VULNCON

vulncon.in

The Soul of the Hacker

By Vicky Ray

VULNCON 2025 | 14th & 15th JUNE 2025 | NSSC, IISc, Bengaluru

RayvenX

RayvenX

paloalto NETWORKS

BARCLAYS

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

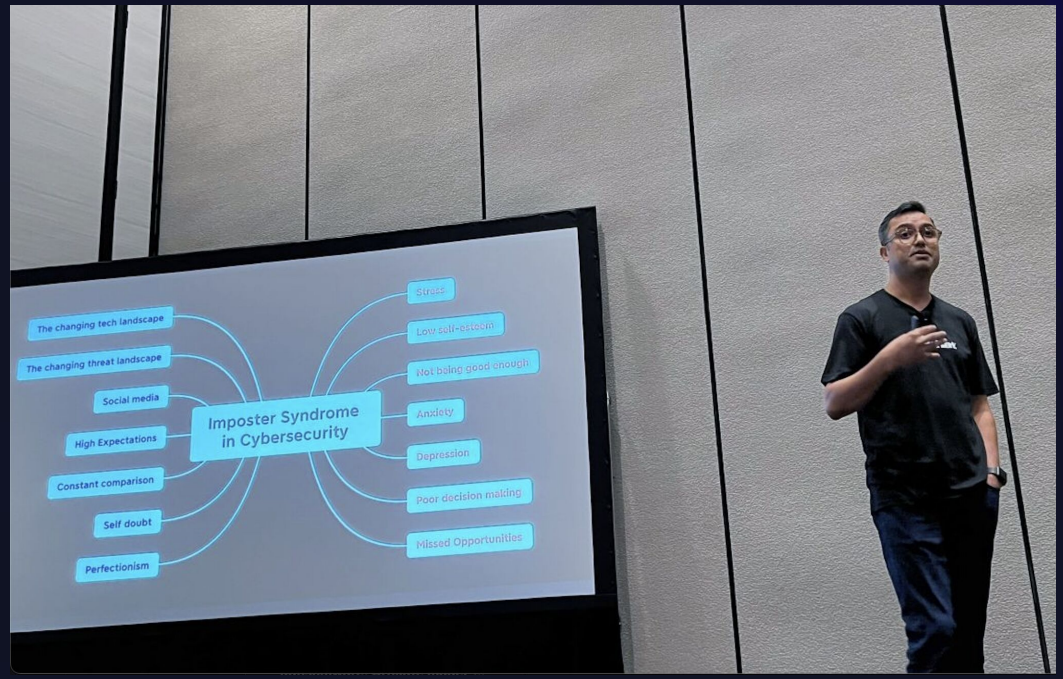
ATT&CK

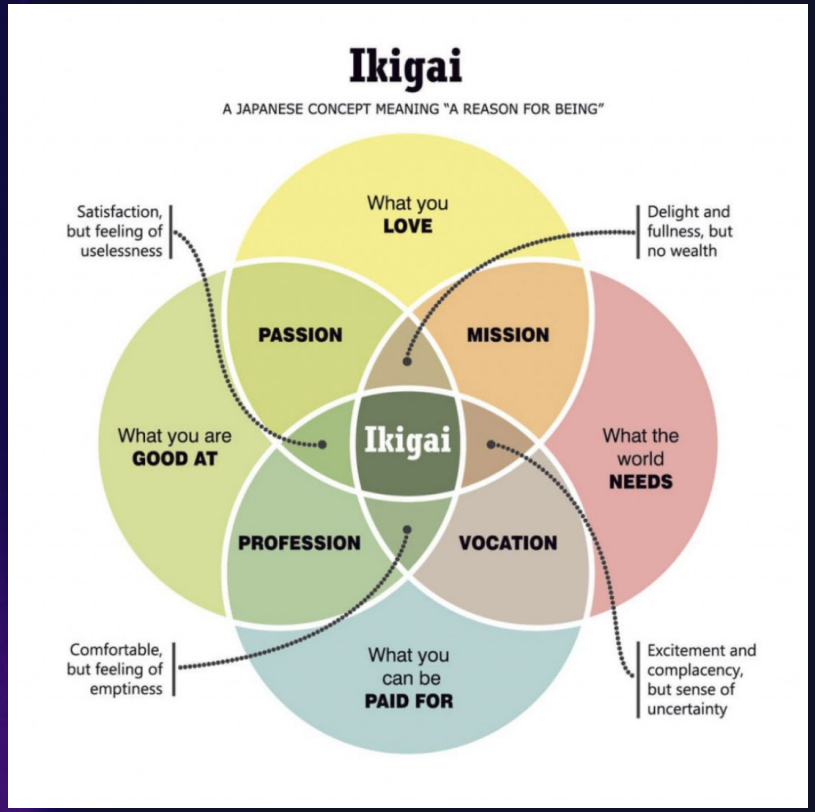
CTI CMM

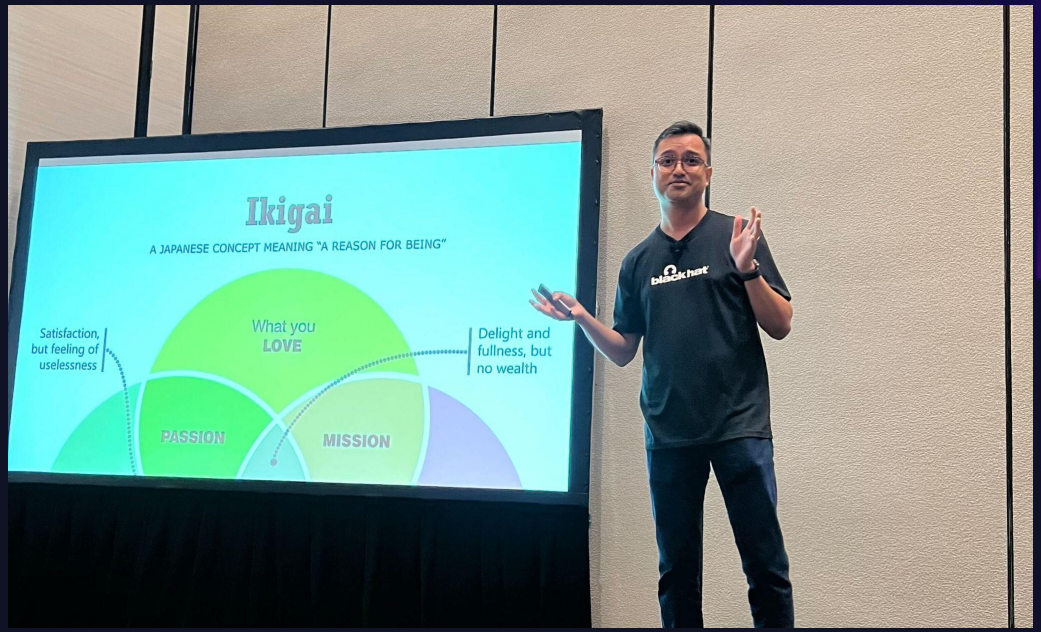
- Close to two-decades in the cybersecurity industry
- Founder of RayvenX
