Network Vulnerability Assessment

Abstract

The purpose of this vulnerability assessment is to survey, log, analyze, and identify all alive hosts on the target network. The goal is to identify potential network and host vulnerabilities based operating system (OS) and service (SVC) versioning, availability and configuration. The results found are derived from a combination of active network scanning & passive network traffic analysis.

Scope

While the scope of this vulnerability assessment was illdefined, I have decided to use the following scope. * Network Range : `10.168.27.1/24` * No-Touch Items : `NONE` * Target Range : `10.168.27.1/24` * Assessment Goals : - Survey alive hosts of network - Survey network hosts - Open ports - Services - OS's - Versions - Conduct promiscuous network traffic analysis on target IP range - Identify anomalies in network traffic

Network Scanning - Network Topology

The network is a Class A network (`10.168.27.0/8`), as we can see from the results of running `ip addr sh` on the operators host machine. The target network is a subnet of the Class A network, and is a Class C network `10.168.27.1/24`.

ip-addr-sh

After conducting active tcp syn scans against said network, 6 hosts were identified as alive. One of which is the host machine `10.168.27.1`

nmap-tcp-syn | Network-Topology

Subsequent scans revealed that there did not appear to be any subnetting or network isolation within the target network, and that all but one of the alive hosts appeared to be either servers, end user systems, or the network gateway.

Network Scanning - Intensive

After gaining a basic idea of the network topology, the process of surveying systems began. This included the gathering OS information, scanning open ports, and looking for published services.

```
 nmap -A 10.168.27.10
nmap -A 10.168.27.14
nmap -A 10.168.27.15
nmap -A 10.168.27.20
nmap -A 10.168.27.132
```

nmap-A-10-168-27-10 | nmap-A-10-168-27-14 | nmap-A-10-168-27-15 | nmap-A-10-168-27-20 | nmap-A-10-168-27-132

We can now see a lot more information about the service versions as well as the target OS versions. It appears there is a pretty even split between linux & windows systems. There also appears to be a number of odd services running, as well as insecure services.

Network Scanning - Vulnerability Scanning

Once the more intensive scan results have come in, it is time to move on to identifying possible vulnerabilities. Nmap has a useful scripting engine built into it, that helps us to do this. In order to not reinvent the wheel, try using `vulscan`[3].

Download & Install vulscan

git-clone-vulscan | ln-s-vulscan

Run NMAP service scan with vulscan script

nmap-sV-vulscan-10-168-27-10 | nmap-sV-vulscan-10-168-27-14 | nmap-sV-vulscan-10-168-27-15 | nmap-sV-vulscan-10-168-27-20 | nmap-sV-vulscan-10-168-27-132

> Looking at the included screenshots for the vulscan, you should notice the output has been redirected to files, and then uploaded to an external site. This was done so that the full output could be included with this report. It is being included because of the vast size of each vulnerability scan, which averaged ~10k vulnerabilites per host. Though it should be pointed out that a number of those identified vulnerabilities aren't actually vulnerable.
>
> After running all of these, I went back and built a script to help me better understand the output of the vulnerability scans. The final product can be found here & here, and the output of the scan can be seen below.

!custom-scan-1 !custom-scan-2 !custom-scan-3 !custom-scan-4 !custom-scan-5 !custom-scan-6 !custom-scan-7 !custom-scan-8-udp

Analysis - Vulnerabilities

After conducting the vulnerability scans, and finding such a large number of results, it was decided that only a small representative selection would be addressed here. Overall the identified vulnerabilities were either denial of service oriented or remote code execution oriented. Since a number of the identified vulnerabilities were information disclosure oriented though it is highly likely that an adversary would first leverage exploits against those vulnerabilities to attempt to compromise the credentials for an existing user and then exploit additional vulnerabilities to escalate their privileges once on the machine.

> If you would like to view the entire results of the vulnerability scan the outputs for each scan are stored in the `/src/scans` subdirectory included in the zip file.

