Modern Defensive Mindset

Who Am I? Mahdi Mirsoltani (MSN_Security)

- +7 years Experience in Cyber Road
- I tried to enjoy the track... ☺
- I Love Data Analysis
- Attending more than 30 cyber incidents …
- I have a good feeling about transferring the modern defensive mentality to the real world.
- And I’m a kind teacher ☹ that’s real? Don’t know

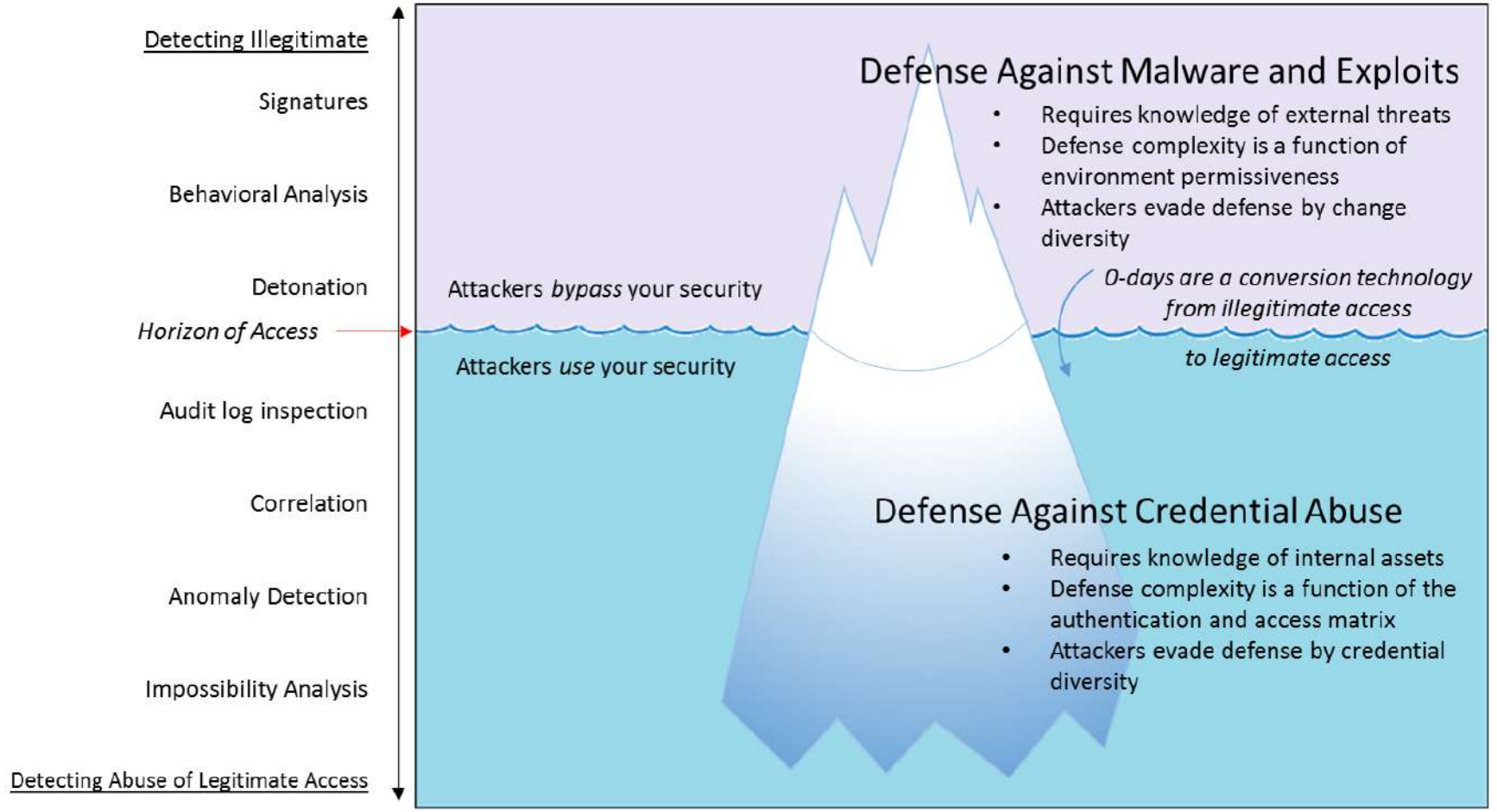
آکادمی راویـــن

Attackers seek to turn illegitimate access into legitimate access

- Your network often provides all the accesses and capabilities the attacker needs — because after all you need to manage the network too. If they obtain your legitimate credentials, they can use the tools and means you have put in place to achieve their goals. So while malware and exploits may play some part in their toolkit, attackers are just IT with different goals.