- One of the early members of the world renowned UNIT 42 Threat-Intelligence team of Palo Alto Networks, leading the Asia Pacific and Japan region for 10 years.
- Advisor to enterprises, governments & law-enforcements globally.
- Published several research reports on cybercrime and nation state cyber attack campaigns.
- Worked with INTERPOL and various global law-enforcement on real-world cybercrime operations.
- Adjunct lecturer at Nanyang Technological University, Singapore.

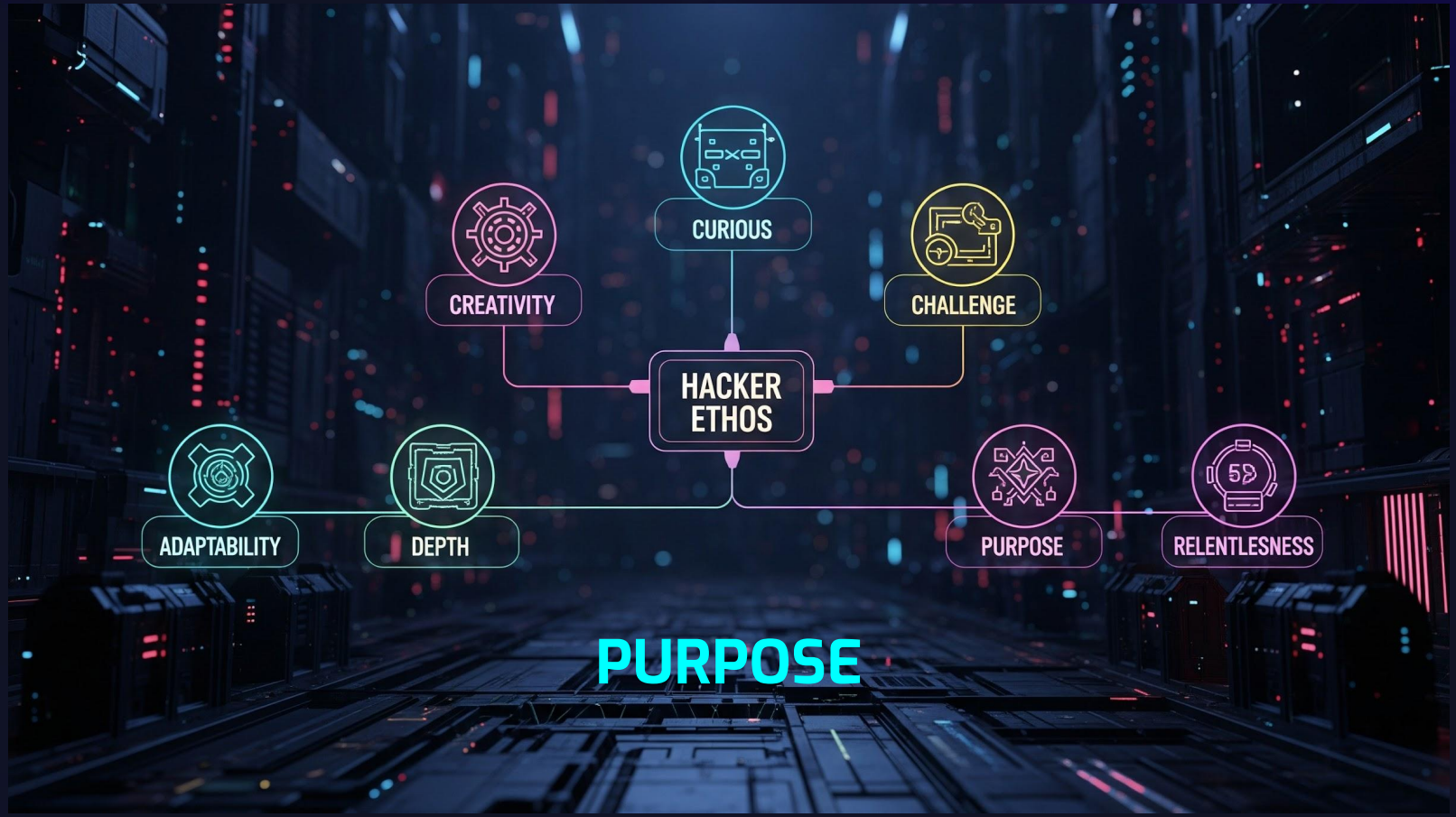
Will AI replace us?