Vulnerabilities - Denial of Service

- `10.168.27.15` : `echo`, `chargen`, and `daytime` services
  - The `echo` service is almost like a proxy service, except that it doesn't do any processing on the content. It simply "echoes" whatever data it receives back to the apparent sender. This could potentially pose a security problem, if for instance an attacker decides to try a Denial of Service (DoS) attack, by sending garbage data to the service with a spoofed sender address. [7.1]

    - The above implications also apply to the `chargen`, `time`, and `daytime` services.
    - The only positive thing about this is that it is TCP and not UDP, so they would still need to continuously interact with the service to conduct DoS
- `10.168.27.15` : `qotd` service
    - The Quote of the Day (qotd) service is used to provide a quote to the connecting client. When contacted over UDP, the responses can be 500x the size of the corresponding request and can be used to conduct traffic amplification attacks against other assets, typically in the form of distributed reflected denial of service (DRDoS) attacks. [5.1]
- `10.168.27.15` : `SMB` / `microsoft-ds` service (CVE-2010-0476)[26]
    - SMB Client Response Parsing Vulnerability
    - The SMB client in Microsoft Windows Server 2003 SP2, Vista Gold, SP1, and SP2, and Windows Server 2008 Gold and SP2 allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code or cause a denial of service (memory corruption and reboot) via a crafted SMB transaction response that uses (1) SMBv1 or (2) SMBv2
    - This can allow an attacker to execute arbitrary code or cause a denial of service.
- `10.168.27.15` : `SMB` / `microsoft-ds` service (CVE-2010-0270)[25]
    - SMB Client Transaction Vulnerability
    - The SMB client in Microsoft Windows Server 2008 R2 and Windows 7 does not properly validate fields in SMB transaction responses, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code or cause a denial of service (memory corruption and reboot) via a crafted (1) SMBv1 or (2) SMBv2 response
    - This can allow an attacker to execute arbitrary code or cause a denial of service.
- `10.168.27.15` : `SMB` / `microsoft-ds` service (CVE-2010-0021)[24]
    - SMB Memory Corruption Vulnerability
    - Multiple race conditions in the SMB implementation in the Server service in Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allow remote attackers to cause a denial of service (system hang) via a crafted (1) SMBv1 or (2) SMBv2 Negotiate packet
    - This can allow an attacker to cause a denial of service.
- `10.168.27.15` : `SMB` / `microsoft-ds` service & `netbios` service (CVE-2009-3676)[23]
    - SMB Client Incomplete Response Vulnerability
    - The SMB client in the kernel in Microsoft Windows Server 2008 R2 and Windows 7 allows remote SMB servers and man-in-the-middle attackers to cause a denial of service (infinite loop and system hang) via a (1) SMBv1 or (2) SMBv2 response packet that contains (a) an incorrect length value in a NetBIOS header or (b) an additional length field at the end of this response packet
    - This can allow an attacker to cause a denial of service.
- `10.168.27.15` & `10.168.27.10` : `SMB` / `microsoft-ds` service (CVE-2011-1267)[22]
    - SMB Request Parsing Vulnerability
    - The SMB server in Microsoft Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (system hang) via a crafted (1) SMBv1 or (2) SMBv2 request
    - This can allow an attacker to cause a denial of service.

Vulnerabilities - Information Disclosure

- `10.168.27.10` : `ldap` is available
    - since ldap is not an encrypted service, it provides the potential for an adversary to eaves drop on user accounts being verified, allowing for them to conduct user enumeration operations. The potential also exists that they could inject their own requests or modify the responses to yours. [4.2], [4.1]
- `10.168.27.15` : `ftp` service
    - similarly to the issue specified with ldap above, `ftp` is not encrypted. This allows for an adversary to look at any captured `ftp` traffic in plain text. This could easily include things such as logins and passwords. [2.1]
- `10.168.27.15` : `http` service
    - similarly to the issue specified with ldap above, `http` is not encrypted. This allows for an adversary to look at any captured `http` traffic in plain text. This could easily include things such as logins and passwords. [3.1]
- `10.168.27.15` : `http` / `IIS` service (CVE-2014-4078)[21]
    - IIS Security Feature Bypass Vulnerability
    - The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the "IP Address and Domain Restrictions" list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request

Vulnerabilities - Direct Unauthorized Remote Access

- `10.168.27.15` & `10.168.27.10` : `rpc` service (CVE-2017-8461)[20]
    - Windows RPC Remote Code Execution Vulnerability
    - An attacker who successfully exploited this vulnerability could execute code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. [8.1]
- `10.168.27.15` : `zeus-admin` service
    - This Zeus is a webserver that is no longer in active development/supported status. It is most commonly used as an embedded web server for things like admin consoles, but is vulnerable to simple XSS attacks, so it should not be published on the network. [6.2]
    - it is vulnerable to Cross-site scripting (XSS) attack [6.1]
- `10.168.27.15` : `ftp` anyonymous access
    - the `ftp` service is configured to allow anyonymous access to the `ftp` server. This allows direct and un-authenicated access to the server.

