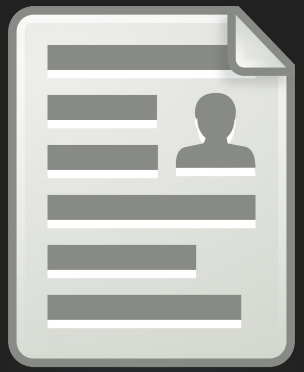
CYB 4510: Cyber Forensics Case Study

Unauthorized Privilege Escalation

Story



- **While performing routine log analysis a system administrator at a small company named CYBERX found evidence of unauthorized privilege escalation.**

- **During this analysis it was discovered that an employee with the username “drphil73” used the shared directory “/usr/local/share/EmployeeFiles” containing employee files to find the password hash for the user “admin32”.**

Story

- **The attacker used the password cracking software “hashcat” to crack the password and then proceeded to login to the account “admin32” which has superuser privileges.**

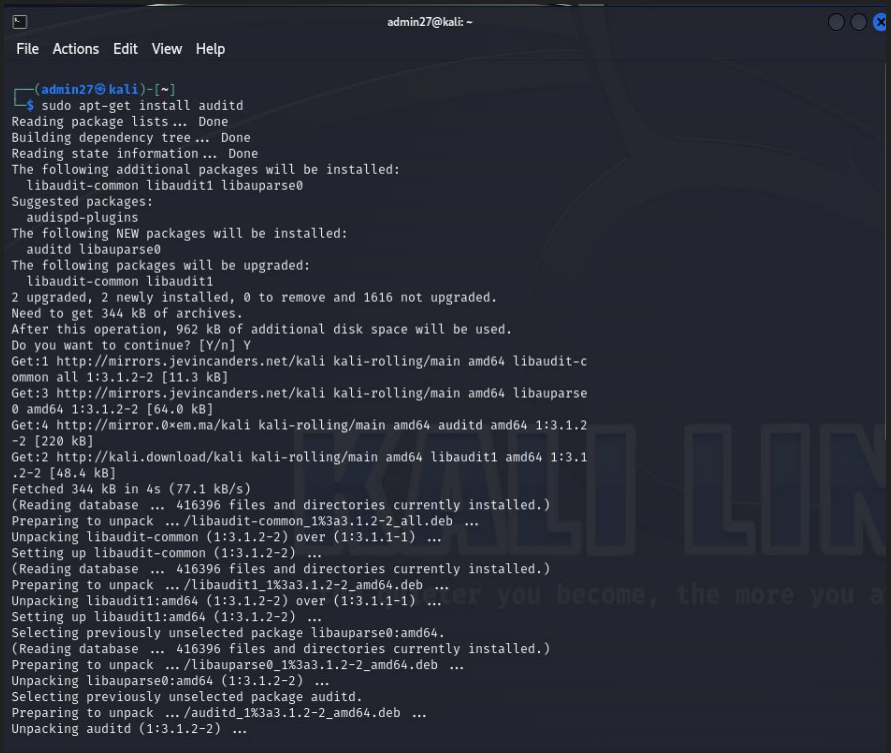
- **The attacker then used their unauthorized access to view sensitive data files containing Wells Fargo company banking information.**

Security Policies

- **At CYBERX the system administrator utilized the “auditd” tool which is part of the Linux Audit system to capture commands inputted in each users shell.**

- **The tool is installed using the following command:**

  $ sudo apt-get install auditd



Security Policies

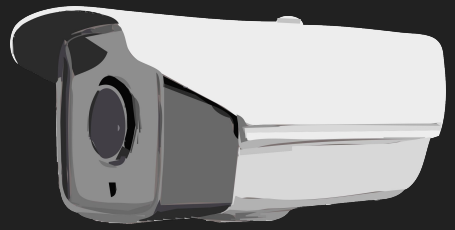
- **Each user is monitored via custom rules added by the system administrator.**
- **To capture all of the shell commands inputted by the user “drphil73”, and in the case of privilege escalation “admin27”, the following commands were used:**

```
┌──(root㉿kali)-[~]
└─# sudo auditctl -a always,exit -F arch=b64 -F euid=drphil73 -S execve -k shell_commands

┌──(root㉿kali)-[~]
└─# sudo auditctl -a always,exit -F arch=b64 -F euid=admin27 -S execve -k shell_commands

┌──(root㉿kali)-[~]
└─# sudo auditctl -l
-a always,exit -F arch=b64 -S execve -F euid=1001 -F key=shell_commands
-a always,exit -F arch=b64 -S execve -F euid=1002 -F key=shell_commands

┌──(root㉿kali)-[~]
└─#
```

Forensic Investigation

- **During routine security audits, the system administrator is required to review and analyze the logs captured by the custom shell command rules for each user.**