Assume Breach and Defend Against Abuse of Legitimate Access

By @JohnLaTwC



آکادمی راویـــن

Prevention is the guardian of detection. Prevention creates the whitespace to detect and respond to the most important things.

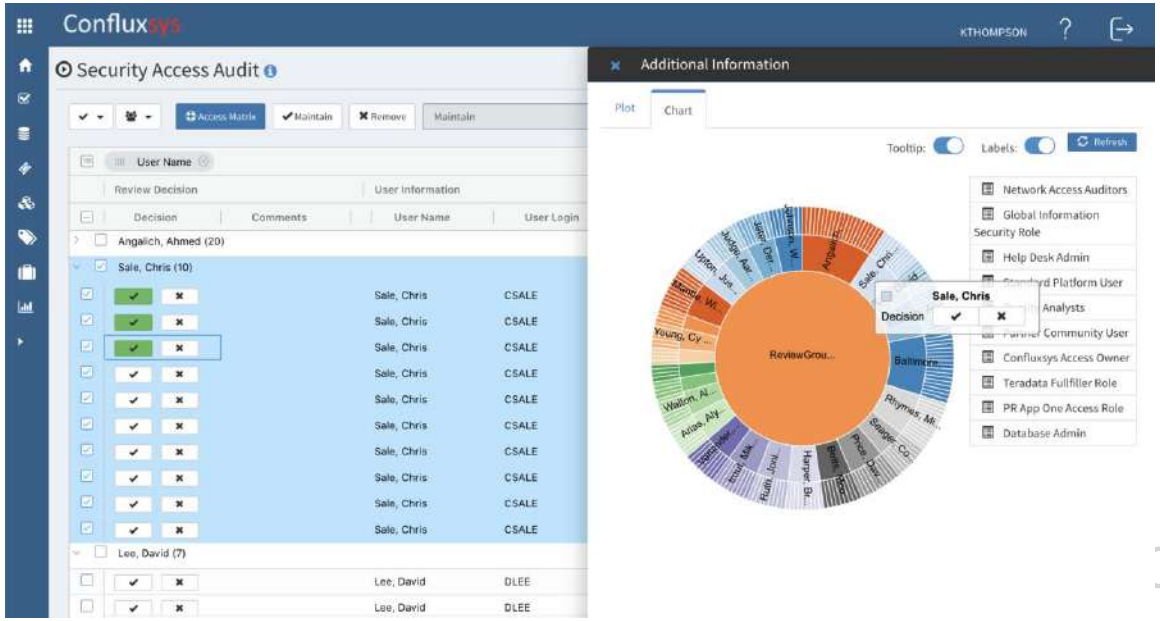
- A point with this one is that it’s easy to get lost and overwhelmed in a noisy network. Your SOC will be flooded with alerts and won’t have the time to find the threats that truly matter. Your prevention approach (whitelisting, asset management, patching, identity management) can lower the noise level and give defenders the whitespace they need.

White space is our friend.

