

Sysmon & SplunkForwarder established

A screenshot of a computer

Description automatically generated

Splunk Endpoint established

A screenshot of a computer

Description automatically generated

Splunk Endpoint event reporting receiving events

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Set up Sysmon and splunk on both devices, and configure endpoint reporting to receive reports

A screenshot of a computer

Description automatically generated

DC1 set to Active Directory Manager, user accounts added for IT and HR departments, and users.

A screenshot of a computer

Description automatically generatedTarget computer users assigned, RDP established, connection to Active Directory Server established.  
A screenshot of a computer

Description automatically generated  
A screenshot of a computer

Description automatically generated

Kali Linux Machine, Password list established  
A screenshot of a computer program

Description automatically generated

A screenshot of a computer screen

Description automatically generated

Crowbar installed  
A screen shot of a computer code

Description automatically generated

Target located, assumed used nmap for enumeration, IP of kali machine changed to match the same 192.168.10.0/24 Network as target for ease. Crowbar launched against target machine, password found.

A screenshot of a computer

Description automatically generated

Event logged and located on Splunk server, multiple counts of failed login attempts identified, code 4625 ~20 attempts all at the same time, indicating brute force attempt.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Kali virtual machine identified on event code 4624, successful login. IP address logged.

A screenshot of a computer program

Description automatically generated

Installed Git

A screenshot of a computer

Description automatically generated

Git not recognized, added to path

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Git resolved, Atomic Redteam Files downloaded, Firewall exclusion on C:/ drive prevented antivirus from interfering

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Installing atomic red team

A screenshot of a computer program

Description automatically generated

After Atomic Red Team is installed, Invoke-AtomicTest T1136.001 to create a New Local Account ‘NewLocalUser’

A screen shot of a computer program

Description automatically generated

Event Captured in Splunk

A screenshot of a computer

Description automatically generated

Attempt additional attacks on target machine: T1059.001, PowerShell attacks

A screenshot of a computer program

Description automatically generated

Windows defender detected and blocked multiple threats

A screenshot of a phone

Description automatically generated

A screenshot of a computer error message

Description automatically generated

Events logged and detected on Splunk

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated