2019-06-04 On site visit

Tuesday, 4 June 2019 15:58

Customer complaint:

- Many devices blocked due to failed snmp authentication following change of expected result to *.* by Portnox
- Devices with mac prefix 000279 sometimes fail although mac authentication for such prefix exist

Customer actions:

- Deleted 3 snmp auth rules defined by Portnox
- Define auth expected result

Summary:

- All blocked devices due to incidents are already authenticated (allegedly due to customer fix). Issue believed to be caused due to expected result defined as "*.*" and thus any result returned without a period failed. Wildcard in snmp expected result should be "*" only (Portnox converts the string to regex and thus in logs "*" will appear as ".*")
- Device failed auth due to snmp expected result defined as "v6.9*". Once updated to "*v6.9*" authentication succeeded but took over 8 minutes. It seems MAC authentication was the last authentication attempted
- Enforcer 21 is failing to load rule base and thus causing auth failure (due to specific device which was loaded successfully by other enforcers)
- Enforcer 21 restarted and loaded rule base. Devices then authenticated successfully
- Logs collected
- NG Experience (extreme) slowness experienced when searching in NAS View by "all" for device IP
- System status is stable and thus decided not to deploy private fix to issue of snmp decrypt of string with space

- Showed customer how to simulate snmp authentication using deployment helper
- Showed customer how to export users to NG

FRs:

- Indication and automatic action for enforcer failing to load rule base
- SNMP expected result - increase field length. Customer is using multiple (5) rules due to field length limit
- In NG Experience, allow selection of multiple users to edit. Customer has large amount of users exported from classic and need to set similar permissions to all.
- Add filter to Users page to allow selection of users by property (e.g. locked)

Action Items:

- Dev. to analyze logs and understand why enforcer 21 failed to load rule base
- Dev. to fix NG UI performance
- Customer will raise a flag once MAC authentication fails for Portnox to analyze
- Consider change authentication order mechanism (e.g. MAC auth first, then SSH/Windows/SNMP and last OSFP)