Global Information Assurance Certification Paper

Secure
Remote Desktop
And
Remote Desktop Web Connections

By
Joshua Bruch

GSEC Practical Assignment
Version 1.4b Option 1

February 8, 2004

Abstract

Many companies are turning to Microsoft's Remote Desktop (RD) as a way to provide remote administration of their Windows XP desktop environment. Whether your role is Systems Administrator, Tech Support, Help Desk or End User you can benefit from this tool. Microsoft has taken steps to ensure the security of Remote Desktop, but there are additional steps that need to be taken to ensure the security of your organization when using RD at an enterprise level. This paper does not provide step-by-step instructions on how to install and configure RD though an overview of the technology will be presented. It is intended to be a good reference for security issues surrounding the use of RD in a corporate environment. I will also cover some of the tools out there to help audit your systems to assist in a higher level of security. This paper will end with a checklist for the security conscious Systems Administrator who is looking to deploy Windows XP with Remote Desktop enabled.

The Remote Desktop and Remote Desktop Web Connection Overview

Remote Desktop and Remote Desktop Web Connection make Windows XP Microsoft's most versatile platform to date. These technologies use the Remote Desktop Protocol (RDP) version 5.1, which is the same protocol used in Windows 2003 Terminal Services. RDP operates over TCP/IP port 3389 by default. RDP only transmits keystrokes, mouse movements and display output data[1]. I will briefly discuss each of these two technologies and then highlight some of their most glaring strengths and weaknesses from a security standpoint. These are things a Security Manager, System Administrator, or Power User will want to know.

Remote Desktop

Remote Desktop uses the same technology found in Windows 2003 Server Terminal Services using the RDP 5.1 protocol to transmit keystrokes, mouse movements, and display readouts. Remote Desktop (RD) is more limited than Terminal Services in that it only allows one connection at a time. A few useful purposes for RD include Help Desk support and support for the telecommuter.

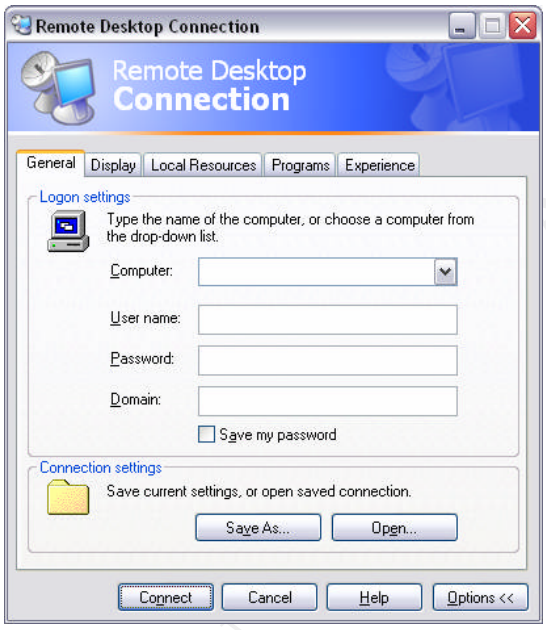
For Help Desk support, this native Windows technology replaces the need for third party software such as PC Anywhere[2], Remotely Anywhere[3], Radmin[4], and

[1] Windows XP Professional Resource Kit, Part 2, Chapter 8.
[2] PC Anywhere can be found at www.symantec.com.
[3] Remotely Anywhere can be found at www.remotelyanywhere.com.
[4] Radmin can be found at www.radmin.com.

VNC[5] to name a few. In some cases RD also provides more functionality and greater security than third party vendors can provide. Remote Desktop allows Help Desk associates to connect to the target machine, see the errors their users see, make configuration changes or resolve the errors and then disconnect. Connections are encrypted and access is restricted to a local security group on the target computer.

Support is provided for the telecommuter because of their need to connect over slower dialup connections yet still be able to use their main applications. The lightweight RDP protocol allows the telecommuter to run those applications on their desktop back on the corporate LAN; only the display readout get transmitted over the slow connection thus saving time in having to download, for example, large amounts of email[6].

