ProLUG Security Engineering
Unit 4 Worksheet

Instructions

Fill out this sheet as you progress through the lab and discussions. Hold your worksheets until the end to turn them in as a final submission packet.

Discussion Questions:

Unit 4 Discussion Post 1: Review some of the blogs here:
https://aws.amazon.com/search/?searchQuery=air+gapped#facet_type=blogs&page=1
https://aws.amazon.com/blogs/security/tag/bastion-host/ or that you find on your own about air-gapped systems.

1. What seems to be the theme of air-gapped systems?
2. What seems to be their purpose?
3. If you use google, or an AI, what are some of the common themes that come up when asked about air-gapped or bastion systems?

Unit 4 Discussion Post 2: Do a Google or AI search of topics around jailing a user or processes in Linux.

1. Can you enumerate the methods of jailing users?
2. Can you think of when you've been jailed as a Linux user? If not, can you think of the useful ways to use a jail?

Definitions/Terminology

Air-gapped

Bastion

Jailed process

Isolation

Ingress

Egress

Exfiltration

Cgroups

Namespaces

- Mount
- PID
- IPC
- UTS

Notes During Lecture/Class:

Links:

- https://www.sans.org/information-security-policy/
- https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/
-

Terms:

Useful tools:

- STIG Viewer 2.18
- SCC Tool (version varies by type of scan)
- OpenScap

Lab and Assignment

Unit4_Bastions - To be completed outside of lecture time.

Digging Deeper

1. While this isn't, strictly speaking, an automation course there is some value in looking at automation of the bastion deployments. Check out this ansible code: https://github.com/het-tanis/stream_setup/blob/master/roles/bastion_deploy/tasks/main.yml

   a. Does the setup make sense to you with our deployment?
   b. What can improve and make this better?

2. Find a blog or github where someone else deploys a bastion. Compare it to our process.
3. Knowing what you now know about bastions, jails, and air-gapped systems. Reflect on the first 3 weeks, all the STIGs you've reviewed and touched. Do any of them seem moot, or less necessary if applied in an air-gapped environment?
   a. Does your answer change if you read about Zero Trust and know how much of a hot topic that is in the security world now?
      i. Why or why not?
4. Think of a Linux system where you would like to deploy a bastion (If you cannot think of one, use ProLUG Lab). Draw out how you think the system works in excalidraw.com.

Reflection Questions

1. Does it matter if the user knows that they are jailed? Why or why not?

2. What questions do you still have about this week?

3. How are you going to use what you've learned in your current role?