# Beginner's guide:
# Open source network security tools

With so many open-source tools available to help with network security, it can be tricky to figure out where to start, especially if you are an IT generalist who has been tasked with security.

We all have to start somewhere…

# The question is, where?

AT&T Business

The sheer number of open-source network security tools available can make it difficult to choose a place to start. This is complicated by the fact that most of these tools often have a very steep learning curve, and can be hazardous to run on a production network.

Let's take a look at a few of the tools available, which will not only provide some answers, but also help you learn more about the topic.

AT&T Business

# Start small

We have all heard the advice to "start small" when trying to learn something new. Well, it's hard to get smaller than the data packets themselves. Packet analysis is not only a good place to start on security, but it is also a good way to brush up on networking in general. This is a core skill set for any security professional.

While there are a number of tools out there for packet analysis, none of them compare to Wireshark. This utility is cross-platform, stable, and comes with a CLI peer application (Tshark) that uses all of the same filters and can be used to analyze from hosts without a UI. Wireshark also has a tremendous wealth of resources including Documentation, References, and even Sample Captures to download and review.

AT&T Business

# Discover the network around you

It's often said, "You can't manage what you can't measure." If you want to protect your network, it's critical to start by learning what's actually on it.

A good network discovery tool should let you know not only what devices are on your network, but also what OS is running, what ports are listening, and as much detail on what services are listening on those ports as possible.

With a number of tools available, you'll find a solid contender in the market with Nmap. Nmap is a cross platform command line utility for network discovery and enumeration. This tool has an amazing amount of depth, with so many options available that they have literally  written entire books on the switches available for this tool. The Nmap team also blazed the trail on enumeration, with built in flexibility for the type, depth, speed, and aggressiveness of scans.

Like Tshark, Nmap also has a partner cross-platform GUI, Zenmap, which provides a simpler to use UI, but also displays the filters used in the command-line interface (CLI) as a learning aid. Documentation will also not be an issue with this utility as Nmap has a very thorough documentation section on their site.

AT&T Business

# Catching the scent

Although most often considered a reactive tool, the network intrusion detection system (IDS) is still a valuable tool for preventing  issues, as it can help you discover a variety of issues that other network security tools just do not see.

There are a number of good open-source tools available, but these are actually one of the more difficult classes of tools to learn how to use effectively. The reason for this is that network IDS  tools tend to walk the line on false positives, and the field of play is always changing. It's like playing baseball on a field where the bases are on tracks that slide along.

Bro IDS, Snort, and Suricata are 3 capable Network IDS tools for analyzing network traffic to detect target activity. These tools are better run from a server or workstation, than on a mobile unit, because they require configuring port mirroring on the network infrastructure.

AT&T Business

# Catching the scent

A good choice for learning these is to install either a standalone server, or to install a SIEM, which includes a Network IDS such as Security Onion. You can then use the same server when you move on to learning about correlation.

You can also install these as modules in some open source firewalls, such as pfSense. In this particular case, Snort would be an excellent option, as it has a much more robust selection of documentation available.

AT&T Business

# No open-door policy

While a good patch management policy will help address many vulnerability issues on your network, it will never be able to close all holes, and any door left open is much easier to walk through. For this reason, vulnerability testing is an absolute necessity for any network.

## This brings up an important set of points on vulnerability scanners.

AT&T Business

# (1) Vulnerability scanner tips
# Version analysis

**While necessary, version analysis is not enough.** Some vulnerability scanners check the advertised version of a service or system and compare it to a list of known versions. While this is important, it does not account for systems configured not to report version, or to deliberately misreport this information. Because of this fact, we need to scan for other factors.

AT&T Business

## (2) Vulnerability scanner tips
# Behavioral analysis

**Behavioral analysis should also be a component of any scanner.** Keep in mind, however, that BA does not account for features that are not currently enabled, or for conditional faults (our favorite conditional fault is a previous internet information services (IIS) defect that is only exploitable if there is a folder with a 15 character or longer name starting with an "a" in the root of the public folder).

AT&T Business

**Vulnerability scanner tips**

# (3) False positives may not be fun, but they are much better than any false negative

Vulnerability scanners work on the edge, testing for vulnerabilities that cannot be confirmed without causing damage to the system. As this is a rather large gray area to work in, even the best vulnerability scanner can be expected to generate some false positives. This is, unfortunately, part of the game here.

AT&T Business

**Vulnerability scanner tips**

# (4) A false positive could also be a conditionally false positive

Never assume that a result is a false positive because it was last time. A number of vulnerabilities are highly conditional. A configuration change, an update to the operating system, another application on the system, or a simple file or folder saved in the wrong place or with the wrong name can create a vulnerability that needs attention.