Remote Desktop is disabled by default and is fully configurable through Windows Group Policies. The connection is initiated by the remote user. There are two ways to connect. One requires the Remote Desktop Connection (RDC) client seen on the left. This comes with Windows XP Home or Professional CD or can be downloaded for free from Microsoft. You can also install the RDC client on Windows 98, ME, NT and 2000. The other way to connect is via the Remote Desktop Web Connection discussed in the next section. Once you have the RDC client all you need is a valid username and password to gain access to the desktop. Once connected the remote user has complete control of the desktop. With the RDC client the remote user's printers and disk drives can be brought through to the target machine. Files can be copied and pasted from the remote user's machine directly into the remote session; and audio can be brought through as well.[7] Let's look at some of the strengths and weaknesses of this technology from a security standpoint.



Strengths

- Data is sent encrypted. By default 128 bit encryption is used for all connections. This includes the sending of usernames and passwords. 128-

[5] VNC can be found at www.realvnc.com.
[6] Russell, Tuning Remote Desktop.
[7] The Features of the Remote Desktop Client in Windows XP.

bit encryption is important because 56 bit encryption is generally considered not secure as the amount of time to break 56 bit encryption can now be counted in minutes.[8] Legacy Terminal Services clients that don't support 128 bit encryption can try to connect to RD at a lower encryption level but they will not be allowed to connect unless the user specifically sets the encryption level to Client Compatible. This setting will negotiate the highest level possible.

- In addition to Administrators, remote access can be granted to users put in the Remote Desktop Users group. This is a local group on the computer used to allow non-Administrators access to the desktop remotely. This is particularly useful for the telecommuter who needs remote access to their desktop but who is not in the local Administrators group due to the company's security policy of no users in the local Admin group.

- Only one session can access the desktop at a time. This is a security strength since you know if you are working on the desktop, then no one else is. Microsoft Knowledge Base Article 280828[9] explains what happens when someone tries to connect to your machine while you are logged in.

- Local console session is shut down when someone is connected remotely. RD disables display of the session on the computers monitor and disables input via the local keyboard and mouse.[10] This is important because you never know who could be sitting at the computer while you are remoted into it. Imagine Sally sitting at the monitor watching you remotely read email *about* Sally for example.

- Port number that RDP uses can be changed. The default is 3389. Keeping it the default would allow people snooping around to be able to more easily find your Remote Desktop enabled Windows XP workstation.

- RD can be configured through Group Policy. Group Policies enforced at the domain level help ensure a base level of security. Users won't be able to weaken security by making there own Remote Desktop configuration changes.

Weaknesses

- Remote Desktop does not support certificates. Certificates enable the users and computers to prove their identities to each other. This would protect you from connecting to a hacker's computer which is impersonating your own. This would also protect your computer from dictionary-based or brute force

[8] Silverman, A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths
[9] How a Remote Desktop Connection Affects Windows XP Professional.
[10] Windows XP Professional Resource Kit, Part 2, Chapter 8

password cracking since your computer would be expecting private key encryption instead of a simple alpha-numeric password.

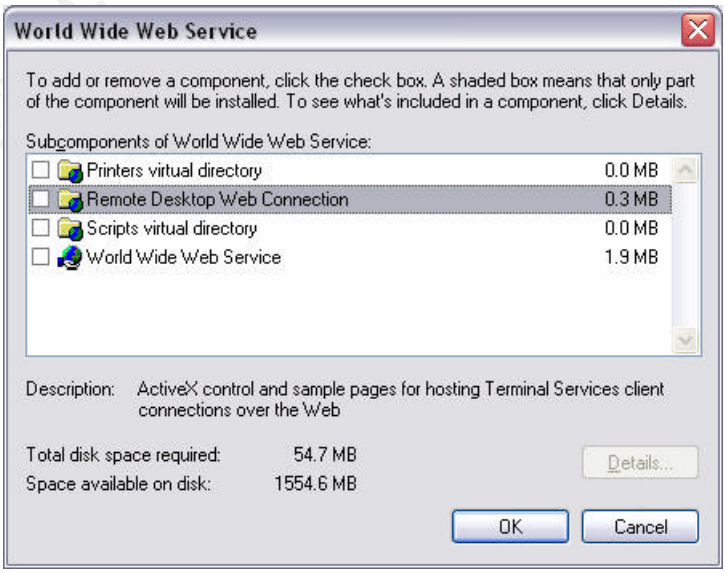
- Locks out session after 6 bad username\password attempts. This sounds like a strength until you look a little closer. Upon entering the 6th bad password, the console window closes. You are then permitted to immediately open another session and keep trying though. There is no lockout period. But, at least the 6th bad password attempt wrote a warning in the Security Log, right? Wrong. The only entry is an Information alert in the Application log, which blends right in with the hundreds of other Information alerts found there. Why not write a password guessing tool that guesses 5 passwords at a time that opens a new session each time? No one would ever know of the attempted intrusion. These tools exist and are covered later in this paper.

