# APT1 Recon BAT

@echo off

ipconfig /all>>"C:WINNT\Debug\1.txt"

net start>>"C:\WINNT\Debug\1.txt"

tasklist /v>>"C:\WINNT\Debug\1.txt"

net user >>"C:\WINNT\Debug\1.txt"

net localgroup administrators>>"C:\WINNT\Debug\1.txt"

netstat -ano>>"C:\WINNT\Debug\1.txt"

net use>>"C:\WINNT\Debug\1.txt"

net view>>"C:\WINNT\Debug\1.txt"

net view /domain>>"C:\WINNT\Debug\1.txt"

net group /domain>>"C:\WINNT\Debug\1.txt"

net group "domain users" /domain>>"C:\WINNT\Debug\1.txt"

net group "domain admins" /domain>>"C:\WINNT\Debug\1.txt"

net group "domain controllers" /domain>>"C:\WINNT\Debug\1.txt"

net group "exchange domain servers" /domain>>"C:\WINNT\Debug\1.txt"

net group "exchange servers" /domain>>"C:\WINNT\Debug\1.txt"

net group "domain computers" /domain>>"C:\WINNT\Debug\1.txt"

# Sample Automation Script: Get-ACL

Get-ChildItem c:\data -recurse | Get-ACL | fl > acl\_baseline.txt

Get-ChildItem c:\data -recurse > Get-ACL | fl > acl\_current.txt

Compare-object (get-content acl\_baseline.txt) (get-content acl\_current.txt) > results.txt

sendEmail -f user@domain.com

 -t user2@domain.com

 -u "ACL Change Alert"

 -m "Please see attached alert."

 -s mail.domain.com:25

 -a results.txt

# Sample Automation Script: OpenVAS

(to detect wireless access points connected to the wired network)

OpenVAS-Client -c /home/auditor/openvas.rc -T html -qx 127.0.0.1 9390 /home/auditor/results.html

sendEmail -f user@domain.com

 -t user2@domain.com

 -u "Wireless Device Alert"

 -m "Please see attached alert."

 -s mail.domain.com: 25

 -a /home/auditor/results.html

# Sample Automation Script: Get-WMIObject

Get-WMIObject Win32\_Useraccount | Select Name, SID > user\_baseline.txt

Get-WMIObject Win32\_Useraccount | Select Name, SID > user\_current.txt

Compare-Object (Get-Content user\_baseline.txt) (Get-Content user\_current.txt) > results.txt

sendEmail -f user@domain.com

 -t user2@domain.com

 -u "User Change Alert"

 -m "Please see attached alert."

 -s mail.domain.com:25

 -a results.txt