The anxiety & stress in our industry




Ikigai
A JAPANESE CONCEPT MEANING "A REASON FOR BEING"
What you LOVE
Satisfaction, but feeling of uselessness
Delight and fullness, but no wealth
PASSION
MISSION
What you are GOOD AT
Ikigai
What the world NEEDS
PROFESSION
VOCATION
Comfortable, but feeling of emptiness
What you can be PAID FOR
Excitement and complacency, but sense of uncertainty

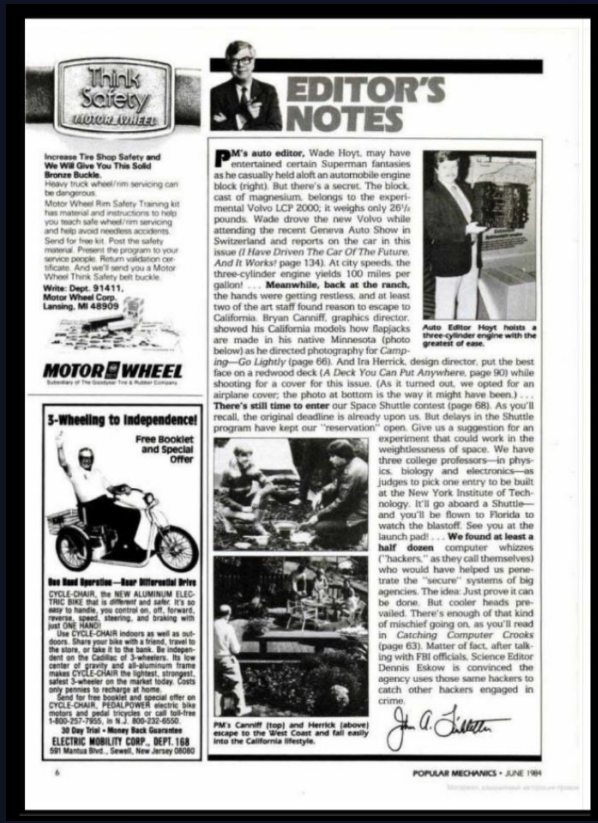

Ikigai
A JAPANESE CONCEPT MEANING "A REASON FOR BEING"
Satisfaction, but feeling of uselessness
What you LOVE
Delight and fullness, but no wealth
PASSION
MISSION
black hat


CURIOUS
CREATIVITY
CHALLENGE
HACKER ETHOS
ADAPTABILITY
DEPTH
PURPOSE
RELENTLESSNESS
PURPOSE

Who is a Hacker, Really?

Story of the misfit

Story of the misfit



Think Safety
MOTOR WHEEL

Increase Tire Shop Safety and We Will Give You This Solid Bronze Buckle.
Heavy truck wheel/rim servicing can be dangerous.
Motor Wheel Rim Safety Training kit has material and instructions to help you teach safe wheel/rim servicing and help avoid needless accidents.
Send for free kit. Post the safety material. Present the program to your service people. Return validation certificate. And we'll send you a Motor Wheel Think Safety belt buckle.
Write: Dept. 91411,
Motor Wheel Corp.
Lansing, MI 48909

MOTOR WHEEL
Subsidiary of The Goodyear Tire & Rubber Company

3-Wheeling to independence!
Free Booklet and Special Offer

One Hand Operation—Rear Differential Drive
CYCLE-CHAIR, the NEW ALUMINUM ELECTRIC BIKE that is *different* and *safer*. It's so easy to handle, you control on, off, forward, reverse, speed, steering, and braking with just ONE HAND!
Use CYCLE-CHAIR indoors as well as outdoors. Share your bike with a friend, travel to the store, or take it to the bank. Be independent on the Cadillac of 3-wheelers. Its low center of gravity and all-aluminum frame makes CYCLE-CHAIR the lightest, strongest, safest 3-wheeler on the market today. Costs only pennies to recharge at home.
Send for free booklet and special offer on CYCLE-CHAIR, PEDALPOWER electric bike motors and pedal bicycles or call toll-free 1-800-257-7555, in N.J. 800-232-6550.
30 Day Trial • Money Back Guarantee
ELECTRIC MOBILITY CORP., DEPT. 168
591 Mantua Blvd., Sewell, New Jersey 08080

