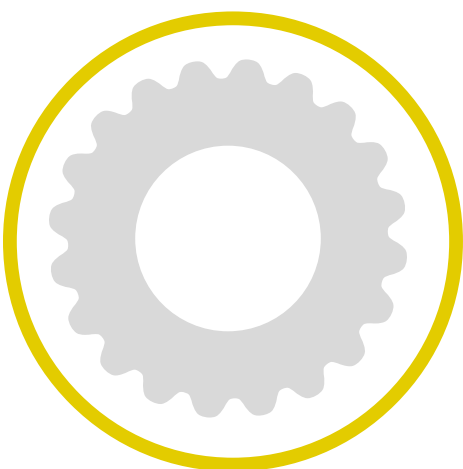


4 STUPID THINGS SEEN IN PEN-TESTS



IMPROPERLY DISPOSED NETWORK GEAR

It's surprising how often there are still configurations on network gear after disposal. This is putting your company at risk beyond their lifespan.

DEVICES WITH EASILY GUESSED SNMP COMMUNITY STRINGS

Easily guessable SNMP community strings give bad actors the ability to manipulate networks at the most fundamental level.



LAZY IT PERSON DEBRIS

Issues arise when VMs aren't properly managed or retired. Therefore one can find default credentials, and more, to access the database.



MULTI-FUNCTION PRINTERS

Oftentimes, the vendors who install these machines don't coordinate with internal IT members. The result is being left with easily Googleable default credentials and access to privileged account information.



These are just four examples of the most common mistakes found in pen-testing. Surprised? The team at Core Security has a list of 8 Tips for Pen-Testing to avoid any of the above mishaps.