Lockdown Black Team

DEPLOYMENT PROCEDURE

We deploy EVERYTHING using ansible. For previous deployments refer to UBNetDef git. Example deployment repo:

https://github.com/ubnetdef/Lockdown-v6-Deployment

To make the deployment with Ansible possible we need to ensure that requirements for deployment templates are satisfied. Please check the TEMPLATE REQUIREMENTS section for more info

Black Team Should manually log in to EVERY computer to test passwords, and ensure that the applications are cached, and VMs are fast when competitors are using them.

TEMPLATE REQUIREMENTS

- All:
  - Copy Paste Enabled
  - Graphics to support Full HD/Automatic Graphics Detection
  - Ensure time Synchronized
  - Potentially disable DHCP
  - Make sure the best NIC type is attached “vmxnet3” → “vmxnet2” → etc
- Linux:
  - VMware tools(Not open-vm-tools)
  - Depending on how old ansible is, try to install python2 and python3
  - SSH server (installed, enabled, running)
  - Decrease swappiness to 10
  - Python2 and python3 installed (less headache if you are using ansible)
  - Ubuntu-specific:
    - Ensure networkd is a renderer
    - Install resolvconf to configure DNS on 18.*
  - Fedora specific:
    - Depending on implementation look into installing network-scripts
    - Install libselinux-python
  - Ensure Release of child OSes match supported OS: https://kb.vmware.com/s/article/1005870
- Windows:
  - VMWare tools
  - Enable WinRM: https://docs.ansible.com/ansible/latest/user_guide/windows_setup.html#winrm-setup
  - From the link above, please also run Winrm memory Hotfix, and dotnet upgrade
  - Windows 7 and below: ensure to run following PowerShell script https://github.com/ansible/ansible/issues/52316#issuecomment-473639984 (More info: https://docs.ansible.com/ansible/latest/user_guide/windows_winrm.html#tls-1-2-support)
  - Ensure that Windows Remote Management service is started Automatically
  - Enable Ping via Firewall (Allow ICMP Packets)

    - Disable/Uninstall Windows Defender (Registry/GPO)
    - Disable Windows Updates (Registry/GPO/Services)
    - Make sure ansible deployment has a unique AD_Name for every host, to avoid hostname collisions
    - Allow remote connections to the computer, under “Remote” tab of System Properties
    - Ensure Sleep is disabled
    - Try to Debloat as much as possible: https://github.com/Sycnex/Windows10Debloater (Might not worth it)
    - Sometimes windows may start randomly shutting down. In which case please look into the following
    - Use High-performance Battery Profile
    - Windows 10 Enterprise specific:
        - Make sure when Template is deployed, it has an Ethernet Access. If it doesn't have one, it will reboot endlessly: https://superuser.com/questions/933754/why-does-windows-10-shut-down-hourly-with-initiated-power-off-on-behalf-of-nt-a
- Pfsense:
    - Ensure VMware Guest tools installed
    - Ensure to install https://github.com/ubnetdef/Lockdown-v6-Deployment/blob/master/roles/pfsense_deploy_provision/files/provision.php on PFsense so that scripts become runnable.

Post Deployment Checklist

- Ensure you clean up the history of all applications/shells
- Ensure you take a snapshot of the entire infrastructure after deploying your malware
- Manually login to every VM after the red team is done pre-staging. This ensures that everything is still operational, and in addition, it loads a lot of things from disk to memory, which ensures a smoother experience at the start of the competition.
- If the performance of VMs is very slow, try to lower the number of snapshots or use the snapshots that were created are no longer than a day before the competition.

TEMPLATE LOCATIONS

General Templates are located under Templates/Competitions/Lockdown Templates/Base

Every template for past competitions will be located under General Templates are located under Templates/Competitions/Lockdown Templates/ in their own appropriate folders

RED TEAM REQUESTS

Sometimes Red Team might request the Black Team to deploy/prebake something for them. In that case please ensure that Black Team Lead and Red Team Lead Figure out everything that has to be done prior to deployment

Things that are typically requested:

- Windows:
  - Dotnet https://dotnet.microsoft.com/download
  - Python executables
- C2 Servers

Naming Conventions

Virtual Machines:

- Team%02d-AD
- Team%02d-Client{X}
- Team%02d-DB
- Team%02d-WEB
- Team%02d-FTP
- Team%02d-Router
- Team%02d-GitLab

Examples: Team06-Client1, Team10-AD

Folders

- Team%02d

Examples: Team01, Team12

Templates:

- Lockdownv{X}_MachineName

Examples: Lockdownv6_Router, Lockdownv6_AD

Users:

- lockdown-teamX

Examples: lockdown-team13

Note: %02d just represents a padded 0.

Aibek to Aibek: PLEASE FIX ANSIBLE RELATIVE PATHING