آکادمی راویـن

Biggest problem with network defense is that defenders think in lists. Attackers think in graphs. As long as this is true, attackers win

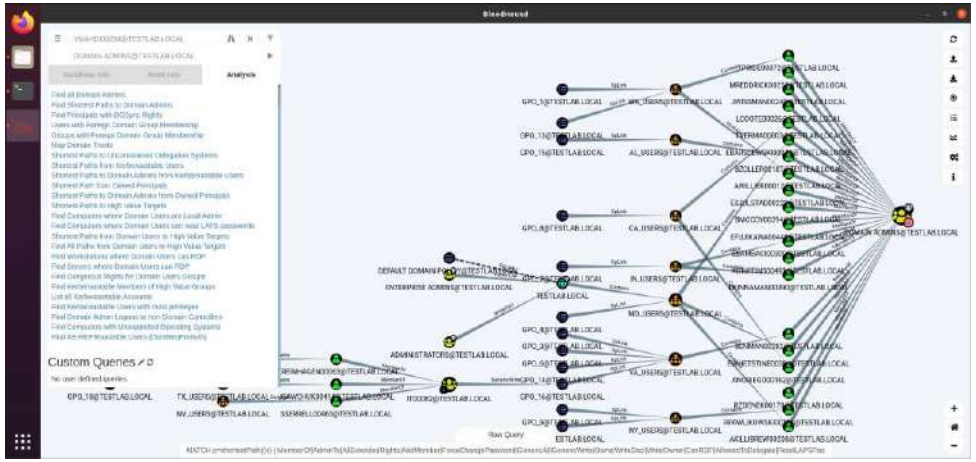
- This is meant as a call to action to defenders to see their network as attackers do — as a set of nodes connected by control relationships and dependencies. Credentials give you access to nodes. Elevated credentials give you power over them. In turn this can unlock additional credentials due to stored credentials on the node or give you control over other nodes due a security dependency. This creates a graph of connectivity.



آکادمی راویـــن