Vulnerabilities - Remote Code Excution (RCE)

- `10.168.27.15` : `SMB` / `microsoft-ds` service (CVE-2011-1268)[19]
    - SMB Response Parsing Vulnerability
    - The SMB client in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote SMB servers to execute arbitrary code via a crafted (1) SMBv1 or (2) SMBv2 response
    - allows attackers to execute arbitrary code on remote servers
- `10.168.27.15` : `SMB` / `microsoft-ds` service (CVE-2011-0661)[18]
    - SMB Transaction Parsing Vulnerability
    - The SMB Server service in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly validate fields in SMB requests, which allows remote attackers to execute arbitrary code via a malformed request in a (1) SMBv1 or (2) SMBv2 packet
    - allows attackers to execute arbitrary code on remote servers
- `10.168.27.15` : `SMB` / `microsoft-ds` service (CVE-2011-0660)[17]
    - SMB Client Response Parsing Vulnerability
    - The SMB client in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote SMB servers to execute arbitrary code via a crafted (1) SMBv1 or (2) SMBv2 response
    - allows attackers to execute arbitrary code on remote servers
- `10.168.27.15` : `SMB` / `microsoft-ds` service (CVE-2010-0477)[16]
    - SMB Client Message Size Vulnerability
    - The SMB client in Microsoft Windows Server 2008 R2 and Windows 7 does not properly handle (1) SMBv1 and (2) SMBv2 response packets, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code via a crafted packet that causes the client to read the entirety of the response, and then improperly interact with the Winsock Kernel (WSK)
    - allows attackers to execute arbitrary code on remote servers

- `10.168.27.15` : `SMB` / `microsoft-ds` service (CVE-2010-0476)[15]
  - SMB Client Response Parsing Vulnerability
  - The SMB client in Microsoft Windows Server 2003 SP2, Vista Gold, SP1, and SP2, and Windows Server 2008 Gold and SP2 allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code or cause a denial of service (memory corruption and reboot) via a crafted SMB transaction response that uses (1) SMBv1 or (2) SMBv2
  - allows attackers to execute arbitrary code on remote servers or cause a denial of service.
- `10.168.27.15`` : SMB / microsoft-ds` service (CVE-2010-0270)[14]
  - SMB Client Transaction Vulnerability
  - The SMB client in Microsoft Windows Server 2008 R2 and Windows 7 does not properly validate fields in SMB transaction responses, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code or cause a denial of service (memory corruption and reboot) via a crafted (1) SMBv1 or (2) SMBv2 response
  - allows attackers to execute arbitrary code on remote servers or cause a denial of service.
- `10.168.27.15` : `SMB` / `microsoft-ds` service (CVE-2010-0269)[13]
  - SMB Client Memory Allocation Vulnerability
  - The SMB client in Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 does not properly allocate memory for SMB responses, which allows remote SMB servers and man-in-the-middle attackers to execute arbitrary code via a crafted (1) SMBv1 or (2) SMBv2 response
  - allows attackers to execute arbitrary code on remote servers.

Vulnerabilities - Privilege Escalation

- `10.168.27.15` & `10.168.27.10` : `rpc` service (CVE-2020-1472)[13]
  - A vulnerability in Microsoft Windows Netlogon Remote Protocol (MS-NRPC), a core authentication component of Active Directory, could allow an unauthenticated attacker with network access to a domain controller to completely compromise all Active Directory identity services. [8.5]
  - an attacker with a foothold on your internal network to essentially become Domain Admin with one click. [8.4]

Analysis - Network Traffic Anomalies & Implications

SEE pcap1.md

Summary

Host	Apparent Type	OS	Svc's	Ports
10.168.27.1	gateway?			
10.168.27.10	server	Windows Server 2012R2	ldap, rpc, netbios, ldaps	135,139,389,445,636,5x{ephemeral ports$_{\text{see appendix}}$}
10.168.27.14		Linux : Kernel v2.6.32	ssh,zeus-admin	22,9090
10.168.27.15	server	Windows 2008R2 or Windows 8.1	echo,discard,daytime,qotd,chargen,ftp,http,rpc,netbios,microsoft-ds	7,9,13,17,19,21,80,135,139,445,3x{ephemeral ports$_{\text{see appendix}}$}
10.168.27.20		Linux : Kernel v2.6.32	ssh	22
10.168.27.132		Linux : Kernel v2.6.32	ssh,zeus-admin	22,9090

Recommendations

1. disable ldap, convert only to ldaps
2. disable echo, daytime, chargen, services
3. disable http, convert to https, also setup a redirect to force any http requests on port 80 to https on port 443.
4. disable zeus-admin as a published service. It may be used as a wholly localhost embedded webserver, but should be avoided if possible.
5. update to windows 2016+ or windows 10.
6. update to a current version of linux, at a minimum the >3.x.x kernel version.

