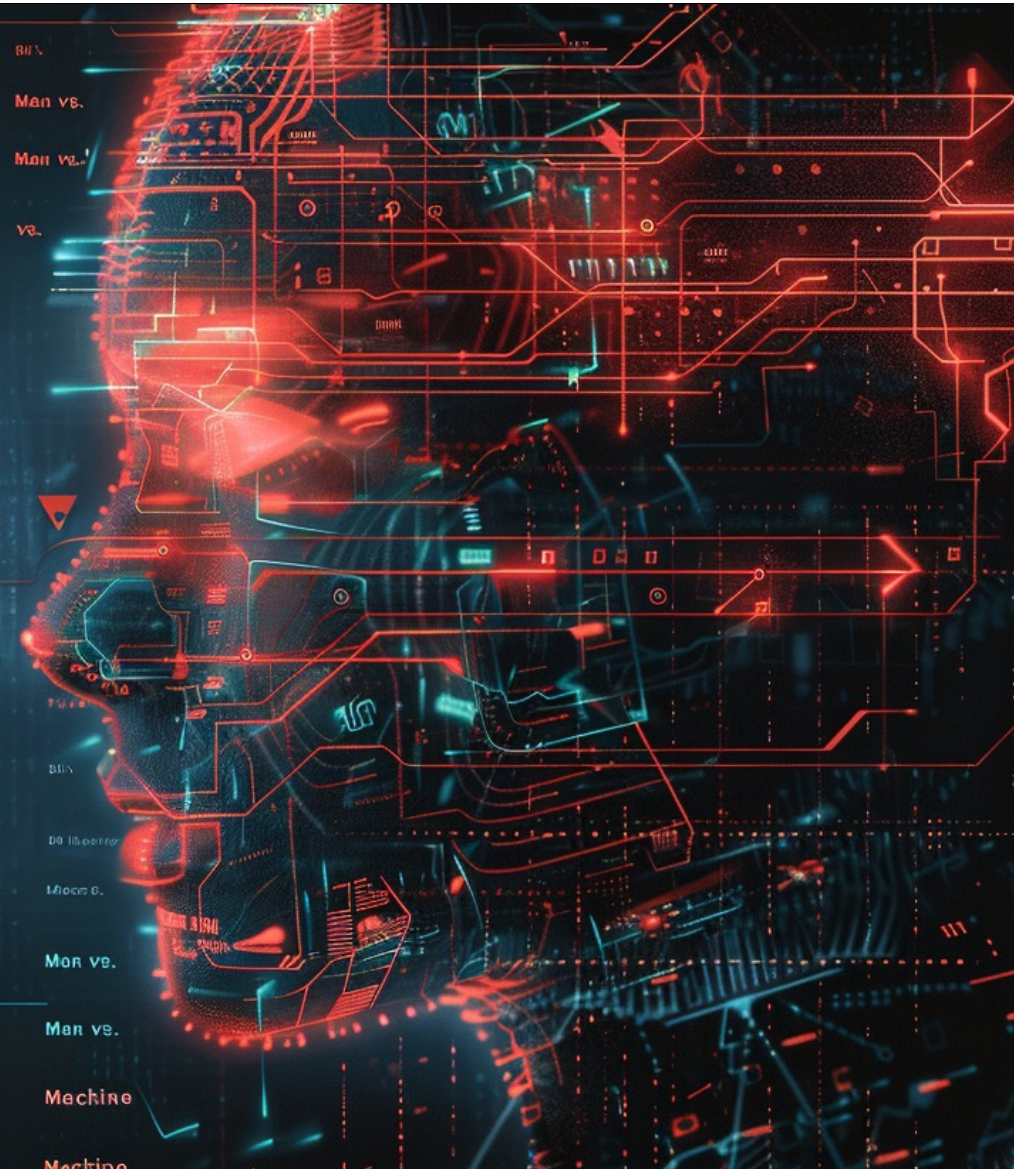




MAN VS. MACHINE

Terry Bradley
Founder , Mile High Cyber



WHY THIS TALK MATTERS

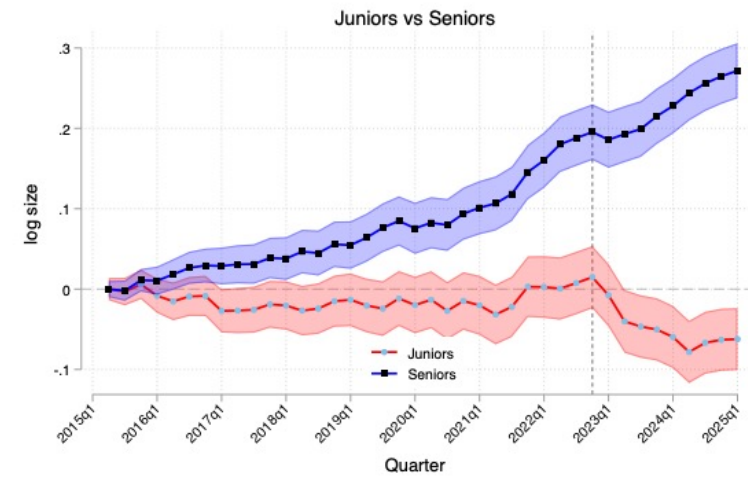


Figure 3: Employment Differences Between Adopters and Non-Adopters Over Time

Notes: The graph presents the estimated coefficients β_j from Equation 1, run separately to juniors and seniors. Standard errors are clustered in firm level.