Biggest problem with network defense is that defenders think in lists. Attackers think in graphs. As long as this is true, attackers win

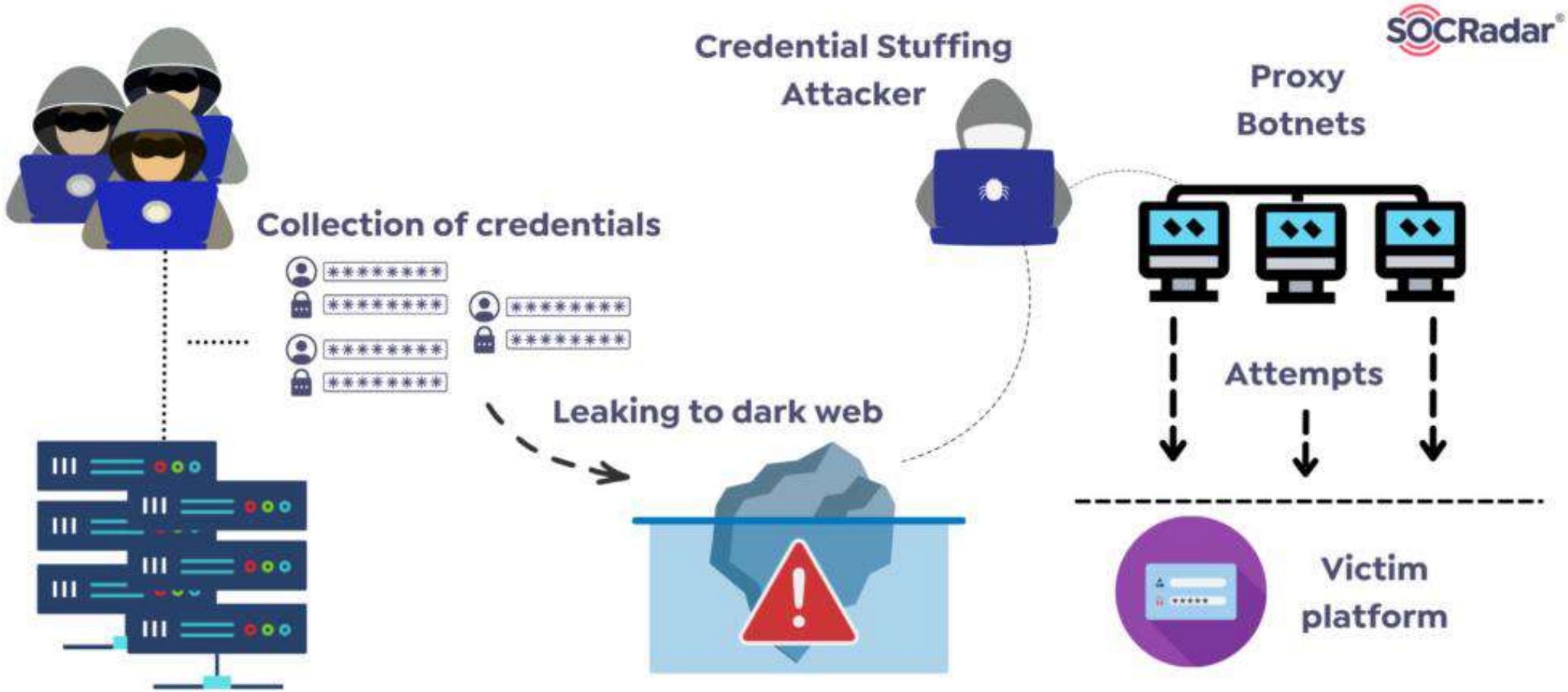
- Attackers land somewhere in the graph by spearphishing or finding an exposed server. Hacking is pivoting around the graph. Exploiting vulnerabilities or obtaining master secrets that allow one to forge identities is tantamount to creating new edges in the graph. While networks can be massive, careful study of a graph may reveal a small number of nodes or credentials that allow dominance over the graph because of the chain of pivots they allow. Tools such as Bloodhound help you do this kind of study.