Forensic Investigation



- **During this analysis the system administrator runs a keyword search on the logs for each user. If the keyword search has results that may insinuate malicious behavior, an investigation will be conducted.**

- **The results of the routine audit and the commands used for the evidence acquisition for the user “drphil73” is shown in the following slide.**

Evidence Acquisition

```
┌──(root㉿kali)-[~]
└─# sudo ausearch -k shell_commands -ua drphil73 | grep admin27
type=CWD msg=audit(1712623614.160:538111): cwd="/usr/local/share/EmployeeFiles/admin27"
type=CWD msg=audit(1712623617.962:538136): cwd="/usr/local/share/EmployeeFiles/admin27"
type=CWD msg=audit(1712623629.620:538207): cwd="/usr/local/share/EmployeeFiles/admin27"
type=CWD msg=audit(1712623633.200:538228): cwd="/usr/local/share/EmployeeFiles/admin27"
type=CWD msg=audit(1712624646.568:545212): cwd="/usr/local/share/EmployeeFiles/admin27"
type=CWD msg=audit(1712624661.591:545393): cwd="/usr/local/share/EmployeeFiles/admin27"
type=CWD msg=audit(1712624676.032:545578): cwd="/usr/local/share/EmployeeFiles/admin27"
type=CWD msg=audit(1712624676.036:545579): cwd="/usr/local/share/EmployeeFiles/admin27"
type=CWD msg=audit(1712624676.040:545580): cwd="/usr/local/share/EmployeeFiles/admin27"
type=CWD msg=audit(1712624685.843:545701): cwd="/home/admin27/PersonalInfo"
type=CWD msg=audit(1712624692.844:545786): cwd="/home/admin27/PersonalInfo"

┌──(root㉿kali)-[~]
└─# sudo ausearch -k shell_commands -ua drphil73 | grep nano
type=PATH msg=audit(1712623617.962:538136): item=1 name="/usr/bin/nano" inode=1184426 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1712623617.962:538136): item=0 name="/usr/bin/nano" inode=1184426 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=EXECVE msg=audit(1712623617.962:538136): argc=2 a0="nano" a1="pass.txt"
type=SYSCALL msg=audit(1712623617.962:538136): arch=c000003e syscall=59 success=yes exit=0 a0=5556299e86d0 a1=5556299fdf70 a2=555629a511a0 a3=321031140ab1c50f items=3 ppid=178610 pid=179667 auid=1001 uid=10
01 gid=1001 euid=1001 suid=1001 fsuid=1001 egid=1001 sgid=1001 fsgid=1001 tty=pts1 ses=16 comm="nano" exe="/usr/bin/nano" subj=unconfined key="shell_commands"
type=PATH msg=audit(1712624646.568:545212): item=1 name="/usr/bin/nano" inode=1184426 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1712624646.568:545212): item=0 name="/usr/bin/nano" inode=1184426 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=EXECVE msg=audit(1712624646.568:545212): argc=2 a0="nano" a1="pass.txt"
type=SYSCALL msg=audit(1712624646.568:545212): arch=c000003e syscall=59 success=yes exit=0 a0=55be2ad18dc0 a1=55be2aca4e50 a2=55be2ad174a0 a3=c033a0bca60a50b5 items=3 ppid=204243 pid=205094 auid=1001 uid=10
01 gid=1001 euid=1001 suid=1001 fsuid=1001 egid=1001 sgid=1001 fsgid=1001 tty=pts1 ses=16 comm="nano" exe="/usr/bin/nano" subj=unconfined key="shell_commands"
type=PATH msg=audit(1712624692.844:545786): item=1 name="/usr/bin/nano" inode=1184426 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1712624692.844:545786): item=0 name="/usr/bin/nano" inode=1184426 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=EXECVE msg=audit(1712624692.844:545786): argc=2 a0="nano" a1="WellsFargo.txt"
type=SYSCALL msg=audit(1712624692.844:545786): arch=c000003e syscall=59 success=yes exit=0 a0=55a92df96950 a1=55a92de9b030 a2=55a92dea1c40 a3=8db0b12298890d9b items=3 ppid=205817 pid=206229 auid=1001 uid=10
02 gid=1002 euid=1002 suid=1002 fsuid=1002 egid=1002 sgid=1002 fsgid=1002 tty=pts1 ses=16 comm="nano" exe="/usr/bin/nano" subj=unconfined key="shell_commands"

┌──(root㉿kali)-[~]
└─# sudo ausearch -k shell_commands -ua drphil73 | grep hashcat
type=PATH msg=audit(1712623629.620:538207): item=1 name="/usr/bin/hashcat" inode=1239977 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1712623629.620:538207): item=0 name="/usr/bin/hashcat" inode=1239977 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=EXECVE msg=audit(1712623629.620:538207): argc=5 a0="hashcat" a1="-m" a2="0" a3="pass.txt" a4="/home/drphil73/Downloads/rockyou.txt"
type=SYSCALL msg=audit(1712623629.620:538207): arch=c000003e syscall=59 success=yes exit=0 a0=555629a531a0 a1=5556299fa8c0 a2=555629a511a0 a3=321031140ab1c50f items=3 ppid=178610 pid=179943 auid=1001 uid=10
01 gid=1001 euid=1001 suid=1001 fsuid=1001 egid=1001 sgid=1001 fsgid=1001 tty=pts1 ses=16 comm="hashcat" exe="/usr/bin/hashcat" subj=unconfined key="shell_commands"
type=PATH msg=audit(1712623633.200:538228): item=1 name="/usr/bin/hashcat" inode=1239977 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1712623633.200:538228): item=0 name="/usr/bin/hashcat" inode=1239977 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=EXECVE msg=audit(1712623633.200:538228): argc=6 a0="hashcat" a1="-m" a2="0" a3="pass.txt" a4="/home/drphil73/Downloads/rockyou.txt" a5="--show"
type=SYSCALL msg=audit(1712623633.200:538228): arch=c000003e syscall=59 success=yes exit=0 a0=555629a534f0 a1=5556299fa8c0 a2=555629a511a0 a3=321031140ab1c50f items=3 ppid=178610 pid=180032 auid=1001 uid=10
01 gid=1001 euid=1001 suid=1001 fsuid=1001 egid=1001 sgid=1001 fsgid=1001 tty=pts1 ses=16 comm="hashcat" exe="/usr/bin/hashcat" subj=unconfined key="shell_commands"
type=PATH msg=audit(1712624661.591:545393): item=1 name="/usr/bin/hashcat" inode=1239977 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1712624661.591:545393): item=0 name="/usr/bin/hashcat" inode=1239977 dev=08:01 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=EXECVE msg=audit(1712624661.591:545393): argc=6 a0="hashcat" a1="-m" a2="0" a3="pass.txt" a4="/home/drphil73/Downloads/rockyou.txt" a5="--show"
type=SYSCALL msg=audit(1712624661.591:545393): arch=c000003e syscall=59 success=yes exit=0 a0=55be2ad199f0 a1=55be2accaf30 a2=55be2ad174a0 a3=c033a0bca60a50b5 items=3 ppid=204243 pid=205455 auid=1001 uid=10
```