<https://www.linkedin.com/pulse/blind-disruption-ceos-who-missed-future-steve-blank-jil1c/>

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=5425555

ABOUT TERRY BRADLEY



MYTH #1: THE MANUAL PEN TEST

MYTH #2: HUMAN PEN TESTERS ARE BETTER

MYTH #3: AUTOMATED PEN TESTS ARE FASTER

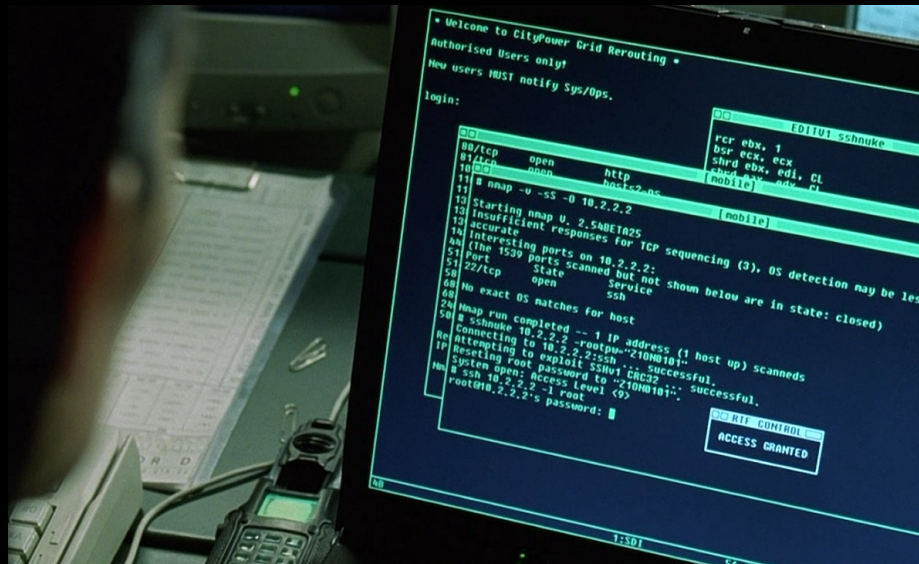
MYTH #4: AUTOMATED PEN TESTS ARE CHEAPER

MYTH #5: HUMAN-LED PEN TESTS ARE SAFER

MYTH #1: THE MANUAL PEN TEST



HUMAN PEN TESTERS RELY ON AUTOMATED PEN TEST TOOLS TO FIND SECURITY FLAWS AND ENSURE GOOD TEST COVERAGE



EARLY PEN TEST TOOLS

```
% echo "GET / HTTP/1.0\n" | netcat localhost 80
HTTP/1.1 200 OK
Date: Sat, 07 Jan 2006 08:43:27 GMT
Server: Apache
Last-Modified: Wed, 28 Dec 2005 08:09:31 GMT
ETag: "13c6e-14-1ea644c0"
Accept-Ranges: bytes
Content-Length: 20
Connection: close
Content-Type: text/html

nothing to see here
% █
```