آکادمی راویـــن

Your network is a directed graph of credentials. Hacking is graph traversal. See the graph or all you'll see is exfil.

- Each host on your network contains a set of credentials that can be stolen from it — credentials in memory, saved in files, stored in browser cookies, and the like. These credentials grant access to other systems. You can model this as a directed graph. Lateral movement is navigating the graph. Dumping credentials gives you more paths to follow. Every time you log onto a host in a way that leaves a credential in memory, you just changed the connectivity of the graph, making it more connected than before. Understand the dynamic nature of this graph, and you'll see a network the way an attacker does.



آکادمی راویـــن

Modern defenders know security controls create attack surface. Beware the attack graph you make practicing InfoSec

- This statement and accompanying infographic and blog are about how IT controls are not made of different stuff than the infrastructure they are protecting. IT management tools and DevOps pipelines are composed of infrastructure themselves. They have accesses, dependencies, credentials, and attack surface themselves.

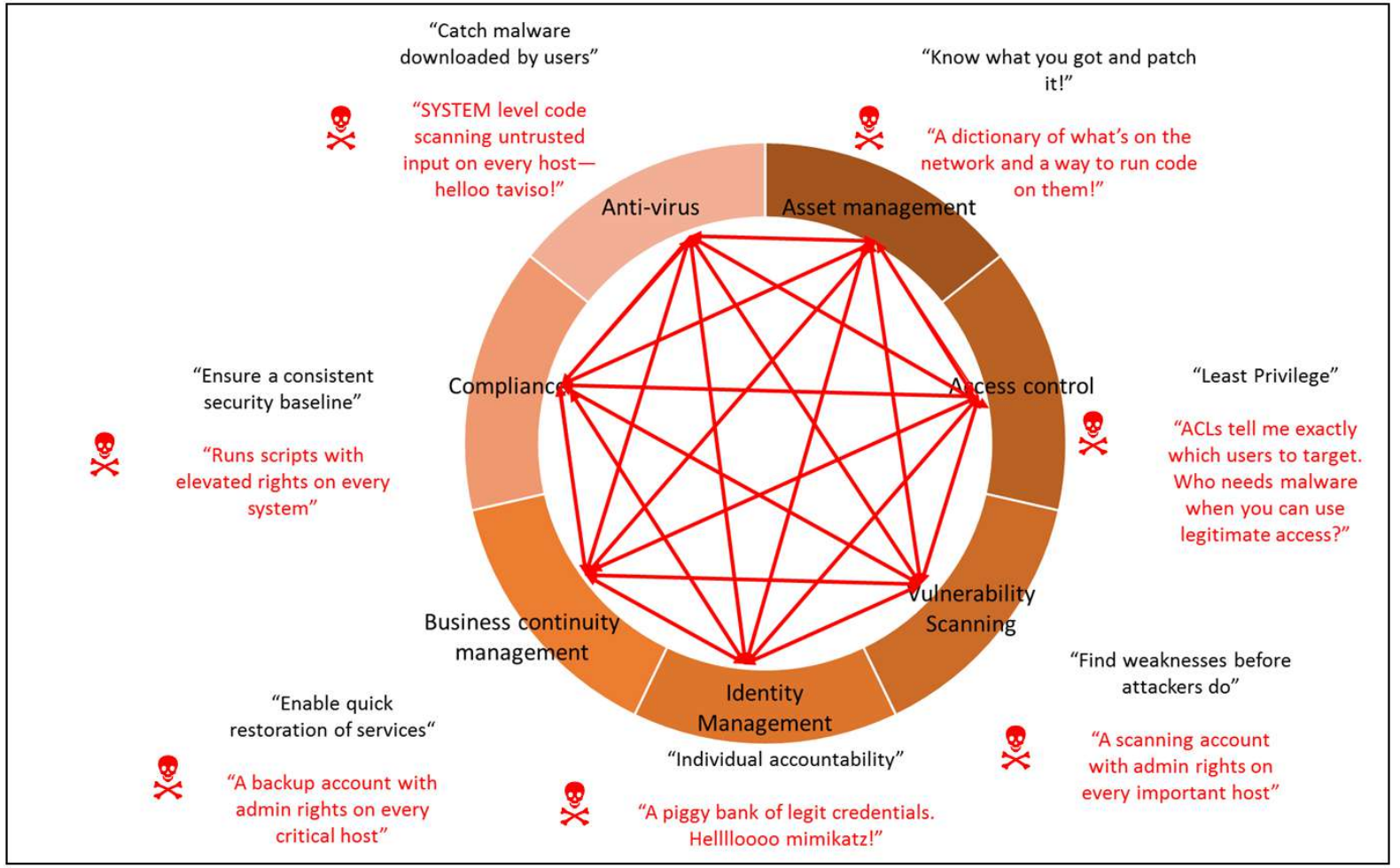
آکادمی راویـن

Beware the Attack Surface of InfoSec by @JohnLaTwC

Traditional defenders see security controls as solving InfoSec problems.

Attackers see security controls as an attack graph of points of compromise.

See Both.



آکادمی راویـــن

A choice of technology is a choice of attack surface

- Technology is not a standalone set of bits or interfaces. It is code that comes from somewhere — a build system, a release pipeline, and a team of developers. Developers make choices about whether the defaults are secure and make changes as the technology goes through its lifecycle. It is hosted on some infrastructure for its consumers. That infrastructure is maintained by someone, often a different organization than the one who built the technology. The dependencies stack up quickly. A point is that there are many controls needed to keep technology secure and it represents an attack surface that must be defended. Each technology comes with its own spiderweb of attack surface. Don’t fear it. Understand it and make informed choices.

What is the most important network security spend: Sensor appliances? SIEM? Threat intelligence feeds? It’s your analyst team.

