

Overview

Today you will use Atomic Red Team to simulate a known TTP mapped to MITRE ATT&CK on a local test VM, then analyze the results and implement countermeasures

Part 1: Staging

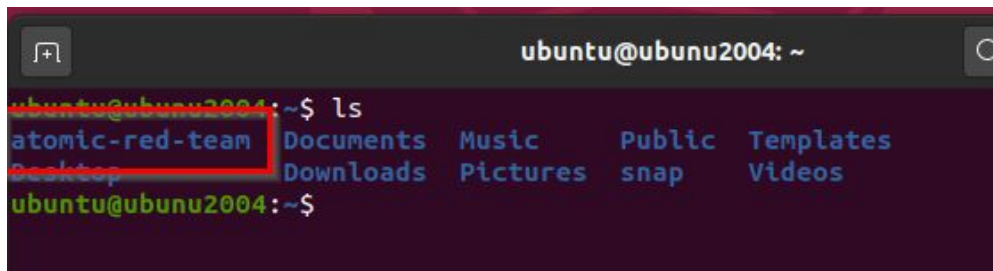
Familiarize yourself with the MITRE ATT&CK database as well as the Atomic Red Team Github Repo.

Step 1- Git clone or download as an archive the Atomic Red Team Github Repo to your local system.

Step 2- Identify one TTP from MITRE ATT&CK that was utilized by an APT.

Step 3- Cross-reference the Atomic Red Team Github Repo and see if you can find specific attack techniques.

Gitclone installed

A terminal window titled 'ubuntu@ubunu2004: ~' with a search icon in the top right. The command 'ls' has been executed, displaying a directory listing. The entry 'atomic-red-team' is highlighted with a red rectangular box. The listing includes 'atomic-red-team', 'Desktop', 'Downloads', 'Documents', 'Music', 'Pictures', 'Public', 'snap', 'Templates', and 'Videos'.

```
ubuntu@ubunu2004: ~  
ubuntu@ubunu2004:~$ ls  
atomic-red-team  Documents  Music      Public    Templates  
Desktop         Downloads  Pictures   snap      Videos  
ubuntu@ubunu2004:~$
```

ATT&CK [Tactic link](#)

The attack that was associated with the Target Corp. breach was alleged to be caused by a password sniffing malware. The tactic that parallels with the Target APT is Enterprise Network Sniffing Tactic name Stolen Pencil id T1040. A stolen pencil is a tool used to sniff networks for passwords. The specific tool that was linked to the Target attack was named Citadel based on Zeus.

Part 2: Atomic Testing Cycle [Atomic test link](#)

Step 1- Complete the three-step Atomic Testing

- Step 1: Execute the Test
- Step 2: Collect Evidence
- Step 3: Develop Detection

Step 2- Review ATT&CK threat mitigation documentation.

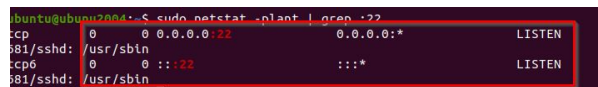
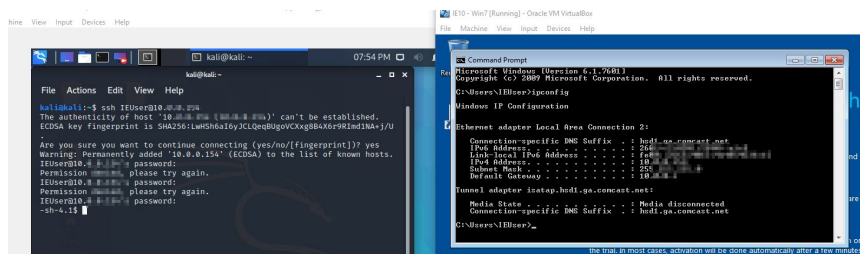
Step 3- Based upon your findings, recommend improvements to system defenses.

The Atomic test that is connected is the packet capture attack, this allows adversaries to sniff the network and capture packets including credential information that is passed over the network.

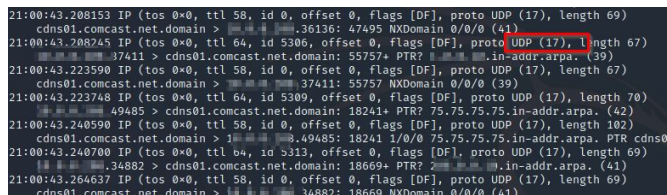
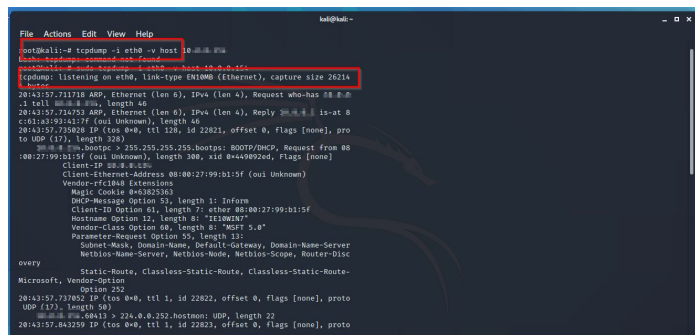
My test consisted of a Linux pc and a target Windows PC, the test started with gaining access to the target PC through an ssh connection, once I was in the target I was able to run commands that would dump the remote traffic on, Linux box.

SSH into target

Listening ports



Evidence dump



Recommendation:

A sniffing attack could be detected if they are using a MITM where traffic is being diverted from the intended endpoint, if this traffic diversion is recognized early it can be used to prevent an attacker from moving to the next steps of the kill chain. Ways this sniffing activity could be mitigated is by secure ports such as ssh and https and encryption important data that is traveling over the network, another way is to incorporate MFA to ensure the person sending or receiving the data is authorized to do so.

Part 3: Report

- Additional defenses implemented, explaining the type of security controls recommended: Detective, preventative, and/or corrective
 - I would recommend creating policies for password complexity and rotation with a 6 month or a year rotation of passwords, also policies and procedures around patch management to ensure that server and operating systems are secure with the latest security patches/
- Evaluation of the second Atomic Testing Cycle as to whether your security controls were successful
 - I was not successful after making some changes, but this is debatable because some of the security features were disabled for the initial attempt to allow for successful testing. It's possible that the initial testing would have also failed if the security features would have been enabled.