netcat
1995



SATAN
1995

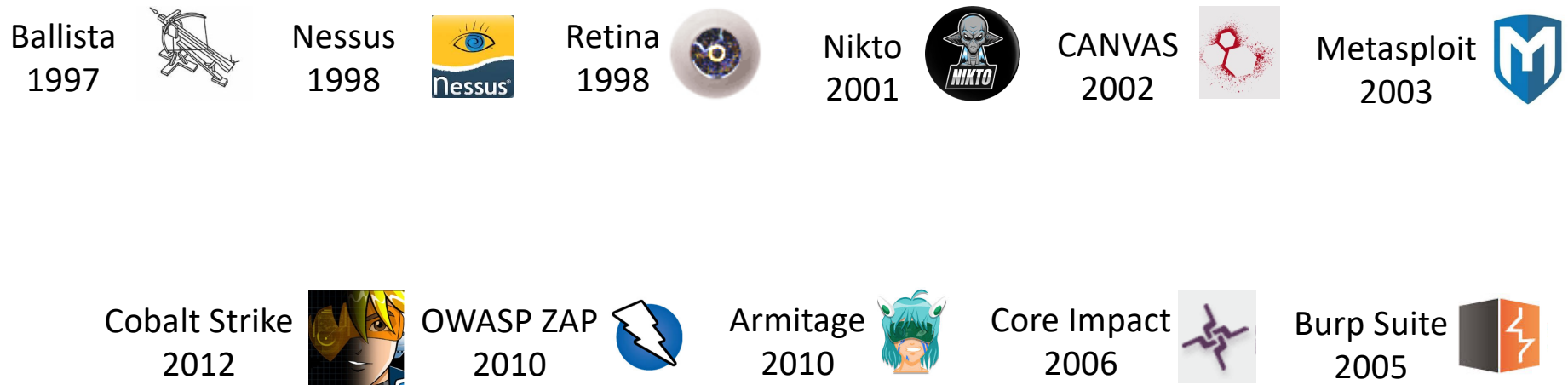
```
---[ Phrack Magazine   Volume 7, Issue 51 September 01, 1997, article 11 of 17
-----[ The Art of Port Scanning
-----[ Fyodor <fyodor@dhp.com>

[ Abstract ]

This paper details many of the techniques used to determine what ports (or
similar protocol abstraction) of a host are listening for connections. These
ports represent potential communication channels. Mapping their existence
facilitates the exchange of information with the host, and thus it is quite
useful for anyone wishing to explore their networked environment, including
hackers. Despite what you have heard from the media, the Internet is NOT
all about TCP port 80. Anyone who relies exclusively on the WWW for
information gathering is likely to gain the same level of proficiency as your
average AOLer, who does the same. This paper is also meant to serve as an
introduction to and ancillary documentation for a coding project I have been
working on. It is a full featured, robust port scanner which (I hope) solves
some of the problems I have encountered when dealing with other scanners and
when working to scan massive networks. The tool, nmap, supports the following:
```

Nmap
1997

TREND → MORE AUTOMATION



MYTH #2: HUMAN PEN TESTERS ARE BETTER





B. ALL PEN TESTERS HAVE GOOD/BAD DAYS

C. WILD DISAGREEMENT ON WHAT “GOOD” MEANS

In my experience, the results the top automated pen test platforms available today are very comparable to human-led pen tests.

ISSA CYBER FOCUS WEEK 2024

The Kinds of Security Bugs Scanners Miss

- **Business Logic Errors**
- **Insufficient Process Validation**
- **Race Conditions**
- **User Enumeration**
- **Authentication and Session Management Flaws**

The Kinds of Security Bugs Pen Testers Miss

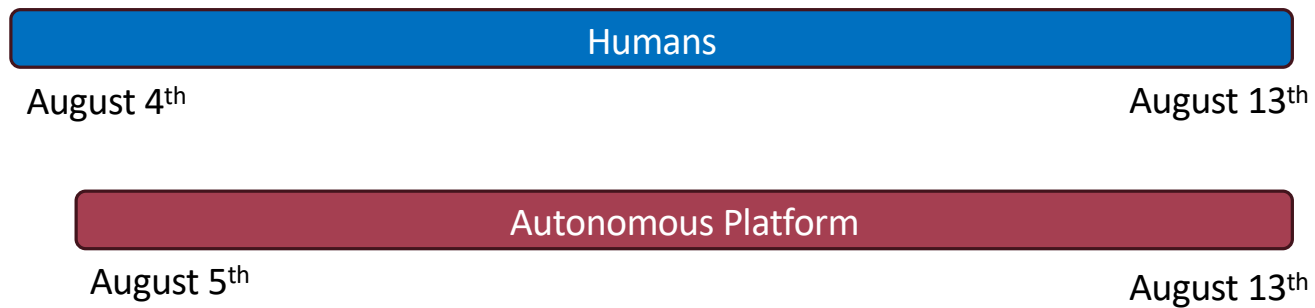
- **Business Logic Errors**
- **Insufficient Process Validation**
- **Race Conditions**
- **User Enumeration**
- **Authentication and Session Management Flaws**
- **Multi-step Data Leakage**
- **Chain of Vulnerabilities**
- **Complex Access Control Issues**

MYTH #3: AUTOMATED PEN TESTS ARE FASTER



RECENT EXTERNAL NETWORK PEN TEST

- Local government client
- ~100 external IP addresses with numerous web applications

