buttressIT: Artificial Intelligence for Network Audits

Brent Kirkpatrick *

December 15, 2017

Intrepid Net Computing

www.intrepidnetcomputing.com

*bbkirk@intrepidnetcomputing.com

Abstract

The buttressIT network audit provides protection and support without penetration testing. Hackers want to intrude on your network, steal data, and break computers. As a preventative network audit, buttressIT protects you from security intrusions and supports your cybersecurity.

At the completion of your buttressIT network audit, you will have a network map, a list of network vulnerabilities, and a priority order for your upgrades. This means you can order a buttressIT audit without any preperation on your part.

Save on your IT budget and prevent intrusions. Our buttressIT approach is grounded in artificial intelligence and analyzes network data. It detects vulnerabilities and prevents intrusions.

Keywords: Cybersecurity, artificial intelligence, knowledge base, incident data, network audit

1 Introduction

Intruders could compromise your network without you knowing. Many network breaches go undetected during the initial phases of the attack. Protect yourself with routine network audits through buttressIT [1].

Internet crime is now commonplace. Most attacks begin with network compromise and network reconnisance. After that, the damage phases of the attack begin, including fraud, data theft, and broken computers. Email fraud is very expensive and frequently reported [2]. Data theft is common with $141 being the average cost for each stolen record [3]. Additionally, hackers often break computer software and hardware, causing IT costs to soar.

IT teams often detect the damage phases of an attack and begin re-securing their networks. Unfortunately, the chance of recurring data breach is 27.7% [3]. This means that most IT teams are unable to immeadiately resecure their networks.

The buttressIT network audit prevents intrusions and helps clean up existing compromise. Intrepid Net Computing [4] uses artificial intelligence to map your network, assess its security, and prioritize upgrades. This is done *without* penetration testing. Acting on the findings of the audit will repair vulnerabilities and make intrusion less likely.

2 Methods

The buttressIT approach is based in artificial intelligence and does *not* rely on penetration testing. Intrepid Net Computing relies on network data. First, the audit maps the topology of the network, the computers and how they are connected. Second, the audit assesses the vulnerabilities of the network. After the audit, the lessons learned from the data are prioritized and shared with you.

The network to audit can be large or small. Large networks would be whole states or cities. Small networks would be business networks. The artificial intelligence techniques used by the buttressIT audit scale well from small networks to very large ones.

The buttressIT network audit produces a map of the network. Many important computers and communication links between them are represented in the map. Less imporant computers may be left out, but the backbone of the network will be discovered.

After mapping the network, the buttressIT network audit assesses the network's vulnerabilities. These include flaws in physical infrastructure and software infrastructure.

With buttressIT you can perform an audit with little to no preparation. Unlike some auditors who require a hand-drawn network map, the buttressIT network audit has no such requirement. The audit is able to analyze some potiential routes of intrusion and assesses network vulnerabilities.

By acting on the results of your buttressIT audit, you will be able to upgrade your network security, based on the priorities determined by the audit. This economizes your defenses and helps you determine how much of your budget to spend on certain upgrades.

3 Results

With the buttressIT network audit you will be able to

1. discover the network layout,
2. prioritize network upgrades,
3. save on IT costs,
4. spend less money on security, and
5. have fewer intrusions.

Furthermore, the audit does *not* use penetration testing. No new vulnerabilities will be introduced, and the auditors do not need special access permission.

4 Conclusions

Save yourself the headache of being hacked. Data breaches do not happen when intruders are stopped at the door. Use buttressIT for corporate, city, or state networks.

buttressIT is intrepid cybersecurity in an audit. Fearless cybersecurity.

Web

The on-line information for buttressIT can be found at `http://www.intrepidnetcomputing.com/security/audit.html`

References

[1] buttressIT. `http://www.intrepidnetcomputing.com/security/audit.html`. Accessed: 2017-12-14.

[2] FBI. 2016 internet crime report. *ic3*, 2016.

[3] Ponemon Institute. 2017 cost of data breach study: Global analysis. *Ponemon Institute Research Report*, 2017.

[4] Intrepid Net Computing. `http://www.intrepidnetcomputing.com/`. Accessed: 2017-12-4.