PENETERATION TESTING AND RED TEAMING

شرکت ارتباط گستر خاورمیانه

خدمات پر کاربرد OFFENSIVE SECURITY

- Vulnerability Scanning
- Vulnerability Assessment
- Peneteration Testing
- Red Team and Adversary Emulation

Vulnerability Scanning

- رویکرد کلی : اسکن اتوماتیک Assetها (با استفاده از ابزار)
- هدف : شناسایی آسیب پذیری های شناخته شده ی قبل و بعد از احراز هویت
- پیاده سازی : کاملا ابزار محور
- کانون توجه : ضعف های امنیتی تکنولوژی ها تنظیمات و سرویس ها
- تناوب : هفتگی یا ماهیانه

Vulnerability Assessment

- رویکرد کلی : بررسی اتوماتیک و دستی همه ی Asset ها برای شناسایی ضعف های امنیتی
- هدف : شناسایی همه ی ضعف های امنیتی Asset های درون Scope
- پیاده سازی : ۳۰٪ ابزار محور و ۷۰٪ نیرو محور
- کانون توجه : بررسی ها عمیق تر و معمولا شامل بررسی سیاست ها و رویه های سازمانی
- تناوب : سالیانه و یا برای دریافت گواهینامه

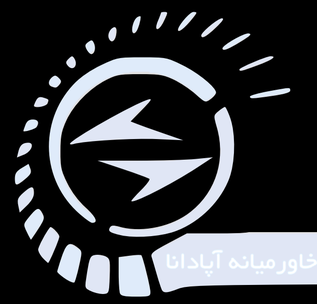
Peneteration Testing

- رویکرد کلی : شبیه سازی تکنیک های مورد استفاده توسط مجرمان سایبری برای شناسایی و expliot کردن ضعف های امنیتی در محیط کنترل شده برای شناسایی ریسک ها و تاثیر حملات موفق
- هدف : گزارش همه ی ضعف های قابل exploit در محیط کنترل شده
- پیاده سازی : ۱۰٪ ابزار محور و ۹۰٪ نیرو محور
- کانون توجه : تایید وجود ضعف های امنیتی و مشخص کردن عواقب exploit کردن این ضعف ها
- تناوب : سالیانه

Peneteration Testing Stages

Red Teaming

- روکرد کلی : شبیه سازی تکنیک ها تاکتیک ها و روندهای اجرا شده توسط دشمن سایبری
- هدف : بهبود عملکرد blue team
- پیاده سازی : نیرو محور با کمک گیری از بعضی ابزارها
- کانون توجه : بهینه سازی سیاست های Detection and Response تیم Blue
- تناوب : new exploit, tool or TTP



فلسفه ی Red Teaming

- راهی برای ورود به شبکه توسط نفوذگر پیدا خواهد شد.
- این روش ها معمولا از تکنیک های social Engeenring کمک می گیرند
  - Email (phishing), Social Media, In Person
- سیستم ها و فرایندهای فعلی سازمان چقدر در کشف رد پای نفوذگر در شبکه ی داخلی موفق هستند ؟

The Cyber Kill Chain by Lockheed Martin®

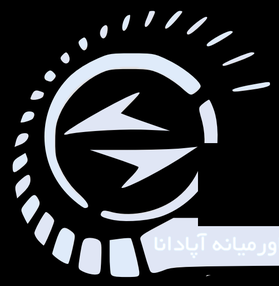
تکنیک های پنهان سازی

- استفاده از پروتکل ها و وسایل ارتباطی که خود کاربران شبکه نیز از آن استفاده می کنند :

- smb (TCP/445)
- WMIC (135 and higher)
- RDP (3389)
- SSH(22)
- VNC
- Windows Remote Management (5985)
- Powershell
- ICMP

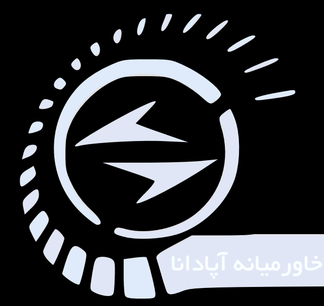
چالش های Red Teaming

- Anti Virus or internet Security Software
- Application Whitelisting
- Active Defense
- Security Awareness



ابزارها مورد استفاده :

- ابزارهای Open Source
- Metasploit, Empire, Pupy, Open Vas, NMap, Maltego ....
- ابزارهای Comercial
- NESSUS ,Cobalt Strike ,Core Impact, NetSparker, AppScan, CANVAS ...
- ابزارهای اختصاصی



پایان

شرکت ارتباط گستر خاورمیانه