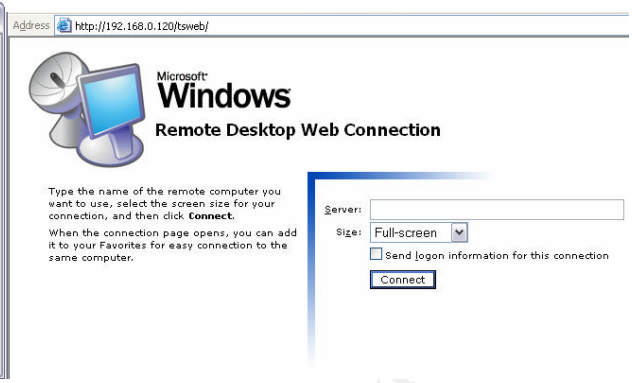
Be sure to read the Defense Checklist at the end for many steps to help increase security of a Remote Desktop environment.

Remote Desktop Web Connection

An alternative to the Remote Desktop Client is the RD Web Connection. This allows anyone with Internet Explorer 5 or later to connect to a Remote Desktop enabled computer.

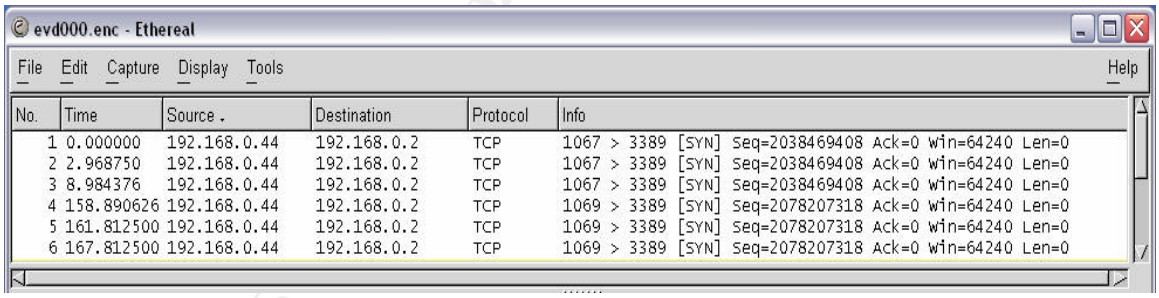
You must have access to a Windows 2003 server or a Windows XP computer with IIS installed in order to initiate the connection. As you can see here, Remote Desktop Web Connection is not installed by default in IIS. Once installed you connect to the http server by point you browser to http://*servername*/tsweb. This will download the Remote Desktop Active X control seen below.





Once the Active X control is installed you are presented with the web page on the right. Enter in the name or IP address of the target machine and off you go. Keep in mind that the IIS server never touches the Windows XP computer. All IIS does is download the Active X control to your computer. When you enter the Windows XP computer name or IP address you connect directly from your remote machine to the target machine. This is done over RDP port 3389 just like any normal Remote Desktop connection.

To show this I initiated a remote connection using the RD Web Client to connect to a target machine which had a Black Ice firewall running (www.iss.net). The firewall log is shown below. (Log viewed in Ethereal – www.ethereal.com) You can see the packets from my 192.168.0.44 remote pc destined for port 3389 on the 192.168.0.2 target machine. There are no entries for the web server.



This proves that even though you connect to the IIS server to initiate the Remote Desktop Web Connection, the IIS server is doing nothing more than redirecting your RDP connection to the target machine.