Analysis

- **Looking closely at the evidence we can begin to piece the commands executed by “drphil73” together and see that the user gained unauthorized access to the user account “admin27”.**

Analysis

type=CWD msg=audit(1712623614.160:538111): cwd="/usr/local/share/EmployeeFiles/admin27"

- **This line shows that the user “drphil73” navigated to the directory "/usr/local/share/EmployeeFiles/admin27” given that it was his cwd (current working directory).**

Analysis

```
type=EXECVE msg=audit(1712624646.568:545212): argc=2 a0="nano" a1="pass.txt"
```

- **This line shows that the user “drphil73” used the text editor nano to examine and identify the password hash for the user “admin27”.**

Analysis

```
type=EXECVE msg=audit(1712623629.620:538207): argc=5 a0="hashcat" a1="-m" a2="0"
a3="pass.txt" a4="/home/drphil73/Downloads/rockyou.txt"
```

- **This line shows that the user “drphil73” used the password cracking software hashcat with the password hash of the user “admin27” as the 3rd argument and the wordlist rockyou.txt as the 4th argument.**

Analysis

```
type=CWD msg=audit(1712624685.843:545701): cwd="/home/admin27/PersonalInfo"
```

- **This line shows that the user “drphil73” was successful in cracking the password of the user “admin27” and gaining unauthorized access to that user’s account. This shows that the attacker navigated to the “PersonalInfo” directory of the user “admin27”.**

Analysis

```
type=EXECVE msg=audit(1712624692.844:545786): argc=2 a0="nano" a1="WellsFargo.txt"
```

- **This line shows that the user “drphil73” used the text editor nano to read the contents of the file “WellsFargo.txt” which contained sensitive data regarding the banking info for the company only viewable by the system administrator “admin27” with superuser privileges.**

Conclusion

- **Therefore the analysis shows that the attacker was able to use the shared directory “/usr/local/share/EmployeeFiles” used by the company to store employee data to obtain the password hash for the system administrator “admin27”.**

Conclusion

- **The attacker was then able to crack the password hash using the software hashcat and the wordlist “rockyou.txt”**
- **The attacker then used the credentials to escalate his privileges and gain unauthorized access to the user “admin27” which allowed him to view the file “WellsFargo.txt” which contained sensitive company banking information.**