwords are sent in plain text. Passwords could be compromised |
|  |  |  | x.x.x.x | DESKTOP-VRCV5VC |  | rdp | 3389 |  |
|  |  |  | x.x.x.x | DESKTOP-C4A6F7Q |  | rdp | 3389 |  |
|  |  |  | x.x.x.x | DESKTOP-2KNPIKJ |  | rdp | 3389 |  |
|  |  |  | x.x.x.x | DESKTOP-V9TCO4U |  | rdp | 3389 |  |
|  |  |  | x.x.x.x | DESKTOP-VMIC8DG |  | rdp | 3389 |  |
|  |  |  | x.x.x.x | DESKTOP-6A4CVTQ |  | rdp | 3389 |  |
|  |  |  | x.x.x.x | DESKTOP-R6G1HHN |  | rdp | 3389 |  |
|  |  |  | x.x.x.x |  |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-F0F2AFF |  | rdp | 3389 |  |
|  |  |  | x.x.x.x | DESKTOP-5IQTLVK |  | msrpc-netbios-microsoftds-mswbtserver | 135-139-445-3389 |  |
|  |  |  | x.x.x.x | DESKTOP-7QD4CUT |  | rdp | 3389 |  |
|  |  |  | x.x.x.x | DESKTOP-EB225O6 |  | rdp | 3389 |  |
|  |  |  | x.x.x.x | DESKTOP-94RHENG |  | rdp | 3389 |  |
|  |  |  | x.x.x.x | DESKTOP-T3L90OC |  | rdp | 3389 |  |
|  | ip- x.x.x.x | Linux | x.x.x.x |  |  | ssh-telnet-rpcbind-xrdp | 22-23-111-3389 | Telnet should not be used. Passwords are sent in plain text. Passwords could be compromised |
|  |  |  | x.x.x.x | DESKTOP-ASHJVR3 |  | rdp | 3389 |  |
|  | ip- x.x.x.x | Linux | x.x.x.x |  |  | ssh-telnet-rpcbind-xrdp | 22-23-111-3389 | Telnet should not be used. Passwords are sent in plain text. Passwords could be compromised |
|  | ip- x.x.x.x | Linux | x.x.x.x |  | 34.208.204.111 | ssh-telnet-rpcbind-xrdp | 22-23-111-3389 | Telnet should not be used. Passwords are sent in plain text. Passwords could be compromised |
|  |  |  | x.x.x.x | DESKTOP-L8D49MN |  |  |  |  |
|  |  | Windows | x.x.x.x | DESKTOP-ARMN11D |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-9UAI5SO |  |  |  |  |
|  | ip-x.x.x.x | Linux | x.x.x.x |  | 54.187.186.33 | ssh-telnet-rpcbind-xrdp | 22-23-111-3389 | Telnet should not be used. Passwords are sent in plain text. Passwords could be compromised |
|  |  |  | x.x.x.x |  |  |  |  |  |
| syslog |  | Linux | x.x.x.x |  |  |  |  |  |
|  | router |  | x.x.x.x |  |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-HQHAGNR |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-0JKN7PP |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-1IOOGBR |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-36GHQGJ |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-4KH53HK |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-9FEU3SF |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-C774PCI |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-EG0B6E4 |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-S3ALQD9 |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-T4RIL0I |  |  |  |  |
|  |  |  | x.x.x.x |  |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-0E9P6G7 |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-1G5PRCJ |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-37HNU77 |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-CV4ABFQ |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-971D46R |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-DBAT6P5 |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-G5EM65C |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-M29OSPG |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-NG0TCSK |  |  |  |  |
|  |  |  | x.x.x.x | DESKTOP-S8PLJT7 |  |  |  |  |