Strengths

- All of the strengths and weaknesses from the Remote Desktop Client section apply to this section as well.

- One added benefit is that since you must connect to the IIS server first, you can secure http://*servername*/tsweb with SSL and require authentication.

This adds another layer of security since you can restrict access to the site to whoever you wish.

- Even though RD Web uses HTTP port 80 traffic to access the initial Remote Desktop Web Connection page on IIS, the RD Web client still uses port 3389 to connect to the target machine. This means that RDP traffic can still be restricted at the firewall by blocking inbound port 3389.

Weaknesses

The same weaknesses mentioned in the Remote Desktop Client section apply here.

Free internet tools to be weary of…Oh, I mean…

Auditing Tools

The internet is a wonderful and scary place. These are some of the tools that can be downloaded for free from the internet to help you test your network for rogue Remote Desktop activated computers as well as testing the strength of passwords. These tools will also work for Terminal Servers. The first 2 tools are ProbeTS and TSGrinder available at www.hammerofgod.com.

ProbeTS

This tool is used for finding rogue Remote Desktop enabled devices on your network even if the default port was changed from 3389.

> ProbeTS will scan a full C-Class for you to determine if terminal services are being offered up regardless of what port is actually being used. [11]

Some catches here that make is more of an auditing tool and less of a hacking tool are that you need to be able to use RPC and you have to be in a group allowed to access the box via Remote Desktop. This would be Administrators or those in the local Remote Desktop Users group. An attacker would already have to be on your LAN with an Admin password to really be able to use this tool.

TSGrinder:

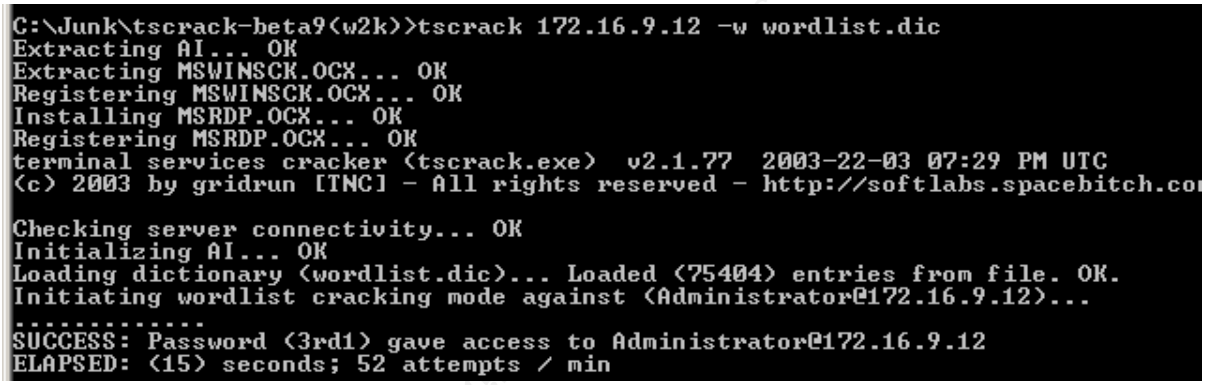
This tool claims to be the first Terminal Server brute force tool. And remember, Remote Desktop is based on Terminal Server technology. It takes advantage of the fact that the computer's local Administrator account cannot be locked out.

[11] Hammerofgod.com.

Remember how mentioned earlier that you can have up to six incorrect logon attempts before a log entry is made. Well this is the tool that guesses five times and then opens a new session to continue guessing with out a log entry. [12] It also claims to be not detectable by Intrusion Detection Systems since the logon process in encrypted.

TSCrack

Like TSGrinder, TSCrack uses word lists to guess passwords. It is available for free at http://softlabs.spacebitch.com/tscrack/. By default it tries to guess the Administrator password, though you can tell it to use whatever you like. Like TSGrinder it attempts five passwords before opening a new session to continue guessing. I used TSCrack to guess the password of a test computer and the results are seen below.



I gave the Administrator the password of "3rd1", which was on the word list I provided for TSCrack to use. It took 15 seconds at an average rate of 52 attempts per minute.