EDITOR'S NOTES

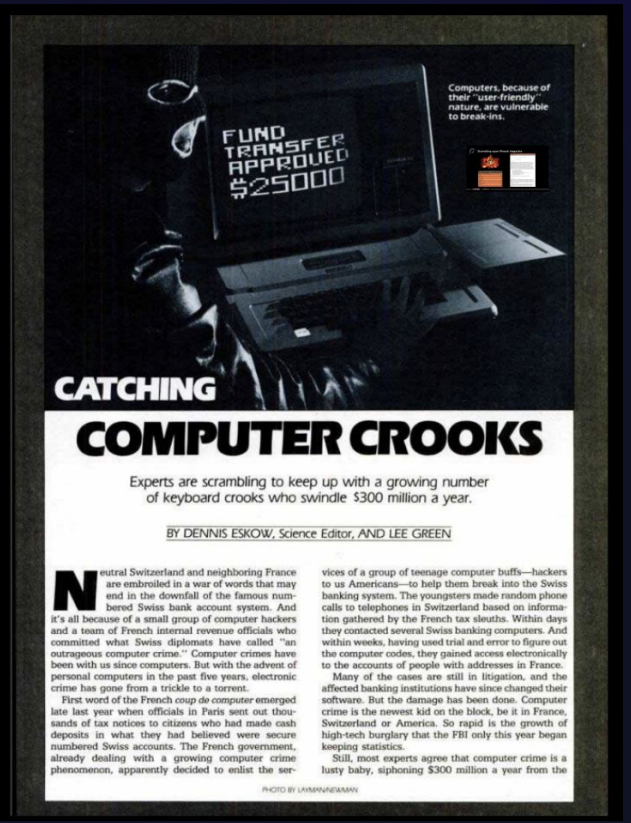
PM's auto editor, Wade Hoyt, may have entertained certain Superman fantasies as he casually held aloft an automobile engine block (right). But there's a secret. The block, cast of magnesium, belongs to the experimental Volvo LCP 2000; it weighs only 26½ pounds. Wade drove the new Volvo while attending the recent Geneva Auto Show in Switzerland and reports on the car in this issue (*I Have Driven The Car Of The Future. And It Works!* page 134). At city speeds, the three-cylinder engine yields 100 miles per gallon! . . . **Meanwhile, back at the ranch,** the hands were getting restless, and at least two of the art staff found reason to escape to California. Bryan Canniff, graphics director, showed his California models how flapjacks are made in his native Minnesota (photo below) as he directed photography for *Camping—Go Lightly* (page 66). And Ira Herrick, design director, put the best face on a redwood deck (*A Deck You Can Put Anywhere*, page 90) while shooting for a cover for this issue. (As it turned out, we opted for an airplane cover; the photo at bottom is the way it might have been.) . . . **There's still time to enter** our Space Shuttle contest (page 68). As you'll recall, the original deadline is already upon us. But delays in the Shuttle program have kept our "reservation" open. Give us a suggestion for an experiment that could work in the weightlessness of space. We have three college professors—in physics, biology and electronics—as judges to pick one entry to be built at the New York Institute of Technology. It'll go aboard a Shuttle—and you'll be flown to Florida to watch the blastoff. See you at the launch pad! . . . **We found at least a half dozen** computer whizzes ("hackers," as they call themselves) who would have helped us penetrate the "secure" systems of big agencies. The idea: Just prove it can be done. But cooler heads prevailed. There's enough of that kind of mischief going on, as you'll read in *Catching Computer Crooks* (page 63). Matter of fact, after talking with FBI officials, Science Editor Dennis Eskow is convinced the agency uses those same hackers to catch other hackers engaged in crime.

Auto Editor Hoyt hoists a three-cylinder engine with the greatest of ease.

PM's Canniff (top) and Herrick (above) escape to the West Coast and fall easily into the California lifestyle.

6

POPULAR MECHANICS • JUNE 1984



CATCHING

COMPUTER CROOKS

Experts are scrambling to keep up with a growing number of keyboard crooks who swindle $300 million a year.

BY DENNIS ESKOW, Science Editor, AND LEE GREEN

Neutral Switzerland and neighboring France are embroiled in a war of words that may end in the downfall of the famous numbered Swiss bank account system. And it's all because of a small group of computer hackers and a team of French internal revenue officials who committed what Swiss diplomats have called "an outrageous computer crime." Computer crimes have been with us since computers. But with the advent of personal computers in the past five years, electronic crime has gone from a trickle to a torrent.

First word of the French *coup de computer* emerged late last year when officials in Paris sent out thousands of tax notices to citizens who had made cash deposits in what they had believed were secure numbered Swiss accounts. The French government, already dealing with a growing computer crime phenomenon, apparently decided to enlist the services of a group of teenage computer buffs—hackers to us Americans—to help them break into the Swiss banking system. The youngsters made random phone calls to telephones in Switzerland based on information gathered by the French tax sleuths. Within days they contacted several Swiss banking computers. And within weeks, having used trial and error to figure out the computer codes, they gained access electronically to the accounts of people with addresses in France.

Many of the cases are still in litigation, and the affected banking institutions have since changed their software. But the damage has been done. Computer crime is the newest kid on the block, be it in France, Switzerland or America. So rapid is the growth of high-tech burglary that the FBI only this year began keeping statistics.

