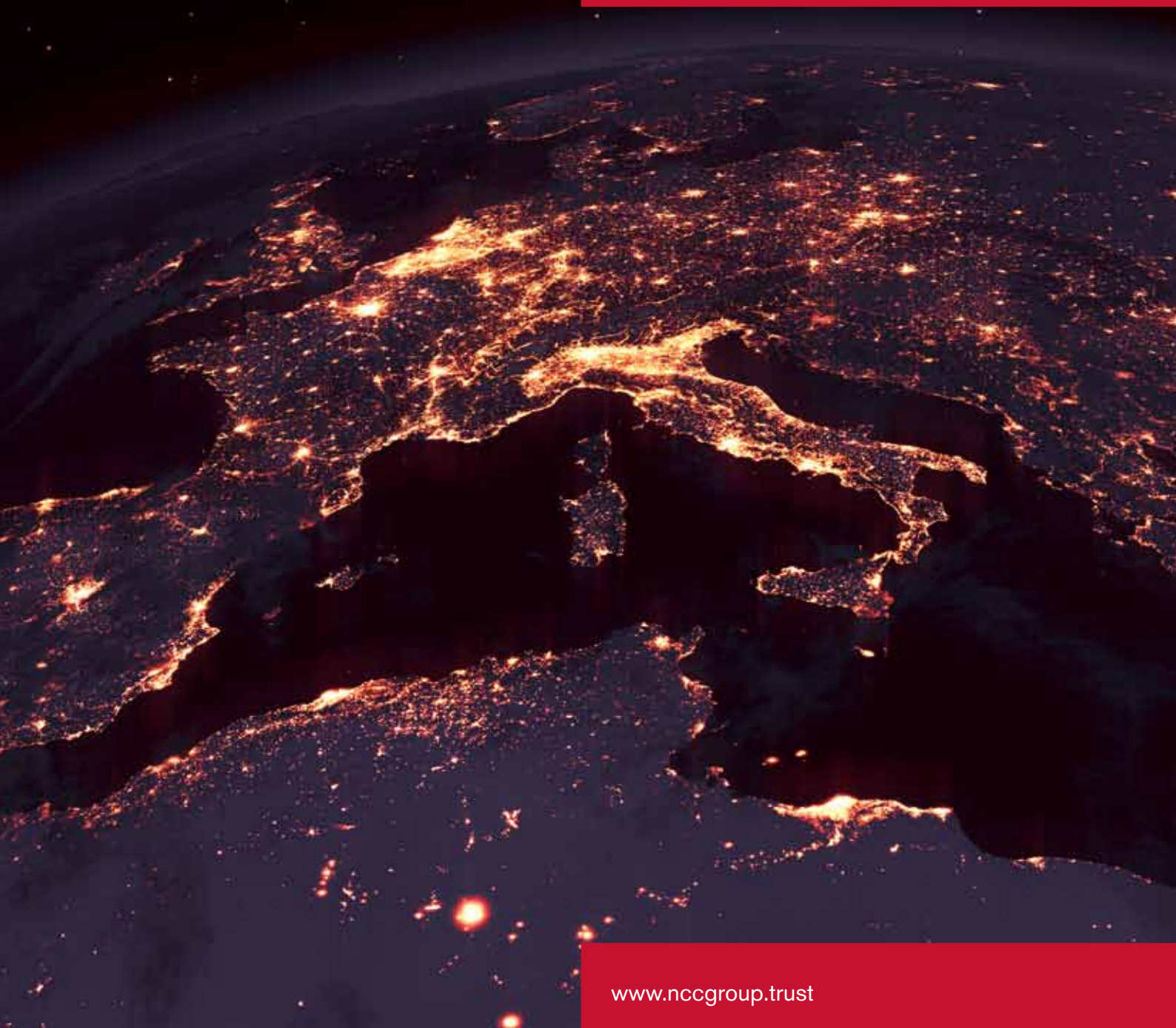
nccgroup
freedom from doubt

RESEARCH INSIGHTS

Common Issues with Environment Breakouts



www.nccgroup.trust

CONTENTS

AUTHOR

DAVE SPENCER

Dave is a principal consultant within the Security Consulting team at NCC Group, he has more than ten years' technical IT security experience and his specialisms include environment breakouts, web application assessments, and red team engagements. Dave's penetration testing and consultancy experience spans all manner of technologies across all sectors and many FTSE 100 companies.