- It is common to see infosec budgets focus on appliances, threat intel feeds, and tools. There is nothing wrong with that but ultimately those tools are used by analysts. They are the ones investigating alerts. An investigation can hit a point of diminishing returns, but should you instead keep going? These crucial decisions fall to your analysts. Investing in them is not just about salary. I have yet to meet someone in infosec that doesn’t want to improve their skills. Find ways to have them make connections with peers in industry, learn new skill domains they are excited about (reverse engineering, redteam, forensics, machine learning, big data, Splunk). Investing in them means ensuring they have predictable downtime to spend outside of work on their personal pursuits. Create whitespace to allow for projects that need additional time to get traction. Improve the baseline sensor system and environment so they have much better data to work with.

آکادمی راویـــن

If you shame attack research, you misjudge its contribution. Offense and defense aren’t peers. Defense is offense’s child.

- Some thought this tweet was a form of offense worship. Others pointed out that offense and defense co-evolve. My point is that defense starts from a mindset of protecting something (a system or a quality) from abuse or harm. I think it’s very important for defenders to have an attacker’s mindset too, otherwise we can fall victim to thinking that is ignorant of countermove. Defending means thinking about side effects from your defenses — defensive controls have attack surface too. It also means anticipating what the attacker will do next, whether you have a solution for that, and what the work factors are on the offense and defense side to see if you’ve truly moved the needle.

On vulnerabilities: You can argue over exposure, difficulty, and likelihood. Security researchers write exploits because they like the truth.

- Developers can spend a lot of time analyzing bugs to understand if they are truly exploitable. Can an attacker reach this code, is the race condition winnable in practice, is the way something crashes just a nuisance or exploitable? I remember one bug a pentester found in decompression code written in assembly language where the code missed popping a register in an error branch. The dev owner blew off the bug because he didn’t think it was exploitable. That pentester spent the entire weekend to build a working exploit. When analysis is in doubt, exploits are truth.

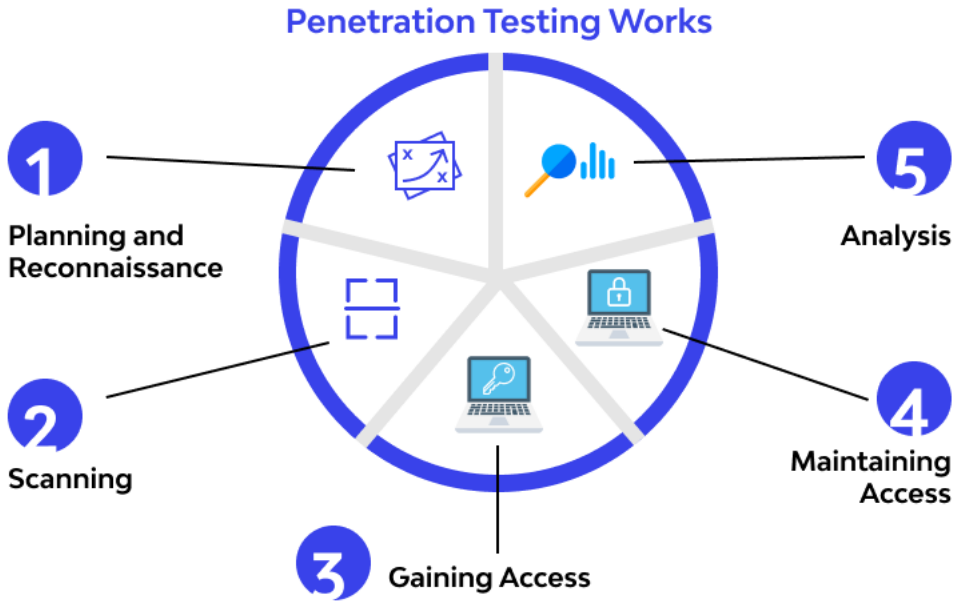
آکادمی راویـن

Defenders, you’re not stopping attacks. You’re increasing attacker requirements. ‘Stopping’ breeds a mindset ignorant of countermoves.

