BuildReviews

Build Review Cheatsheet

[+] Main tasks:

Any third party installed software and all associated versions.
Password policy applied locally via net accounts commands.
Domain policy applied, including domain password policy.
Logging settings.
Running services and unquoted service paths.
Permissions set on services.
List of patches and hotfixes installed.
Efficacy of AV solutions. May require import of a benign Eicar test file.
USB policy and removable media access (including firewire, CD etc).
Disk encryption (if relevant)
BIOS passwords set.
Proxy settings (if relevant).
Nessus Scan (With Credentials).

[+] Windows Hosts:

[+] Server Roles
[+] Server Manager
[+] System Properties
[+] Default Domain Policy
[+] Global Domain Policy

[+] Net accounts/Users/groups/Administrators
[+] IPConfig/Routing

[+] Installed Programs
[+] Installed System Updates
[+] AV Version/Definition Dates
[+] Check Computer folders

[+] Firewall Configuration
[+] Audit Policy
[+] Password/Lockout Policy
[+] Security Policy
[+] User Rights Policy

[+] Lanman Parameters (HKLM - System - Current Control - Services - LanmanServer - Parameters)
[+] LSA (HKLM - System - Current Control - Control - LSA)
[+] MSV (HKLM - System - Current Control - Control - LSA - MSV1_0)

systeminfo command

BIOS password
boot to usb
file system
- encrypted?
- grab /Windows/System32/config/SAM SECURITY SYSTEM
- put C:\Program.exe (eg calc)

Control Panel
- Windows Firewall
   - enabled
   - editable
   - logs
- System Info
- Windows Update

Anti-Virus
- config
- logs
- version
- dates
- EICAR

```
cmd.exe
script.cmd
- ipconfig /all
- netstat
- net accounts
- net accounts /domain (review password policy)
- net user hacker Password@1 /add
- regedit
- ping
- sched
- tracert
- net use \\IP address_or_host name\ipc$ "" /user:""  # null session
- net use
- net view
- net start ■
- tasklist

mount usb
usb autostart

copy over files
- nc
- enum
- nmap
- DIRE
- EICAR

# SAM files in backtrack
/Windows/System32/config/SAM SECURITY SYSTEM

# mounting on desktop review
# mount <target> <mydir>
# sda1 = client hdd, sdb2 = my usb part 2
# mkdir /mnt/client-hdd
# mount /dev/sda1 /mnt/client-hdd
# mkdir /mnt/win-usb
# mount /dev/sdb2 /mnt/win-usb

hosts file C:\Windows\System32\drivers\etc\hosts.txt

SYSVOL GPO preference item, check for obscured passwords in xml
http://blogs.technet.com/b/grouppolicy/archive/2008/08/04/passwords-in-group-policy-preferences.aspx

The history file is readable by any authenticated user, as shown below:
C:\Users\All Users\Microsoft\Group Policy\History\{A1C0C41B-D2F8-401B-A5D1-437DA197A809}\Machine\Preferences\Groups\Gro
The same Group Policy Preference XML configuration file is also accessible via the following UNC path on the Domain Con
\\Domain_Controller\sysvol\Domain_Name\Policies\{A1C0C41B-D2F8-401B-A5D1-437DA197A809}\Machine\Preferences\Groups\Group


[+] Unix Based Hosts:

hostname
whoami
uname -a
cat /etc/lsb-release
dmesg | grep Linux
cat /etc/passwd
cat /etc/sudoers
netstat -antup
ps -aux
ps aux | grep root
crontab -l
/sbin/ifconfig -a
iptables -L
arp -e
cat ~/.bash_history
cat ~/.ssh/authorized_keys
mount

- Check installed applications
- Check installed compilers/interpreters
```