Defense Checklist

- Ensure Windows XP has the latest Service Pack to patch known vulnerabilities like Remote Desktop Denial of Service (DoS) attacks.[13]
- Apply all post SP1 patches as well to fix known issues such as Remote Desktops "Checksum" and "Keystroke" vulnerabilities.[14]
- Change the local Administrator's account name to something other than Administrator. Also adopt a policy for complex passwords that have a mixture

[12] Mullen & Russell, TS Grinder Black Hat USA 2003 Briefing.
[13] Securiteam.com, Microsoft Windows XP Remote Desktop Denial of Service Vulnerability.
[14] Cohen, Microsoft Windows Remote Desktop Protocol Checksum and Keystroke Vulnerabilities.

of upper and lowercase letters and numbers. Both of these steps will help protect against automated password-guessing brute force tools.

- Change the port RDP listens on. Steps to do this can be found are in Microsoft's Knowledge Base Article 306759[15]. Basically, you use Regedit and navigate to the key below and then change the value to some other unused port number.

  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp\PortNumber

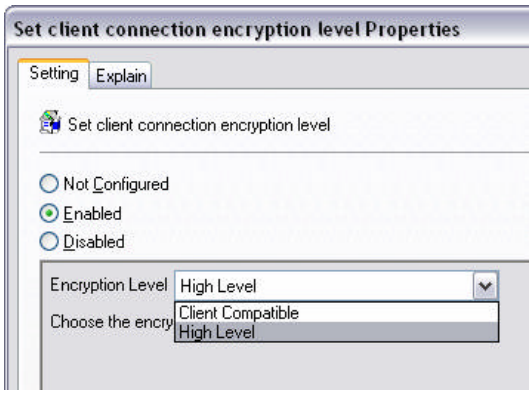
- Do not allow 3389 inbound on your corporate firewall. If you need to allow RDP in consider changing the port as mentioned above and then restrict the RDP access to the particular IP address that you need to connect to. Another alternative to opening a firewall hole for RDP would be to configure a Virtual Private Network (VPN) tunnel into you network and gain Remote Desktop access that way.

- If your Windows XP computer is connected directly to the internet, you should turn on your Windows XP Personal Firewall:

  > In the **Network Connections** window, right-click the connection through which you will use Remote Desktop, and then click **Properties**. Click the **Advanced** tab, and then select the checkbox for **Protect my computer and network by limiting or preventing access to this computer from the Internet**. Click the **Settings** button. In the **Services** list, select the checkbox for **Remote Desktop**.[16]

- Configure a domain Group Policy to enforce a secure Remote Desktop standard. Important setting:

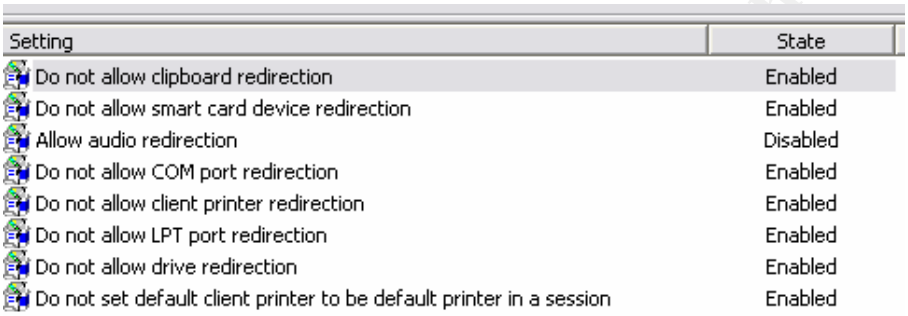
  - Enforce 128 bit encryption. If you have legacy Terminal Service clients that don't support 128 bit encryption and they need to connect to Remote Desktop, you should replace them with the new Remote Desktop client.



[15] How to Change the Listening Port for Remote Desktop.
[16] FAQ About Remote Desktop.