Appendix

1. **Ephemeral Port Range** : 49152–65535 [1]
2. **Microsoft-ds** :
   - Microsoft DS is the name given to port 445 which is used by SMB (Server Message Block). SMB is a network protocol used mainly in Windows networks for sharing ressources (e.g. files or printers) over a network. It can also be used to remotely execute commands. You use it basically every time you use Windows to access a file share, a printer, or any other ressource located on the network. Over time, there were a lot of vulnerabilities found in the SMB implementation of Windows, some of which allowed for execution of arbitrary commands over the network, partly without any authentication. Also very common are weak configurations of SMB in networks that provide an easy attack surface. Together these points lead to SMB being a major attack point. [10.1] [10.2]
3. **Vulscan** : https://github.com/scipag/vulscan
4. **tcpwrapped** : Refers to tcpwrapper, a host-based network access control program on Unix and Linux. When Nmap labels something tcpwrapped, it means that the behavior of the port is consistent with one that is protected by tcpwrapper. Specifically, it means that a full TCP handshake was completed, but the remote host closed the connection without receiving any data. It is essential to note that tcpwrapper protects programs, not ports. This means that a valid (not false-positive) tcpwrapped response indicates a real network service is available, but you are not on the list of hosts allowed to talk with it. [11.1] [11.2] [11.3]

Sources

1. Wikipedia - Ephemeral Ports
    - "The Internet Assigned Numbers Authority (IANA) and RFC 6335 suggests the range 49152–65535 (215 + 214 to 216 − 1) for dynamic or private ports."
    - IANA port number assignments
        - https://www.iana.org/assignments/port-numbers
    - Cotton, M.; Eggert, L.; Touch, J.; Westerlund, M.; Cheshire, S. (August 2011). "Port Number Ranges". Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry. IETF. sec. 6. doi:10.17487/RFC6335. RFC 6335. Retrieved November 14, 2021. "the Dynamic Ports, also known as the Private or Ephemeral Ports, from 49152-65535 (never assigned)"
2. FTP
    1. https://kinsta.com/knowledgebase/ftp-vs-sftp/
    2. https://www.cerberusftp.com/ftps-vs-sftp-understanding-the-difference/
3. HTTP
    1. https://www.hostinger.com/tutorials/http-vs-https
4. LDAP
    1. https://www.veracode.com/security/ldap-injection
    2. https://security.stackexchange.com/questions/60913/is-it-secure-to-be-using-ldap-or-is-ldaps-the-only-secure-option
5. QOTD
    1. https://www.rapid7.com/db/vulnerabilities/qotd-amplification
6. Zeus-Admin
    1. https://www.exploit-db.com/exploits/22000
    2. https://stackoverflow.com/questions/11222222/unknown-service-zeus-admin-running-on-my-server
7. echo service
    1. https://unix.stackexchange.com/questions/170066/enable-echo-service-and-linux-security-loophole-issues
8. RPC (Remote Procedure Call)
    1. https://etutorials.org/Networking/network+security+assessment/Chapter+12.+Assessing+Unix+RPC+Services/12.2+RPC+Service+Vulnerabilities/
    2. https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-8461/
    3. https://www.securityweek.com/ntlm-relay-attack-abuses-windows-rpc-protocol-vulnerability
    4. https://www.isgtech.com/secure-rpc-the-windows-server-vulnerability-you-must-address-before-february-9th/
    5. https://cyber.dhs.gov/ed/20-04/
9. Netbios 1.
10. SMB / Microsoft-ds
    1. https://security.stackexchange.com/questions/229820/microsoft-ds-vulnerability
    2. https://machn1k.wordpress.com/2012/10/29/smb-exploitation-port-445/
11. tcpwrapped
    1. https://www.janbasktraining.com/community/sql-server/how-to-fix-the-tcpwrapped-error-with-nmap-scan
    2. https://security.stackexchange.com/questions/23407/how-to-bypass-tcpwrapped-with-nmap-scan
    3. https://secwiki.org/w/FAQ_tcpwrapped
12. CVE-2020-1472
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472
13. CVE-2010-0269
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0269
14. CVE-2010-0270
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0270
15. CVE-2010-0476
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0476
16. CVE-2010-0477
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0477
17. CVE-2011-0660
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0660
18. CVE-2011-0661
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0661
19. CVE-2011-1268
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1268
20. CVE-2017-8461
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8461
21. CVE-2014-4078
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4078
22. CVE-2011-1267
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1267
23. CVE-2009-3676
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3676
24. CVE-2010-0021
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0021
25. CVE-2010-0270
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0270
26. CVE-2010-0476
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0476