- Here the point is to think about how attackers will respond to your actions. You put up a firewall to block inbound attacks, and they go after endpoints through spearphishing. You deploy whitelisting, and they live off the land with LOLBAS. You deploy multi-factor authentication, and they steal tokens from endpoints that have already authenticated. Prevention is valuable — it raises the bar on many kinds of attacks and quiets the network so defenders have whitespace. But be ready for countermove.

Pentest is the most misused security practice. Pentest is diagnostic. Go from treating the bugs as output, to treating them as input.

- This is lamenting the fact that all too often a pentest is used as either a report card or compliance check-box. Pentest is diagnostic. What's in scope matters. What techniques are tried and applied matters. How findings are characterized matters. Use the results from pentest in a continual improvement program. It's not output — it's input.



آکادمی راویـن

Attackers use your infrastructure. Make it a sensor with event collection. It’s not the bite that makes a spider successful–it’s the web.

- Adversaries enter your infrastructure to pull off their attacks. They obtain your credentials to access systems, perform lateral movement to pivot around nodes, and use your network to take things in and out of it. Select the techniques you’re most concerned about, enable the appropriate event logging and collection at scale, and index it so analysts can perform powerful queries and write rich detections. Locard’s exchange principle is “every contact leaves a trace”. Your magnifying glass is a query prompt. Turn your network into a set of microphones wired to floodlamps.

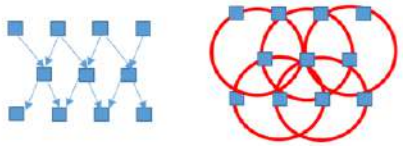
آکادمی راویـن

Adversaries need credentials more than malware. Deny them by avoiding the sins of Windows credential administration.

Sins of Windows Credential Administration

Sins of Mirror Imaging

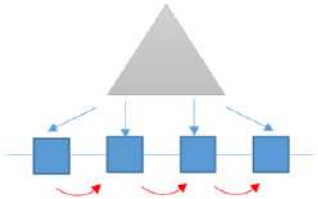
Seeing the network the way you manage it versus how an attacker sees it



Admins operate in the realm of the manageable and attackers operate in the realm of the possible

Sins of Abdication

Failing to manage local accounts



Local logons have no visibility to a domain controller and credentials rarely expire

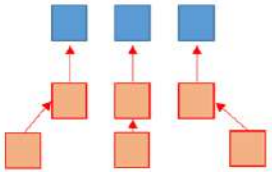
Sins of Tradeoffs

Excessive credential lifetime to reduce service interrupts

Your attackers appreciate credential longevity even more than your end users

Sins of Incompleteness

Securing servers but not the admin workstations or other security dependencies



Your network is not a list of assets but a directed graph of credentials and logon rights

Sins of Wishful Thinking

Being enamored on 2FA but forgetting:

$$\lim_{OS<Win10} mimikatz(2FA) = 1FA$$

Single sign on converts 2FA authentication into a single factor which can be dumped and reused

Sins of Hygiene

Failing to securely store credentials

آکادمی راویـــن

WHEN IS CYBER DEFENCE TRADITIONAL?

When firewalls started being deployed you didn’t just deploy a tool. You also introduced the goal of keeping threats out of your systems. Virus scanners reinforced that idea and with that, the concept of traditional cyber defense was born: create a hard shell around the perimeter of your network and keep threats out. Within traditional cyber defense there is no place for the notion that your system might get compromised.

آکادمی راویـن

WHY IS TRADITIONAL CYBER DEFENSE NO LONGER SUFFICIENT?

Attackers have changed and adapted. They no longer focus on exploiting vulnerabilities in the lower half of the OSI model but have started to abuse the top half very successfully. Most attacks nowadays start with exploiting application vulnerabilities and social engineering, instead of directly targeting your network stack. A firewall can’t distinguish TCP packets containing valid mail from TCP packets containing phishing mail. Nor can it detect that the end-users are less tech-savvy than the CTO imagined.

آکادمی راویـن

@ravinacademy