Still, most experts agree that computer crime is a lusty baby, siphoning $300 million a year from the

PHOTO BY LAYMANNEWMAN

Title : The Art of Scanning

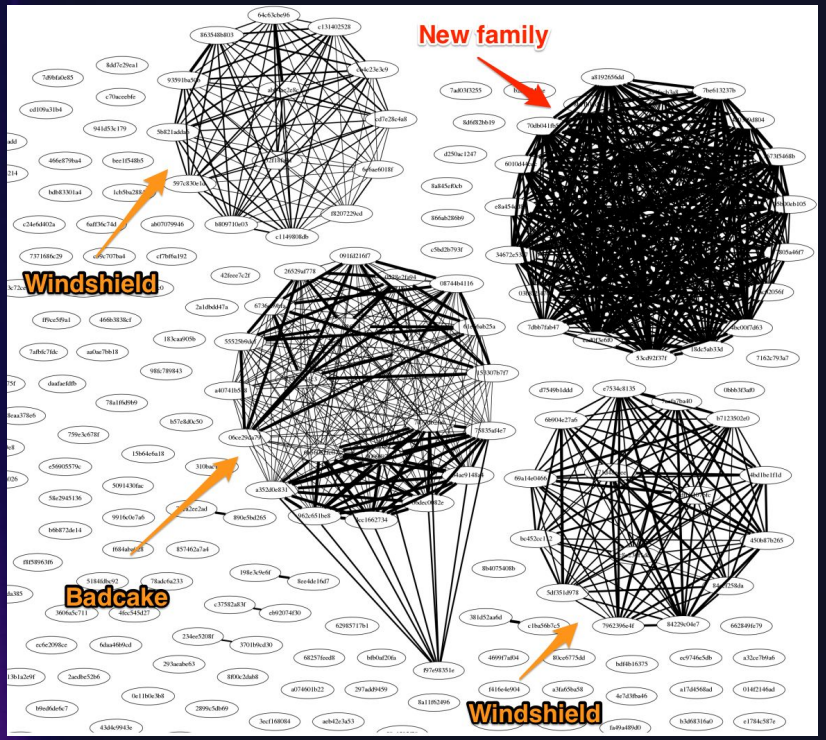
Author : Fyodor

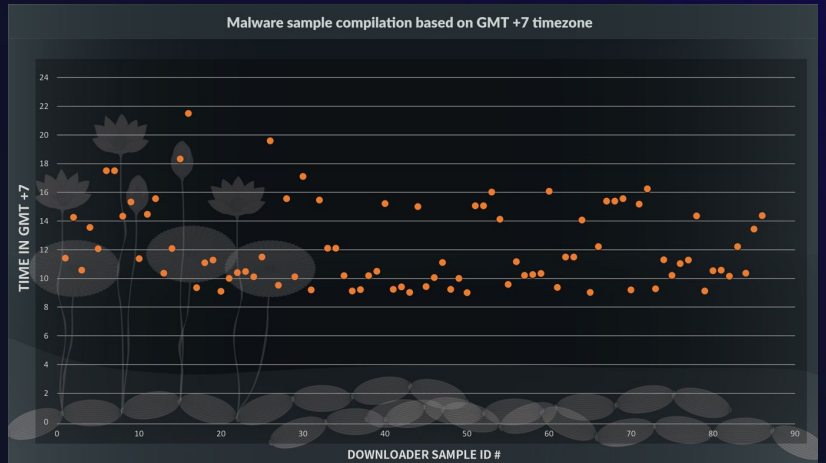
```
---[  Phrack Magazine   Volume 7, Issue 51 September 01, 1997, article 11 of 17


-------------------------[  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:

    - vanilla TCP connect() scanning,
    - TCP SYN (half open) scanning,
    - TCP FIN (stealth) scanning,
    - TCP ftp proxy (bounce attack) scanning
    - SYN/FIN scanning using IP fragments (bypasses packet filters),
    - UDP recvfrom() scanning,
    - UDP raw ICMP port unreachable scanning,
    - ICMP scanning (ping-sweep), and
    - reverse-ident scanning.

The freely distributable source code is appended to this paper.



[ Introduction ]

Scanning, as a method for discovering exploitable communication channels, has
been around for ages.  The idea is to probe as many listeners as possible, and
keep track of the ones that are receptive or useful to your particular need.
Much of the field of advertising is based on this paradigm, and the "to current
resident" brute force style of bulk mail is an almost perfect parallel to what
we will discuss.  Just stick a message in every mailbox and wait for the
responses to trickle back.

Scanning entered the h/p world along with the phone systems.  Here we have this
tremendous global telecommunications network, all reachable through codes on
our telephone.  Millions of numbers are reachable locally, yet we may only
be interested in 0.5% of these numbers, perhaps those that answer with a
carrier.
```