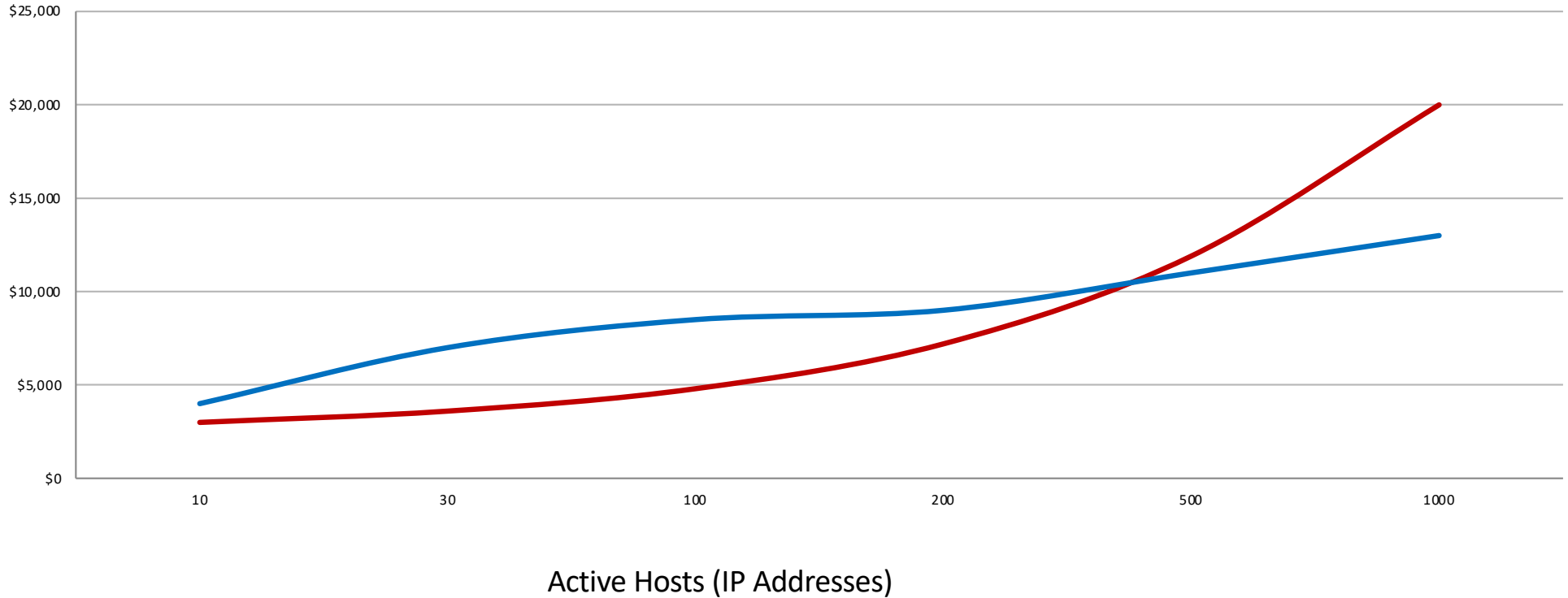


MYTH #4: AUTOMATED PEN TESTS ARE CHEAPER



ROUGH PRICING FOR PEN TESTS

Automated vs. Human



MYTH #5: HUMAN-LED PEN TESTS ARE SAFER





TRAIN WRECKS I'VE
WITNESSED...



WHAT IF I TOLD YOU

HYBRID APPROACH

Capability	Automated vulnerability scanning	Autonomous penetration testing with NodeZero® platform	Hybrid approach with manual testing and NodeZero® platform	Fully manual penetration testing
Discovery of live hosts within the in-scope networks	✓	✓	✓	✓
Vulnerability identification	✓	✓	✓	✓
Dedicated project management	✓	✓	✓	✓
Exploitation and privilege escalation		✓	✓	✓
Lateral movement		✓	✓	✓
Proof of exploitation		✓	✓	✓
Hands-on exploit development and analysis			✓	✓
Deep dives into specific vulnerabilities				✓

<https://www.nccgroup.com/uk/technical-assurance/network-infrastructure-architecture-container-security/network-penetration-testing-services/>

OBSERVATIONS



HUMAN-LED PEN TESTS

- Capacity / bench are big issues
- Project / Reporting is slower
- Personal interaction and tailoring is good*
- Relationship building*
- Ability to dig-deeper / assess business context is superior*

* If you're doing it right...



AUTOMATED PEN TESTS

- Testing is not very tailored
- No capacity / no bench issues
- Testing and reporting are fast
- Super-consistent testing with
- "One-click retests"
- Potentially cheaper
- Bonus features, depending on license

FINAL TAKEAWAYS

AI is here to stay and it's a force multiplier

- Threat actors are already leveraging automation and AI *
- Agentic AI platforms are on the horizon...

Decreasing junior cyber roles / increase the value of senior experts

- Harvard study ‡

Purely automated / AI pen test service offerings are not yet fully trusted but successful firms will integrate them into their offerings

* <http://catonetworks.com/blog/cato-ctrl-threat-research-analyzing-lamehug/>

‡ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5425555



THANK YOU

Terry Bradley
719-310-5454

terry.bradley@milehighcyber.com