INTRODUCTION

With more and more organisations implementing bring-your-own-device (BYOD) environments and thin client-based remote access solutions, IT departments are facing the task of securing devices that they neither own or control.

This has led to a rise in the number of environment breakout assessments being requested, as organisations test how secure their remote environments really are.

In a remote environment, restrictions are often imposed to prevent users from accessing functionality other than that which is required, so that the potential attack surface is minimal.

Environment breakout assessments attempt to bypass these restrictions and move the user into a less restricted context.

However, these are not just limited to the traditional restricted desktops and applications published via Citrix and remote desktop protocol (RDP), but have been expanded to cover other scenarios such as ATMs, the Internet kiosks found in hotels, and even vending machines.

The risks associated with environment breakouts differ depending on the deployment, but can be broadly categorised into:

Access to other devices – In the worst-case scenario this could be a remote attacker who breaks out of a Citrix session and uses the underlying server as an attack platform to target the internal network.

Data theft – In the case of ATMs or Internet kiosks this could be the theft of credit card details or social media credentials.

Data modification – For vending machines this could be modification of the corporate branding or prices.

This Research Insights paper aims to highlight some of the common security issues that NCC Group has found when performing environment breakouts.

How we are breaking in (or out)

	Method	Description	Solution
Physical Access	**Boot in to other OS and change password**	Numerous live operating systems exist for both the Universal Serial Bus (USB) and compact disc (CD) ports. These are used to reset the password on the device to a known value. An attacker with physical access to either the CD drive or USB slots can insert the bootable media and modify the boot order; it is then a case of rebooting the device, which can be achieved by pulling the power cord out and logging in with the newly set password.	Password-protect the basic input/output system (BIOS). Encrypt the hard drive.
	Mount on different device	When it isn't possible to modify the boot order, an easy bypass is to remove the physical drive and mount it on another machine. This gives access to the data and the ability to change the passwords. The drive can then be transferred back to the original machine.	Whitelist the applications that are allowed to run. Reduce attack surface.
	FireWire	By design FireWire devices are allowed read/write access to the operating system via Direct Memory Access (DMA); this can be abused to extract information such as encryption keys from memory, or to write or patch to memory, which may lead to unlocking the Operating System (OS) without knowing the password. The only requirements are that the device is powered on and logged in, and the session locked.	Reduce attack surface. Whitelist the applications that are allowed to run.
	Easily-guessed passwords	When the examples above do not work it is time to start brute-forcing passwords, using a combination of default or common passwords and company-specific base words.	Implement a robust password policy that does not allow default or weak passwords. Do not reuse passwords.
Environmental Techniques	**View source**	Many popular browsers allow access to the underlying operating system by using the "view source" function. Old versions of Internet Explorer and Firefox web browsers used to open the default text editor when a user viewed the source; now, instead of opening the text editor, they have their own functionality to display the source of a page. This functionality can still be used to access the filesystem.	Whitelist the applications that are allowed to run. Reduce attack surface.
	Shortcuts or hotkeys	A number of applications contain hotkeys or keyboard shortcuts to make the use of the application easier; these can sometimes be abused to open other applications or break out.	Whitelist the applications that are allowed to run. Reduce attack surface.

"Implement a robust password policy that does not allow default or weak passwords."

	Method	Description	Solution
Environmental Techniques cont...	**Help**	Most applications have help functions, which generally start an instance of a web browser or open an interface to Windows Help and Support.	Whitelist the applications that are allowed to run. Reduce attack surface.
	Printing	If any of the available applications have the option to print then there are a number of ways to use the print function to break out of the environment.	Whitelist the applications that are allowed to run. Reduce attack surface.
Common Software (Note that these are all Microsoft-specific as that is most commonly deployed)	**Microsoft Internet Explorer**	Internet Explorer is a web browser that ships with Microsoft Windows operating systems by default; it also functions in much the same way as Windows Explorer (explorer.exe).	Whitelist the applications that are allowed to run. Reduce attack surface.
	Developer Tools	Microsoft Internet Explorer Developer Tools are installed by default from Internet Explorer 8. They can be launched by pressing Windows hotkey F12 or selecting Tools→ F12 developer tools from IE. They offer a lot of useful functionality. From a breakout standpoint, the ability to modify the page source code on the fly is useful, regardless of Internet access and local Intranet zone setup. Load any website, for example www.google.co.uk, then press F12, select the HTML tab in the developer toolbar, press the Edit button, and edit the source code adding, for example, a hyperlink. Most locked-down environments force you to load a page or application on the local Intranet zone, which is perfect for using Java applets and ActiveX controls to own the system in most default set ups. The ability to inject arbitrary JavaScript into the current page through the use of the Microsoft JScript debugger console is also interesting.	Whitelist the applications that are allowed to run. Reduce attack surface.