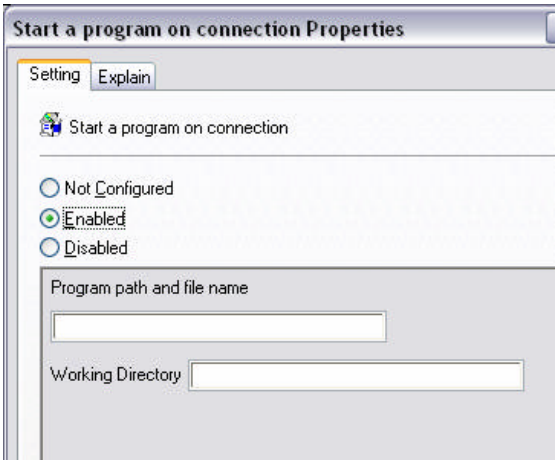
- Enable “Always prompt client for password upon connection”. This will force users to log onto the computer after the Remote Desktop connection has been established. People who have the unsafe habit of checking that box to Save Password on their Remote Desktop Connection screen would still have to enter their password with this policy enabled.

- The following options are normally configured by the client when they establish their connection. These Group Policies allow system administrators to control exactly what a user can and cannot do.



*When working with Group Policies pay close attention to the wording of the policy. The above picture shows the most secure policies, yet the third item down says Disabled. This is because the decision to choose Disabled or Enabled depends on whether the policy begins with “Allow” or “Do not allow”. Just take you time.

- This setting creates a single purpose Remote Desktop connection. It allows access to only the application you choose here by starting that application automatically when the session starts. The session is then disconnected when the application is closed. This means that the Start Menu and Desktop are not accessible to the remote user.



- When using the RD Web Client think about using the extra layer of security provided by SSL and authentication on the IIS server.

Conclusion

In conclusion, Remote Desktop and Remote Desktop Web Client are becoming more and more popular to meet the remote control needs of corporate IT and the telecommuter. Microsoft has taken good steps to ensure security of this technology documented above by its many strengths and few weaknesses. Nothing is ever 100% secure, but having an understanding of the technology, using what tools are available for auditing, and following a defense checklist will help you make your environment as secure as it can be.

References

Windows XP Professional Resource Kit, Part 2, Chapter 8. Microsoft Products and Technologies. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/prork_overview.asp?frame=true (2 Feb. 2004)

Russell, Charlie. Tuning Remote Desktop. URL: http://www.microsoft.com/windowsxp/expertzone/columns/russel/august27.asp (2 Feb. 2004)

The Features of the Remote Desktop Client in Windows XP. Microsoft Knowledge Base Article – 300698. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;300698 (2 Feb. 2004)

Silverman, Robert D. A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths. April 2000. URL: http://www.rsasecurity.com/rsalabs/bulletins/bulletin13.html (6 Feb. 2004)

How a Remote Desktop Connection Affects Windows XP Professional. Microsoft Knowledge Base Article – 280828. URL: http://support.microsoft.com/default.aspx?kbid=280828&product=winxp (3 Feb. 2004)

HammerofGod.com. Downloads and Stuff. URL: http://www.hammerofgod.com/download.htm (4 Feb. 2004)

Mullen, Timothy M. & Russell, Ryan L. TS Grinder Black Hat USA 2003 Briefings and Training. July 2003. URL: http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-mullen.pdf (4 Feb. 2004)

Spacebitch.com Softlabs in association with The Ninja Corporation [TNC}. TSCrack 2.0 URL: http://softlabs.spacebitch.com/tscrack/. (4 Feb. 2004)

Securiteam.com. Microsoft Windows XP Remote Desktop Denial of Service Vulnerability. 18 May 2002. URL: http://www.securiteam.com/windowsntfocus/5TP0F2A8AY.html (5 Feb. 2004)

Cohen, Ben. Microsoft Windows Remote Desktop Protocol Checksum and Keystroke Vulnerabilities. 16 Sep. 2003. URL: http://www.securityfocus.com/archive/1/292127 (5 Feb. 2004)

How to Change the Listening Port for Remote Desktop. Microsoft Knowledge Base Article – 306759. 10 Oct. 03. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;306759 (2 Feb. 2004)

FAQ About Remote Desktop: 25 Oct. 2001. URL: http://www.microsoft.com/windowsxp/remotedesktop/faq.asp (2 Feb. 2004)

Last Updated: May 27th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event