RED TEAM MINDSET

Uri Fridman – uri@digitalopsgroup.com

TODAY

ATTACKERS BYPASS THE MOST PARANOID SECURITY MEASURES.

Information is being extracted.

In most cases attackers leave without the target ever knowing they were there.

RED TEAMS

A red team is a group of highly skilled people that continuously challenge the plans, defensive measures and security concepts.

These exercises result in a better understanding of possible adversaries and help to improve counter measures against them and future threats.

A **RED TEAM** views a problem from an **ADVERSARY** or attacker's **PERSPECTIVE**

“There is no such thing as perfect security. Attackers get smarter and change tactics all of the time.”

ADAPTABILITY

THE MINDSET OF AN ATTACKER

ADVERSARIES DON'T PLAY BY THE SAME RULES; IN FACT THEY DON'T HAVE RULES AT ALL. THEY ADAPT.

In the scary cases, the attacker is a focused adversary who is looking to steal sensitive data or maintain a strategic foothold.

“Red Teaming Law #11: The superior red teamer discerns webs of perception, intent, and effect; others just see a cigar. Of course, ‘sometimes a cigar is just a cigar’ (or is it?)”

RED TEAM JOURNAL LAWS
(http://redteamjournal.com/red-teaming-laws/)

SITUATIONAL AWARENESS

LOOKING AT THE PROBLEM FROM THE ATTACKER'S SIDE

SOMETIMES ALL IT TAKES IS A LOW-TECH APPROACH TO DEFEAT A HI-TECH PROBLEM.

Adversaries can exploit any and all known attack vectors. They will also create new ones. attackers are very creative.

WHAT IS THE REAL WEAK LINK?

SOCIAL ENGINEERING

“Amateurs hack systems, professionals hack people.”

BRUCE SCHNEIER

THINKING

Just thinking like a security conscious person won't do. We need LINEAR THINKING combined with LATERAL THINKING and RIDICULOUS THINKING.

Having an understanding of who the adversary is and how it might exploit the security holes will make the organization better.

Reacting security is not the ideal security posture; instead be proactive, try to go 2 or 3 moves ahead of him. Place detection and deception measures. Make a future attack harder.

SOFTWARE VULNERABILITIES

PLEASE NOTE

PATCHED ≠ SECURE

DESIGN VULNERABILITIES

A word about “OPSEC” & “OSINT”

OPSEC & OSINT

When people brag, OPSEC goes out the window. OSINT is your friend. spend time developing good OSINT prior, during and after an operation.

FOLLOW THE OPSEC RULES FOR YOUR TEAM (SEE NEXT SLIDE)

OPSEC RULES

1- Never reveal your operational details
2- Never reveal your plans
3- Never trust anyone
4- Never confuse recreation with work
5- Never operate from your own safe house / HQ
6- Be proactively paranoid, it doesn't work retroactively
7- Keep your personal life and work separated
8- Keep your personal environment free of work related stuff
9- Don't give anyone power over you
10- ALWAYS VERIFY!

THE PROBLEM WITH LACK OF OPSEC:

ROBIN SAGE

THE MOST IMPORTANT CONTROL IS…

Wait for it…

US

INTELLIGENCE-DRIVEN SECURITY IS THE NEW BLACK

INTELLIGENCE-DRIVEN ATTACKS THEN, ARE THE NEW WHITE

“Develop the situation. Don't let the situation develop itself.”

PETE BLABER: THE MISSION, THE MEN AND ME

LEARN FROM ATTACKS THAT DIDN'T WORK

DIGITAL SITUATIONAL AWARENESS

Identify patterns that link individual to systems to networks to the full target.

BLEND IN.

Create false trails. Develop a noisy attack and let the target follow it. Have a secondary stealthy one ready to perform the attack.

UNDERSTANDING HOW THE ATTACKERS THINK IS KEY

“7 P’s: Proper Planning and Preparation Prevents Piss Poor Performance.”

DRY RUNS

Perform dry runs. Built a simulated environment as close to the target's as possible.

Dry runs will show you in most cases what could work and what might not. Have contingencies for everything.

Remember PACE:

Primary, Alternate, Contingency, and Emergency.

TOO PARANOID?

THANK YOU

CONTACT: URI@DIGITALOPSGROUP.COM