AT&T Business

# Vulnerability scanning tools

A very popular vulnerability scanning tool is OpenVAS, which is a fork of NESSUS. Documentation on the project is more than a little behind, but the theory of operation is documented very well with the now-closed-source NESSUS tool.

Like the IDS solutions described above, these tools are often best installed as part of a static server—it is difficult to configure, is very resource intensive,

and tends to be very slow to scan. You could consider installing a SIEM that includes one or more of these tools. Conveniently, AlienVault® Unified Security Management® (USM™) by AT&T Cybersecurity provides such a capability, with integrated network IDS, vulnerability scanning and management and network asset discovery, with host IDS as well, giving a very clear picture of what's going on in your network.

AT&T Business

# Taking the game to them

The next step is to look at a penetration testing distribution, or pentesting. Pentesting is a way of proactively taking on security, because the best way to know if something can be exploited is to exploit it.

Assuming you have written permission to perform these tests, this allows you to probe the network carefully, using the same techniques that an infiltrator would use, and is one of the best methods for discovering how security is practiced, and how it is compromised.

There are several pentesting distributions on the market (Pentoo, NodeZero, Kali, and BackBox are
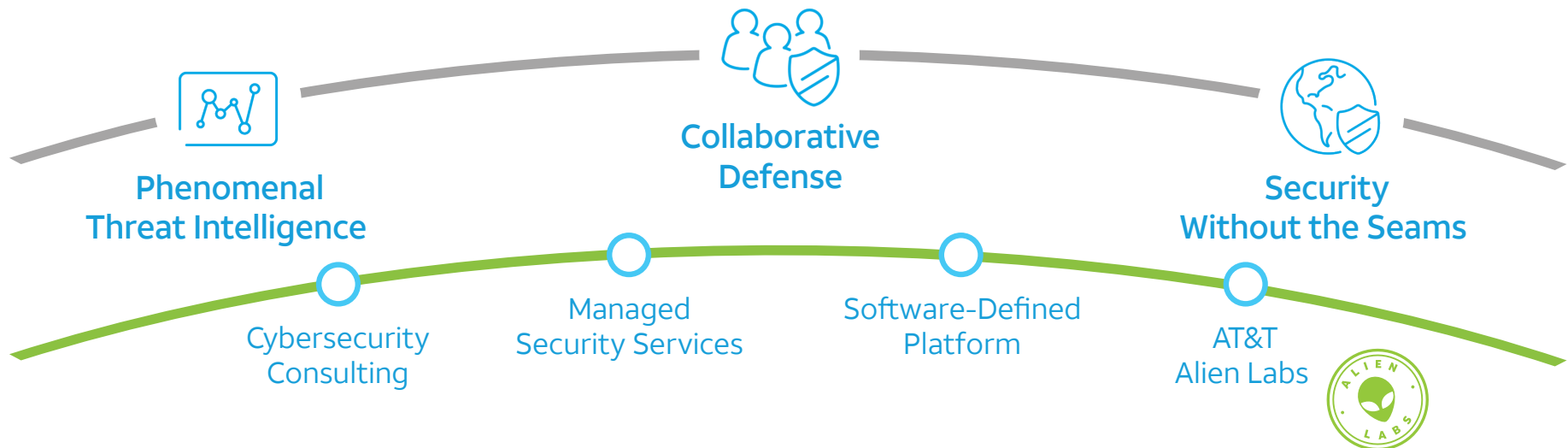
good examples) loaded with tools and utilities. Unfortunately, these offer so many tools, they don't help answer the question of where to start. So, it boils down to personal preference; you can download and try each of them to find which you are most comfortable with.

Hopefully, this will get you started in the right direction as you explore open source network security tools. Once you start rolling, you will be able to start adding new tools to your toolset pretty regularly, and move right out of that "beginners" category.

AT&T Business

# About AT&T Cybersecurity

AT&T Cybersecurity's edge-to-edge technologies provide phenomenal threat intelligence, collaborative defense, security without the seams, and solutions that fit your business. Our unique, collaborative approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from Alien Labs researchers, Security Operations Center analysts, and machine learning—helping to enable our customers around the globe to anticipate and act on threats to protect their business.

## Unified Security Management

**Phenomenal Threat Intelligence**

**Collaborative Defense**

**Security Without the Seams**

Cybersecurity Consulting

Managed Security Services

Software-Defined Platform

AT&T Alien Labs

AT&T Business