NCAE_Hunting_Guide

Hunting Guide

Introduction

Keeping bad guys out is as important as getting your infrastructure up. Servers don't help when they get knocked offline. To help you track down those pesky Red Teamers, use the information below as reference for some areas you may find anomolies.

(HINT: Often, IT and SecOPs teams work together to keep services functioning and secure. If your infrastructure is in good shape, a dedicated 'analyst' might help you in the long run)

Top Tips and Tricks

Protect

```
#Check all services
service --status-all

#Service information
ps -aux

#Check for start jobs
ls /etc/init/*.conf

#Backup existing firewall (iptables) rules
iptables-save > iptables_rules.out

#Modify export if needed
vi iptables_rules.out

#Restore iptables rules
iptables-restore < iptables_rules.out

#List rules
iptables -L

#Change password
passwd
```

Detect

```
#*NETWORK*
#Look at live network traffic tcpdump
#Save PCAP to remote host (Kali?)
tcpdump -w - | ssh <remote ip address here> -p <port> "cat - >
/tmp/<filename>.pcap"

#Monitor for new tcp connections (netstat has to be installed, yum install
net-tools)
netstat -ac 5 | grep tcp

#Monitor traffic remotely (from kali?)
ssh <user>@<remote ip of host to monitor> tcpdump -i any -U -s -) -w - 'not
host <kali ip>'

#*LOGS* (look below for common linux logs) #Look at log
cat /path/to/log

#Look at log in real time
tail -f /path/to/log

#Look for keyword in log
grep -i "<keyword>" /path/to/log

#Look for sudo activity
grep -i sudo /var/log/auth.log
```

Triage

```
#View logged in users
w

#Check remote login activity
lastlog

#Check failed logins
faillog -a

#View local accounts and groups
cat /etc/passwd
cat /etc/shadow
cat /etc/group
cat /etc/sudoers

#Show root accounts
awk -F: '($3 == "0") {print}' /etc/passwd

#Active network connections
netstat -antup

#View routes
route

#List processes listening on ports
lsof -i

#Check croncrontab -l
cat /etc/crontab
ls /etc/cron.*

#Stop a process (hint, use a command above for checking process info)
kill <process pid>
kill -9 -I <process name>

#Remove execution from a process (or just delete it)
chmod -x /path/to/malicious/file
```

```
#Move the malicious file to analyze it for potential attacker information
mv /path/to/malicious/file ~/quarantine
strings ~/quarantine/<malicious_file>
```

Last Modified: 2/12/23 (spoons)