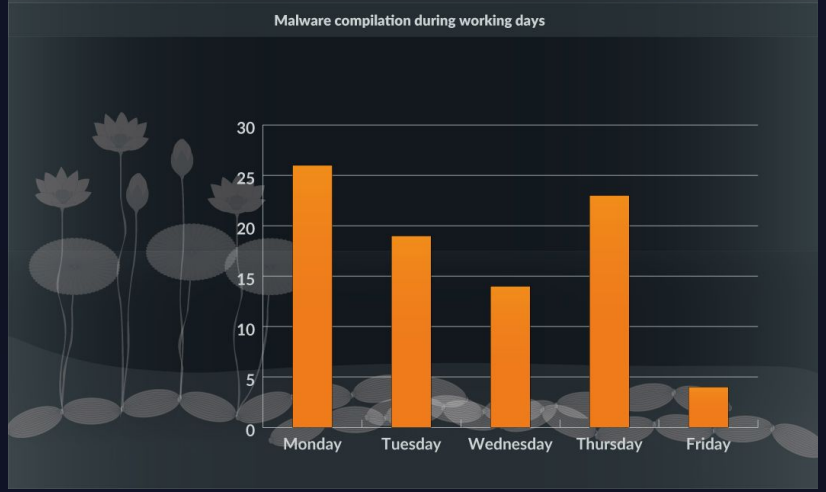

HN/P

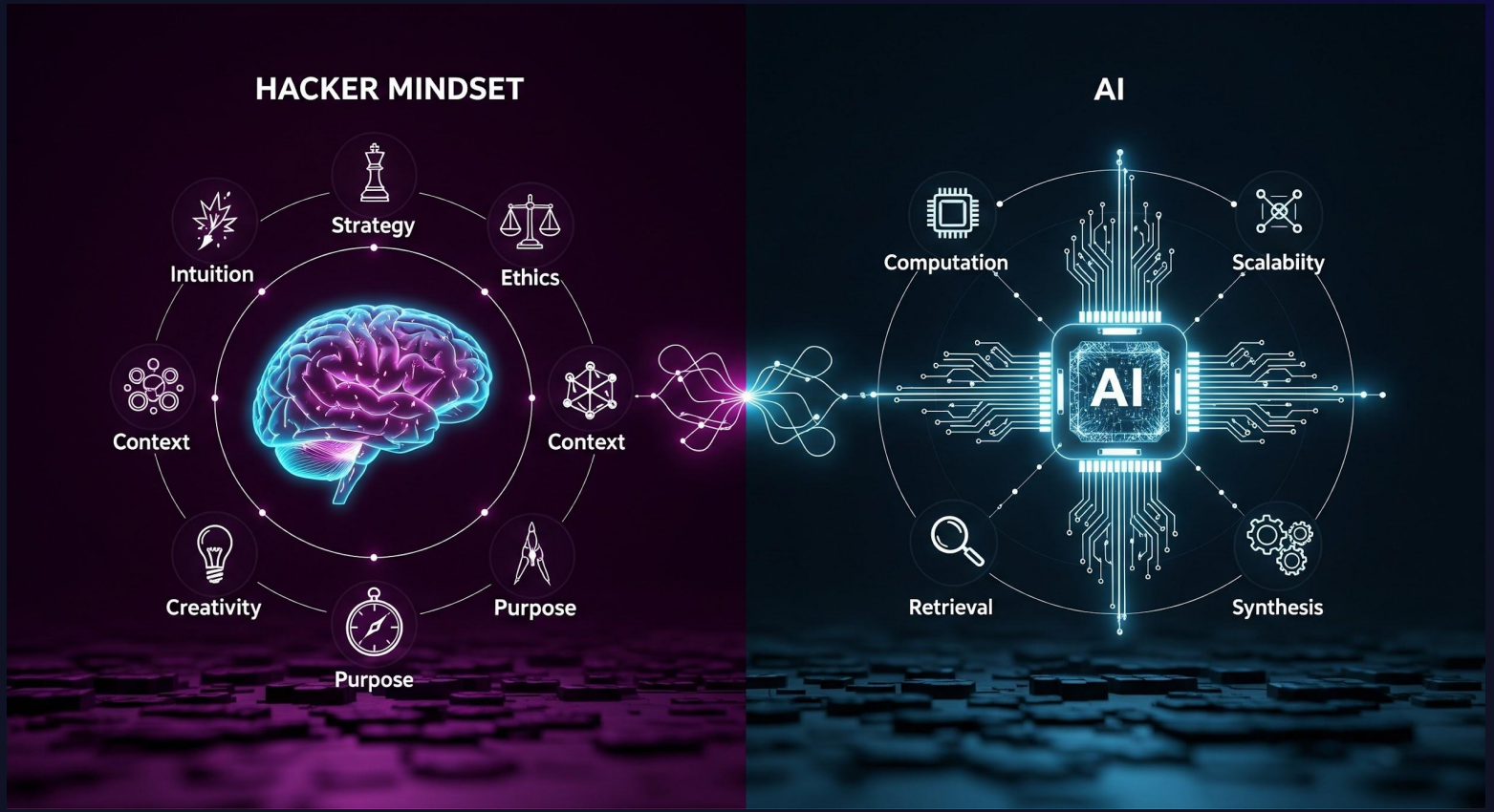
VULNCON

vulncon.in





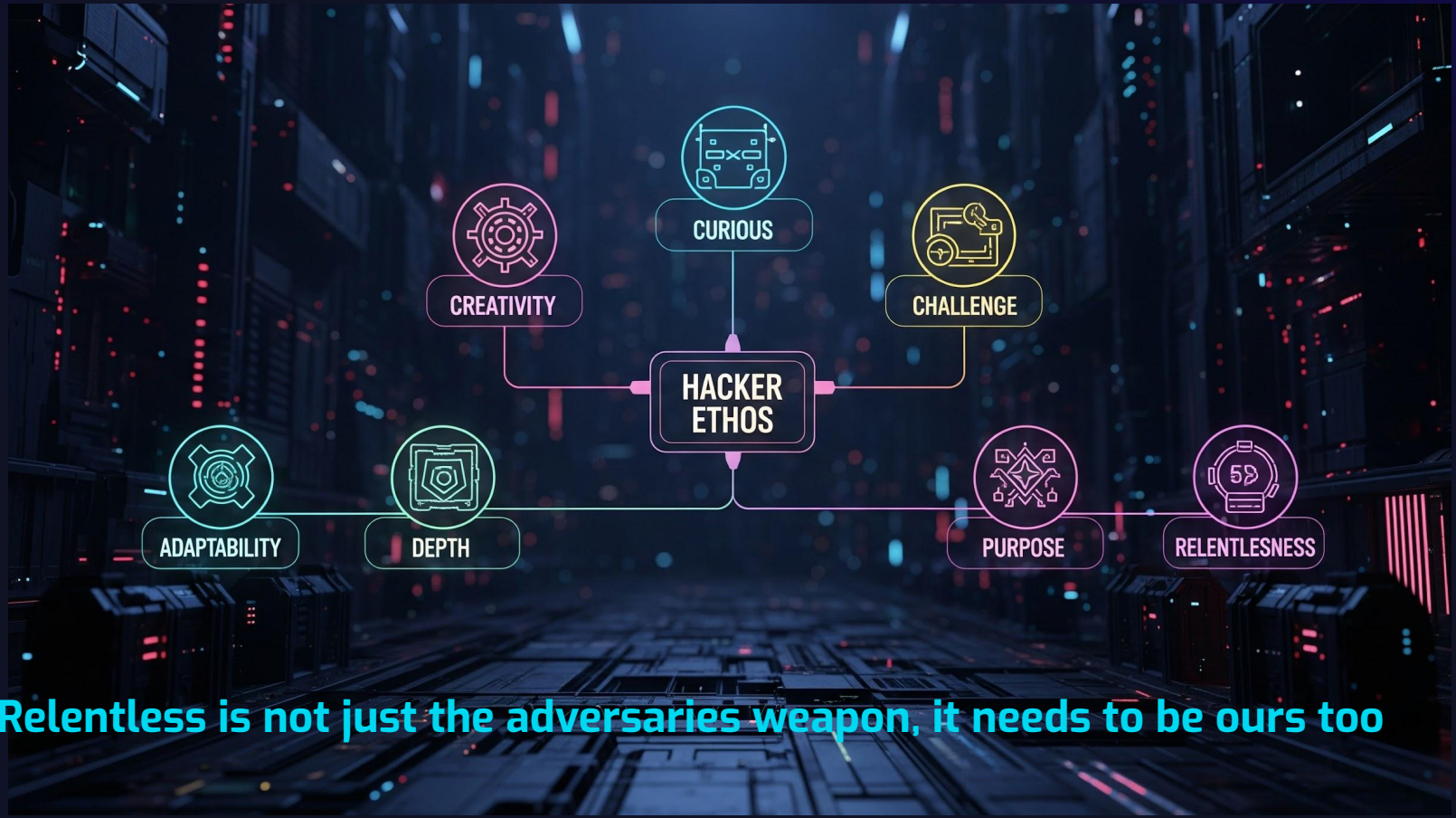



HACKER MINDSET
Strategy
Intuition
Ethics
Context
Context
Creativity
Purpose
Purpose
AI
Computation
Scalabiity
AI
Retrieval
Synthesis

VULNCON

vulncon.in

What comes next is ours to shape


CREATIVITY
CURIOUS
CHALLENGE
HACKER ETHOS
ADAPTABILITY
DEPTH
PURPOSE
RELENTLESSNESS
Relentless is not just the adversaries weapon, it needs to be ours too