How we are breaking in (or out) cont...

	Method	Description	Solution
Common Software (Note that these are all Microsoft-specific as that is most commonly deployed) cont...	**Word and Excel**	Widely used Microsoft applications such as Word and Excel are usually easy to break out of, a File → Open might result in you not being able to open the file you want, but right-click and you might get a lot more options. Right-click and select Explore to run Windows Explorer. From this screen you can often move about with fewer restrictions. Auto-complete is a handy option if you do not know the path.	Whitelist the applications that are allowed to run. Reduce attack surface.
	Visual Basic	Both Microsoft Word and Excel have built-in Visual Basic support; this can be accessed by either pressing ALT+F8 or selecting Tools → Macro → Create. In Office 2010 you first have to enable the Developer tab from the File → Options → Customize Ribbon menu.	Whitelist the applications that are allowed to run. Reduce attack surface.
	rundll32.exe	The rundll32.exe executable is responsible for running dynamic-linked-libraries (DLLs) and placing its libraries in the memory. This program works by invoking a function that is exported from a specific DLL module. It allows access to certain functions that are explicitly written to be available to this executable file.	Whitelist the applications that are allowed to run. Reduce attack surface.

“Reducing the attack surface can be achieved by removing any uncessary functionality, reducing available entry points and limiting access to known users.”

Conclusion

As can be seen from the table on pages 6-8, while there are many attack avenues for breaking out of a restricted environment, the solutions generally fall in to one or more of the following three categories:

Hard drive encryption – A strong full-disk encryption solution should be deployed on the devices, especially those located in potentially-hostile locations such as publicly-accessible areas. Removing the ability to mount the hard drive reduces the risk of data retrieval or modification to those that know the decryption value.

Robust password policy - Ensure that a suitably strong password policy is in place, commensurate with any defined policies for the application, system, or organisation. Passwords should be at least eight to ten characters long, and should be forced to include at least one uppercase character, at least one lowercase character, at least one special character and at least one digit. For administrator or higher-privileged accounts, a minimum length of twelve characters is typically recommended, with enforced complexity. Common passwords should also be prevented (using a blacklist of common weak passwords), as should passwords based on the username, application, or system.

Reduced attack surface – The attack surface consists of all the areas where a threat actor can either enter or extract data from the environment. Reducing the attack surface can be achieved by removing any unnecessary functionality, reducing available entry points, and limiting access to known users. All programs and hardware should be assessed and, if not required, removed or disabled; this includes USB and FireWire ports and all software present in the environment. Anything required should be restricted in such a way that only those that need to access it can. As part of the attack surface reduction, all applications should be reviewed and only those explicitly defined should be allowed to run. This can be achieved on Windows 7 and 8 via gpedit.msc: navigate to User configuration → Administrative Templates → System, and set “Run only specified Windows Applications” to “enabled”. Select “list of allowed applications” and add the applications wanted.

NCC Group has developed a suite of tools which take advantage of the lack of application whitelisting within an RDP environment to transfer files and tunnel traffic over the RDP protocol. These tools can be found on GitHub:

https://github.com/nccgroup/Loki

https://github.com/nccgroup/Sleipnir

https://github.com/nccgroup/Fenrir

CONTACT US

0161 209 5200
response@nccgroup.trust
@nccgroupplc
www.nccgroup.trust

United Kingdom

Manchester - Head office

Basingstoke

Cambridge

Cheltenham

Edinburgh

Glasgow

Leatherhead

Leeds

London

Milton Keynes

Wetherby

Europe

Amsterdam

Copenhagen

Luxembourg

Munich

Zurich

North America

Atlanta

Austin

Chicago

New York

San Francisco

Seattle

Sunnyvale

Asia Pacific

Sydney

www.nccgroup.trust
@nccgroupplc