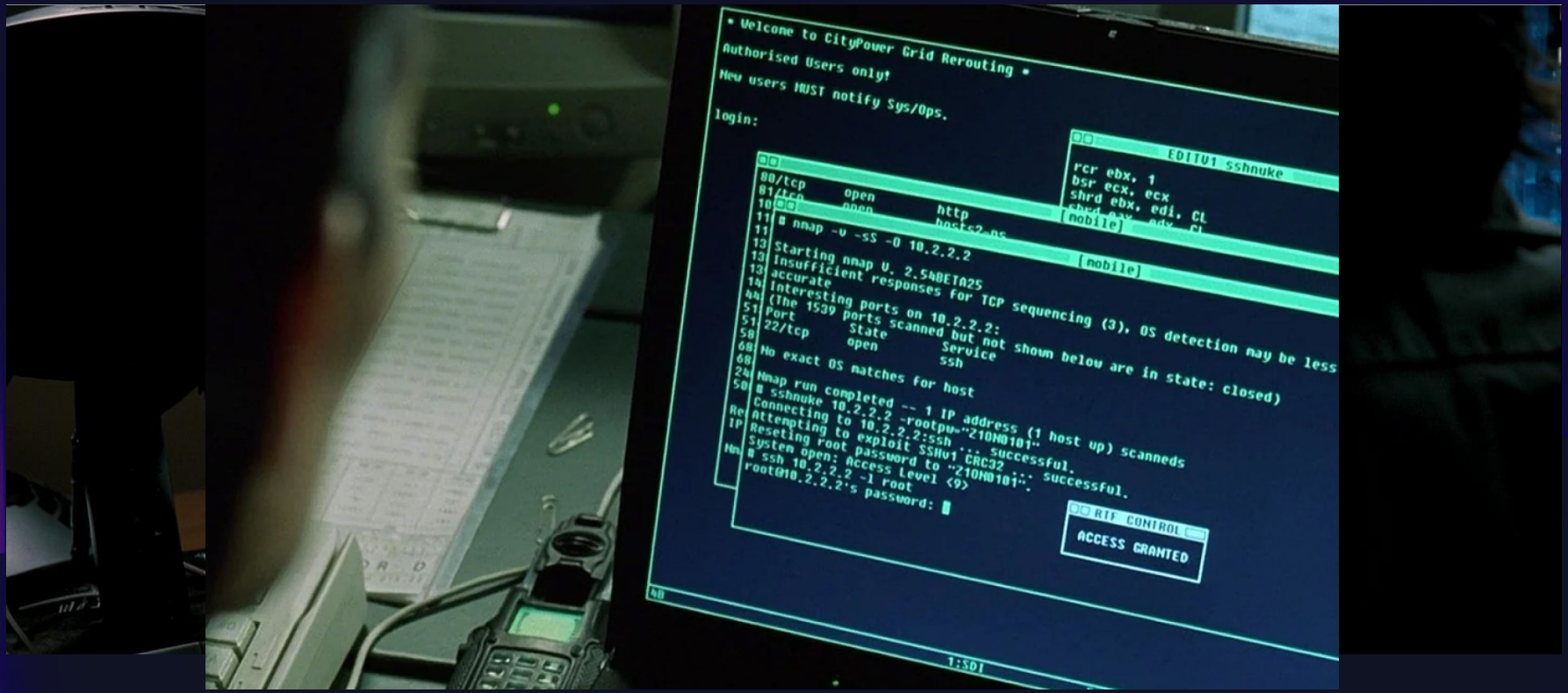
VULNCON

vulncon.in

Day 1
June 14, 2025

Day 2
June 15, 2025

START	END	Talks (JN TATA AUD)	CXO Tracks (Hall A)	VulnX (Hall C)	Workshop (Hall B)	Village
08:00	09:15	Registration				
09:15	09:30	Inaguration & Lamp Lighting				
09:30	10:10	[KeyNote] The Soul of the Hacker by Vicky Ray				
10:15	10:55	Exposing the Unseen: Malware Hunting from the Dark Corners of Memory by Monnappa K A		VulnX CTF		
10:55	11:15	High Tea Break				
11:20	12:00	Reinventing Access Control: Fingerprinting for Credential Protection by Aditya Singh	Security Left, Right, and Center: How Modern Security Teams Bake It In		Building a Kubernetes Breach & Attack Simulation Program From Scratch: A Hands-On Practical Guide by Monty Shyama	
12:05	12:45	The Zombie 'App-ocalypse': Game Theory for Disrupting Dormant and Orphaned Cloud Identities by Joshua Bahirvani	The generation of machine whisperers			
12:45	14:00	Lunch Break				
14:00	14:40	eKYC Crisis: Securing Locker by Kartik Lalan	Product Security Maturity: From Startup to Enterprise			
14:45	15:25	Laughing in the Face of Enterprise Security: Fun-Filled Adventures in Network Pwnage by Manish Tanwar	AI-Powered Threats vs. AI-Powered Defenses: Who Wins the Cyber Arms Race?		Threat Hunting and Detection - How modern data-driven threat hunting is done by Archan Choudhary	Solder & Spark Badge Village by Mohammed Saqeeb Shariff & Karthik Ekanathan
15:30	16:10	IoT's Dark Secret: Uncovering Security Risks in Devices We Trust by Suhash Nayak	Securing AI-Driven Enterprises: Challenges and Strategies			
16:10	16:25	High Tea Break				
16:25	17:05	Sacrificial Lambs of the Internet: How EPP Loopholes and Orphaned Nameservers Led to Widespread DNS Hijacking Vulnerabilities by Devansh Batham	Secure by Design: Embedding Security Across the Software Lifecycle			
19:00	21:45	Cocktail Network Party				


* Welcome to CityPower Grid Rerouting *
Authorised Users only!
New users MUST notify Sys/Ops.
login:
EDIT V1 sshnuke
rcr ebx, 1
bsr ecx, ecx
shrd ebx, edi, CL
[mobile]
nmap -v -sS -O 10.2.2.2
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection may be less accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open ssh
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scanned
sshnuke 10.2.2.2 -rootpw="Z1ON0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Resetting root password to "Z1ON0101".
System open: Access Level (9)
ssh 10.2.2.2 -l root
root@10.2.2.2's password:
RIF CONTROL
ACCESS GRANTED
1:SDI